GLOBALPLATFORM

THE STANDARD FOR SMART CARD INFRASTRUCTURE

GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging

White Paper
April 2009

secretariat@globalplatform.org | www.globalplatform.org |

GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging

Contents:

About GlobalPlatform

GlobalPlatform is the leading, international association, focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuers, service providers and technology suppliers.

GlobalPlatform Specifications are freely available and have been adopted worldwide by many public and private bodies. As of October 2008, there were an estimated 305.7 million GlobalPlatform-based smart cards in circulation across the world and an additional two billion mid range USIM/SIM cards using GlobalPlatform technology to enable over-the-air (OTA) application downloads for 3G and GSM mobile networks. These figures are expected to increase significantly throughout 2009.

GlobalPlatform is an independent, not-for-profit organization and its strategy is defined and prioritized by a Board of Directors. GlobalPlatform is currently chaired by Sebastien Tormos, Vice-President of Marketing, Datacard Group, and vice-chaired by Marc Kekicheff, Vice President Product Technology, Visa Inc. Kevin Gillick serves the membership on a full-time basis as its Executive Director.

For further information, visit www.globalplatform.org.

Publication Acknowledgements

GlobalPlatform wishes to offer special thanks to the members of the UICC System Role Task Force and their respective organizations for their contributions and involvement in developing this white paper.

Participants include:

Full Members:
- Gil Bernabeu – Gemalto
- Enrico Perin – Gemalto
- Jean Henaff – Datacard
- Gael Gerard – Orange FT Group
- Ahmad Saif – Orange FT Group
- Jean Christophe Bernard – Orange FT Group
- Sophie Diallo – Oberthur
- Kiushan Pirzadeh - Visa, Inc

Participating Members:
- Mathias Lerch – Inside Contactless
- Johannes Hoier Sörensen – Smart Trust

Observer Members:
- Sebastien Pierrel – Ericsson

Consultant Members:
- Jean Philippe Ameil – Nextendis

Public Entity
- Pierre Terrée - RATP

GlobalPlatform team:
- Kevin Gillick – Executive Director of GlobalPlatform
- Alliances Management – Operations Secretariat

Executive Summary

Near Field Communication (NFC) presents significant business opportunities when used in mobile phones for applications such as payment, transport ticketing, loyalty, physical access control, and other exciting new services. To support this fast evolving business environment, several entities, in addition to Mobile Network Operators (MNO), will become involved in the NFC mobile ecosystem. By nature of their individual roles, these players will need to communicate with each other and exchange messages in a reliable and interoperable way.

Equally important to these entities or players, will be the need for ongoing security and confidentiality of sensitive applications and data downloaded to and stored on an NFC enabled handset for performing contactless transactions. The component in a mobile phone providing the security and confidentiality required to support various business models in this environment, is referred to as a Secure Element (SE).

As a neutral and cross-industry organization, GlobalPlatform intends to define and provide the specifications necessary to support three types of secure elements selected as options for NFC mobile. These are:

- Universal Integrated Circuit Card (UICC)
- Embedded Secure Element
- Secure Memory Card

The primary purpose of this white paper is to discuss the new functional features that will be required in the back-office management systems or infrastructure to optimally manage a GlobalPlatform Secure Element with initial focus on products compliant with the GlobalPlatform UICC Configuration [2]. The GlobalPlatform Embedded Secure Element Configuration will be defined next and, once completed will be incorporated as a secure element option.

The second objective is to clarify where trusted entities from a key management point of view are needed. The business rationale to work with a trusted and reliable partner, and the need to have a third party entity facilitate key or certificate management, are often intertwined. From a key and certification management point of view, security requirements will be very different for a business partner compared to a trusted third party.

The third objective is to explain how the GlobalPlatform Messaging Specification [3] can provide the necessary interoperability in the NFC ecosystem thanks to the definition of standardized messages that can be exchanged between disparate systems in a GlobalPlatform compliant environment. Support is provided for the issuance and post-issuance updates of GlobalPlatform Secure Elements compliant with the UICC Configuration specification [2].

GlobalPlatform is well-positioned to facilitate the creation of a standard infrastructure necessary to allow service providers, trusted service managers and mobile network operators to manage application download and personalization without being limited to a single type of Secure Element. Hence, most of the contents and conclusions of this paper will be applicable, or easily transposable, to other Secure Elements, provided that they are compliant with the GlobalPlatform Card Specifications.

The target audience for this white paper is all the entities involved in the NFC ecosystem including service providers, mobile network operators, trusted service manager, system integrators and system developers, participating in GlobalPlatform smart card implementations, and developing infrastructure components and support systems. Such systems include:

- Data Preparation Systems,
- Personalization Systems,
- Application Management Systems,
- Smart Card Management Systems,
- Personalization Collators/Decollators.

This white paper is intended to be informational but is rather technical in nature and could therefore be seen as a technical brief.

This paper is also intended to be used as input to the technical evolution of the GlobalPlatform Messaging specification [3] planned for 2009.

SECTION 1: Introduction

It is envisaged that end-users will in the near future use NFC enabled mobile phone for payment, transport ticketing, loyalty, access and many others contactless services. Several pilots are already in progress in a number of locations across the world but these are typically in closed environments, or limited in scope and number of players involved.

A central obstacle to roll-out is scalability beyond the current phase of initial pilots with a small number of actors involved today. To overcome this, a way must be found to resolve the issue of how to create an interoperable mobile NFC ecosystem that makes it easy for Service Providers (SP) and Mobile Network Operators (MNO) to work together.

GSM Association's answer was to create the role of Trusted Service Manager (TSM) who establishes the link between the service providers' and MNO's worlds from a technical perspective. The TSM role is also to ensure a level of trust and confidentiality between the actors.

Use of the term "trusted" in this role may be misleading and incorrectly associated with the key management function. In most cases this entity will not be managing keys, neither for the MNO nor the service provider.

Figure 1-1 illustrates the chaotic nature of the business environment without a TSM and the role the TSM plays in providing services to various entities within the ecosystem.

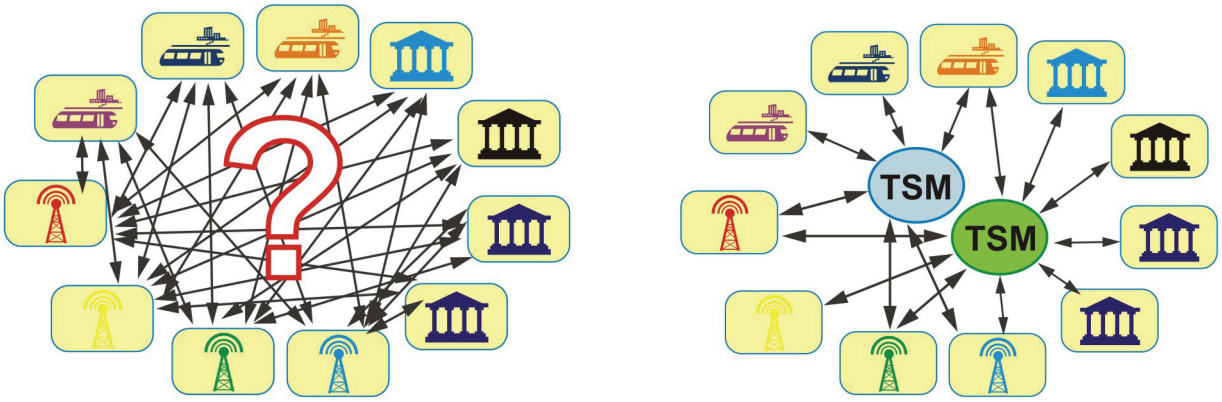

Figure 1-1 – Trusted Service Manager Role

The mobile NFC ecosystem requires the inter-connection of several entities or actors, coming from different business environments and using heterogeneous systems, facilitating critical data exchange to support business functionality. It will require change in current process flows to facilitate new functionality.

For example, allowing a mobile service to be set up via Over-the-Air (OTA), changes current process flows and data exchanges as follows:

Existing:	Service provider to card through a personalization bureau,
New:	Service provider to the card via an OTA platform

The main actors taking part in the processes when the SE is a UICC card within the mobile NFC ecosystem are the following:

- Mobile Network Operators (MNO) who are the owners of the UICC card and also own in most of the cases an OTA platform
- Service Providers (SP) who are entities such as banks, transport companies, retailers, etc., providing a service to consumers and need to have their application implemented on a UICC card
- Trusted Service Managers (TSM) who enable the link between the SP and MNO providing (subcontracting) the technical capability to:
    - Allow the MNO to send messages to the SP
    - Allow the MNO to perform NFC services management
    - Allow the SP to send messages to the MNO
    - Allow the SP to perform NFC services management
    - Optionally, have commercial roles (aggregator, commercial intermediate, commercial agent, end user support, etc.)
- Confidential Key Loading Authority (CKLA) who is responsible for enabling the initial key set in a GlobalPlatform card in a confidential way

In most of the NFC trials conducted worldwide over the past two years, a single MNO, SP and TSM were involved. These trials received good end-user feedback. Facilitating expansion requires several SPs connected simultaneously to multiple MNOs with potentially multiple TSMs, collectively requiring exchange of data in a reliable and interoperable fashion. To enable this capability, the issue as to how to guarantee an interoperable way of exchanging messages between the different actors must be addressed.

For example, where new end-users want to have their bank cards enabled on their mobile phones, the following practicalities need to be addressed:

- How to be sure that the UICC and the mobile phone are NFC enabled
- How to request creation of a security domain (SSD) and download and personalize the banking application in a confidential way
- How to handle a subsequent transfer of service from one UICC to another

Certain initiatives, especially in Europe, have defined some of the messages to be exchanged between the MNO and SP but not necessarily the messaging format to be used. However, these initiatives intend to be fully compliant with the GlobalPlatform specifications. Any isolated or proprietary efforts to describe additional ways of exchanging messages would be unproductive and increase the level of complexity of the system. Where platforms are required to comply with multiple specifications, development and maintenance costs increase, and consistency and interoperability are at risk.

