Table of Contents

1 Introduction 4
  1.1 Background 4
  1.2 Overview 4
  1.3 Scope 4
  1.4 Definition of Terms 4
  1.5 Document Cross-References 5
  1.6 Conventions 5

2 Process Implementation reference 6
  2.1 Representation of the exchanges 6
  2.2 High level Sequence Diagram – Service Deployment 7
  2.3 Eligibility and scoring sub-processes 8
  2.3.1 Sub-process A – MNO eligibility 8
  2.3.2 Sub-process B – SP compatibility 9
  2.3.3 Sub-process C – SP scoring 9
  2.4 Service discovery and inquiry processes 9
  2.4.1 Process 1 – Online service discovery 9
  2.4.2 Process 2 – Inquiry to the Service Provider 9
  2.4.3 Process 3 – Inquiry to the Mobile Network Operator 9
  2.5 Subscription processes 9
  2.5.1 Process 4 – Subscription to a Mobile NFC Service 9
  2.6 Installation processes 10
  2.6.1 Process 5 – Mobile NFC UICC application installation 10
  2.6.2 Process 5 Update – Mobile NFC UICC application update 13
  2.6.3 Process 6 – Service Provider MMI installation / Update 15
  2.6.4 Process 7 – MMI and UICC application binding 17
  2.7 Life cycle processes 18
  2.7.1 Process 8 – Change UICC 18
  2.7.2 Process 9 – Change mobile phone number 19
  2.7.3 Process 10 – Change mobile handset 20
  2.7.4 Process 11 – Lost or stolen Mobile Equipment, end user contacts MNO 21
  2.7.5 Process 12 – Lost or stolen Mobile Equipment, end user contacts Service Provider 23
  2.7.6 Process 13 – Recover Mobile Equipment after a loss 24
  2.7.7 Process 14 – Get new Mobile Equipment after a loss or theft 25
  2.7.8 Process 15 – End User requests temporary mobile service suspension 27
  2.7.9 Process 16 - Change in contract ownership 28
  2.7.10 Process 17 – End user swaps Mobile Network Operator 28
  2.8 Termination processes 29
  2.8.1 Process 18 – Termination of Mobile subscription or NFC option by end user 29
  2.8.2 Process 19 – Mobile service termination by Mobile Network Operator 30
  2.8.3 Process 20 – Mobile NFC service termination 31

3 GP Messaging functions use and restrictions matrix 33
  3.1 Convention 33
  3.2 Eligibility check 33
  3.3 Service Management life cycle 33
  3.4 Mobile Subscription Life Cycle 34
  3.5 Secure Element Life Cycle 34
  3.6 CCCM certificate management 35
  3.7 Secure Element Management 35
  3.7.1 SE Card Content Management 35
  3.7.2 Delegated Management 36
  3.7.3 Script Sending 36
3.7.4 SE Audit 37
3.7.5 SCWS Service Portal 37
3.7.6 Device Application Management 37

**Document Management** 38
  - Document History 38
  - Other Information 38
1 Introduction

1.1 Background

This document is concerned with the matter of interoperability between Trusted Service Manager (TSM) and Mobile Network Operator (MNO) platforms in order to facilitate consistent deployment and management of end users’ NFC services.

The document builds upon the interaction processes as defined in the Association Française du Sans Contact Mobile (AFSCM) Interface Specification document [AIS], with an aim to provide a foundation which will allow for safer deployment between the different interaction protocols available today.

In particular, this document focuses on Global Platform (GP) protocols to deploy those processes.

The goal of this document is to set out a framework for MNOs who:

a) Have deployed AFSCM protocols, but wish to migrate to GP protocols and have a secure way in doing so; or

b) Do not deploy AFSCM protocols, but seek a convenient process context in which to manage their GP deployment, reaching full interoperability with GP protocols.

1.2 Overview

This document sets out requirements for the implementation of AFSCM processes and proposes an alternative implementation of AFSCM Processes defined in [AIS] using GP protocols in [GPSM].

1.3 Scope

The objective of this paper is to define the implementation of AFSCM business processes using GP Messaging Specification and to facilitate the transition from AFSCM interfaces to GP ones.

1.4 Definition of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFSCM</td>
<td>Association Française du Sans Contact Mobile</td>
</tr>
<tr>
<td>AID</td>
<td>Application (or Applet) Identifier</td>
</tr>
<tr>
<td>Device</td>
<td>In the context of this specification, the Device term is used to represent any electronic equipment into which a NFC Secure Element can be plugged, and that provides a capability for a server to reach the SE through an Over The Air (OTA) or Over The Internet (OTI) link. A mobile phone is a good example of such device.</td>
</tr>
<tr>
<td>DM</td>
<td>Delegated Management (SD privilege in GP)</td>
</tr>
<tr>
<td>GP</td>
<td>Global Platform</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile equipment defines the pair Device + SE</td>
</tr>
<tr>
<td>MIDP</td>
<td>Mobile Information Device Profile</td>
</tr>
<tr>
<td>MMI</td>
<td>Man-Machine Interface (or user interface). In this specification, MMI only refers to mobile phone MMI.</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator. A MNO provides the technical capability to access the mobile environment using an Over The Air (OTA) communication channel. The MNO is also the UICC Provider. MNO provides a UICC OTA Management System, which is also called the OTA Platform.</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>SD</td>
<td>Security Domain</td>
</tr>
</tbody>
</table>
1.5 Document Cross-References

