Ensure interworking between multiple Contactless Card Emulation Environments

White Paper

January 2017

Table of Contents

About ETSI

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, aeronautical, broadcast and internet technologies and is officially recognized by the European Union as a European Standards Organization. ETSI is an independent, not-for-profit association whose more than 800 member companies and organizations, drawn from 67 countries across five continents worldwide, determine its work programme and participate directly in its work.

The ETSI Technical Committee on Smart Card Platform (ETSI SCP) is in charge of the development and maintenance of specifications for Secure Elements in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of such Secure Elements.

For more information please visit: www.etsi.org

About GlobalPlatform

GlobalPlatform defines and develops specifications to facilitate the secure deployment and management of multiple embedded applications on secure chip technology. Its standardized infrastructure empowers service providers to develop services once and deploy across different markets, devices, and channels. GlobalPlatform's security and privacy parameters enable dynamic combinations of secure and non-secure services from multiple providers on the same device, providing a foundation for market convergence and innovative new cross-sector partnerships.

GlobalPlatform is *the* international industry standard for trusted end-to-end secure deployment and management solutions. The technology's widespread global adoption across finance, mobile/telecom, government, healthcare, retail and transport sectors delivers cost and time-to-market efficiencies to all. GlobalPlatform supports the long-term interoperability and scalability of application deployment and management through its secure chip technology open compliance program.

As a non-profit, member-driven association, GlobalPlatform has cross-market representation from all continents. 120+ members contribute to technical committees and market-led task forces. For more information on GlobalPlatform membership visit www.globalplatform.org.

About NFC FORUM

The NFC Forum (www.nfc-forum.org) was launched as a non-profit industry association in 2004 by leading mobile communications, semiconductor, and consumer electronics companies. The Forum's mission is to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. The Forum's global member companies are currently developing specifications for a modular NFC device architecture, and protocols for interoperable data exchange and device-independent service delivery, device discovery, and device capability. The NFC Forum's Sponsor members, which hold seats on the Board of Directors, include leading players in key industries around the world. The Sponsor members are: Apple Inc., Broadcom Corporation, Dai Nippon Printing Co. Ltd., Google, Inc., Intel, MasterCard Worldwide, NXP® Semiconductors, Qualcomm, Samsung, Sony Corporation, STMicroelectronics, and Visa Inc.

Executive Summary

The mobile contactless market is currently highly fragmented because the management of multiple Contactless Card Emulation Environments (CEEs) hosted in the same device (e.g. in HCE and several contactless SEs) is not standardized. This lack of standardization leads to unpredictable behaviors that depend on:

- the model, version, and configuration of the device, and implementation choices made by the Contactless Frontend (CLF) manufacturer and/or the OEM
- the presence of other Contactless Card Emulation applications in the device, whatever their location (HCE, UICC, or embedded SE)

Service Providers are not confident that their contactless services will work properly. End users are confused, especially when using non-payment applications or when several CEEs are available, by lack of clarity of device configuration options or by side effects of one application on the others.

The value proposition of the shared work between GlobalPlatform, ETSI SCP, and NFC Forum is to provide a standardized solution allowing the coexistence of contactless applications located in different CEEs, with predictable behavior and a simplified user experience whatever device these contactless applications are running on. It enables Service Providers to deploy their contactless services safely on a large number of devices with a higher level of interoperability, a reduced fragmentation and at lower costs.

The GlobalPlatform Managing Entity specification defines a framework which supports:

- The coexistence of Contactless Card Emulation applications hosted in different CEEs, with the detection of potential conflicts.
- Perfectly defined behavior when Contactless Card Emulation applications from different CEEs are activated at the same time, whatever the number of CEEs available in the device.
- Dynamic management of Contactless Card Emulation application life cycle changes (installation, activation, deactivation, deletion, etc.).
- Handling of specific requirements from applications such as transport applications that are not selected by AID and that require specific RF protocol parameters that may not be compliant with those required by EMVCo.
- Simplification of the end-user experience through services offered by the GlobalPlatform Managing Entity to the Wallet(s) or Service Provider UIs.

The GlobalPlatform Managing Entity specification also defines a fallback mechanism to manage legacy Secure Elements (e.g. UICC or eSE) that are not implementing the new specification.

The framework defined in the specification is compatible with P2P applications and has no impact on Reader Mode applications running at the same time on the device.