The GlobalPlatform Messaging specification [3] already defines a set of standard messages for data exchange between disparate systems in a GlobalPlatform smart card environment. This functionality is applicable to UICC NFC enabled cards which are in fact part of the GlobalPlatform smart card environment in which security domains and secure messaging concepts are already in use.

This makes GlobalPlatform the ideal organization for defining the necessary message formats to be used for data exchange in the mobile NFC ecosystem.

The main advantages of using GlobalPlatform's Messaging specification [3] are:

- Avoid proprietary solutions to exchange information

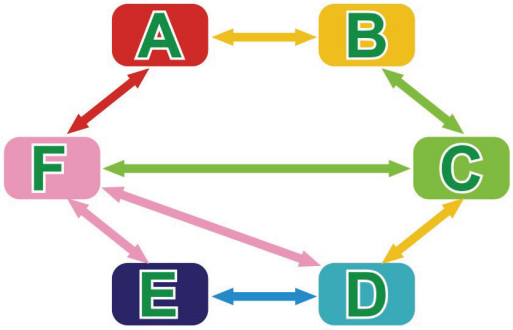

Figure 1-2 – Proprietary solutions to exchange information

- Promote standard interactions between entities

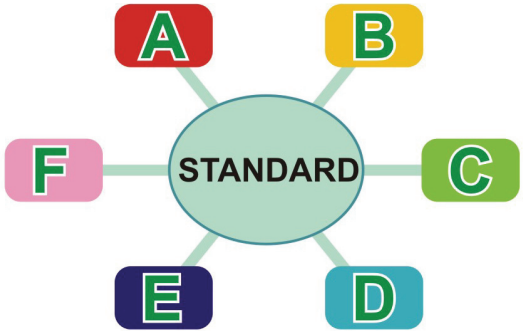

Figure 1-3 – Standard interactions between entities

- Facilitate integration of new partners in the smartcard ecosystem

Figure1-4 – Easy integration of new partners

Section 2: GlobalPlatform Messaging

The primary objective of the GlobalPlatform Messaging specification [3] is to standardize the most common messages that will be exchanged between disparate systems from a range of suppliers. By creating standards for these fundamental messages, the intention is to reduce systems integration impacts typically associated with constructing systems architecture from a variety of solution providers. Messages can be exchanged between any number of parties, and in some cases the recipient may not necessarily be the entity required to act on the message but may be to route the message onto the relevant party.

It is important to note that the objective of the GlobalPlatform Messaging specification [3] is not to prescribe or specify messages internal to the supplier of a system. Thus, where a supplier's product, or product solution, internalizes the interchanges of two or more actors identified in the specification, the implementation of these particular interchanges is left to the design discretion of the supplier. In such instances, where the product eventually needs to interface with other systems, the required messages for these interfaces are defined in the GlobalPlatform Messaging specification [3].

The principle of the GlobalPlatform Messaging specification [3] is to bring interoperability at multiple levels, i.e., business data, business process and data exchange.

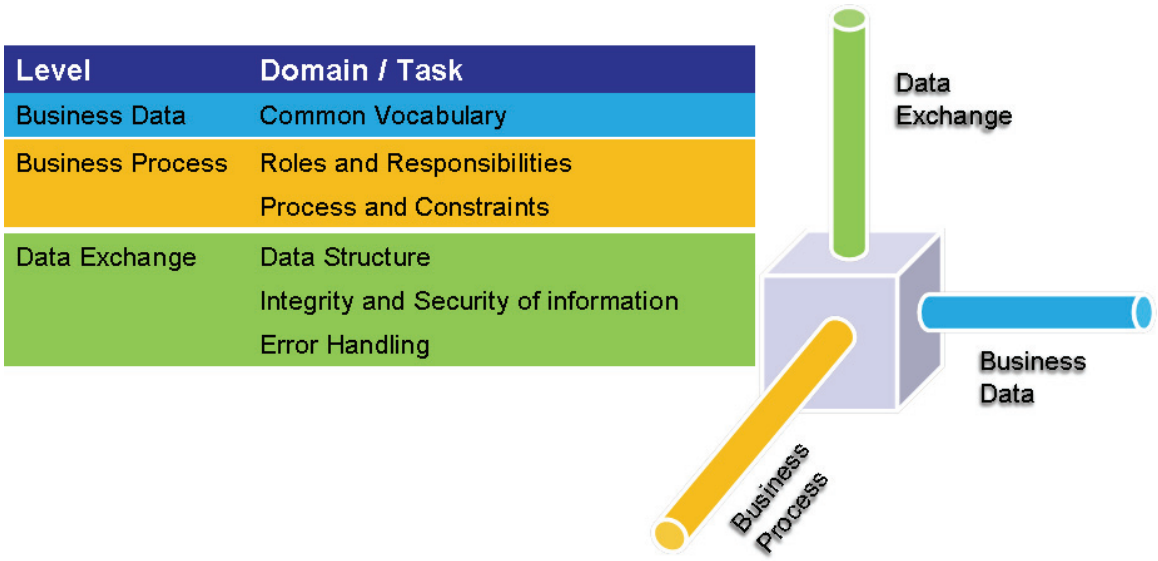

Figure2-1 – Multiple levels of interoperability

The three levels of interoperability provided by the GlobalPlatform Messaging specification are described individually below:

Business Data

The business data level provides a common vocabulary facilitating:

- A clear understanding and agreement of terms being used, and
- Clear rules about how and where defined terms can be used in a meaningful way.

Business Process

The business process level defines role and responsibilities. A role is an abstract model which specifies a set of duties and tasks whereas responsibilities consist of:

- A comprehensive list of actions and functions to be performed, and
- Business data to be exchanged.

Data Exchange

At the data exchange level, data structures are defined:

- XML Structure
- XML Schemas for validation
- Protocol independent

The messages described in the GlobalPlatform Messaging specification [3] all utilize a standard XML message header. The purpose of a standardized header is to facilitate message identification by systems utilizing the specification. This header will, at a minimum, describe the:

- Message Identifier
- Message Type
- Message Source
- Message Recipient
- Message Security

The messages described in the GlobalPlatform Messaging specification [3] can be grouped into two different categories:

- Messages for GlobalPlatform profiles. These messages focus on the card, application and key management interchange.
- Messages for GlobalPlatform card customization. These messages focus on personalization data preparation and personalization enablement, including post issuance delete, load, install and personalization. This category also includes audit trail messages.

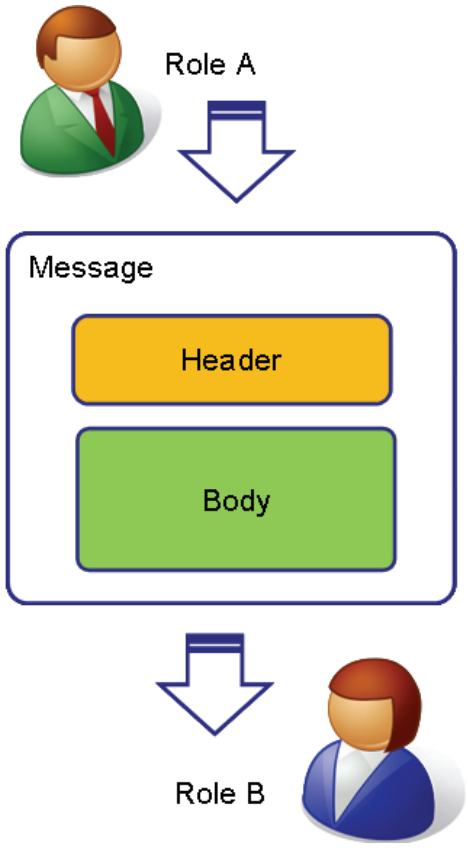

Figure2-2 – Message Structure

Extensible Markup Language (XML) is the language of choice for structuring messages. XML provides the flexibility and a standards-based approach that messages require to be unambiguous, support different versions of messages as they evolve, and be conducive to ease of information parsing and maintenance. XML is easily adaptable by actors involved in the card personalization process, and facilitates future changes in the content model as these changes need only be reflected in the XML schemas used by message providers. As a result, XML as a choice to represent messages using an open approach should be tenable to everyone involved in smart card implementations.

2.1 Actors Roles and Responsibilities

There are various actors involved in the production, distribution and maintenance of a multi-application smart card program. The current GlobalPlatform Messaging specification [3] already defines a simple model describing the roles necessary in such programs.

Actors are the entities responsible for playing certain roles, i.e., taking defined actions. Roles are the functions to be performed. Responsibilities describe more specifically the actions and the scope of actions that are performed.

An actor may perform a single, dual or even multiple roles. For example, a card issuer could conceivably also be the application provider as well as the application loader. At a high level an actor can also perform roles that appear similar or may be identical. At a lower level of detail, the specific responsibilities of actors distinguish the roles they play.

Additionally, several actors may combine responsibilities to accomplish a certain function. For example, while there may be only one actor responsible for application loading, the application provider, or the cardholder, has responsibilities that result in the initiation of application loading. All have some common set of responsibilities with respect to loading but each may deploy different processes and instruments to allow the application to be loaded.

Although the GlobalPlatform Messaging specification [3] may be used to implement interfaces internal to a role, it does not dictate any interface or messaging exchanged internally to a role or even to an actor performing multiple roles. It is essential for an actor playing one or multiple roles to know which data elements it is expected to send and receive with respect to the messages exchanged.

Section 3: What changes are needed for NFC Mobile?

Mobile service deployment requires the use of the most recent GlobalPlatform technology specifications, including the GlobalPlatform 2.2 [0], with its amendments [1], and the UICC Configuration [2]

The GlobalPlatform Card specification 2.2 [0] proposes a new business model allowing a service provider to manage a designated part of the card completely autonomously. The confidential card content management [1] provides a standard mechanism to:

- Confidentially load the initial key set of a security domain using a 3rd party entity
- Confidentially load application code
- Confidentially send APDU scripts to a security domain for performing application personalization or content management

Two main changes necessary for aligning the current GlobalPlatform Messaging specification [3] with the needs of new actors and roles in the new ecosystem brought about by NFC have been identified.

