UICC Configuration for Mobile NFC Payments v1.1

August 2014

Table of Contents

1. Introduction

This paper defines SIMalliance's recommendations for UICC configuration and feature requirements in mobile near field communication (NFC) payments. The aim of this document is to provide guidelines that support service providers, mobile network operators (MNOs), manufacturers and implementers of mobile NFC payment services, by facilitating system integration, simplifying interoperability and reducing market fragmentation.

Tabulated features are presented within this paper and SIMalliance's recommendations are indicated alongside. Features are labelled as follows:

- Required: Features necessary for interoperability and to reduce market fragmentation. These features will also simplify integration.
- Optional: Features needed only for specific markets or environments.
- Evolutionary: Features regarded as important for future advancements.

This paper is compliant with various UICC guidelines published by other organisations, including those from GlobalPlatform and the GSMA. To ensure an efficient and interoperable mobile NFC payment deployment, SIMalliance recommends compliancy with the following documents:

- GlobalPlatform's End-to-End Simplified Service Management Framework v1.0
  The security domain configuration for the UICC is not detailed in this paper. As such, SIMalliance recommends the use of the payment configuration profiles defined in this framework document published by GlobalPlatform.

- EMVCo's EMV Profiles of the GlobalPlatform UICC Configuration v1.0
  This document defines the requirements for UICCs intended to host a payment system's mobile payment application within mobile consumer devices and provides the UICC configuration profiles acceptable to be used in a mobile proximity payment programme based on EMV® requirements.

- GSMA's NFC UICC Requirements Specification v4.0
  Compliancy to the newer version in progress (v5.0) could be considered important for future evolutions.

In addition to the above guidelines, different countries or regions may have additional specifications, for example, AFSCM in France, ISIS in the US, etc.

2. Mobile NFC Payment System Overview

The development of new NFC services has resulted in a variety of new players appearing on the NFC landscape. Providers of payment, identification and other services are creating new opportunities for added value in the mobile space and as new partnerships, networks and services are established, the need for interoperability across the mobile NFC ecosystem has become increasingly important, yet remains one of the biggest challenges the market faces.

The SIMalliance Interoperability Working Group offers a full overview of secure element (SE) configurations within NFC deployments in its NFC Secure Element Stepping Stones v1.0 document, which promotes interoperability between the different actors in the NFC ecosystem. Other organisations such as the Association Française du Sans Contact Mobile (AFSCM), GlobalPlatform and the GSMA have also developed homogeneous product configurations to increase interoperability and speed up NFC deployments.

In the GSMA Mobile Commerce in Retail white paper (page 6), the GSMA outlines its commitment to maintain a set of interoperable industry specifications it published in November 2011, designed to accelerate the adoption of a range of SIM-based NFC services. It states: “These specifications, which define common handset application programming interfaces (APIs) to support SIM-based NFC services, are designed to drive economies of scale by creating a common framework for implementation and product interoperability.” Significant documents already published by the GSMA include:

- TS.26 NFC Handset Requirements v5.0
- TS.27 NFC Handset Test Book v3.0
- NFC.04 NFC UICC Requirements Specification v4.0 (new release expected in 2014) NFC SP Applet Development Guideline v2.0 (new release expected in 2014)

Additionally, a Test Book for NFC UICC is expected to be released by the GSMA soon.

This chapter gives an introduction to the use of NFC in the payment ecosystem. With many different specifications and standards bodies now addressing mobile NFC technology, this chapter aims to provide an overview, and establish a common understanding, of mobile NFC technology architecture and the different actors involved in the mobile NFC payment ecosystem, including MNOs, service providers, handset and UICC manufacturers.

