TRUSTED CONNECTIVITY ALLIANCE

Device Implementation Guidelines

Published by simalliance now Trusted Connectivity Alliance

June 2013

Document History

Version	Date	Editor	Remarks
1.1	07/06/2013	Handset Task Force	- Requirement on NULL procedure byte management removed to get wider industry consensus after liaisons with other bodies - Annex A (linked to above requirement) removed.
1.0	04/02/2013	Handset Task Force	Public release

Table of Contents

1. Introduction

This document is a collection of guidelines and recommendations for optimal support of the UICC by device manufacturers designing handsets, tablets, modems and other devices making use of a telecom UICC. The document uses ETSI SCP and 3GPP Release 10 as the baseline release and also refers to relevant documents provided by GSMA, GlobalPlatform and OMA.

This document is also applicable to the functional requirements of both M2M and eUICC, but does not include specific requirements (like hardware) requested for either M2M or eUICC.

The purpose of this document is to complement existing standards by highlighting their key requirements, clarifying their optional parts and providing recommendations that will help to avoid implementation issues. All the requirements described in this document are compliant with the appropriated standards.

The document is split in several chapters describing the different UICC-related features needed for devices. At the beginning of the document a global compliancy table indicates which features, together with their associated level of priority, are needed for generic devices, NFC devices and LTE devices.

1.1 Scope of document

The document is aimed at product and technical teams working in organizations involved in the telecom ecosystem. It is especially targeting manufacturers designing devices or chipsets with telecom network connectivity (handsets, tablets, modems etc.) and mobile network operator teams in charge of device requirements.

1.2 References

Specification	Description
ISO/IEC 14443	Identification Cards – Contactless integrated circuits – Proximity cards – Part 4: Transmission Protocol
ISO/IEC 10373-6	Identification cards — Test methods — Part 6: Proximity cards
ETSI 102 221	Smart cards; UICC-Terminal interface; Physical and logical Characteristics
ETSI 102 223	Smart cards; Card Application Toolkit
ETSI 102 310	Smart Cards; Extensible Authentication Protocol support in the UICC
ETSI 102 483	Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal
ETSI 102 600	Smart Cards; UICC-Terminal interface; Characteristics of the USB interface
ETSI 102 613	Smartcards; UICC-CLF Interface; Physical & Logical characteristics (SWP)
ETSI 102 622	Smart Cards; UICC – Contactless Front-end (CLF) interface; Host Controller Interface (HCI)

ETSI 102 694-1	Smartcards; Test specification for Single Wire Protocol (SWP) interface; Part 1: Terminal features
ETSI 102 695-1	ETSI 102 695-1 Smartcards; Test specification for the Host Controller Interface (HCI); Part 1: Terminal features
ETSI 122 011	Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);LTE; Service accessibility
ETSI 123 122	Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
3GPP 31 101	UICC-terminal interface; Physical and logical characteristics
3GPP 31 102	Characteristics of the Universal Subscriber Identity Module (USIM) application
3GPP 31 103	Characteristics of the IP Multimedia Services Identity Module (ISIM) application
3GPP 31 111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
3GPP 31 122	Universal Subscriber Identity Module (USIM) conformance test specification
3GPP 33 220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)
3GPP 33 234	3G security; Wireless Local Area Network (WLAN) interworking security
3GPP2 C.S0065-B	cdma2000 Application on UICC for Spread Spectrum Systems
3GPP2 C.S0016-C	Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards
3GPP2 C.S0035	CDMA Card Application Toolkit
JSR-118	Mobile Information Device Profile – Trusted MIDlet suites using X509 PKI
JSR-177	Security & Trust Services API for J2ME
JSR-257	Contactless Communication API
GSMA	NFC Handset APIs & Requirements – version 3.0 October 2012
GlobalPlatform	Device Technology – Secure Element Access Control v1.0
SIMalliance	SIMalliance Open Mobile API specification v1.2
OMA	TS Smart Card Web Server v1.2
EMVCo AAUI	EMVCo Application Activation User Interface v1.0