The first change is the addition of the Controlling Authority (CA) to manage exchanges with an optional third party entity when required by the deployment model. The Controlling Authority supports two responsibilities and can be performed by two different actors:

- One responsibility is to control a specific controlling authority security domain which can enable confidential keys loading (Confidential Key Loading Authority) for setting up the initial keys of a security domain.
- The other responsibility is to control a specific security domain used to enable Mandated Data Authentication Pattern (Mandated DAP Authority). The Mandated DAP deployment model allows an actor to securely sign all application code before it is loaded in a GlobalPlatform card.

In a mobile contactless environment, to ensure a correct responsibility scheme, the CA role cannot be performed by an entity playing the loader role and the card issuer or the SSD manager roles.

The second change is the necessity of having a Supplementary Security Domain (SSD) manager different from the already defined "card issuer". In many cases the role of the SSD manager will not be to manage applications in the card but rather manage an intermediate security domain to manage card content and perform cryptographic services for confidentiality.

The SSD manager is responsible for managing instantiated security domains on a card. It holds the Secure Channel Protocol (SCP) keys (SCP02 and/or SCP80) and/or certificates belonging to the security domain it is in charge of. It is also responsible for managing the secure communication to the security domain it is in charge of. The SSD manager may have the capability to load, install, extradite or personalize applications on behalf of the service provider or the issuer who granted the right for doing so.

The interfaces for actors exchanging messages with the controlling authority, application provider, card issuer and SSD manager, need to be revised as new roles are defined.

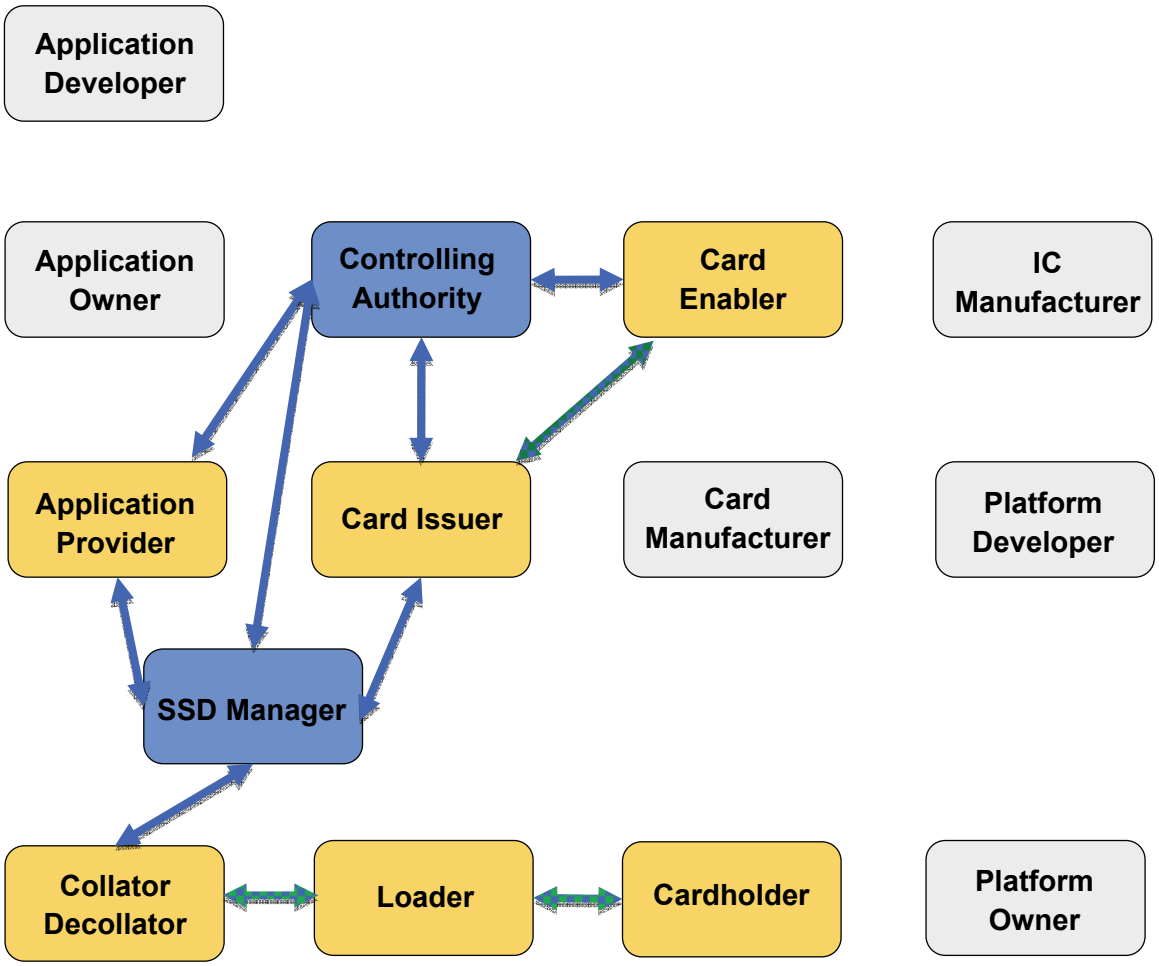

Fig. 3-1 – GlobalPlatform Messaging: Actors and Roles Proposal

In the above diagram, new actors as well as new roles are indicated in blue. Existing roles requiring some modification are shown in turquoise.

3.1 Role description

As discussed in the preceding sections and illustrated in figure 3.1 above, the mobile NFC ecosystem will consist of a large number of actors and roles. These roles are described below:

3.1.1 Application Developer

The Application developer designs and writes application code.

3.1.2 Application Owner

The application owner defines and maintains the application specifications.

3.1.3 Application Provider
The application provider procures the necessary components to load a complete application (i.e., application code, application data, application keys and/or certificates, and data belonging to a specific cardholder) onto a card. The application provider has a direct business relationship with and provides a card-based service to the Cardholder.

3.1.4 SSD Manager
The supplementary security domain manager manages instantiated security domains on a card. (For more details, see section 4: Examples of Deployment Cases)

3.1.5 Controlling Authority
The controlling authority manages exchanges with an optional third party entity when required by the deployment model. (For more details, see section 4: Examples of Deployment Cases)

3.1.6 Card Issuer
The card issuer holds ultimate responsibility for the GlobalPlatform card. A card issuer may be the only authority to allow load, install, delete, extradition or personalization of applications, or the card issuer may delegate load, install, extradition or personalization of the applications to a third party such as an application provider, via the SSD manager.

The Card Issuer issues cards to the cardholders. The card issuer is responsible for securely managing all the pre-issuance production processes culminating in a card specifically prepared for a cardholder, and for many post-issuance processes, including final decommissioning of a card.

The card issuer determines a portfolio of applications to be supported and offered to its card base. The issuer manages authorization of applications permitted to reside on its cards.

3.1.7 Cardholder
The cardholder is the entity receiving the card. A cardholder maintains the contents of the chip with the authorization of the card issuer.

3.1.8 Card Enabler
The card enabler performs pre-personalization functions, specifically the loading of the initial Issuer, a controlling authority security domain and, if any, application provider security domains. Furthermore, the card enabler can personalize the security domain with issuer, controlling authority or application provider specific data. The card enabler prepares the platform for subsequent application loading.

3.1.9 Collator/Decollator
The collator/decollator performs the collation (data aggregation) of personalization data from all service providers for one cardholder and after use by the loader, performs the decollation function to return information to the Issuer and the appropriate application providers. In the context of NFC and post-issuance, this responsibility is managed by an already present actor performing the loader or SSD manager role. The role has been kept in this white paper for consistency sake.

3.10 Loader
The loader loads card issuer specific cards with applications and/or personalization/customization data according to the instructions of the application provider, complying with security policies and procedures set by the card issuer. It may also place the final security domain keys on the card.

3.11 Card Manufacturer
The card manufacturer is the entity that manufactures (fabricates) cards to the requirements of the card issuer.

3.12 IC Manufacturer
The entity that fabricates wafers containing chips with a specified ROM configuration.

3.13 Platform Specification Owner
The platform specification owner defines and maintains the card platform operating system specifications.

3.14 Platform Developer
The platform developer is responsible for the development of GlobalPlatform cards in accordance with the Specifications provided by the GlobalPlatform consortium.

SECTION 4: Examples of Deployment Cases

In the NFC ecosystem, the MNO (Mobile Network Operator) owns the UICC hosting the service provider applications. Therefore, each MNO may choose an appropriate business model(s) and consequently select the personalization features to be supported by the UICC and available to its partners (service providers and trusted service managers). Three main UICC configuration scenarios are proposed by GlobalPlatform to support the different business models:

- Simple Mode : An Issuer centric model, where card content management is only performed by the MNO but is monitored by the TSM,
- Delegated Mode : card content management can be delegated to a TSM but each operation requires preauthorization from the MNO,
- Authorized Mode: card Content management is fully delegated to a TSM for a sub area of the UICC.

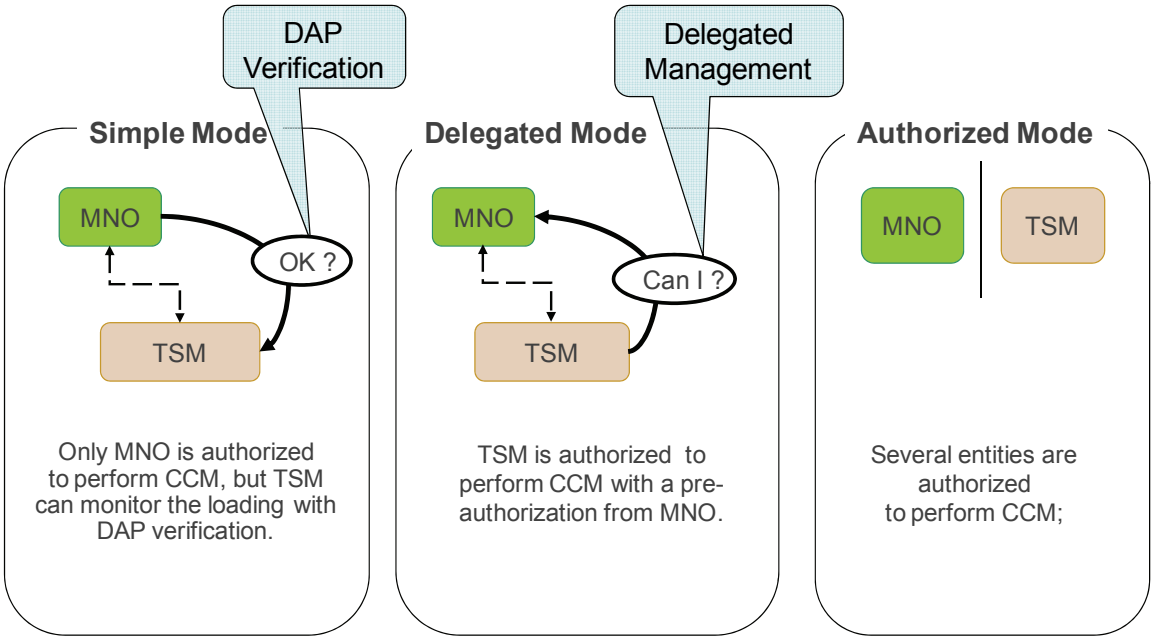

Figure 4-1 – Different business models for application management

The GlobalPlatform Messaging specification [3] will support all three of these modes. This section aims at providing examples of possible implementations for each mode and describes the main features presented by GlobalPlatform Messaging specification [3] to exchange information between the different actors.