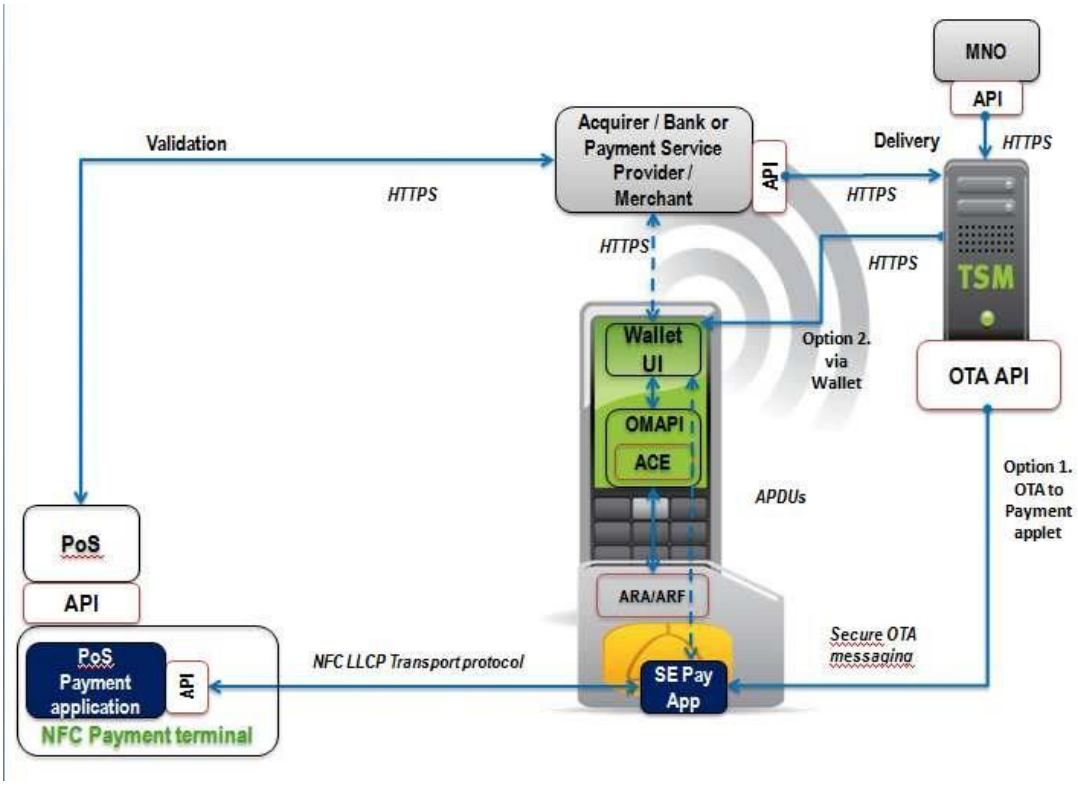

Figure 1: Mobile NFC payments service illustration

2.1 The NFC ecosystem

The NFC ecosystem is comprised of many components, however from the UICC's perspective (defined in this whitepaper) the three most significant are:

1. **The NFC handset**: The main purpose of the mobile phone is to provide mobile voice and data services. It additionally contains the NFC chip that supports contactless services.

Reference sources for handset support and interoperability with NFC UICC are:

a. SIMalliance NFC Secure Element Stepping Stones v1.0
b. GSMA NFC Handset APIs Requirement Specification v4.1

2. **Trusted Service Manager (TSM)**: The TSM securely distributes the service providers' services to the MNOs' customer-base and manages those services. The TSM's role is to provide a single point of contact for service providers to access their customer-base through the MNOs, and to manage the secure download and lifecycle of the NFC mobile payment application on behalf of the service provider.

The TSM acts as an interface between:

- A service provider and a MNO in the case of a UICC-based SE;
- A service provider and handset manufacturer in the case of an embedded SE (eSE);
- A service provider and another service provider in the case of smart microSD.

There are two categories of TSM: TSM-SP and TSM-MNO. Each has the relative interface for communication with service providers and MNOs.

Reference sources for TSM and secure over-the-air (OTA) messaging are:

a. SIMalliance NFC Secure Element Stepping Stones v1.0
b. GlobalPlatform System Messaging_Specification_for_Management of Mobile_NFC_Services v1.1.2

3. **Point of Sale/Service (PoS)**: The PoS can be equipped with a NFC payment terminal.

Reference sources for PoS are:

a. EMV Contactless Communication Protocol Specification v2.4

There are a number of actors involved in the mobile NFC payment ecosystem:

- **Acquirer:** A payment service provider that enables the merchant's transaction to be processed through an authorisation and clearing network.

- **Bank** (or payment service provider): The bank provides the mobile NFC payment service to the customer. It is responsible for provisioning the mobile NFC payment application to the UICC in the customer's mobile handset, and personalising the application with the customer's data.

- **Merchant:** This is the actor that accepts a mobile NFC payment scheme as payment for goods or services. The merchant has an agreement with an acquirer and is equipped with a NFC payment terminal.

- **MNO:** The mobile network operator.