<table>
<thead>
<tr>
<th>Ref</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>[GPCS]</td>
<td>GlobalPlatform Card Specification v2.2.1</td>
</tr>
<tr>
<td>[GPUC]</td>
<td>UICC configuration 1.0.1</td>
</tr>
<tr>
<td>[AIS]</td>
<td>110902 - AFSCM TECH - LIVBL - Interface Specification - V2.1.doc</td>
</tr>
<tr>
<td>[AIG]</td>
<td>110902 - AFSCM TECH - LIVBL - Interconnection Guidelines - v2.0.1.doc</td>
</tr>
</tbody>
</table>

1.6 Conventions

Throughout this document, normative requirements are highlighted by use of capitalized key words as described below.

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as follows:

- **SHALL** - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is a mandatory requirement of the specification.
- **SHALL NOT** - This phrase means that the definition is a mandatory prohibition of the specification.
- **SHOULD** - This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** - This phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- **MAY** - This word mean that an item is truly optional. One supplier may choose to include the item because a particular marketplace requires it or because the supplier feels that it enhances the product while another supplier may omit the same item.
2 Process Implementation Reference

This chapter presents the reference implementation, between the IT systems of the TSM and the MNO. A TSM may be managed and hosted directly by the Service Provider (SP) or by a trusted SP Partner. This implementation is based on the process definition in [AIS] §2

2.1 Representation of the Exchanges

To simplify the representation of the exchanges in the sequence diagrams of this section, acknowledgments and exceptions will not be explicitly represented in the diagrams.

The legend used in the diagrams is presented below:
2.2 High level Sequence Diagram – Service Deployment

This high level sequence diagram shows the 2 ways to sequence subscription and installation steps (full service deployment). Service Deployment starting and ending are notified with `HandleStart/EndServiceStateChangeNotification`. All sub processes and processes are specified in the following paragraphs.

**Sequence diagram**

![Sequence diagram](image)

**Description**

This deployment sequence diagram corresponds to the use cases 1 and 3 which are defined in [AIS] §2.2. A Mobile NFC service is considered completely installed, and is indeed fully operational for the end user, once the UICC application(s) AND the MMI(s) are installed. The Man-Machine Interface (MMI) installation (Process 6) MAY also occur parallel to the UICC application installation (Process 5) if supported by the MNO.
**Description**

This deployment sequence diagram corresponds to the use case 2 which is defined in [AIS] §2.2. As the MNO is not involved in the MMI installation process (in this mode), the service deployment starts after. The service deployment will be directly triggered from inside the MMI. This deployment mode is particularly suitable when the MMI is downloaded through an independent store.

### 2.3 Eligibility and Scoring Sub-Processes

#### 2.3.1 Sub-Process A – MNO eligibility

**Sequence diagram**

Figure 4: Sequence diagram of Sub-process A – MNO eligibility
**Description**

This function requests the eligibility of the Mobile Subscription and Mobile Equipment (ME). It **SHALL** check whether the commercial contract allows access to NFC services and whether the ME is setup to enable NFC services. MNOs **MAY** also check if there is available memory space on the UICC.

### 2.3.2 Sub-Process B – SP Compatibility

**Sequence diagram**

![Sequence Diagram](image)

**Figure 5:** Sequence diagram of Sub-process B – SP compatibility

**Description**

`GetSECapabilityProfileId` requests the identifier of a SE profile.

`GetDeviceCapabilityProfileId` requests the identifier of a device profile that gives information about the device currently associated to a particular Mobile Subscription. This information is used to check the service compatibility with the end user’s ME.

### 2.3.3 Sub-process C – SP scoring

This process does not require any exchange between the MNO and the TSM.

### 2.4 Service Discovery and Inquiry Processes

#### 2.4.1 Process 1 – Online Service Discovery

This process does not require any exchange between the MNO and the TSM.

#### 2.4.2 Process 2 – Inquiry to the Service Provider

This process does not require any exchange between the MNO and the TSM.

#### 2.4.3 Process 3 – Inquiry to the Mobile Network Operator

This process does not require any exchange between the MNO and the TSM.

### 2.5 Subscription Processes

#### 2.5.1 Process 4 – Subscription to a Mobile NFC Service

This process does not require any further exchange between the MNO and the SP other than those described in **Sub-Process A – MNO eligibility**, **Sub-Process B – SP Compatibility** and **Sub-process C – SP scoring**.
2.6 Installation Processes

2.6.1 Process 5 – Mobile NFC UICC Application Installation

The installation process is a succession of several requests on the TSM/ Mobile Network Operator interface.