The following assumptions apply to all the scenarios described in the following sections when using confidential key loading:

- As described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2], a controlling authority entity is mandatory when confidential application loading and personalization are used.

- The CA keys and certificate are loaded into the controlling authority secure domain by the card manufacturer during UICC manufacturing.
- The "Confidential Setup of Initial Secure Channel Keys" requires that the CA entity must be a trusted third party to the Link Platform Operator (an entity operating an OTA platform, i.e., the MNO or TSM) and the entity in charge of the application personalization (i.e. either the TSM or SP). The controlling authority may be a Certificate Authority or the SIM vendor itself.
- According to the scenario selected for "Confidential Setup of Initial Secure Channel Keys", some GlobalPlatform messaging may be needed between the CA and the entity in charge of application personalization (i.e., either the TSM or the SP).
- For any scenario, DAP verification or Mandated DAP may be used to authenticate and check the integrity of the service provider application loaded onto the UICC.
- As specified in the UICC Configuration [2], TSD and APSD can support either secure channel protocol SCP02, SCP80 or both. One of the major requirements for a GlobalPlatform card is the ability to provide a minimum level of cryptographic functionality. This cryptography is, for example, used for the generation of digital signatures, and is available for use by applications present on the card. The intent of this configuration is to host applications already deployed in the contactless area that rely on SCP02 cryptographic services (as an example, EMV CPS compliant application):
    - SCP02 is a symmetric secure channel protocol allowing script messaging that can be received directly via the contact and contactless interfaces and can be either encapsulated into OTA (SCP80) messaging transported by a parent SD.
    - SCP80 (ETSI TS 102.225) is an OTA secure channel protocol enabling direct access to the SD from an OTA platform through the MNO's GSM network.

Please note that the scenarios discussed in the sections following, are **examples only** and should not be considered as the only way of allocating roles to the various entities. Also, in order to highlight the confidential management features proposed by the UICC configuration, all update commands sent by a MNO, TSM or Service Provider to the card, use an OTA channel (SCP80 based on OTA ETSI standards). However, if confidential management is not needed, a direct interaction via a SCP02 channel can be used instead.

In the illustrations below representing the various scenarios, roles in light grey remain unchanged from their current definition in the GlobalPlatform Messaging specification 1.0 [3], based on an issuer centric and pre-issuance oriented approach. The arrows represent the GlobalPlatform message flows between entities and dotted arrows are used where the GlobalPlatform message flows are optional. New entity names (i.e., the Controlling Authority and SSD Manager) are shown in blue.

For simplicity sake, the schemes below only represent one SP, one TSM, one MNO, etc. However, in a real implementation one SP will most likely deal with multiple MNOs and eventually several TSM entities. These constraints are anticipated in the GlobalPlatform Messaging specifications designed to cope with a multiple entity environment.

4.1 Examples of Simple Mode deployment cases

In the simple mode management case, only the UICC Issuer, i.e. the MNO, can load applications into the UICC. Two scenarios are described depending on whether or not the TSM operates its own OTA platform for application personalization.

4.1.1 Simple Mode using MNO OTA platform

This scenario is based on the following assumptions:

- The service provider delegates full management of its application to a TSM. This encompasses the creation of its Application Provider Security Domain (APSD) and management of its application loading and personalization.
- The TSM will use the MNO OTA platform both for APSD creation and application loading, and personalization. There is no TSM OTA platform involved in this scenario.
- The APSD keys are created or retrieved by the TSM in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem in this case can be represented as follows.

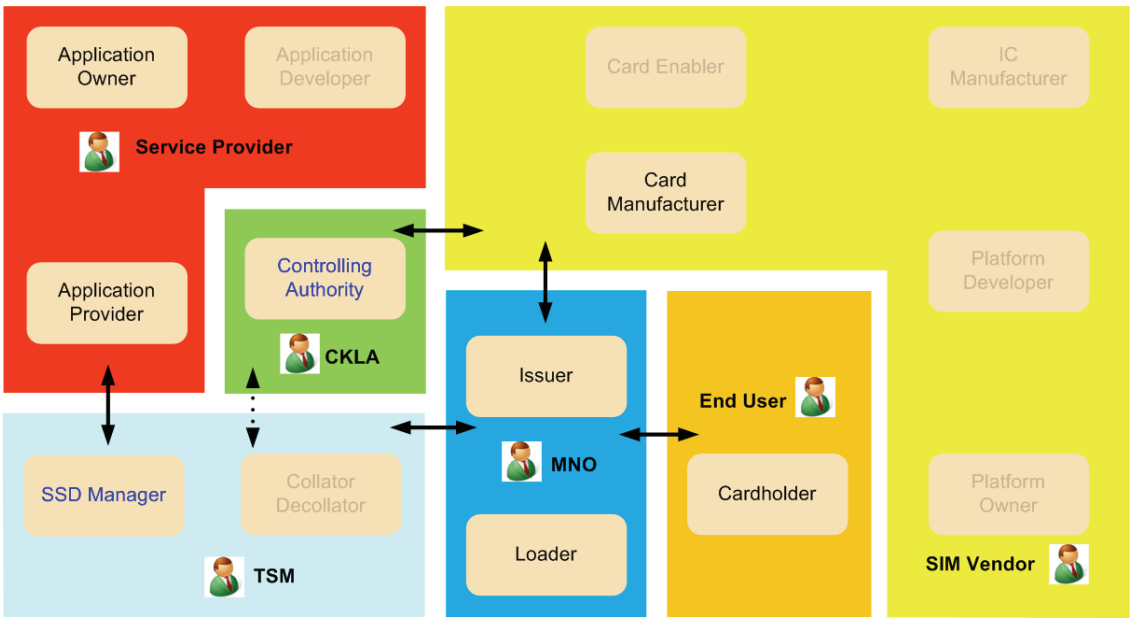

Figure 4-2 – Roles splitting for "Simple Mode using MNO OTA platform"

The corresponding representation of the on card SD hierarchy is as follows.

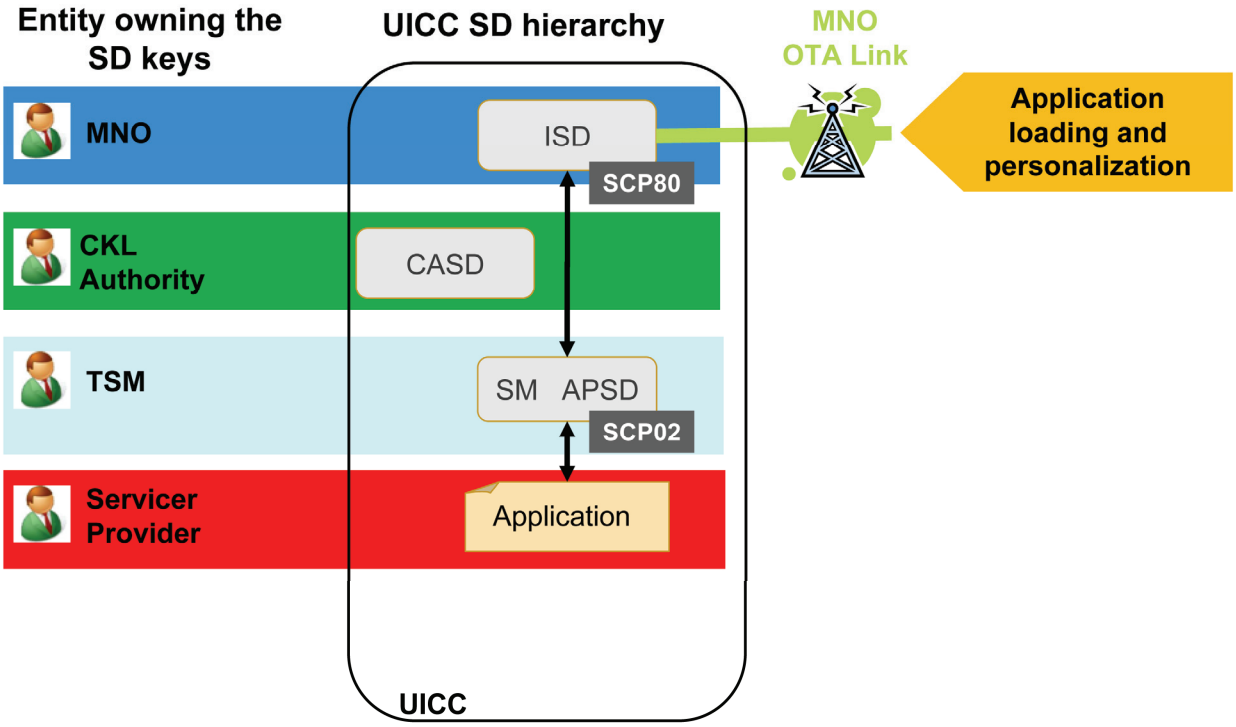

Figure 4-3 – On card view of "Simple Mode using MNO OTA platform"

Note:
SM APSD: Application Provider Security Domain with no card content management privilege (simple mode) and SCP02 keyset.