Descriptions of other components that are fundamental to the mobile NFC payment environment include:

1. **Wallet User Interface (UI):** The mobile wallet is a software application that is loaded onto a mobile phone for the purpose of managing payments made via the handset. The application can also host and control a number of other applications (for example, transit and loyalty) in much the same way as a physical wallet may contain credit, debit and loyalty cards.

   Reference sources:
   a. EMV Contactless Mobile Payment - Application Activation User Interface v1.0
   b. GSMA NFC Core Wallet Requirements v2.0

2. **Open Mobile Application Programming Interface (OMAPI):** This API enables mobile applications to access different SEs in a mobile handset, such as UICCs or eSEs.

   Reference source:
   a. SIMalliance Open Mobile API Specification v2.05

3. **Access Rule Application (ARA) and Access Rule File (ARF):** For more information about access control and ARA/ARF please refer to chapter 6 of this paper**.**

4. **SE Pay App**: For more information about secure element payment applications please refer to chapter 7 of this paper.

5. **Access Control Enforcer (ACE):** This is a module that is integrated in to the OMAPI. It reads the access rule from the ARA-M according to the applications certificate and application identifier (AID) of the applet to be accessed when a communication channel is opened. The access policy is not stored in the ACE itself; all data is read from the SE, the ARA-M. Please refer to chapter 6 of this paper**.**

3. UICC Telecom Requirements

The UICC telecom functionality complies with a set of specifications mainly defined by ETSI, 3GPP and 3GPP2, that includes ETSI TS 102 223 (CAT) / 3GPP TS 31.111 (USAT), ETSI TS 102 613 (SWP), ETSI TS 102 622 (HCI), ETSI TS 102 241 (UICC API) /3GPP TS 31.130 (USIM API).

In the above specifications, specific contactless functionalities are described. SIMalliance recommends that these functionalities are compliant to at least version 9 of the related specification.

If the card is deployed in a long term evolution (LTE) network, it is recommended that LTE services are enabled using SIMalliance LTE UICC Profile v1.01. This will ensure a fast connection and reduced latency. Even if LTE connectivity is not an essential requirement for NFC services, NFC cards are usually mostly capable of supporting advanced LTE features.

Deploying UICCs with LTE profiles in a NFC ecosystem can future-proof the deployment, in case there should be a future requirement for LTE network activation. This allows more efficient remote OTA card operations due to faster LTE data transfer rates (low latency and faster download).

For more details please refer to the SIMalliance LTE UICC Profile v1.01.

ETSI has introduced specific mechanisms in the Card Application Toolkit (ETSI TS 102 223) and Card Toolkit API (ETSI TS 102 241) to enhance support for contactless applications.

These include:

- Contactless ACTIVATE[1)], (if class “l” is supported), is a card toolkit command allowing the UICC to request the terminal to activate a specified interface (for example the UICC-CLF interface).
- CONTACTLESS STATE CHANGED[2)] (if class “r” is supported), is a card toolkit command allowing the UICC to inform the terminal that the contactless functionality has been enabled or disabled.
- Contactless state request event (if class “r” is supported), is a card toolkit event allowing the terminal to inform the UICC whether the contactless functionality was activated or deactivated by the user.
- HCI connectivity event (if class “m” is supported), is a card toolkit event allowing the terminal to inform the UICC that an event occurred on the HCI transport layer.

Feature	***Required features***	***Optional***	***Evolution***
ACTIVATE proactive command	X		
CONTACTLESS STATE CHANGED proactive command		X	

This toolkit command can either be sent from the UICC's OS or from a Toolkit-Applet (e.g. CRS-Applet)

Contactless state request event		X	
HCI connectivity event		X	
Terminal capability command	X		
LTE (as per LTE profiles by SIMalliance)		X	

4. UICC NFC Requirements

The NFC interface in the UICC requires the support of the SWP/HCI protocols according to ETSI TS 102 613, and TS 102 622. For Card Emulation Mode the GlobalPlatform Card Contactless Services Card Specification v2.2 Amendment C v1.1 specifies how to set the contactless parameters and it defines a contactless API for applets and the NFC-Registry on the SE. The following sections describe the NFC related features of the SE.

4.1 Single Wire Protocol (SWP)

The SWP, as defined in ETSI 102 613, is the physical link for the NFC-communication between a Contactless Frontend (CLF) controller and the SE (please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, section 2).

The Sliding Window Size will be acknowledged when establishing a SWP session and defines the available I/O buffers of an SWP-endpoint.