This white paper gives an overview of the standardized solution defined in the GlobalPlatform Managing Entity specification ([GPC ME]) and the related ETSI SCP and NFC Forum specifications (respectively [HCI] and [NCI]). The architecture, main interfaces, and role of the GlobalPlatform Managing Entity are described.

In addition, this white paper provides a comparison, based on concrete examples, of the situation within a device *not* implementing the GlobalPlatform Managing Entity as of today and the situation when the GlobalPlatform Managing Entity is implemented.

Intended Audience

This white paper is intended for executives in OEM, contactless products, and service providers, especially Mobile Network Operators, payment service providers, transport

service providers, and all service providers offering contactless services to be hosted in devices such as mobiles.

It informs system integrators and engineers how GlobalPlatform technologies can be used to build a standardized NFC-ecosystem integrating several Card Emulation Environments.

SECTION 1: Introduction

Many mobiles now support NFC technology, and the number of contactless payment terminals has greatly increased in recent years.

Like many other contactless readers such as those used in public transport, eID, or border control, the contactless payment terminals are based on ISO/IEC 14443 or ISO/IEC 18092 specification series. To ensure full analog interoperability on the physical transport layer with these contactless readers, the NFC mobiles must implement the requirements defined by NFC Forum Analog 2.0 or later. To support this, NFC Forum provides the necessary test specifications and certification schemes to verify that the NFC mobile is able to establish a reliable RF communication link on the analog layer, which is the essential basis for all contactless applications discussed in this document.

Contactless Card Emulation applications can be hosted in different Contactless Card Emulation Environments (CEEs). A Contactless Card Emulation application (such as a payment, transport, loyalty, or access control application) can be implemented:

- in the Device Host itself, in which case it is called Host Card Emulation (HCE)
- in an NFC UICC
- in the NFC embedded Secure Element (eSE)

Each of these Contactless Card Emulation Environments has its own advantages in term of user experience, availability, deployment, provisioning, security, business model, maturity, etc. Service providers can select the one that is most suitable according to their business requirements and constraints.

It appears that everything is available for Service Providers to accelerate the deployment of their NFC services, whatever the solution selected (HCE, UICC, or eSE; using or not using tokenization for payment, etc.)

However, as explained in section 2, the interworking of Contactless Card Emulation applications located in different CEEs is not ensured in the current devices.

The value proposition of the shared work between GlobalPlatform, ETSI SCP, and NFC Forum is to provide a standardized solution allowing this coexistence with predictable behavior whatever device the contactless applications are running on. Section 3 clarifies the purpose and the scope of the GlobalPlatform Managing Entity specification. Section 4 describes the architecture, including the central role of the GlobalPlatform Managing Entity and the different interfaces it relies on. Section 5 discusses the interface to the User Interface Modules (UIMs), such as Wallets or Service Provider UIs, that interact with the end users.

Finally, section 6 provides a comparison, based on basic use cases, between a solution not implementing the GlobalPlatform Managing Entity – as done by the current devices – and a solution where the GlobalPlatform Managing Entity is implemented. This section demonstrates how concretely the framework proposed by the GlobalPlatform Managing Entity specification ensures predictable behavior of the device, whatever the location of the contactless applications, reducing the time to market for Service Providers to deploy reliable NFC services.

SECTION 2: Background and Current Situation

With Android Kitkat 4.4, Google introduced the ability to implement Contactless Card Emulation applications as Android applications, called HCE applications. Although this feature was already available in Blackberry OS, support of HCE by Android, associated with the development by EMVCo of the EMV Payment Tokenization specification, triggered a lot of market interest. The consequence of the introduction of these features is that Contactless Card Emulation applications could be located either in the Device Host (HCE applications) or in the UICC (UICC applications), requesting the NFC controller to route the incoming RF communication to the right Card Emulation Environment (called CEE), either the Device Host or the UICC.

Apple provides similar functionality using an embedded SE (eSE) in their Apple Pay solution, available since iPhone 6.

Samsung Pay, available since Samsung S6, may include an eSE based payment solution, meaning that in these devices you may host three types of contactless applications: HCE applications, eSE contactless applications, and UICC contactless applications.