The installation in itself can be performed in the two modes, simple Security Domain (SD) mode or delegated management mode; but the first step, Supplementary Security Domain (SSD) creation or assignation, is the same, regardless of the mode that is used.

![Sequence diagram of Process 5 – Mobile NFC UICC application installation](image)

**Figure 6: Sequence diagram of Process 5 – Mobile NFC UICC application installation**

2.6.1.1 SSD creation/assignation sub-process

If the SP has no SSD assigned on the UICC of the end user, the first step of the UICC application installation process is the SSD creation/assignation. The TSM must use the \textit{SECommandsGenerationAndRemoteExecution} request to have a SSD created and assigned. \textit{SECommandsGenerationAndRemoteExecution} which is the GP function for Over The Air (OTA) command generation and execution shall be requested with two SE Commands at least:

- \textit{InstantiateApplicationCommand}
- \textit{CreateFirstSSDKeysetCommand}
- \textit{ExtraditeCommand} if there is hierarchy of SDs to manage.

If the SSD is pre created (SSD assignation), \textit{SECommandsGenerationAndRemoteExecution} SHALL be also requested with same SE Commands. Keyset, Application Identifier (AID) and Toolkit Application Reference (TAR) of the allocated SSD SHALL be returned as output data. A warning can be raised by the MNO as the SSD is already created.
Depending on key data provisioning mode (if final keys are not directly set with CCM scenario 2B mode) and once the SSD is created and assigned, the TSM SHOULD send GP commands to replace the temporary SSD key set with its own key set.

**Sequence diagram**

![Sequence diagram of Sub-Process 5.1 – SSD Creation](image)

2.6.1.2 **SM installation sub-processes**

For the actual UICC application installation, the TSM uses the `SECommandsGenerationAndRemoteExecution` request to ask the MNO to perform the various installation steps.

- Depending on the state of the UICC, the TSM accordingly asks the MNO to perform the loading (`LoadELFCommand`), instantiation (`InstantiateApplicationCommand`) and extradition (`ExtraditeCommand`), registry update (`ApplicationRegistryUpdateCommand`) and activation (`MakeSelectableApplicationCommand`).

The SP or TSM is fully responsible for the personalization step of the UICC application. It could be done OTA if the TSM has this capability or using `BeginConversation`, `SendScript` and `EndConversation` functions.

Depending on the number of steps to perform and the sequencing of the activation and personalization steps, the TSM SHOULD use preferentially grouped commands of the `SECommandsGenerationAndRemoteExecution` request to optimize OTA exchanges.
**Sequence diagrams in simple SD mode**

**Figure 8:** Sequence diagram of Sub Process 5.2.1 – Installation of UICC application in Simple SD mode using grouped requests (activation then personalization)

**Figure 9:** Sequence diagram of Sub Process 5.2.2 – Installation of UICC application in Simple SD mode (personalization then activation)

### 2.6.1.3 DM installation sub-process

In the Delegated Management mode, the TSM is “allowed” by the MNO to perform all the UICC application installation steps.

To be authorized, the TSM uses the `generateDMToken` request to request authorization tokens for each step to perform among package loading, application installation, application extradition, application registry updating and application activation (depending on the state of the UICC).
Once it has the necessary tokens, the TSM sends OTA the GlobalPlatform Card commands [GPCS] to perform these steps.

Each action performed by the TSM must be notified to the MNO using the *verifyDMReceipt* function, when the installation is complete.

**Sequence diagram in delegated management mode**

![Sequence diagram](image)

**Figure 10:** Sequence diagram of Sub Process 5.3 - Installation of UICC application in Delegated Management mode

### 2.6.2 Process 5 Update – Mobile NFC UICC Application Update

The steps of this process differ if the TSM uses the Simple SD mode or the Delegated Management mode.
**Sequence diagram**

![Sequence diagram of Process 5 – UICC application update](image)

**Figure 11:** Sequence diagram of Process 5 – UICC application update

**Using the Simple SD mode**

If the end user’s ME is not compatible with the new version of the UICC application then update SHALL be stopped.

In simple SD mode, TSM uses the `SECommandsGenerationAndRemoteExecution` request to ask the MNO for the deletion of the service (`DeleteCommand`) on the UICC and the `SECommandsGenerationAndRemoteExecution` request for the installation (`LoadELFCommand`, `InstantiateApplicationCommand`, `ExtraditeCommand`, `ApplicationRegistryUpdateCommand`, `MakeSelectableApplicationCommand`) of the new version of the UICC application (as seen in section 2.6.1 Process 5 – Mobile NFC UICC Application Installation).

Using the **Sub-Process A – MNO eligibility** after the former service deletion, the TSM can ensure (if memory space is checked by MNO at eligibility) that there is enough memory space for the new UICC application.
**Using the Delegated Management mode**

The TSM starts this process with the **Sub-Process B – SP Compatibility** as in simple SD mode.