In “low power mode”, as defined in ETSI TS 102 613, UICC power is limited to 5mA compared to 10mA in “full power mode”, therefore the UICC has to limit its performance and transactions may take longer. The full power mode should be used when the device is running under normal operational conditions. SIMalliance also recommends using this mode as the preferred operation type when the device is powered off or the battery is not able to sustain normal operation (please refer to SIMalliance UICC Device Implementation Guidelines v1.1).

4.2 Host Controller Interface (HCI)

The HCI protocol is defined in ETSI TS 102 622 and is used to establish logical links between the Host Controller (CLF) and the Hosts (e.g. SE), that are connected by a physical SWP line (please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, section 2.4).

The HCI “Transaction Event” (ETSI 102 622) allows the SE to trigger an application running on the mobile and forward proprietary (application specific) data to it. A payment applet may send a HCI Transaction Event via the SWP interface and as a result the mobile wallet application on the phone is triggered for further user interaction.

With the HCI “Connectivity Event” (ETSI 102 622) a UICC may use the SWP interface to indicate to the modem of the mobile that it should send a CAT Envelope (Connectivity Event) back to the UICC on the ISO7816-4 interface. This mechanism is mainly used when a contactless transaction should be directly followed by an interaction from the Toolkit Interface (e.g. DisplayText, MenuSelection, etc). (Please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, sections 2.4.1.5.1, and 3.3.1.3.)

The HCI API (ETSI 102 705) allows the SE to retrieve information from the CLF e.g. the Full/Low Power Mode or the supported HCI Services of the CLF.

4.3 GlobalPlatform Amendment C

GlobalPlatform specifies an API in GlobalPlatform Card Contactless Services Card Specification v2.2 Amendment C v1. that can be used by Java Applets to implement NFC-specific business logic. This API can be used by an optional CRS-Applet (please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, section 3.1.3.2).

The CRS Applet is needed for most payment use cases in order to activate/deactivate the payment instances, collect information from the GP-Registry and enable the global Communication Interface for Card Emulation Mode (please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, section 3.1.3.2).

The OPEN (= GlobalPlatform Environment) is part of the SE Operating System (OS) and can store optional default NFC parameter values during SE personalisation. Post-loaded applications do not have to indicate NFC parameters during installation which avoids parameter conflicts in the field. Please see GlobalPlatform UICC Configuration, Contactless Extension, section 3, for recommended default parameters.

The optional Cumulative Granted Memory (CGM) feature (GlobalPlatform Card Contactless Services Card Specification v2.2 Amendment C v1) - also called "Memory Quota" - allows the exact amount of memory granted to a Security Domain to be specified to its associated applications and its entire sub-hierarchy. This mechanism is used in some specific NFC ecosystems (please refer to SIMalliance NFC Secure Element Stepping Stones v.1.0, section 4.6.3].

The Token Blacklist is an optional extension to the Delegated Management mechanism and allows remote entities to add DM-Tokens to prevent reuse. A Security Domain with Token-Verification privilege will reject any command list which uses blacklisted tokens. (GlobalPlatform Card Contactless Services Card Specification v2.2 Amendment C v1, section 12.)

Feature		***Required***	***Optional***	***Evolution***
SWP		X		
	Sliding Window Size 3	X		
	Sliding Window Size 4			X
	Low power mode	X		
HCI		X		
	HCI event Transaction	X		
	HCI event Connectivity	X		
	HCI API (Device information)	X		
GlobalPlatform Amendment C		X		
	Support for GP CRS	X		
	GP OPEN parameters	X		
	CGM / Quota mechanism		X	
	Token Blacklist			X

5. UICC OTA Management Requirements

There are several successful mechanisms in the field which allow UICC content to be managed by a remote platform. SIMalliance recommends the following:

- OTA over HTTPs
- CAT TP
- OTA through a Proxy Agent on the Mobile Phone

The UICC may support multiple remote management mechanisms but at least one of the three mechanisms listed above has to be supported to provide OTA management functionalities.

5.1 OTA over HTTPs

The card administration is performed using HTTP as the end-to-end transport protocol. The Transport Layer Security (TLS) layer provides security to the remote APDU which is embedded in HTTP messages as illustrated below.