However, the behavior and the end user experience when using one or another of these applications may vary from one device to the other depending on decisions taken by the device manufacturer. The consequences are that:

- The end user experience may vary a lot depending on the location of the contactless application.
- The end user experience may change when swapping from one device to another.
- Service Providers cannot be sure that their services will work properly in the different devices or that their services will not be disrupted because another service is being installed.
- Device Manufacturers have to define custom interworking rules to support the requirements of some customers or certification authorities, increasing the fragmentation of their implementations.

In addition, the handling of transport services (or any services that are not AID-based, such as MIFARE services) is even worse, as they are not at all covered by the existing frameworks (e.g. Android HCE architecture), leading to an even deeper fragmentation depending on the interworking rules implemented by each device manufacturer.

SECTION 3: Purpose and Scope of GlobalPlatform Managing Entity Specification

The purpose of the GlobalPlatform Managing Entity specification ([GPC ME]) is to provide a framework which permits the following abilities:

- Contactless Card Emulation applications hosted in different CEEs can coexist.
- The expected behavior is perfectly defined when Contactless Card Emulation applications from different CEEs are activated at the same time.
- A fallback mechanism manages legacy Secure Elements (e.g. UICC or eSE) that are not implementing the new specification.
- Contactless Card Emulation application life cycle changes (installation, activation, deactivation, deletion, etc.) are dynamically managed.

This framework is compatible with P2P applications and has no impact on Reader Mode applications running at the same time on the device.

The GlobalPlatform Managing Entity specification defines the interworking rules between different Card Emulation Environments (CEE) and their hosted Contactless Card Emulation applications, through a central entity called the GlobalPlatform Managing Entity. These rules cover:

- Collection of the configuration requested by each Contactless Card Emulation application in all the CEEs.
- Detection of the potential conflicts between the Contactless Card Emulation applications active at the same time with involvement of the user for the resolution.
- Configuration of the CLF according to the requirements from all the activated Contactless Card Emulation applications, including the configuration of the routing table and of the RF protocol parameters used for establishing the contactless communication with the contactless reader and then route the contactless commands to the appropriate CEE.
- Automatic reconfiguration in response to changes in the life cycle of the Contactless Card Emulation applications in the different CEEs, such as installation or deletion of an application, its contactless activation or deactivation, or changes in its requirements (e.g. specific RF parameters).
- Automatic reconfiguration in response to insertion or removal of a CEE (e.g. UICC).

The GlobalPlatform Managing Entity specification also defines services available to the application(s) in charge of the interaction with the end user, called User Interface Module (UIM) in the specification. Those services allow the UIM to:

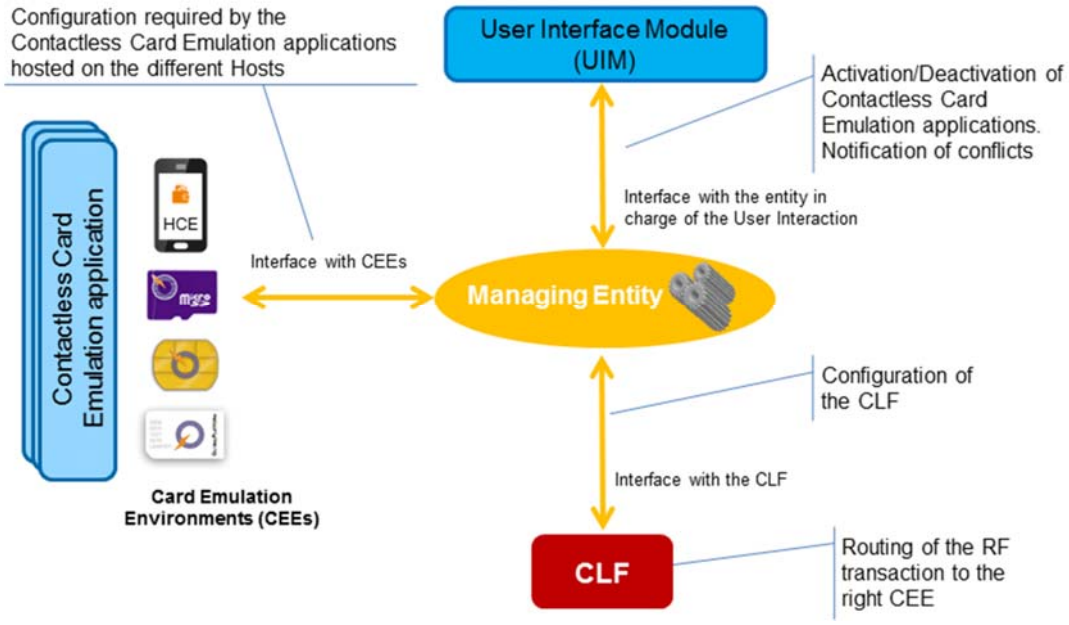
- Access the list of Contactless Card Emulation Applications.
- Request activation (reporting conflict(s), if any) or deactivation of a Contactless Card Emulation Application.
- Handle the fallback mechanism defined to manage legacy SEs.