4.1.2 Simple Mode using MNO & TSM OTA platforms

The current example is based on the following assumptions:

- The service provider delegates to a TSM the full management of its application. This encompasses the creation of its Application Provider Security Domain (APSD) and management of its application loading and personalization.
- The TSM will use the MNO OTA platform for APSD creation and application loading. For application personalization, the TSM will use its own OTA platform.
- The APSD keys are created or retrieved by the TSM in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem for the simple mode deployment case can be represented as illustrated below.

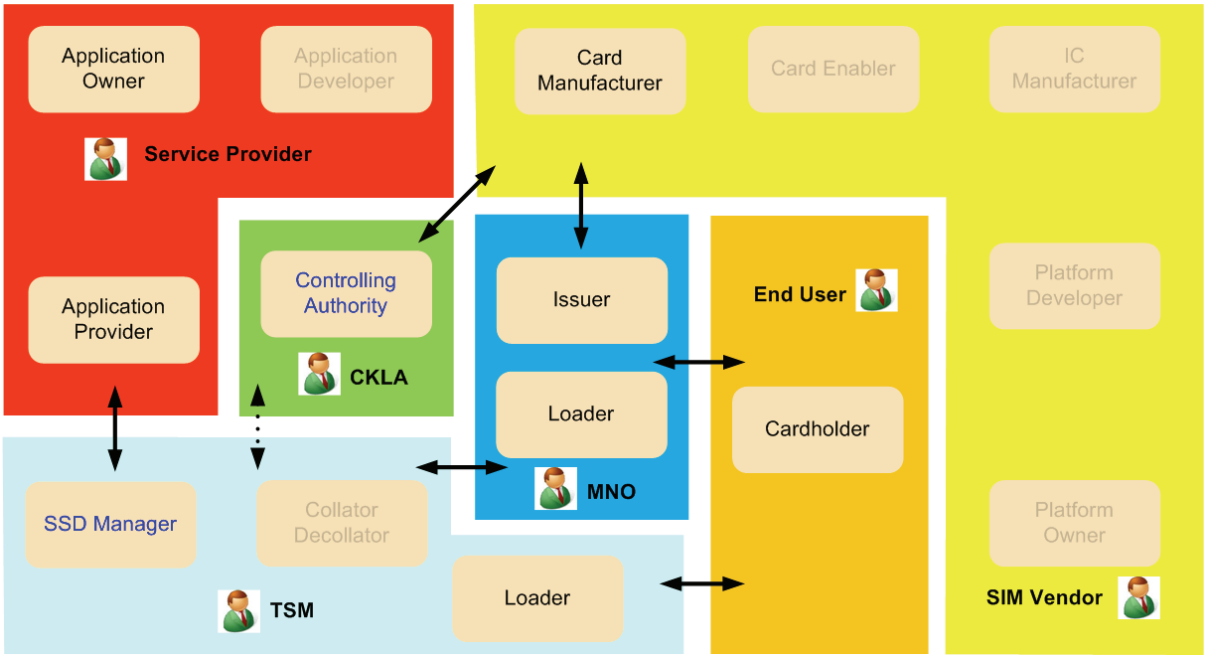

Figure 4-4 – Roles splitting for "Simple Mode using MNO & TSM OTA platforms"

The corresponding representation of the on card SD hierarchy is shown below.

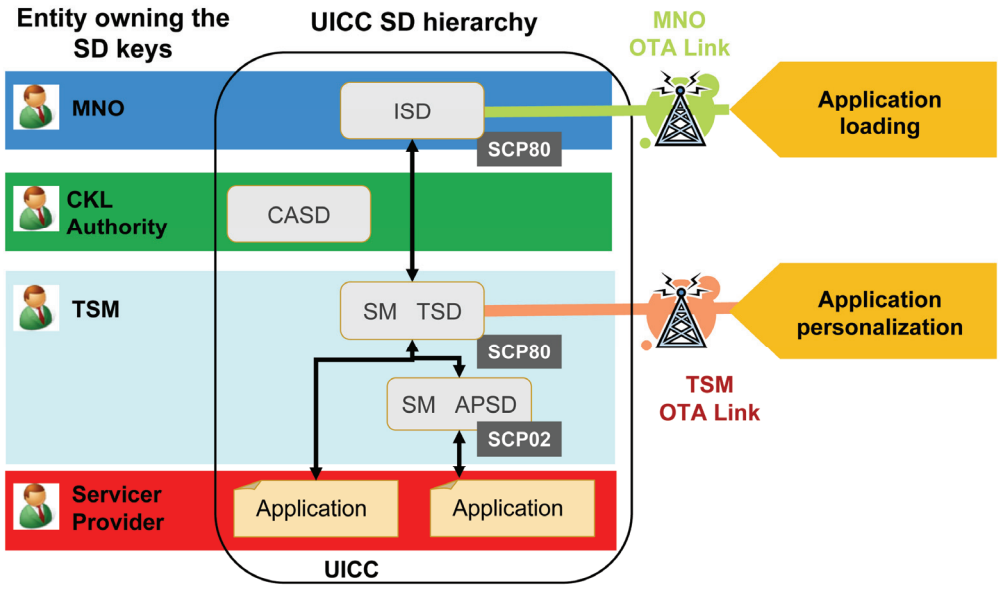

Figure 4-5 – On card view of "Simple Mode using MNO & TSM OTA platforms"

Note:

SM TSD: TSM Security Domain with no card content management privilege (simple mode) and SCP80 (OTA) keyset.

SM APSD: Application Provider Security Domain with no card content management privilege (simple mode) and SCP02 keyset.

4.2 Delegated Management Deployment Case

The delegated management deployment use case is organized around the delegated mode card capability. The MNO is no more in charge of loading, installing, activating or removing the application. Card content management is performed by the TSM with a pre-authorization from the MNO.

In some cases, for privacy reasons, the SP may manage their application personalization internally to prevent the possibility of third party manipulation of application keys or application data relating to their customers.

Two scenarios are described below depending whether the SP delegates its application personalization to the TSM or not.

4.2.1 Delegated Mode with full delegation to the TSM

This example is based on the following assumptions:

- The service provider delegates to a TSM full management of its application. This encompasses the creation of its Application Provider Security Domain (APSD) and the management of its application loading and personalization.
- The TSM will use its own OTA platform but a token must be delivered to the TSM by the MNO for a pre-authorized card content management action.
- No DM token is needed in the case of application lock/unlock and personalization.
- The APSD keys are created or retrieved by the TSM in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem for the delegated management mode deployment case are represented as follows.

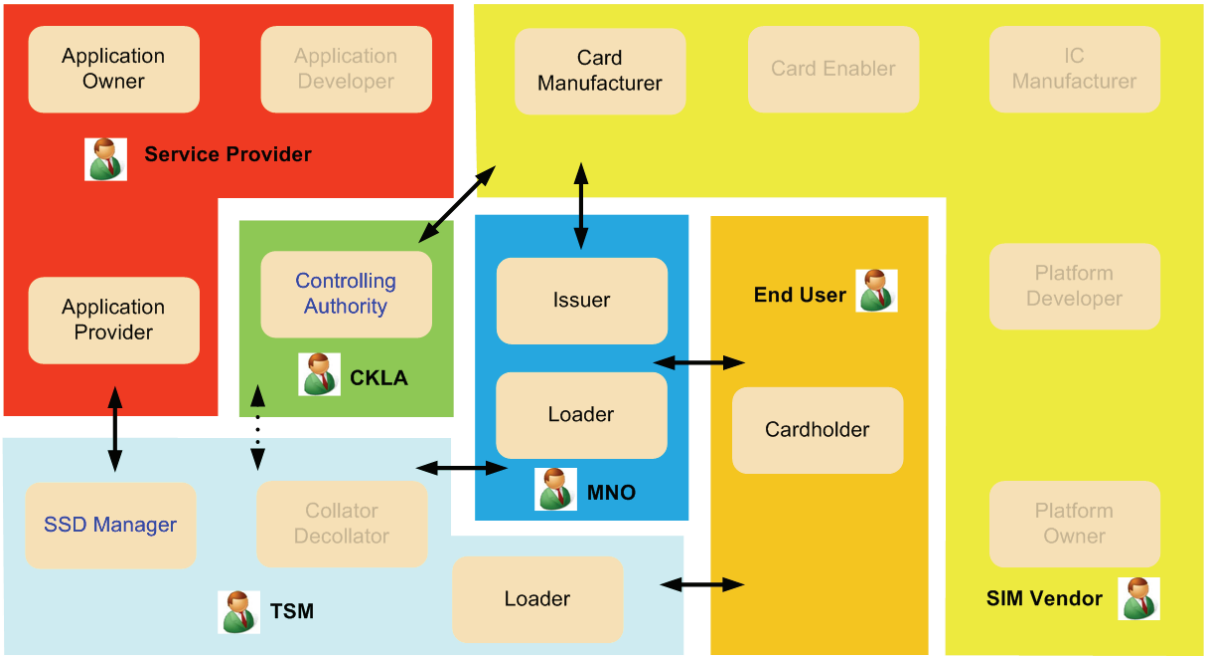

Figure 4-6 – Roles splitting for "Delegated Mode with full delegation to the TSM"

The corresponding representation of the on card SD hierarchy is shown below.