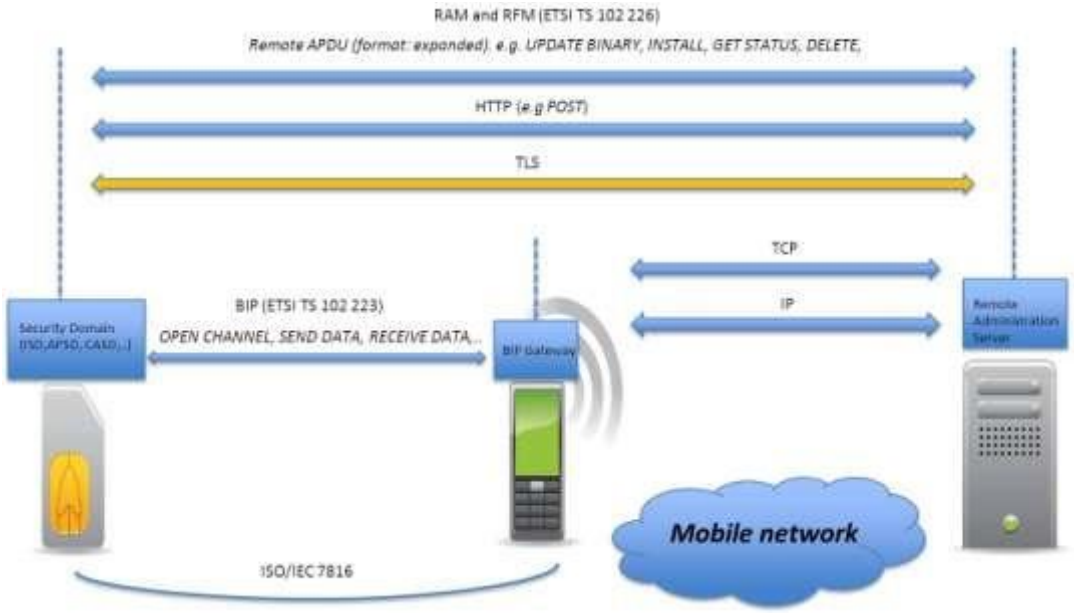

Figure 2: TLS layer provides security to the remote APDU

OTA over HTTPs features:

Feature		*Required*	*Optional*	*Evolution*
PUSH mechanism through SMS		X		

	Support of Administration Session triggering parameters (GlobalPlatform Amendment B)	X		

Remote APDU (ETSI TS 102 226 and 3GPP 31.116)		X		
	Compact data format	X		
	Expanded Format with indefinite length support (streaming)	X		
Remote File Management commands		X		
Remote Application Management commands (GlobalPlatform Card Specification 2.2.1)		X		
	GP Security Domain configured to be accessible via OTA	X		
BIP (ETSI TS 102 223)		X		
RAM/RFM over HTTPs support (GlobalPlatform Amendment B)		X		
	Support of HTTP as transport protocol	X		
	Support of PSK-TLS security layer (SCP 81)	X		
	PSK-TLS v1.0	X		
	PSK-TLS v1.1		X	
	PSK-TLS v1.2			X
	Retry policy for the SD	X		
	Loading of PSK TLS keys through PUT KEY command	X		

	Loading of PSK TLS keys through STORE DATA command		X	
	GlobalPlatform API for Administration Session Triggering	X		
	Java Card Connection Oriented Service API for RAM/RFM over HTTPs (ETSI TS 102 267)			X

5.2 OTA over CAT_TP

The card administration is performed using CAT_TP as the end-to-end transport protocol as follows:

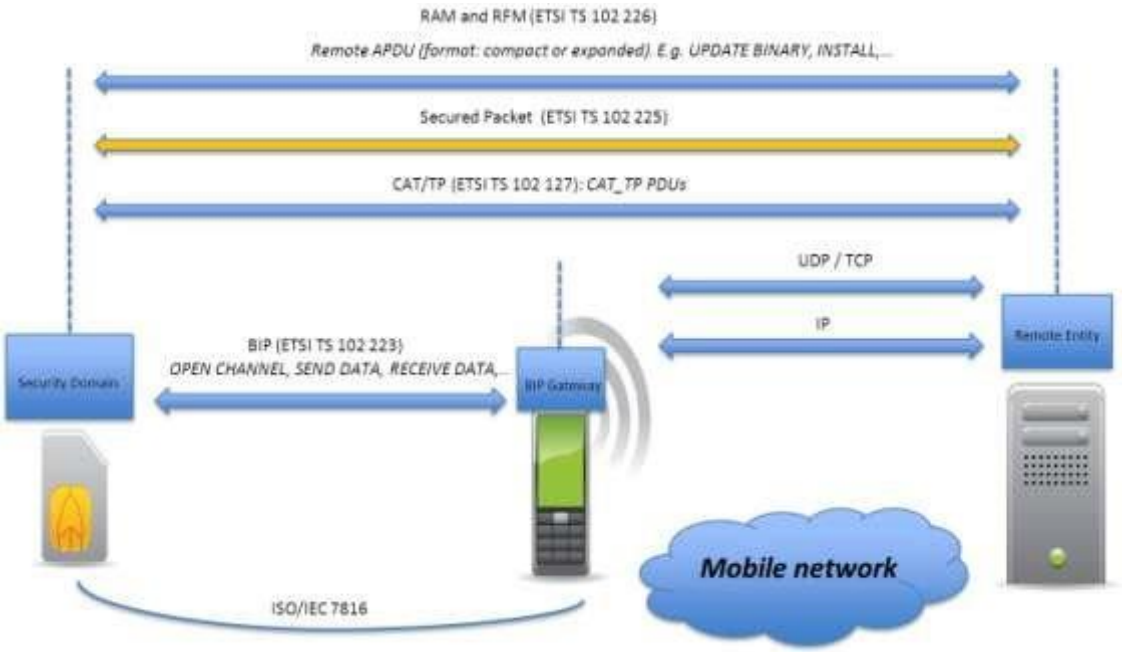

Figure 3: Card administration performed using CAT_TP as the end-to-end transport protocol

OTA over CAT_TP features:

Feature		*Required*	*Optional*	*Evolution*
PUSH mechanism through SMS		X		
	ENVELOPE SMS PP Data Download with support of PUSH command for CAT_TP link establishment (ETSI TS 102 226)	X		

Remote APDU (ETSI TS 102 226 and 3GPP 31.116)		X		
	Compact data format	X		
	Expanded data		X	
Remote Application Management commands (GlobalPlatform		X		
Card Specification 2.2.1)				
	GlobalPlatform Security Domain configured to be invoked by RAM	X		
Secured Packet (ETSI TS 102 225 and 3GPP 31.115)		X		
BIP (ETSI TS 102 223)		X		
RAM/RFM over CAT-TP support		X		
	CAT-TP Client mode	X		
	CAT-TP Server mode			X
	Java Card API for CAT-TP (ETSI TS 102 267)			X

5.3 OTA administration via a Proxy Agent (Admin Agent)

GlobalPlatform Secure Element Remote Application Management v1.0 provides another administration OTA protocol for UICCs, based on an Admin Agent application within the mobile phone. The Admin Agent (HTTP client) manages the HTTP communication with a remote/administration server (HTTP Server) and forwards the OTA administration commands to the UICC. The communication between Admin Agent and UICC is out of the scope of this paper.

Feature	***Required***	***Optional***	***Evolution***

RAM/RFM through Admin Agent (GlobalPlatform Secure Element Remote Application Management V1.0)			X	

5.4 PUSH mechanism through SMS

This feature allows the remote OTA server to start an administration session with the UICC (either for OTA over CAT_TP and OTA over HTTP). A SMS message is sent to wake up the card. All the parameters needed by the card to establish the OTA session can be provided by this message. In the case of an OTA over CAT_TP session, such parameters are within the PUSH command for establishing the CAT_TP link (ETSI TS 102 226). In the case of an OTA over HTTPs session, Administration Session triggering parameters are used (GlobalPlatform Card Remote Application Management over HTTP Card Specification v2.2 – Amendment B v1.1.2).

5.5 Remote APDU

Remote application and file management is performed by sending remote APDUs indicated in ETSI TS 102 226. GlobalPlatform Card Specification v2.2.1 describes all the commands needed by the OTA server to perform application management (e.g. installation, deletion, etc.) on the card. For RAM the UICC should have a Security Domain with card content management capability (e.g. ISD or SD with AM or DM privilege).

5.6 BIP

Bearer Independent Protocol (BIP) (ETSI TS 102 223) is required either for OTA over CAT_TP or OTA over HTTPs connections. When the UICC opens a BIP channel (OPEN CHANNEL command), the device establishes a TCP/IP connection with the OTA server. The BIP channel allows all data exchange sent by the OTA platform to be submitted to the UICC and all data sent from the UICC is forwarded to the OTA server.

5.7 Secure Packets

ETSI TS 102 225 provides end-to-end security between the OTA server and the UICC for remote APDUs exchange. This security layer is used for remote administration over CAT_TP.