SECTION 4: Architecture and Interfaces

The GlobalPlatform Managing Entity specification relies on a new neutral[1] and central entity called the GlobalPlatform Managing Entity. This entity provides interfaces:

- With each CEE to collect information from the different Contactless Card Emulation applications. This interface is based on new messages defined in the GlobalPlatform Managing Entity specification that can be transported over new events defined in the ETSI HCI specification (ETSI TS 102 622 [HCI]). The interface may use an internal API when the Managing Entity is hosted in the same host as the CEE (e.g. the CEE is HCE).
- With the CLF to configure the routing table, RF protocol parameters, and RF technologies as defined in NFC Forum NCI 2.0 specification ([NCI]).
- With the UIM(s) to provide services to interact with the end user, such as providing the list of Contactless Card Emulation applications, means to activate or deactivate them, or information to solve conflicts if any when activating an application.

Figure 4-1: Overview of the Architecture



The GlobalPlatform Managing Entity specification defines all the flows to be implemented by the different CEEs and the Managing Entity in order to manage the different events corresponding to:

- changes in the life cycle of a CEE (e.g. CEE inserted or removed)
- changes in the life cycle of Contactless Card Emulation applications hosted in a CEE (e.g. Contactless Card Emulation application installed or deleted)
- changes in the contactless activation state of Contactless Card Emulation applications (e.g. activation or deactivation by the end user)

[1] In this context, the Managing Entity does not implement any business policy.

- changes in the requirements of Contactless Card Emulation applications (e.g. change of the RF protocol parameters)

When such events occur, the GlobalPlatform Managing Entity will reconfigure the CLF to take the changes into account.

SECTION 5: Interaction with User Interface Module(s)

The purpose of the Managing Entity is not to interact directly with the end user but to provide services to User Interface Modules (UIMs). A UIM can be a Wallet; the device application of a Service Provider, called a Service Provider UI; or even a menu in the device.

Through those services, User Interface Module(s) will be able to interact with the user to:

- Provide information on the different CEEs and the Contactless Card Emulation applications they are hosting, such as a list of all the Contactless Card Emulation applications.
- Notify the user if a new Contactless Card Emulation application is available in a CEE or if a change occurs on a Contactless Card Emulation application (e.g. deletion or deactivation done by OTA).
- Activate or deactivate a Contactless Card Emulation application. If upon activation a conflict is detected, the UIM will be able to resolve the conflict by applying its own business policy or by asking the user to decide which Contactless Card Emulation application(s) will be deactivated.
- Manage priority between Contactless Card Emulation applications.
- Enable or disable the Contactless Card Emulation or a specific RF technology of the device.
- Switch between the nominal mode and the fallback mechanism if a legacy SE is available in the device.

SECTION 6: Simplified Deployments and Predictable Behavior

6.1 Deployments and Management with the GlobalPlatform Managing Entity

Thanks to the GlobalPlatform Managing Entity specification and the evolutions introduced in the NFC Forum NCI 2.0 ([NCI]) and ETSI TS 102 622 ([HCI]) specifications, the deployment of Contactless Card Emulation services and their integration with other services already present in the device is simplified and service availability becomes predictable, whatever the number of Contactless Card Emulation Environments available (e.g. HCE and one or several SEs).

When deploying a banking service on a Secure Element:

- The banking service is dynamically added to the list of available Contactless Card Emulation services.
- If the service is composed of several SE Contactless Card Emulation applications (e.g. domestic and international ones), those applications can be activated at the same time.

When deploying another type of service, such as transport, access control, or loyalty:

- The service is also dynamically added to the list of available Contactless Card Emulation services.

When the end user requests activation of a Contactless Card Emulation application:

- Potential conflicts with the already activated Contactless Card Emulation applications are detected. Those conflicts can be at the AID level or at the RF protocol parameters level, especially if the application requires very specific RF protocol parameters.
- When it detects a conflict, the Managing Entity forwards information on the reason for the conflict and the list of conflicting applications, which may be hosted in different CEEs. It will allow the User Interface Module to apply its own business policy or to prompt the user about which Contactless Card Emulation application shall be deactivated.