1.3 Definition of Terms

Acronyms

Term	Description
3GPP	3rd Generation Partnership Project
AC	Secure Element Access API - Access Control
API	Application Programming Interface
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BIP	Bearer Independent Protocol
CAT	Card Application Toolkit
CLF	Contactless Frontend (NFC chipset)
ETSI	European Telecommunications Standards Institute
FWI	Frame Waiting Time Integer
FWT	Frame Waiting Time
J2ME	Java 2 Mobile Edition
JSR	Java Specification Request
LTE	Long Term Evolution
ME	Mobile Equipment
MNO	Mobile Network Operator
NFC	Near Field Communication
OTA	Over The Air
RAM	Remote Application Management
RF	Radio Frequency
RFM	Remote File Management
SE	Secure Element
SAK	Select Acknowledge
SAT	SIM Application Toolkit
SCWS	Smart Card Web Server
SIM	Subscriber Identity Module

SWP	Single Wire Protocol
UI	User Interface
UICC	Universal Integrated Circuit Card
WTX	Waiting Time eXtension

Terminology

Device makers should note that SIMalliance is not a technical standards body. It is therefore only appropriate for this document to provide recommendations regarding how the technical standards should be implemented. In order to impart the significance of each, however, this document also classifies its recommendations, using the following terms and meanings:

- SHALL: denotes a mandatory requirement
- SHOULD: denotes a recommendation
- M: Mandatory
- O: Optional

2. Overall compliancy matrix

The table below provides a summary of the requirements described in this document, together with an associated "fundamental" or "premium" classification according to three groups: requirements common to all devices, requirements for NFC devices and requirements for LTE devices.

SIMalliance Device: Fundamental guidelines (F)
These guidelines define the basic set of features which are needed for device makers to realize the minimum benefit from the UICC. Here, 'fundamental' is used to specify primary guidelines for UICC technology support; it is not intended to mean 'mandatory' in the conventional sense.

SIMalliance Device: Premium guidelines (P)
These guidelines define the optimum set of features which are needed for device makers to realize full benefit from the UICC.

A requirement may be set as a "premium" requirement when applied to a generic device but as a "fundamental" requirement for NFC or LTE devices.

"N/A" means that the requirement is not applicable for this category of devices.

Feature	Generic devices	NFC devices	LTE devices
UICC Interface			
Class Voltage	F	F	F
Interface Speed	F	F	F
Polling mechanism	F	F	F
Logical channels	F	F	F
Terminal Capability command	P	F	F
(U)SIM Services			
PIN code management	F	F	F
Network files management	F	F	F
Service Name management	F	F	F
UICC Remote Management	F	F	F
Card Application Toolkit & background mode	F	F	F
Card Application Toolkit			
Basic Qualifiers	F	F	F
Alpha Identifier Management	F	F	F
Transparent mode	F	F	F
Basic Commands	F	F	F
Terminal Profile command	F	F	F

Terminal Response	F	F	F
Refresh command	F	F	F
Send USSD command	F	F	F
Provide Local Information command	F	F	F
Set Up Idle Mode Text	P	P	P
Timer Management / Timer Expiration	F	F	F
Set Up Event List command	F	F	F
Call Control by SIM	F	F	F
MO Short Message Control by SIM	F	F	F
Bearer Independent Protocol	F	F	F
Launch browser command	F	F	F
Secure Element Access API & Access Control	P	F	F
NFC device implementation guidelines			
GSMA requirements	N/A	F	N/A
Additional requirements for NFC devices	N/A	F	N/A
LTE device implementation guidelines			
USIM interface for LTE	N/A	N/A	F
USIM toolkit enhancements for LTE	N/A	N/A	F
LTE Access Technology for network selection management	N/A	N/A	F
Bearer Independent Protocol for LTE	N/A	N/A	F
3GPP/3GPP2 Interworking (for LTE/CDMA devices)	N/A	N/A	F
Home eNodeB (HeNB) provisioning	N/A	N/A	F
ISIM (IMS Network Access)	P	P	F
Extended Authentication Protocol (EAP)	P	P	F
Generic Bootstrapping Architecture (GBA)	P	P	F
I-WLAN	P	P	F
Terminal applications launched from the UICC	P	F	P
Smart Card Web Server	P	P	P
High Speed Protocol (HSP)	P	P	P