6. UICC Access Control Requirements

The OMAPI implementations on rich OS mobile handsets make it possible for applications on the handset to access the applications on the UICC. To control access to the UICC applications there is a gatekeeper mechanism between the rich OS and UICC applications; this is called access control. The access control stack consists of two parts: the access control enforcer which resides on the mobile handset OS (a thin layer in the OMAPI) and the access control rules stored on the UICC either in an applet (ARA), or in a PKCS #15 file structure (ARF), or both.

6.1 Workflow – simplified

When a device application wants to access a UICC application it calls an OMAPI function to open a logical channel (1). Upon receiving the openLogicalChannel command, the OMAPI implementation triggers the access control mechanism. The Access Control Enforcer analyses the access rules obtained from the UICC (2) and allows access to the UICC application, but only if the related rule allows it (3). If access is denied, the OMAPI will alert accordingly.

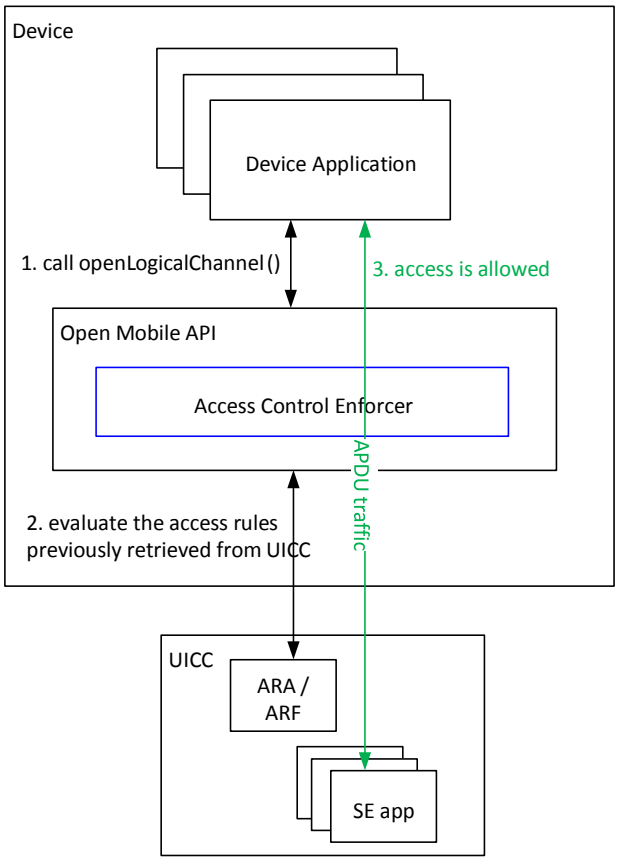

Figure 4: Simplified workflow of access control mechanism

6.2 ARF - ARA migration and compatibility

Although UICCs today contain mostly only ARF (PKCS #15), the migration to ARA is nonetheless expected in the future. To ensure compatibility between UICCs, GlobalPlatform requires that the Access Control Enforcer must be able to support both ARA and ARF.

There are a number of possible scenarios for migration from ARF to ARA. The GlobalPlatform Secure Element Access Control Specification v1.0 details some scenarios in the annex, but there is no specific recommended solution. The most suitable solution should be agreed between the MNO, TSM and the card issuer.

Feature	Required	Optional	Evolutions
PKCS#15	X		
ARA-M	X		
ARA-C		X	

7. UICC Requirements for Payment Applications and Certifications

A mobile NFC payment UICC requires the deployment of one or more Payment Network Organisation (PNO) applications, each of them typically representing a virtual credit card accessible via the contactless interface.

To allow the deployment of payment applications, PNOs require card products to be certified according to specific programmes. PNOs have different programmes, but in general they share the same principles which are:

- A chip security certification is required to demonstrate the robustness of the chip to sophisticated security attacks. The chip security certification is carried out by EMVCo and results in an IC Certificate Number (ICCN). The ICCN can be renewed several times up to a maximum of six years.
- A platform security certification is required to demonstrate the robustness of the card OS to sophisticated security attacks. The platform security certification is carried out by EMVCo and results in a Platform Certificate Number (PCN). The PCN can be renewed several times up to a maximum of six years. The card OS is developed for a specific chip, so to achieve the PCN a chip with a valid ICCN is required.
- A platform functional certification is required, that tests the adherence of the card OS to the GlobalPlatform Specifications, in particular to the UICC Configuration. The GlobalPlatform certification is carried out by GlobalPlatform and results in a Letter of Qualification (LOQ).