As soon as a service is activated:

- The CLF configuration is automatically updated to make the service available to perform an RF transaction.
- If the service is hosted in a Secure Element, the CLF includes the configuration to have the service available when the device is switched off.

At any time, the user is able to manage which service he would like to activate through the Wallet or the Service Provider UI and can be sure that the activated Contactless Card Emulation application will work as expected. This will improve the user experience.

The GlobalPlatform Managing Entity specification also considers the case of legacy SEs and provides a fallback mechanism that offers availability of the services hosted in such SEs. This fallback mechanism guarantees that when the user selects such a service, the CLF is reconfigured so that this legacy SE is considered as the only Contactless Card Emulation Environment available in the device: RF protocol parameters provided by this SE are used and all contactless RF communications are routed to this SE.

6.2 Use Case Comparison with and without the GlobalPlatform Managing Entity

This section compares the deployment, management, and usage of several Contactless Card Emulation applications:

- in a device with proprietary implementation of the existing specifications as of today

- in a device implementing the GlobalPlatform Managing Entity specification

In this example:

- A payment application is installed in the HCE.
- A transport application (such as MIFARE Classic or MIFARE DESFire) and a loyalty application are installed on the UICC.
- The loyalty application and the payment application have similar RF protocol parameter requirements.
- The transport application has specific RF protocol parameter requirements that are not compliant with those required by the payment application.
- The loyalty application and the payment application use AID based application selection.
- The transport application does not use AID based selection. (The contactless readers of the transport infrastructure behave as though the transport Contactless Card Emulation application is unique and do not select an application at the beginning of the RF transaction.)

6.2.1 Behavior with the Current Implementations

This section describes the behavior with the current implementations and HCE as implemented by Android.

When the payment application is installed in HCE, it registers itself through an API available in the device to be recognized as an application belonging to the category “Payment”. The application then becomes available on the Android Tap & Pay menu.

When the loyalty application is installed on the UICC, the Service Provider can indicate the RF protocol parameters required by the application. But in order to be available in the routing table of the CLF, the loyalty SE application needs to have a “companion” application installed in the device. This companion application will have to use an API available in the device to register the SE application as an “off-host” application (i.e. not hosted in HCE) belonging to the category “Other” (i.e. non-payment application). This registration will allow routing of the RF transaction to the UICC when a selection corresponding to the AID of the loyalty application is received by the CLF. The current API available for the companion application doesn’t allow the management of the contactless life cycle states available for SE applications that can be activated or deactivated (i.e. the routing table has a static configuration).

When the transport application is installed on the UICC, the Service Provider can indicate the RF protocol parameters required by the application, but the way those specific RF protocol parameters are managed by the CLF and the detection of the conflict with the RF protocol parameters required by HCE applications (e.g. parameters as defined by EMVCo in our example) are not standardized; rather, they are left to the implementation of the CLF manufacturer and/or the OEM. Even if a companion application exists in the device, this companion application is not able to provide the information required to properly route the corresponding RF transaction to the UICC, as the current Android API doesn’t provide any mechanism to define non-AID based routes. Here again, the solution is left to implementation choices. Some implementations may request the user to select a default route on a device menu with the end user being quite confused by such an option (as he is not really aware of the impacts on other contactless applications). Depending on the implementation choices or on the configuration selected by the end user, the payment application may no longer be accessible, or the transport application may not work properly if the very specific RF protocol parameters requested by the readers on the transport infrastructure are not strictly applied by the CLF.

Beyond the scope of this example: The case of a device hosting two contactless Secure Elements – such as a UICC and an eSE – is even worse, as the current Android HCE APIs don't consider the possibility of defining two off-host entities, so it is not possible to register an application in a UICC and another application in the eSE. The management of payment applications located in several CEEs is also not clearly defined, especially regarding the location of the PPSE application ([AAUI]) that will answer to the Point of Sale reader.

The lack of standard specifications to manage these use cases leads to unpredictable behaviors that will depend on the model, the version, and the configuration of the mobile.