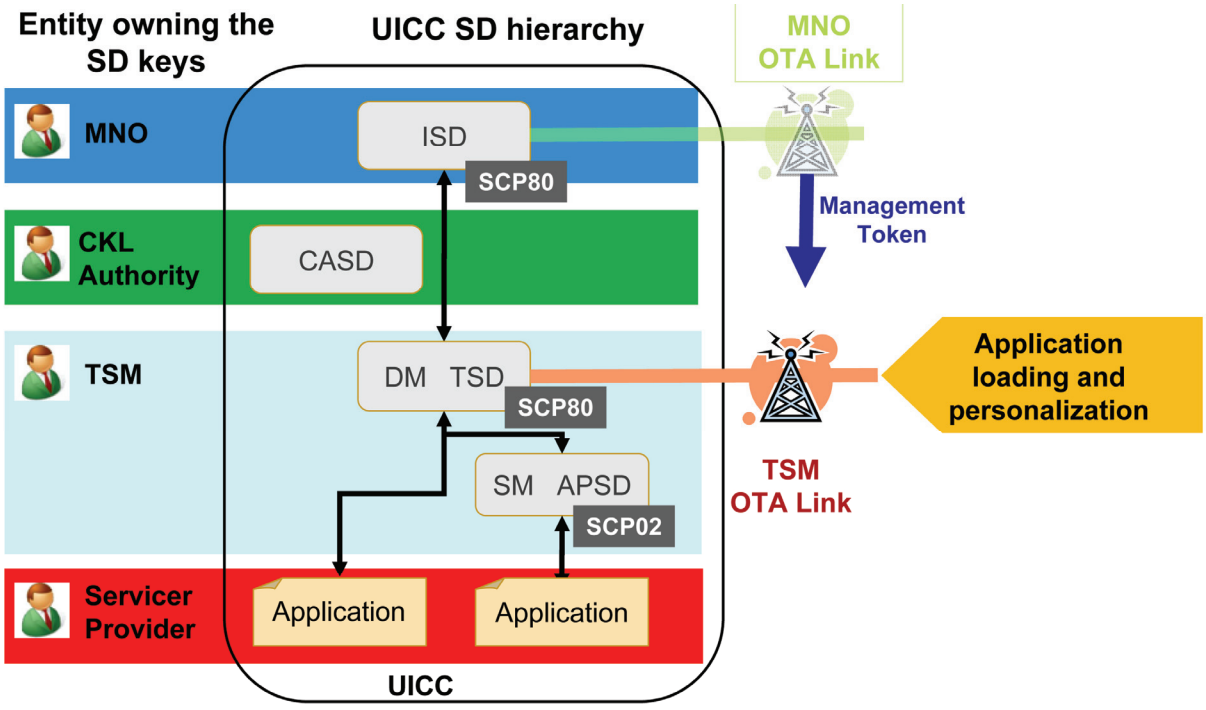

Figure 4-7 – On card view for "Delegated Mode with full delegation to the TSM"

Note:
DM TSD: TSM security domain with delegated management privilege and SCP80 (OTA) keyset
SM APSD: Application provider security domain with no AM/DM privilege (simple mode) and SCP02 or SCP80 keyset.

Different cases are possible for the TSM to organize applications on the UICC as represented in the figure above:

- The SP application can be loaded directly under the TSM SD, OR
- A dedicated APSD can be assigned per application. This does not provide additional security as the TSM owns the APSD keyset and the APSD can be assigned with SCP02 or SCP80 keyset.
  But this option may be requested by SP to TSM in order to enable a seamless handover of SP application to another TSM in the future. The incumbent TSM will simply have to extradite the APSD (and its contents) to the new TSM TSD in this case.

As stated in the introduction, The TSM can use a local SCP02 channel to perform card content management instead of SCP80 via OTA.

4.2.2 Delegated Mode with personalization by SP

This example is based on the following assumptions:

- The service provider delegates the loading and installation of its application to a TSM. This encompasses the creation of its Application Provider Security Domain (APSD) and the management of its application loading and activation.
- The TSM will use its own OTA platform but a token must be delivered to the TSM by the MNO for a pre-authorized card content management action.
- No DM token is needed in the case of application lock/unlock and personalization.
- The SP will perform the application personalization by preparing the personalization script and sending it to the UICC via the TSM OTA link in a confidential way.
- The APSD keys are created or retrieved by the SP in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem for Delegated Management Mode deployment case can be represented as follows.

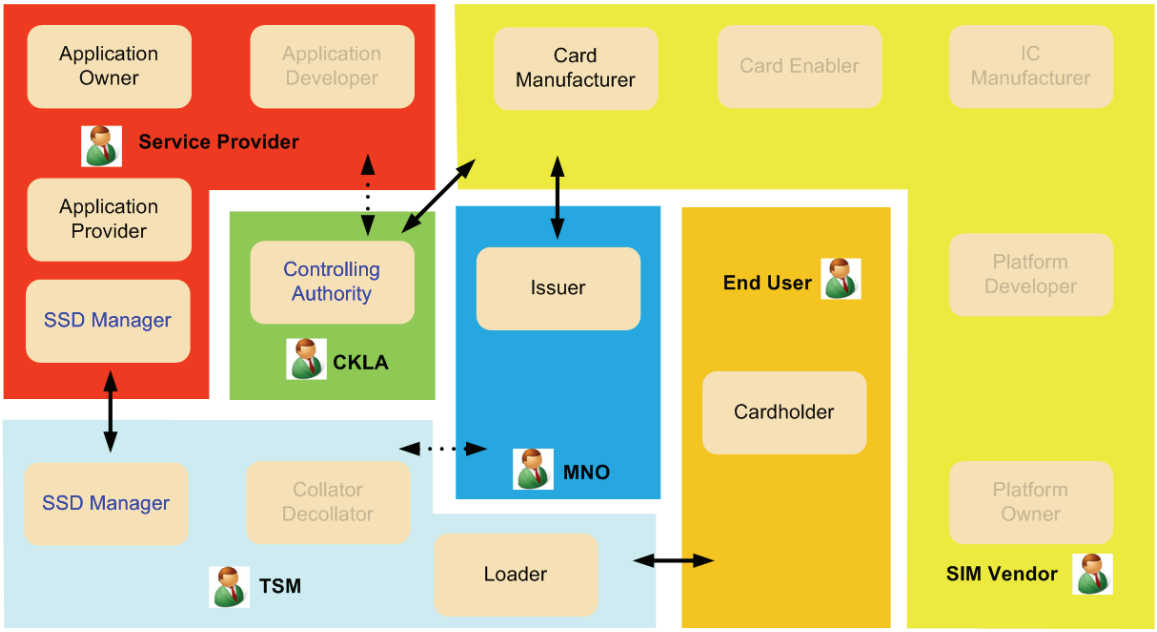

Figure 4-8 – Roles splitting for "Delegated Mode with personalization by SP"

The corresponding representation of the on card SD hierarchy is shown below.

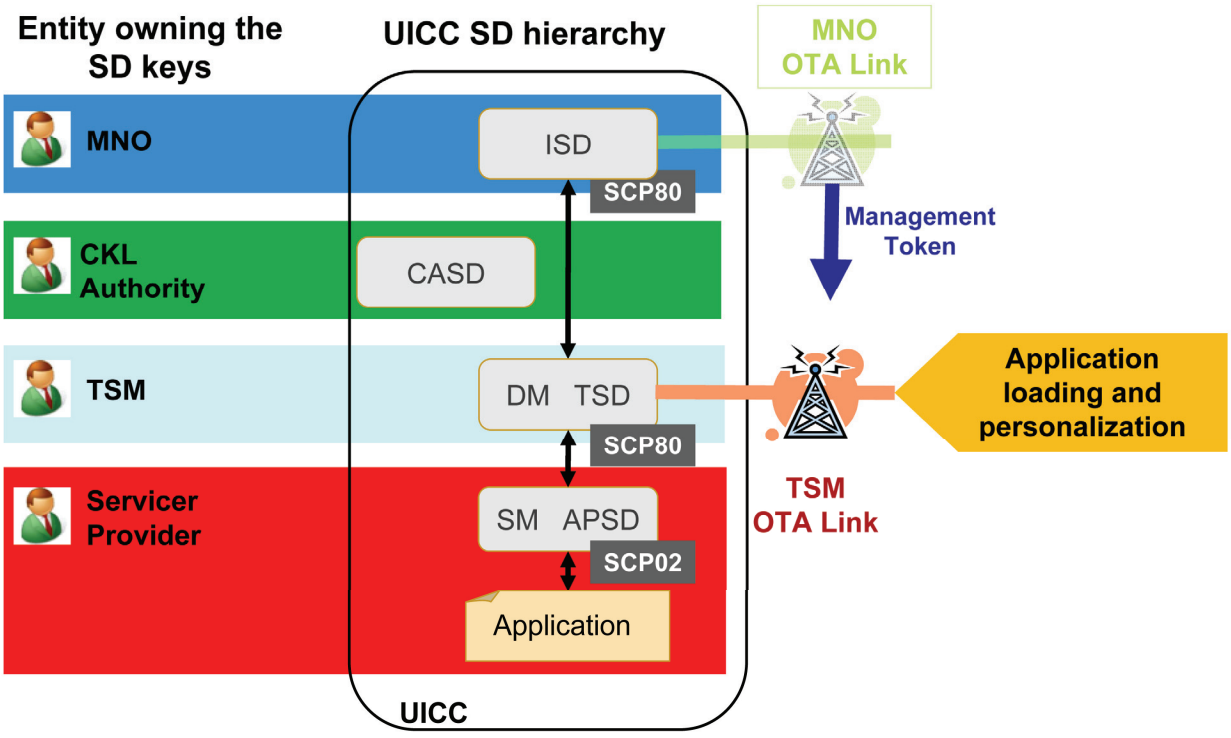

Figure 4-9 – On card view for "Delegated Mode with personalization by SP"

Note:
DM TSD: TSM security domain with delegated management privilege and SCP80 (OTA) keyset.
SM APSD: Application provider security domain with no AM/DM privilege (simple mode) and SCP02 keyset.

4.3 Authorized Management deployment case

The authorized Management deployment use case is organized around the authorized management card capability. The TSM, which holds the SP applications, is able to process directly without authorization provided by the MNO. This mode can be used to enable the TSM to manage its own SD hierarchy and perform card content management without authorization (i.e., a token) from the MNO.

For the same reason as for delegated management mode, three scenarios are described depending on whether the SP delegates its application personalization to the TSM or not.

4.3.1 Authorized Mode with full delegation to the TSM

The current example is based on the following assumptions:

- The service provider delegates the card content management of its application to a TSM. This encompasses the creation of its Application Provider Security Domain (APSD) and management of its application loading and personalization.
- The TSM uses its own OTA platform and has full flexibility to create a security domain and load the application into its TSD hierarchy without MNO authorization. The TSM may nevertheless require an authorization from MNO if a memory quota has been assigned to its TSD hierarchy (indicated by a dotted link between the MNO and TSM).
- The APSD keys are created or retrieved by the TSM in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem for the Authorized Management Mode deployment case can be represented as follows.