In delegated management mode, the TSM uses the `generateDMToken` request to be authorized, and sends OTA the GlobalPlatform Card commands `[GPCS]` in order to delete the former UICC application instance and package and install the new ones. Then, the TSM uses the `verifyDMReceipt` notification to inform the MNO with the token receipt.

Using the **Sub-Process A – MNO eligibility** after the former service deletion, the TSM can ensure (if memory space is checked by MNO at eligibility) that there is enough memory space for the new UICC application.

### 2.6.3 Process 6 – Service Provider MMI installation / Update

![Sequence diagram of Process 6 – MMI installation](image)

**Figure 12:** Sequence diagram of Process 6 – MMI installation
Figure 13: Sequence diagram of Process 6 – MMI update

This process is divided in 3 cases:

- **Case 1**: Upon the TSM’s request, the MNO launches the MMI installation or update.
  - Option i: there is a local mechanism to manage the MMI download on the phone
  - Option ii: the MNO uses a SMS to redirect the end user to the MMI download
- **Case 2**: The TSM launches the MMI installation or update (without requesting the MNO)
- **Case 3**: The MMI installation is done through an independent application store

In cases 1 and 2, the servers hosting the MMI are the SP or TSM’s responsibility. In case 3, they are the application store provider’s responsibility.

If the TSM needs to install n MMIs for the same service, it SHALL request `LoadDeviceApplication` n times with `Device Application Identifier` parameter.

The result of full deployment using the `HandleStart/EndServiceStateChangeNotification` notification is represented in processes which refer to process 6. See [High level Sequence Diagram – Service Deployment](#) for instance.

**Case 1 option i:**
The TSM uses the `loadDeviceApplication` request to ask the MNO to launch the MMI installation.

In this case, the MNO manages the entire installation and informs the TSM once the MMI is actually loaded in the mobile handset using `loadDeviceApplicationResponse`.

In case of connection interruption during the MMI loading, the MNO manages the retries.
Case 1 option ii
The TSM uses the `loadDeviceApplication` request to ask the MNO to launch the MMI installation, and the MNO sends the `loadDeviceApplicationResponse` once the Wireless Application Protocol (WAP) push or text SMS is sent to the mobile handset of the end user. In case of connection interruption during the MMI loading, the TSM manages the retries.

Case 2 and 3
In case 2 and 3, the end user or the TSM manages the MMI installation. There is no requirement for interaction with the MNO.

Requirement on the TSM (or SP) Information System
The MMI is specific for each mobile handset. Therefore the SP or TSM on the SP’s behalf SHALL manage a database with all the MMIs for each available NFC mobile handset. During the MMI installation process in cases 1 and 2, the TSM or the MNO may retrieve the type of mobile handset in order to identify the type of mobile handset and select the appropriate MMI to be downloaded.

MMI update
`HandleStart/EndServiceStateChangeNotification` with `Service Upgrade` parameter is used specifically for this case.

2.6.4 Process 7 – MMI and UICC Application Binding

Sequence diagram

![Sequence diagram of Process 7 – MMI and UICC application binding](image)

**Description**
If the MNO uses MMI and UICC application binding, the TSM must use the `BindDeviceApplicationToSEApplication` request. It should then be used:
- After the installation process, always after Process 5 – Mobile NFC UICC Application Installation
- After the update process, always after Error! Reference source not found.
- Before the MMI update process, for instance if the new MMI is signed with a new certificate that requires an update of the bindings.
2.7 Life Cycle Processes
2.7.1 Process 8 – Change UICC

**Sequence diagram**

![Sequence diagram of Process 8 – Change UICC](image)

**Description**

The MNO SHALL inform the TSM that the end user has a new UICC using the `HandleSERenewalNotification` notification. The TSM will then have to go through the process of UICC application installation, and optionally through the MMI and UICC application binding process if needed (i.e. if the MNO requires binding). Eligibility and compatibility checks are thus required before launching the UICC application installation. Nevertheless a call to `GetSECapabilityProfileId` is not mandatory in Sub-process B as `HandleSERenewalNotification` already provides the required information on the new UICC.
2.7.2 Process 9 – Change Mobile Phone Number

**Sequence diagram**

![Sequence diagram of Process 9 – Change mobile phone number](image)

**Description**

The identifier used for mobile subscription is the MNO’s responsibility and dependent on local regulatory requirements. It can be the Mobile Station International Subscriber Directory Number (MSISDN) or an alternate technical identifier (alias or idtech).

When the MNO changes the end user’s mobile phone number, there are three possibilities:

1. The mobile subscription identifier required by the MNO is an MSISDN. The MNO SHALL notify the TSM with the new MSISDN using `HandleMobileSubscriptionIdentifierChangedNotification(oldMobileSubscriptionId, newMobileSubscriptionId)`.

2. The mobile subscription identifier is a technical identifier. Its generation is dependent on the MSISDN. The MNO SHALL notify the TSM with the new technical identifier using `HandleMobileSubscriptionIdentifierChangedNotification`. This notification SHALL be done per service (or per SP) if the technical identifier is also diversified per service.