Service Providers, whatever type of service (i.e. payment, transport, loyalty, access control, etc.) they provide, cannot be sure that:

- Their services will work properly on any device, with whatever other contactless applications are installed in the device.
- Their services can be easily accessible to the end user (e.g. availability not linked to not-obvious parameters in the advanced configuration of the NFC menu of the device).

End users may also be confused by:

- The side effects of one application on the other (such as an application no longer working properly because another application has been installed).
- The lack of clarity of some device configuration choices presented to them.

The main consequences will be that:

- Service Providers, not confident enough about the reliability of the current solutions and concerned about fragmentation depending on device models, etc., are delaying the rollout of their mobile NFC services.
- End users may try but finally give up on using NFC for Card Emulation services on their mobiles.

6.2.2 Behavior when the GlobalPlatform Managing Entity Is Implemented

When the payment application is installed in HCE, as before the Managing Entity was available, the application registers itself through an API available in the device to be recognized as a Contactless Card Emulation application and potentially be registered to a Wallet such as the Tap & Pay menu. The HCE Contactless Card Emulation application is then automatically added to the list of Contactless Card Emulation applications handled by the Managing Entity and thus will be automatically added to the routing table of the CLF.

When the loyalty application is installed on the UICC, as before the Managing Entity was available, the Service Provider can indicate the RF protocol parameters required by the application. The UICC will automatically add this UICC Contactless Card Emulation application to the list of Contactless Card Emulation applications handled by the Managing Entity, and the AID of the loyalty application will be automatically added to the routing table of the CLF. It is no longer necessary to deploy a "companion" application in the device. Upon deactivation or activation of the loyalty application, the UICC will inform the Managing Entity. When being activated, if the AID of the loyalty application is already used by another activated Contactless Card Emulation application, the Managing Entity detects a conflict and notifies the Wallet or the Service Provider UI handling the conflicting application to solve the conflict.

When the transport application is installed on the UICC, as before the Managing Entity was available, the Service Provider can indicate the RF protocol parameters required by the application. The UICC will automatically add this UICC Contactless Card Emulation application to the list of Contactless Card Emulation applications handled by the Managing

Entity, and the Managing Entity will configure the routing table of the CLF accordingly (i.e. using the different types of routing entries defined in [NCI]). When the transport application is activated, since in our example its specific RF protocol parameters are not compliant with the ones required by the payment and the loyalty applications, the Managing Entity will detect a conflict and notify the Wallet or the Service Provider UI handling the conflicting applications to solve the conflict.

The logic described above is the same whatever the type of SE and whatever the number of SEs available in the device.

The GlobalPlatform Managing Entity also clearly specifies the handling of legacy SEs.

When the Managing Entity is implemented, the behavior becomes predictable. It no longer depends on:

- the model, version, or configuration of the device, or implementation choices made by the CLF and/or the OEM
- the number of SEs available in the device
- the presence of other Contactless Card Emulation applications in the device

The GlobalPlatform Managing Entity provides mechanisms and information for the application(s) in charge of the interaction with the end user (UIMs) that simplify the end user experience.

The GlobalPlatform Managing Entity assures Service Providers that:

- their services can be deployed safely on a large number of devices with a higher level of interoperability and reduced fragmentation
- the availability of their services is no longer subject to business policy or implementation choices made by the OEM
- the availability of their services no longer depends on the presence of other services in the end user device

6.3 Summary

Table 6-1 presents a summary of the handling of the use cases described above, with and without the implementation of the GlobalPlatform Managing Entity.

Table 6-1: Summary with and without the GlobalPlatform Managing Entity

Use cases		Current Situation	With GlobalPlatform Managing Entity
Presence of payment application in HCE and of another application in an SE (UICC or eSE)	The SE application is not a payment application. It can be selected through its AID and its RF protocol parameters are compliant with ones required by the HCE payment application (i.e. EMVCo requirements).		
	The SE application is not a payment application. It cannot be selected through its AID and it requires very specific RF protocol parameters that are not compliant with the ones required by the HCE payment application. This is, for example, a transport application.		
	The SE application is another payment application.		
Presence of several SEs in the device			

Legend:

 Use case properly managed.

 Use case might be managed. If managed, it is done through proprietary implementations that may differ from one device to another depending on the model, version, or configuration of the device, and on the implementation choices made by the CLF manufacturer and/or the OEM.

 Use case not managed.