3. UICC Interface

3.1 Class voltage management

Recent generations or UICC chipsets are supporting both 3V voltage (Class B) and 1.8V (Class C), as defined in the ETSI 102 221 specification. In some cases, upon a MNO request, a UICC can be set to work in 3V mode. Furthermore, many old cards not supporting 1.8V technology are still used in the field.

As a result it is mandatory for the device to support both 3V and 1.8V technologies, always starting with the lowest voltage mode supported during the boot procedure. Support of 5V technology (Class A) is no longer needed.

3.2 Interface speed

Also called "PPS support", interface speed indicates the communication speed of the ISO/IEC-7816 interface. To ensure a correct user experience with UICC applications, TA1= 0x96 (~230 Kb/s) SHALL be supported.

Support of TA1=0x97 (~450 Kb/s) is highly recommended as it will significantly increase overall performance, especially in the case of the download of an application into the UICC from a backend server.

Whether a specific speed is supported or not, a fallback policy must be applied. For example, if the UICC is requesting a TA1=0x97 and the device does not support this value, the device SHALL switch to its highest value supported (e.g. TA1=0x96 or TA1=0x95) and SHALL NOT switch back to the lowest value (e.g. TA1=0x11).

3.3 Polling mechanism

The polling mechanism is managed by the Mobile Equipment which is sending a STATUS command at regular intervals to the UICC. It ensures that the UICC has not been removed during a session for security reasons and also enables starting a SAT session when the UICC is answering with the appropriated code (i.e. 91 xx) to the STATUS command.

The ETSI 102 221 standard specifies that the Mobile Equipment has to send the STATUS command according to default value defined for the UICC detection (i.e. around 30s) or according the value negotiated by the UICC through the proactive command "Poll interval".

The STATUS command, combined with the polling interval mechanism, is used by SAT applications as a way to trigger an application and initiate a proactive session. To limit the effect on the battery life, the polling is only required over a limited time period and when not more used, the polling off command is sent to the device that can resume its usual behavior.

The requirements around the polling mechanism are:

- Devices SHALL manage the default polling interval specified in ETSI 102 221
- Device SHALL at least support polling interval values ranging from 5 seconds up to 5 minutes

- When the proactive command POLLING OFF is used, the device SHALL NOT stop the polling mechanism but it SHALL switch back to the default polling interval
- The device SHALL only manage one polling interval and ensure that the STATUS command is sent to the UICC in accordance with the length of the interval that the UICC has defined. The device SHALL NOT combine a proactive polling interval in addition to the default polling interval

3.4 Logical channels

UICCs are hosting more and more applications. These can be Network Access Applications like USIM, CSIM, ISIM, etc. or specific applications requested to provide Access Control for the SE Access API (ARA-M applet defined by GlobalPlatform or PKCS#15 ADF). They can also be NFC applications (banking, transport) used for NFC transactions over the contactless interface but also by a NFC Wallet or a specific Service Provider UI over the ISO 7816 interface.

To avoid any interference with the telecom applications, each time the device is using a new application; it SHALL select this application on a new logical channel. When the application is no longer used, the device SHALL close the logical channel to free the resources.

All devices SHALL manage at least 4 logical channels. NFC & LTE devices SHALL manage at least 8 logical channels.

3.5 Terminal capability command

The device SHALL follow the terminal capability command described in the ETSI 102 221. The device SHALL support the 3 options defined in the specification:

- Terminal power supply
- Extended logical channels support
- Additional interface support (SWP)

The device SHALL only use this command if the UICC is stating explicitly its support in "supported command field" when answering a SELECT command.