3. The mobile subscription identifier is a technical identifier. Its generation is independent of the MSISDN. It is up to the MNO to generate and notify the TSM (`HandleMobileSubscriptionIdentifierChangedNotification`) with the same technical identifier.

The TSM has to change the mobile subscription identifier for this end user in its information system. The new mobile phone number may or may not be provided by the MNO, depending on the country.
### 2.7.3 Process 10 – Change Mobile Handset

**Sequence diagram**

![Sequence diagram of Process 10 – Change mobile handset](image)

**Description**

When a MNO detects that the end user has changed their mobile handset, the MNO SHOULD send a `HandleSEDeviceChangedNotification` notification to the TSM. The TSM will then have to go through the steps of the MMI application installation process, and optionally of the application binding if needed (for instance if the current binding application is intended for a Mobile Information Device Profile (MIDP) MMI and the MMI compliant with the new mobile handset is ANDROID).

Eligibility and compatibility checks are thus required before launching the MMI application installation. Nevertheless a call to `GetDeviceCapabilityProfileId` is not mandatory in Sub-process B as `HandleSEDeviceChangedNotification` already provides the required information on the new device.
2.7.4 Process 11 – Lost or Stolen Mobile Equipment, End User Contacts MNO

In case of ME lost or stolen, the MNO has two alternative sequence diagrams

**Sequence diagram 1: MNO suspends the line**

![Sequence Diagram 1: MNO suspends the line]

**Description**

When an end user reports a lost or stolen mobile handset, the MNO:

- Informs the TSM of the future line suspension for a loss or theft using `HandleMobileSubscriptionStatusChangeNotification(suspended, lost or theft, approximate date in future)`.

- Attempts to lock:
  - Either attempts to lock the service before line suspension. Service locking MAY be subject to approval by the SP at the provisioning stage;
  - Or attempts to lock the contactless interface of the UICC and notifies this action to the TSM;

- Informs the TSM of the line suspension when it is effectively suspended.

The TSM is responsible to apply its own security policy (blacklist) after the first notification and informs the MNO if an action has been taken (`HandleStart/EndServiceStateChangeNotification`).
**Description**

When an end user reports a lost or stolen mobile handset, the MNO:

- Informs the TSM of the immediate or future line restriction for a loss or theft using `handleMobileSubscriptionStatusChangeNotification`.
- Attempt to lock:
  - Either attempts to lock the service. Service locking MAY be subject to approval by the SP at the provisioning stage;
  - Or attempts to lock the contactless interface of the UICC and notifies this action to the TSM.

The TSM is responsible to apply its own security policy (blacklist) after the first notification and informs the MNO if an action has been taken (`HandleStart/EndServiceStateChangeNotification`).
2.7.5 Process 12 – Lost or Stolen Mobile Equipment, End User Contacts Service Provider

Sequence diagram

Figure 20: Sequence diagram of Process 12 – Lost or stolen mobile equipment, end user contacts SP

Description

When an end user reports a lost or stolen mobile handset, the TSM:

- Informs the MNO of the loss or theft using the `handlesstatuschangenotification` notification,
- Depending on the SP security policy, attempts to lock OTA service and, in case of failure, applies an IS lock on the service; all locks are communicated to the MNO using the `handlestart/endservicestatechangenotification`.

The MNO is responsible to trigger or not the process 11 (see 0) for other TSMs. For instance, the MNO may choose to wait for the end user confirmation before triggering process 11.
2.7.6 Process 13 – Recover mobile equipment after a loss

**Sequence diagram**

![Sequence diagram of Process 13 – Recover mobile equipment after a loss](image)

**Description**

The MNO informs the TSM using `HandleMobileSubscriptionStatusChangeNotification` when the line of the end user is restored after the recovery (following a loss or theft) of their mobile phone. Then depending on the lock mode:

- If the service was permanently locked, the MNO notifies TSM of SE availability using `handlestatuschangenotification` and then the TSM deletes and reinstalls the UICC.
application, but not the MMI. The redeployment is notified using `handlestart/endservicestatechangenvnotiﬁcation` with `SE applications Redeployment` parameter.

- If the service was simply locked OTA by the TSM, the MNO notifies the TSM of the SE availability using `handlesestatuschangenvnotiﬁcation`; then the TSM unlocks the service and informs the MNO using the `handlestart/endservicestatechangenvnotiﬁcation` with `Service Unlocking` parameter.
- If the UICC contactless interface was locked, the MNO SHALL unlock it before sending `handlesestatuschangenvnotiﬁcation`.

2.7.7 Process 14 – Get New Mobile Equipment after a Loss or Theft

*Sequence diagram*

![Sequence diagram of Process 14 – Get new mobile equipment after a loss or theft](image)

**Figure 22:** Sequence diagram of Process 14 – Get new mobile equipment after a loss or theft
**Description**

When the end user gets a new mobile handset (*HandleSEDeviceChangedNotification*) and UICC (*HandleSERenewalNotification*) after a loss or theft, the MNO reactivates the end user’s line. Thus, the MNO uses the *HandleMobileSubscriptionStatusChangeNotification* notifications to inform the TSM.