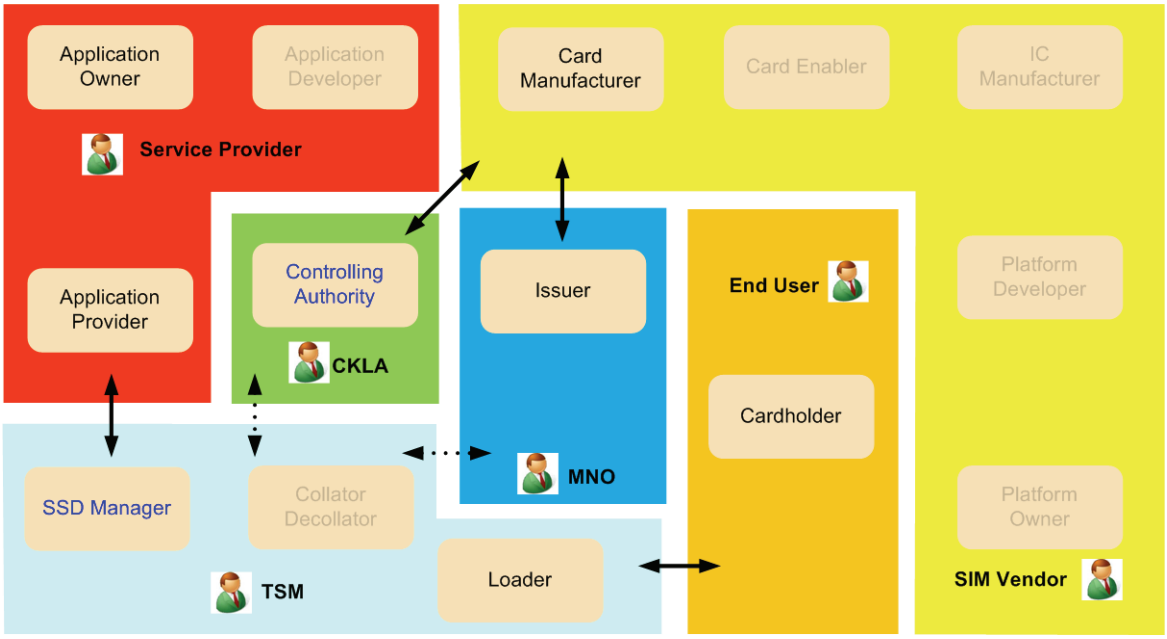

Figure 4-10 – Roles splitting for "Authorized Mode with full delegation to the TSM"

The corresponding representation of the on card SD hierarchy is shown below.

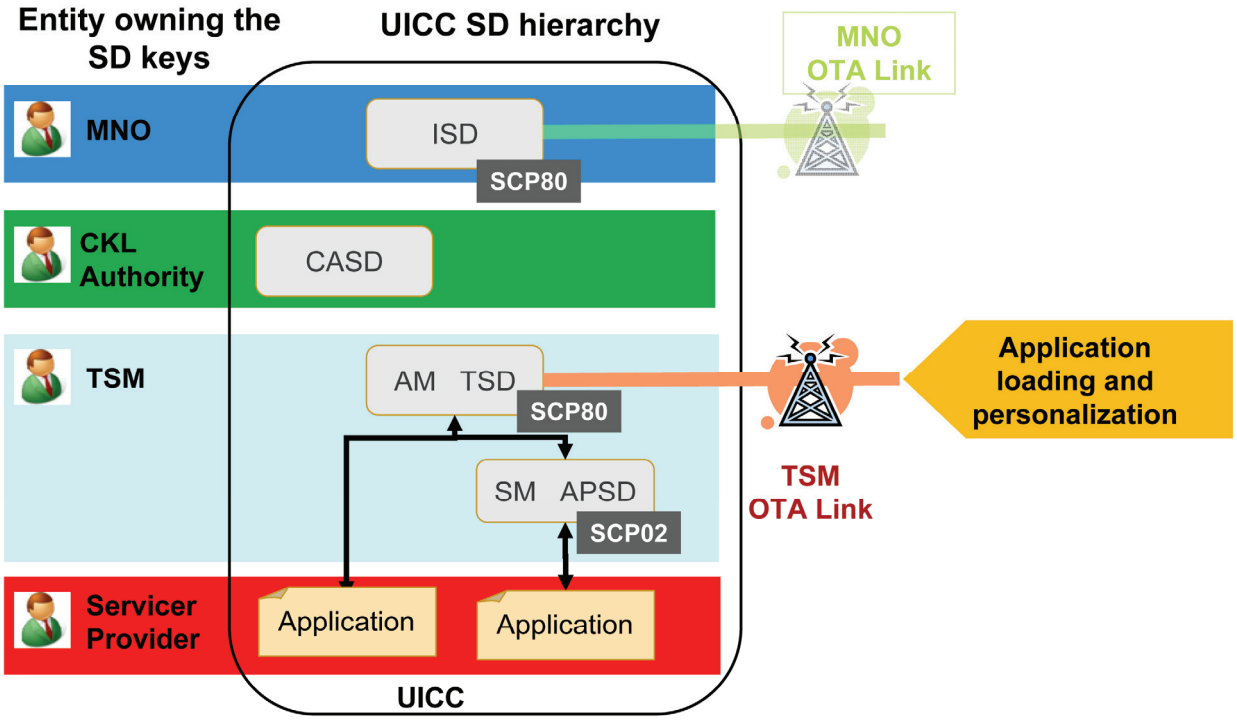

Figure 4-11 – On card view for "Authorized Mode with full delegation to the TSM"

Note:

AM TSD: TSM security domain with authorized management privilege and SCP80 (OTA) keyset.

SM APSD: Application provider security domain with no AM/DM privilege (simple mode) and SCP02 keyset.

4.3.2 Authorized Mode based on SCP02 to the TSM

In order to show how SCP02 can be used for card content management the following alternative is described.

This example is based on the following assumptions:

- The service provider delegates the card content management of its application to a TSM. This encompasses the creation of its Application Provider Security Domain (APSD) and management of its application loading and personalization.
- The TSM will use its own OTA platform to send the commands but will use SCP02 security for card content management, creating security domain and loading the application into its TSD hierarchy without MNO authorization.
- The APSD keys are created or retrieved by the TSM in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys of the UICC Configuration [2].

The roles in the NFC ecosystem for the Authorized Management Mode deployment case can be represented as follows.

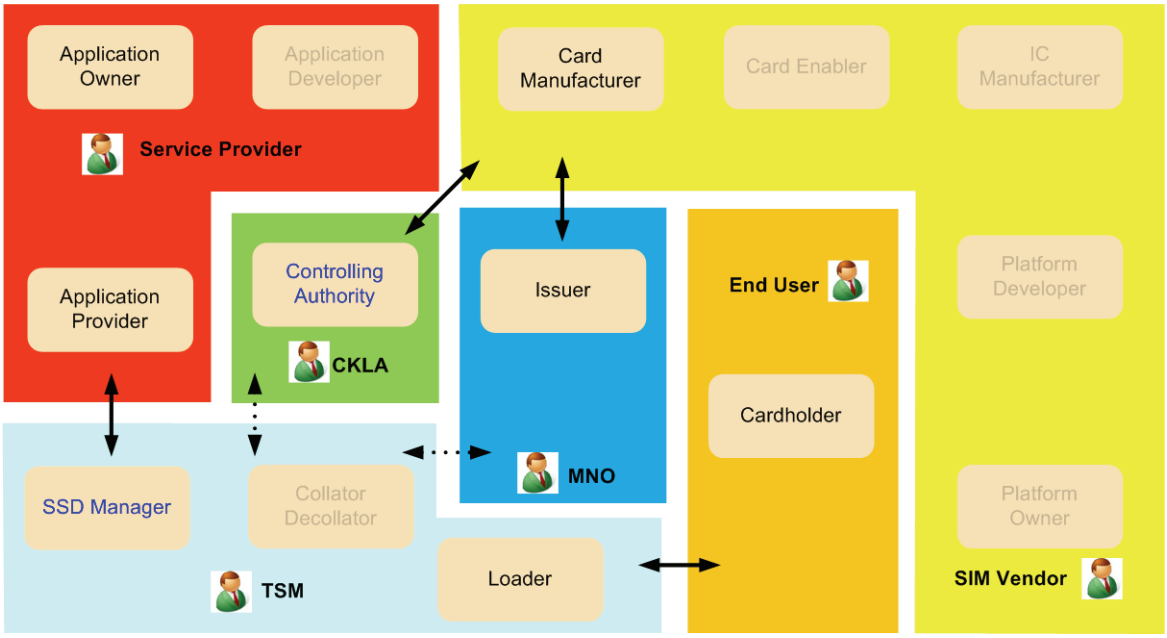

Figure 4-12 – Roles splitting for "Authorized Mode with full delegation to the TSM"

The corresponding representation of the on card SD hierarchy is shown below.