4. (U)SIM Services

4.1 PIN code management

PIN code management is described in the ETSI 102 221 and will not be detailed in this chapter, which focuses on two important recommendations only.

The UICC PIN SHALL NEVER be stored in a persistent way in the device.

The UICC PIN code SHALL NOT be presented automatically by the device in case of a new network attachment triggered by the UICC, for example after the execution on a proactive REFRESH command with a reset parameter. This is especially important in case of the eUICC where the subscription (and thus also the PIN code) can be changed over the air. If the device is using a PIN code cached in its memory, it may be incorrect.

4.2 Network files management

The device shall use the information stored in the UICC related to network selection in order to attach to the network with the highest priority. Several files are dedicated to this mechanism; some of them also include information on the Access Technology.

The device shall refer to ETSI 122 011 and ETSI 123 122 for the network selection process.

The device SHALL especially manage the following files, which are listed in preferred order so the first (if available) SHALL be used before the last. This list is not exhaustive but provides the most important files for network access from the UICC point of view.
If the device is using the SIM application:

- EF PLMNSel (Public Land Mobile Network) with at least 100 network entries
- EF FPLMN (Forbidden PLMN) with at least 10 network entries
- EF HPLMN (Home PLMN)

If the device is using the USIM application:

- EF PLMNwAcT (Public Land Mobile Network with Access Technology) with at least 100 network entries
- EF OPLMNwAcT (Operator PLMN with Access Technology) with at least 100 network entries
- EF HPLMNwAcT (Home PLMN with Access Technology) with at least 10 network entries

If the device is using the CSIM application:

- EF EPRL (Extended Preferred Roaming List) with at least 100 network entries

Upon registration on a network, the device SHALL update accordingly the needed files in the UICC (EF LOCI) and SHALL notify the UICC of any change on the Access Technology using the appropriated proactive event.

4.3 Service Name management

The ETSI specification defines a set of files used to manage the display of the telecom operator name:

- OPL: Operator PLMN list
- PNN: PLMN Network Name
- SPN: Service Provider Name
- SPDI: Service Provider Display Information

SPN & SPDI Files:

EF SPN file provides the service provider name and the appropriate requirements for display by the ME. The service provider name is stored in the USIM. EF SPN file is often used to define the name of the service provider in the case of MVNO, or the name of the MNO in a roaming situation. The EF SPDI provides additional information to define if the service provider name shall be displayed or not. It contains a list of PLMN for which the Service Provider Name shall be displayed.

PNN & OPL files:

It is possible to associate or not PLMN Identifications (MCC+MNC combination) to the Service Provider Name. The PNN file provides the name of the PLMN to be display in place of the one stored in the ME memory (ME firmware) or of the one sent by the network. The OPL file completes the use of the PNN file by adding the list of PLMN for which this mechanism must apply.

EF PNN is used to display the full and short form versions of the network name for the registered PLMN.

Device Implementation Guidelines

The device SHALL support the SPN and PNN display on the same screen.
The device SHALL support at least 80 entries in the OPL and SPDI files.

If the first byte of EF SPN is "00", then the device:

- SHALL display the SPN name
- SHALL NOT display any network name (neither from PNN, or device memory or network) if the registered PLMN is either the HPLMN or a PLMN set in the SPDI file

If the first byte of EF SPN is "01", then the device:

- SHALL display the SPN name
- SHALL display the content of the PNN file in place of any network name stored in the device memory or coming from the network if the registered PLMN is either the HPLMN or a PLMN set in the SPDI file

In general, when registered on the HPLMN or one of the PLMN used for Service Provider Name display (SPDI file):

(i) The service provider name shall be displayed;
(ii) Display of the PLMN Name is an operator's option by setting the appropriate fields in the USIM (i.e. the Service Provider name shall be displayed either in parallel to the PLMN Name or instead of the PLMN Name).

When not registered on the HPLMN or one of the PLMN used for Service Provider Name display (SPDI file):

(i) The PLMN name shall be displayed;
(ii) Display of the service provider name is an operator's option by setting the appropriate fields in the USIM.