These notifications are sent independently and the TSM must use the *HandleMobileSubscriptionStatusChangeNotification* notification as a starting point to trigger the eligibility and compatibility checks and the service installation. Nevertheless calls to *GetDeviceCapabilityProfileId* and *GetSECapabilityProfileId* are not mandatory in Sub-process B as *HandleSEDeviceChangedNotification* and *HandleSERenewalNotification* already provides the required information on the new ME.

The MMI application installation also occur parallel to the UICC installation. If needed (the MNO requires binding) the TSM SHALL also bind its application.
2.7.8  Process 15 – End User Requests Temporary Mobile Service Suspension

Sequence diagram

![Sequence diagram of process 15 – Suspension of mobile service upon end user's request](image)

**Description**

The MNO uses `HandleMobileSubscriptionStatusChangeNotification` to inform the TSM of the line suspension and then, at a later stage, of its re-activation.

The TSM uses `HandleStart/EndServiceStateChangeNotification` to inform the MNO of the lock applied and, later on, unlock.
2.7.9 Process 16 - Change in Contract Ownership

*Sequence diagram*

![Sequence diagram of process 16 – Change in contract ownership](image)

**Description**

The MNO uses the `HandleMobileSubscriptionStatusChangeNotification` to inform the TSM of the change in the end user contract ownership. This process can be implemented as a termination. If the TSM wishes to implement this process, the main impacts are in its Information System.

2.7.10 Process 17 – End User Swaps Mobile Network Operator

*Restrictions specific to this version*

Automated inter-MNO portability of Mobile NFC services is out of scope of this specification.
2.8 Termination processes

2.8.1 Process 18 – Termination of Mobile Subscription or NFC Option by End User

Sequence diagram

Figure 25: Sequence diagram of Process 18 – Termination of mobile subscription or NFC option by end user

Description

The MNO informs the TSM of the line of NFC option termination using the `HandleMobileSubscriptionStatusChangeNotification`. When the transfer of entitlements is done, the TSM applies an Information System (IS) lock on the service and informs the MNO using the `HandleStartServiceStateChangeNotification`.
2.8.2 Process 19 – Mobile Service Termination by Mobile Network Operator

**Sequence diagram**

![Sequence diagram of Process 19 – Mobile service termination by MNO]

**Description**

The MNO uses the `HandleMobileSubscriptionStatusChangeNotification` to inform the TSM first, of the suspension or restriction of the line and then, of its restoration or termination, depending on the status of the dispute process.

When the transfer of entitlements is done, the TSM applies an IS lock on the service and informs the MNO using the `HandleStart/EndServiceStateChangeNotification`.
2.8.3 Process 20 – Mobile NFC service termination

Figure 27: Sequence diagram of Process 20 – Mobile NFC service termination
The removal Sub Process 20.1 is defined below:

![Sequence diagram of Process 20.1 – Sub Process - Mobile NFC service termination](image)

**In Simple SD mode**

In simple SD mode, the TSM SHALL remove the bindings if present (only if the termination process is not a sub process of reinstallation). The TSM then uses the \texttt{SECommandsGenerationAndRemoteExecution} request to ask for the deletion of the service to the MNO who deletes the UICC application instance, the package (if there are no remaining instances linked to it) and the SSD if required. If the SSD deletion is needed, the two \texttt{DeleteCommands} (for the application and for the SSD) can be grouped together for more efficiency.
**In Delegated Management mode**

In delegated management mode, the TSM SHALL also remove the bindings if present (no reinstallation). Then the TSM uses the GenerateDMToken request to be authorized, and sends OTA the GlobalPlatform UICC commands in order to delete the UICC application instance and package. Then, the TSM uses the VerifyDMReceipt notification to inform the MNO with the token receipt.

Finally, the TSM uses the SECommandsGenerationAndRemoteExecution request to ask the MNO to delete the SSD.

### 3 GP Messaging Functions Use and Restrictions Matrix

This section intends to detail the parameters use in each GP function. Sequence diagrams are the first reference. The following descriptions may specify other possibilities or may detail the use of particular parameters.

#### 3.1 Convention

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Mandatory. The function SHALL be implemented</td>
</tr>
<tr>
<td>C</td>
<td>Conditional. The function SHALL be implemented only if the condition is met.</td>
</tr>
<tr>
<td>O</td>
<td>Optional. The function MAY be implemented</td>
</tr>
<tr>
<td></td>
<td>Not Used. The function SHOULD NOT be implemented</td>
</tr>
</tbody>
</table>