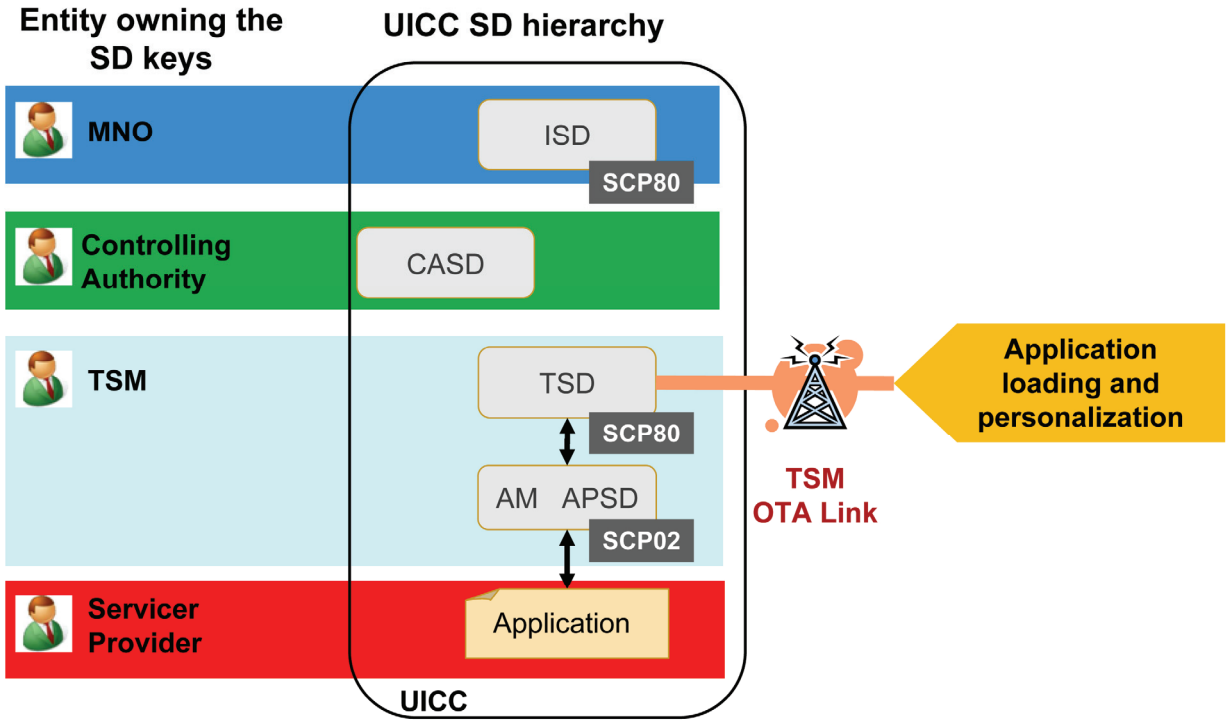

Figure 4-13 – On card view for "Authorized Mode with full delegation to the TSM"

Note:
TSD: TSM Security Domain with SCP80 (OTA) keyset only provides transport (no card content management).
AM APSD: Application provider (or TSM) security domain with authorized management privilege and SCP02 keyset.

4.3.3 Authorized Mode with personalization by SP

This example is based on the following assumptions:

- The service provider delegates the loading and installation of its application to a TSM. This encompasses the creation of its Application Provider Security Domain (APSD) and management of its application loading and activation.
- The TSM will use its own OTA platform and has full flexibility to create a Security Domain and to load application into its TSD hierarchy without MNO authorization. The TSM may nevertheless require an authorization from MNO if a memory quota has been assigned to its SD hierarchy (indicated by a dotted link between the MNO and TSM).
- The SP will perform the application personalization by preparing the personalization script and sending it to the UICC via the TSM OTA link in a confidential way.

- The APSD keys are created or retrieved by the SP in a confidential way as described in Chapter 11 "Confidential Setup of Initial Secure Channel Keys" of the UICC Configuration [2].

The roles in the NFC ecosystem for the Authorized Management Mode deployment case can be represented as follows.

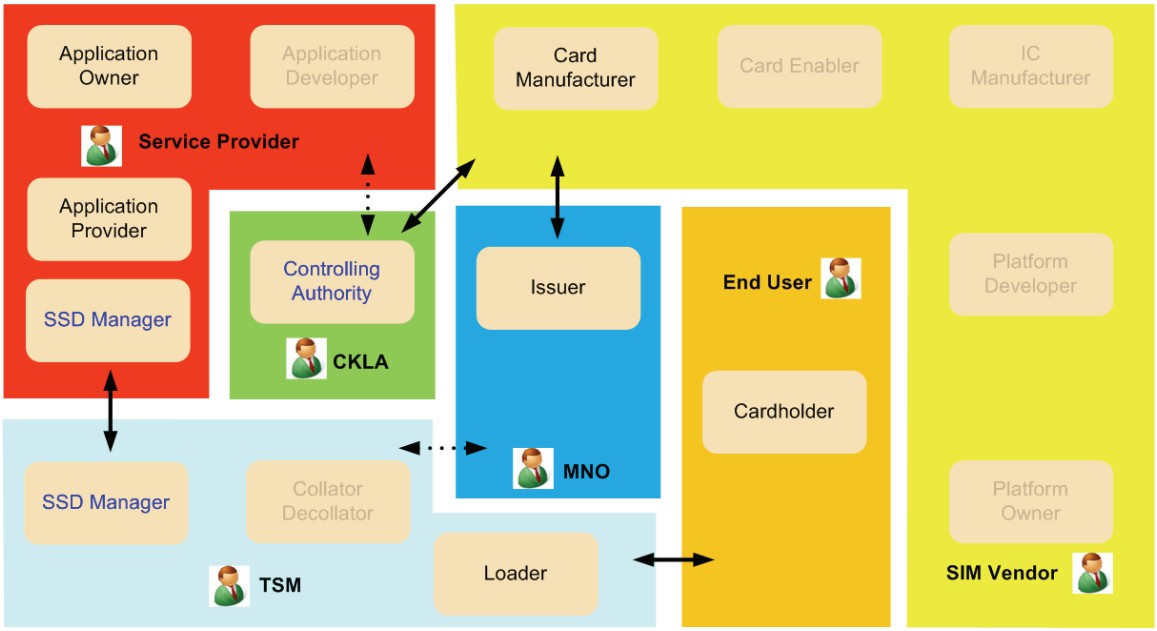

Figure 4-14 – Roles splitting for "Authorized Mode with personalization by SP"

The corresponding representation of the on card SD hierarchy is shown below.

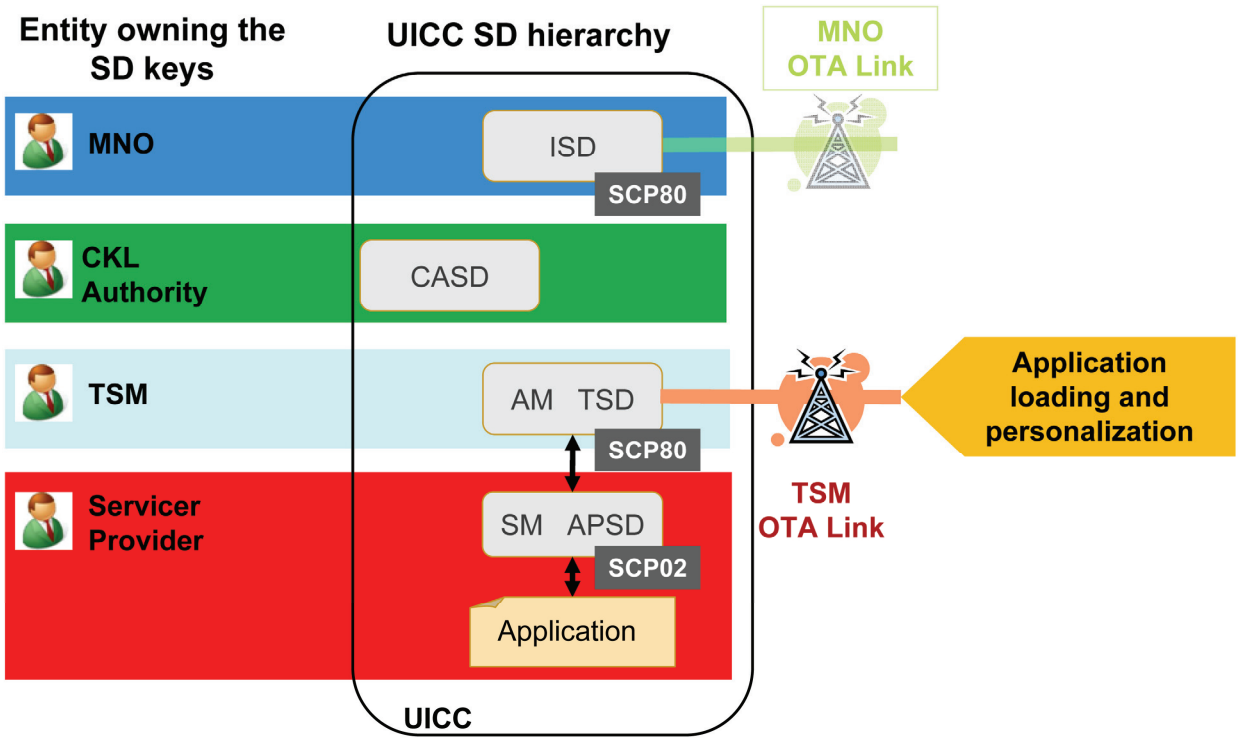

Figure 4-15 – On card view for "Authorized Mode with personalization by SP"

Note:
AM TSD: TSM security domain with authorized management privilege and SCP80 (OTA) keyset.
SM APSD: Application provider security domain with no AM/DM privilege (simple mode) and SCP02 keyset.

SECTION 5: Conclusion

NFC 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 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 NFC mobile environment.

Publication of an updated version of the GlobalPlatform Messaging specification is planned for the end of 2009. 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 NFC ecosystem by the end of 2009. The specifications will include GlobalPlatform 2.2 [0], its amendments [1], and the UICC Configuration [2]. The specifications will facilitate the creation of a standard infrastructure allowing service providers, trusted service managers and mobile network operators to manage application download and personalization of NFC enabled mobile phones, for issuance and post issuance of GlobalPlatform based smart cards 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]

APPENDIX B: Abbreviations and Notations

Abbreviation	Meaning
AP	Application Provider (Actor)
APSD	Application Provider Security Domain
AM	Authorized Management
CA	Controlling Authority (Actor)
CASD	Controlling Authority Security Domain
CCCM	Confidential Card Content Management
CKLA	Confidential Key Loading Authority
DM	Delegated Management
DAP	Data Authentication Pattern
GSM-A	Global System for Mobile Telecommunications Association
ISD	Issuer Security Domain
LPO	Link Platform Operator
MNO	Mobile Network Operator
NFC	Near Field Communication
OTA	Over-The-Air
XML	eXtensible Markup Language
SCP	Smart Card Platform
SE	Secure Element
SP	Service Provider
SSD	Supplementary Security Domain
TSD	Trusted Service Manager Security Domain
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card

APPENDIX C: Figures