5. UICC Remote Management

UICC can be managed remotely Over the Air from the MNO backend system. With the deployment of LTE and NFC technologies, this capability is becoming increasingly important. In some LTE networks, remote management is used to perform the UICC activation while the device/UICC is already in the hands of the end-user.

In NFC, this capability is used to perform the download and personalization of the NFC application as well as ensure their remote management during the UICC life cycle.

Remote management is relying on the Bearer Independent Protocol (BIP) Client mode. Depending on the operators, it is either done over BIP Client in TCP mode (e.g; RAM over HTTPS) or in BIP Client in UDP mode.

Triggering a remote administration session can be done at the initiative of the UICC (also called "pull" mode). It can also be done at the server side initiative (called "push" mode). In this last case, the mechanism is triggered through a "push" SMS.

Device Implementation Guidelines

To enable UICC remote management, the device SHALL support BIP Client mode in UDP and TCP mode as specified in the ETSI 102 223 release 4 and higher, class 'e'.

The transparent mode (Alpha ID = NULL or no Alpha ID) for BIP Client SHALL also be supported as the administration of the UICC shall remain transparent for the end-user.

Several remote servers may need to initiate a remote administration session with the UICC at the same time, the device SHALL thus support at least 2 concurrent BIP client sessions.

"Push" SMS will be send to the UICC using the Envelope PP Data download mechanism defined in the ETSI 102 221 and ETSI 102 223. The device SHALL support this command.

Note: BIP Client in TCP mode should not be confused with BIP - UICC in TCP Server mode needed for SCWS implementation. The BIP Client proactive commands and event are described more in details in the Card Application Toolkit chapter.

6. Card Application Toolkit & background mode

Most non-smartphone devices only permit one application to run at a time. From a Toolkit application perspective, this means that an end-user has to exit the active application before switching to another device application, or coming back to the home screen.

The context is different in the case of smartphones. The device is usually able to manage several applications at the same time and moreover, the end-user may switch an application in background while not being entirely aware of what they are doing. For example, many end-users are using the "home" key of their device as an easy way to exit from an application and free the screen of their device. When doing that, the application is only put in background but not stopped.

Some manufacturers are not allowing the end-user to operate a Toolkit application in background. The end-user therefore has to close the application before switching to another application. This mode allows for robust SIM Toolkit application management and is by far best way for the industry to proceed. Other manufacturers allow the switching of Toolkit applications in background mode (end-user action or network event) and are managing it in different ways:

- Sending a Terminal Response immediately or after a short time out (Terminal Response = 0x12 meaning "No response from user")
- Keeping the application in background without sending a response until the end-user decides to go back to the application and close it. This behavior is causing a major issue with the UICC.
- Sending a Terminal Response after a short time out BUT keeping further Toolkit sessions in background, without displaying the new commands to the end-user. This behavior is also abnormal and could lead to more serious issues with the UICC.

The issue with devices not managing the background mode correctly is that they never send back a TERMINAL RESPONSE to the UICC except if the end-user goes back to the application. It means that the SIM Application Toolkit engine of the UICC can remain "busy" in background for hours or days, until the end-user either explicitly closes the session or reboots the device.

While in this "busy" state, the UICC will not be accessible to Over the Air (OTA) servers, will not be able to initiate BIP communications with remote servers, will not be able to launch toolkit applications following the reception of network events or upon periodic timings, etc. This issue thus blocks the correct execution of mobile network operators applications locally installed in the UICC. Moreover, it is no longer possible to remotely administer the UICC, including the installation/personalization of new services, e.g. NFC services.

In addition, when suspending a SIM Application Toolkit session, some devices are also disabling the mandatory UICC polling mechanism specified by the ETSI standard (TS 102 221).

Device Implementation Guidelines

To avoid issue with Toolkit applications, SIMalliance strongly recommends prohibiting the practice of putting such applications in background mode, instead forcing the end-user explicitly to exit each application before opening another.