The three certifications (ICCN, PCN, LOQ) are the starting point for the composite certification adopted by several PNOs. While each PNO has its own dedicated certification, composite certification means that basic certification tests carried out successfully on behalf of one PNO do not need to be repeated when applying for certification with another. Also the single PNO certifications have renewal and expiration schemes; certifications can typically be renewed for up to six years, however the application for renewal usually has to be made before the PCN and/or ICCN expires.

It is important to note, that certifications apply to a specific combination of OS and chip. Any variation to the OS or to the chip typically results in a delta certification where the security and functional implications of the variation are analysed by the proper entity. As a consequence, the certification process should be executed only once the product is considered stable. For a more detailed description of the certification process, please see SIMalliance Secure Element Stepping Stones v1.0.

Feature		Required	Optional	Evolution
EMVCo ICCN certification		X*		
EMVCo PCN certification		X*		
GlobalPlatform certification		X		
Payment network organisation certification		X**		
	Mastercard MPP certification		X	
	American Express ExpressPay certification		X	

	Visa VMPA certification		X	
	… (Other payment organisations)			

* The EMVCo certifications are mandated in most mobile NFC payment deployments, yet there are several domestic payment schemes that do not mandate such certifications. A product which only supports those domestic payment schemes has no need for EMVCo certification. Global payment schemes (Visa, Mastercard, American Express, etc.) usually do mandate EMVCo certification.

**The only certifications necessary are those required by the project's PNOs. At minimum, one certification is required, but typically more are necessary.

8. UICC Memory Requirements

The ability to manage UICCs via OTA enables more applications to be dynamically installed on the card and for new features to be activated when the card is in the field.

For example, if a user subscribes to a new credit card, which is to be deployed on the UICC, two actions will typically result on the card:

- A Security Domain for the card issuer (e.g. a bank) will be created and personalised.
- A new instance of the credit card application (e.g. a new VISA VMPA instance) will be created and personalised.

In this scenario, memory and resources are needed on the card to store the personalisation information, the Security Domain keys, etc. There are two types of memory on a UICC:

- A ***Non-Volatile Memory*****:** A memory that does not lose the stored value after a card reset, typically based on Flash or EEPROM technology.
- A ***Volatile Memory*****:** A memory that loses the stored value after a card reset, typically based on RAM technology.

Applications require both kinds of resources to be installed, in addition to an OS. The resources required by an application depend not only on the application itself, but also on the card OS, so a generic requirement, such as “the UICC shall have 200 kb of NVM memory available for the UICC issuer” could result in a different number of applications depending on the OS.

As a result, it is advisable to express requirements in terms of the card issuer’s specific needs instead of in terms of resources.

Feature	Required	Optional	Evolution
The UICC should have enough resources to install a minimum number of security domains post-issuance	X (minimum number is up to the MNO)		
The UICC should have enough resources to install a minimum number of payment applications post-issuance	X (minimum number is up to the MNO)		

9. Implications of Other NFC Applications and Interoperability

NFC UICCs usually host several types of applications in addition to PNO applications and Security Domains. For example, a NFC UICC could be required to support transport applications such as MIFARE.

In general, these applications do not interfere with PNO applications; EMVCo certification verifies that the mechanisms which isolate the PNO applications from other applications are robust and correctly implemented.

The coexistence of PNO and non-PNO applications, however, could impact the UICC; third party applications may present new requirements for the UICC OS, such as new protocols or improved UICC performance, resulting in the need to update the OS accordingly. For example, MIFARE classic requires the support of a specific SWP layer (the Contactless Tunneling, CLT) plus the management of MIFARE operations, while contactless applications can be demanding in terms of performance. Even if there is no direct link between the PNO and non-PNO applications, an improvement in performance of the UICC OS typically results in a modification to the OS that affects the security certifications.

Finally, in order not to compromise the security architecture, every EMVCo certificated platform results in specific application guidelines which indicate the application behaviours considered as “malicious”, and subsequent security countermeasures which have to be taken into account.

Such guidelines are usually based on:

- GlobalPlatform Card Composition Model Security Guidelines for Basic Applications v1.0
- GSMA NFC SP Applet Development Guidelines V2

As a consequence, SIMalliance recommends that an OS should only be considered stable and ready for certification after the required applications have been integrated.

Feature	Required	Optional	Evolution
The UICC should support specific non-payment applications	X (the list is up to the MNO)		