#### 3.2 Eligibility Check

<table>
<thead>
<tr>
<th>Eligibility check functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetDeviceCapabilityProfileId</td>
<td>M</td>
<td>Parameters SHALL be used as defined in [GPSTM] § 3.2.1.1.</td>
</tr>
<tr>
<td>GetSECapabilityProfileId</td>
<td>M</td>
<td>Parameters SHALL be used as defined in [GPSTM] § 3.2.1.2.</td>
</tr>
<tr>
<td>CheckMobileSubscriptionEligibility</td>
<td>M</td>
<td>Parameters SHALL be used as defined in [GPSTM] § 3.2.1.3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Sub-Process A – MNO eligibility, Non Eligibility Reason SHALL be set to ‘SE capability: no memory space left’=15 in the response if the MNO implements memory checking.</td>
</tr>
</tbody>
</table>

#### 3.3 Service Management Life Cycle

<table>
<thead>
<tr>
<th>Service Management life cycle functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HandleStartServiceStateChangeNotification</td>
<td>M</td>
<td>Mobile Subscription SHALL be provided</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Element SHALL be ignored if provided</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operation=Service update MAY be supported by the MNO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Process 16 - Change in Contract Ownership, Operation SHALL be set to ‘SE applications Redeployment’=102.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Process 10 – Change Mobile Handset, Operation SHALL be set to ‘Device Applications Redeployment’=103.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Process 13 – Recover mobile equipment after a loss, Operation SHALL be set to ‘SE applications Redeployment’=102.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the Process 14 – Get New Mobile Equipment after a</td>
</tr>
</tbody>
</table>

*GP Messaging Functions Use a nd Restrictions Matrix*
### 3.4 Mobile Subscription Life Cycle

<table>
<thead>
<tr>
<th>Service Management life cycle functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetMobileSubscriptionAlternateIdentifier</td>
<td>C</td>
<td>This function is not represented in the sequence diagram. Depending of the country and of the MNO (due to legal restriction), the use of this function may be enforced. In this case, the TSM SHOULD request at first the alternate identifier in order to proceed further (to eligibility process by example) Service SHALL be set. Other parameters SHALL be used as defined in [GPSM] § 3.2.4.1.</td>
</tr>
<tr>
<td>GetSEMobileSubscriptionIdentifier</td>
<td>O</td>
<td>It is the MNO choice to implement this function or not. If alternate identifier is mandatory for the MNO, it SHOULD NOT implement this function. Parameters SHALL be used as defined in [GPSM] § 3.2.1.2.</td>
</tr>
<tr>
<td>HandleMobileSubscriptionIdentifierChangedNotification</td>
<td>M</td>
<td>This notification SHALL be sent as many times as there are different Mobile Subscription identifiers representing the Mobile Subscription. Parameters SHALL be used as defined in [GPSM] § 3.2.4.3. It is the MNO choice to send the mobile subscription identifier or an alternate mobile subscription identifier.</td>
</tr>
<tr>
<td>HandleMobileSubscriptionStatusChangeNotification</td>
<td>M</td>
<td>This notification SHALL be sent as many times as there are different Mobile Subscription identifiers representing the Mobile Subscription. For the Process 11 – Lost or Stolen Mobile Equipment, End User Contacts MNO : New Status SHALL be set to ‘Suspended’ or ‘Restricted’ Reason SHALL be set to ‘Theft’ or ‘Lost’ or ‘Lost or Theft’ For the Process 16 - Change in Contract Ownership, Reason SHALL be set to Subscription contract owner changed =4. Other Parameters SHALL be used as defined in [GPSM] § 3.2.4.4.</td>
</tr>
</tbody>
</table>

### 3.5 Secure Element Life Cycle

<table>
<thead>
<tr>
<th>Secure Element life cycle functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HandleSERenewalNotification</td>
<td>M</td>
<td>Parameters SHALL be used as defined in [GPSM] § 3.2.5.1.</td>
</tr>
<tr>
<td>HandleSEDeviceChangedNotification</td>
<td>M</td>
<td>Parameters SHALL be used as defined in [GPSM] § 3.2.5.2.</td>
</tr>
<tr>
<td>HandleSEMobileSubscriptionChangedNotification</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>HandleSEStatusChangeNotification</td>
<td>M</td>
<td>For the Process 11 – Lost or Stolen Mobile Equipment, End User Contacts MNO : New Status SHALL be set to ‘Suspended’ or ‘Restricted’ Reason SHALL be set to ‘Theft’ or ‘Lost’ or ‘Lost or Theft’ Date SHALL be set to an approximate date in future (only for the first notification).</td>
</tr>
</tbody>
</table>
For the
Process 12 – Lost or Stolen Mobile Equipment, End User Contacts Service Provider:
New Status SHALL be set to ‘Suspended’
Reason SHALL be set to ‘Theft’ or ‘Lost’ or ‘Lost or Theft’
For the
Process 13 – Recover mobile equipment after a loss:
New Status SHALL be set to ‘Activated’
Reason SHALL be set ‘Recovered’

Note: the MNO MAY ignored the New Status parameter in Process 12.
Other Parameters SHALL be used as defined in [GPSM] § 3.2.5.4

3.6 CCCM Certificate Management

EnrollSSDOwnerCertificate function is not used for the certificate management because the scenario #2.B (Push Model without Application Provider Certificate) is used to create confidentially the first keyset on the SSD.