SECTION 7: Conclusion

The GlobalPlatform Managing Entity specification has been developed in strong collaboration with ETSI SCP and NFC Forum, all sharing the same goal: to provide a whole standardized ecosystem that will offer a reliable and interoperable environment for Service Providers willing to deploy mobile contactless services.

The specification defines a framework based on the implementation of the GlobalPlatform Managing Entity that permits:

- The coexistence of Contactless Card Emulation applications hosted in different CEEs (e.g. HCE and one or several SEs).
- Simplification of the end-user experience through services offered by the GlobalPlatform Managing Entity to User Interface Modules (UIMs) – entities such as Wallets or Service Provider UIs that interact with the end user.
- Perfectly defined behavior when Contactless Card Emulation applications from different CEEs are activated at the same time, whatever the number of CEEs available in the device.
- Handling of specific requirements from some applications such as transport applications that are not selected by AID and require specific RF protocol parameters that may not be compliant with those required by EMVCo.
- Detection of potential conflicts (at the AID or the RF protocol parameter level) between the application being activated and the ones already activated, and notification of UIMs to allow resolution of these conflicts.
- Dynamic management of the Contactless Card Emulation application life cycle changes (installation, activation, deactivation, deletion, etc.).

In addition, the GlobalPlatform Managing Entity specification defines a fallback mechanism to manage legacy Secure Elements (e.g. UICC or eSE) that are not implementing the specification.

With the GlobalPlatform Managing Entity, Service Providers can deploy their contactless services safely on a large number of devices with a higher level of interoperability, a reduced fragmentation and at lower costs. They have assurance that the availability of their services is no longer subject to proprietary implementation choices. They can be confident that their services will not be disrupted by the installation of other contactless services in the device. Thanks to this framework, Service Providers can reduce their time to market to deploy reliable NFC services whatever the CEE they are hosted on (HCE, contactless UICC(s) or contactless embedded SE).

The GlobalPlatform Managing Entity specification and the related ETSI SCP and NFC Forum specifications should be available in Q1 2017.

All feedback is welcome; comments or questions may be submitted to secretariat@globalplatform.org.

APPENDIX A: Abbreviations

Table A-1: Abbreviations

Abbreviation	Meaning
AID	Application ID
APDU	Application Protocol Data Unit
API	Application Programming Interface
CEE	Card Emulation Environment
CLF	Contactless Frontend
eSE	Embedded Secure Element
ETSI	European Telecommunications Standards Institute
HCE	Host-based Card Emulation
MNO	Mobile Network Operator
NFC	Near Field Communication
OS	Operating System
OEM	Original Equipment Manufacturer
OTA	Over-the-Air
P2P	Peer-to-Peer
RF	Radio Frequency
SE	Secure Element
UI	User Interface
UIM	User Interface Module
UICC	Universal Integrated Circuit Card

APPENDIX B: Terminology and Definitions

Table B-1: Terminology and Definitions

Term	Definition
Legacy Secure Element	In the context of this document, a Secure Element not implementing the GlobalPlatform Managing Entity Specification ([GPC ME]).
Mobile	A mobile phone, tablet, or similar device.
Secure Element (SE)	A secure component which comprises autonomous, tamper-resistant hardware within which secure applications and their confidential cryptographic data (e.g. key management) are stored and executed. May exist in any form factor, such as UICC, embedded SE, smartSD, smart microSD, etc. UICC, smartSD, and smart microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.
Secure Element application	A software application installed and running on the Secure Element.
Smart microSD	A small, portable, non-volatile memory card format developed by the SD Card Association (SDA).
Universal Integrated Circuit Card (UICC)	A Secure Element used in the mobile communications industry, as defined in ETSI TS 102 221 [ETSI 102 221].

APPENDIX C: References

Table C-1: Normative References

Standard / Specification	Description	Ref
ETSI TS 102 221	Smart cards; UICC – Terminal interface; Physical and logical characteristics, Release 6, 2004	[ETSI 102 221]
ETSI TS 102 622	Smart Cards; UICC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) – Release 13	[HCI]
GPC_SPE_114	GlobalPlatform Card, Multiple Contactless Card Emulation Environments – Managing Entity, v1.0	[GPC ME]
NFC Forum NCI	NFC Controller Interface (NCI) – Technical Specification – Version 2.0	[NCI]
EMVCo AAUI	EMVCo Contactless Mobile Payment – Application Activation User Interface v1.0	[AAUI]

APPENDIX D: Table of Figures

APPENDIX E: Table of Tables