To retrieve the CASD certificate, TSM SHOULD:
- Send GET DATA command directly on the CASD. This option is valid if the TSM has an OTA capability.
- Or Provision CASD certificate for each UICC profiles
- Or Request MNO the execution of GET DATA command through Script Sending functions.

<table>
<thead>
<tr>
<th>CCCM certificate management functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnrollSSDOwnerCertificate</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>GetCAInformation</td>
<td>O</td>
<td>MNO MAY implement this function even if the three other options to retrieve the CASD certificate is preferred.</td>
</tr>
</tbody>
</table>

3.7 Secure Element Management

3.7.1 SE Card Content Management

<table>
<thead>
<tr>
<th>SE CCCM functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| SECommandsGenerationAndRemoteExecution | M   | Mobile Subscription SHALL be present
Other parameters SHALL be set as defined in [GPSM] § 3.4.1.2. |

As defined in [GPSM], SECommandsGenerationAndRemoteExecution can execute a sequence of SE Commands. The use of Each SE Command is described below:

3.7.1.1 Creating the First Key Set of a Security Domain

CreateFirstSSDKeysetCommand SHOULD be used in Basic Create, Basic Random Create or CCCM Scenario #2.B mode. The other modes MAY NOT be implemented by the MNO.
Other parameters SHALL be set as defined in [GPSM] § 3.4.1.3.1.2
3.7.1.2 Loading of an Executable Load File

LoadELFCommand SHOULD be used as follow:

- **Byte Code** SHOULD NOT be set. The ELF byte code SHOULD be provided at provisioning stage.
- **Byte Code Encrypted** SHOULD NOT be set.
- **DAP Block** SHOULD NOT be set (except if diversified mandated DAP keys are used)

Other parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.1

3.7.1.3 Extraditing Application or Executable Load File

ExtraditeCommand parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.2

3.7.1.4 Instantiating an Application

InstantiateApplicationCommand SHOULD be used as follow:

- **Application Specific Parameters** SHOULD NOT be set.

Other parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.3

3.7.1.5 Make Selectable an Application

MakeSelectableApplicationCommand parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.4

3.7.1.6 Registry Update for an Application

ApplicationRegistryUpdateCommand parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.5

3.7.1.7 Locking and Unlocking an Application

SetStatusCommand parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.6

3.7.1.8 Deleting an Application or Executable Load File

DeleteCommand SHOULD be used as follow:

- **Delete Related Objects** SHOULD NOT be set.

Other parameters SHALL be set as defined in [GPSM] § 3.4.1.3.2.7

3.7.2 Delegated Management

<table>
<thead>
<tr>
<th>DM functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GenerateDMToken</td>
<td>M</td>
<td>Parameters SHALL be set as defined in [GPSM] § 3.4.2</td>
</tr>
<tr>
<td>VerifyDMReceipt</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>

3.7.3 Script Sending

This function group is not represented in the sequence diagram.
If this function is implemented by the MNO and if the SP/TSM doesn’t have OTA capabilities, it SHALL use these functions. These functions are particularly useful for the application or SD personalisation (see Process 5 – Mobile NFC UICC Application Installation).

<table>
<thead>
<tr>
<th>Script sending functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BeginConversation</td>
<td>C</td>
<td>Mobile Subscription SHALL be set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other parameters SHALL be set as defined in [GPSM] § 3.4.3.1</td>
</tr>
<tr>
<td>SendScript</td>
<td>C</td>
<td>Parameters SHALL be set as defined in [GPSM] § 3.4.3.2</td>
</tr>
<tr>
<td>EndConversation</td>
<td>C</td>
<td>Parameters SHALL be set as defined in [GPSM] § 3.4.3.3</td>
</tr>
</tbody>
</table>

### 3.7.4 SE Audit

<table>
<thead>
<tr>
<th>SE management functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetApplicationOrELFStatus</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### 3.7.5 SCWS Service Portal

<table>
<thead>
<tr>
<th>SE management functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoadSCWSServicePortal</td>
<td>O</td>
<td>Parameters SHALL be set as defined in [GPSM] § 3.4.5</td>
</tr>
<tr>
<td>DeleteSCWSServicePortal</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

### 3.7.6 Device Application Management

<table>
<thead>
<tr>
<th>SE management functions</th>
<th>Use</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoadDeviceApplication</td>
<td>M</td>
<td>Parameters SHALL be set as defined in [GPSM] § 3.5</td>
</tr>
<tr>
<td>DeleteDeviceApplication</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>BindDeviceApplicationToSEApplication</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>UnbindDeviceApplicationToSEApplication</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>
Document Management

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Brief Description of Change</th>
<th>Approval Authority</th>
<th>Editor / Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>27/04/12</td>
<td>Document submitted to DAG &amp; EMC for approval final approval date 30th July 2012</td>
<td>PSMC/NFC</td>
<td>Gaël Gérard, Orange</td>
</tr>
</tbody>
</table>

Other Information

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org. Your comments or suggestions & questions are always welcome.