When external events (like an incoming call) need to be managed, a mechanism shall be set in place to automatically return to the toolkit session as soon as the management of the external

event is finished. It is very important to again remove the possibility for the end user to go into another interface (or to go back to home) without closing the SIM Toolkit application properly.

If the device design requires such "home" feature even during the execution of a SIM Toolkit application then the device shall terminate the pending Toolkit session, sending a Terminal Response "TR 0x10 – Proactive session terminated by the user" before going back to the home screen in order to terminate the Toolkit session on UICC side. The device shall also end the application on its own UI.

If the device is entering into an idle screen mode, it shall immediately send a Terminal Response to the UICC with the appropriated status "TR 0x12 - No response from user".

In all cases, the device shall follow the ETSI specification and keeps the polling mechanism alive, sending STATUS command to the UICC on the negotiated polling interval (or using the default interval).

The user experience with SIM Toolkit applications may thus be different compared to applications on other devices, but the impact on mobile network operators' services and on the end-user (preventing, for example, the download of a new service subscribed by the end-user on the UICC) is very important. This is why it is mandatory to limit such behavior.

Alternative implementation

If the above solution cannot be implemented for technical reasons, SIMalliance still recommends to prohibit the practice of putting the SIM Toolkit application in background and suggests instead to terminate the application, sending immediately a "TR 0x10 – Proactive session terminated by the user" when the end-user is switching to the home screen or to another device application.

7. Card Application Toolkit

This chapter does not intend to duplicate the standard, but rather to focus on key requirements related to Card Application Toolkit and to provide additional implementation guidelines to ensure the most adapted device behavior according to the market use cases.

Widely supported commands are mentioned in the "Basic commands" sub-chapter while other commands requiring more clarification on the expected device implementations are described with a dedicated sub-chapter per command.

This document does not integrate specific LTE requirements which are described in chapter 10: LTE device implementation guidelines.

7.1 Basic qualifiers

The following qualifiers or parameters related to basic commands are mandatory and SHALL be supported by the device whenever applicable:

- DCS 7 bits, 8 bits and UCS2 for Text String
- SMS default Alphabet or Digit only
- Normal & High Priority for Get Input
- Clear after delay & Wait for user to clear message for Get Input
- Automatic Scrolling supported and indicated in the Terminal Profile for each command with display function (Select Item, Get Input, Display Text…)

UCS2 shall be supported for languages using 2 bytes encoding (Chinese, Russian, etc. alphabets).

7.2 Alpha Identifier Management

The Alpha identifier field is used in a large set of proactive commands. It holds text that could be displayed on the device screen if the end user needs to be notified of the device action within a Toolkit procedure. The standard specifies three attributes of the Alpha Identifier management:

- If the Alpha Identifier is provided by the UICC and is not a NULL data object, the ME shall use it to inform the user of the ongoing action.
- If the Alpha Identifier is provided by the UICC and is a NULL data object (i.e. length = '00' and no value), this is an indication that the ME SHALL NOT display any information on the ongoing actions.
- If the Alpha Identifier is not provided by the UICC, it is recommended that the device behaves in the same way as with a NULL Alpha Identifier.

Device SHALL support the 3 modes:

- Alpha Identifier Tag provided by the UICC
- NULL data object for Alpha Identifier
- No Alpha Identifier Tag provided by the UICC

7.3 Transparent mode

Several applications need to work in a transparent mode in order to avoid any unnecessary confirmation or information message that can be confusing for the end-user.

Such applications are always under the strict control of the mobile network operators as the UICC security ensures that only an authorized entity (i.e. the operator) is able to install Toolkit applications in the UICC.

Transparent mode is defined by the Alpha Identifier coding with the NULL length for each command using an Alpha Identifier Tag. For commands without Alpha Identifier or if the Alpha Identifier is omitted in a command supporting it, the action SHALL be performed transparently for the end-user. Transparent mode SHALL be implemented for the following proactive commands requiring an Alpha Identifier field:

- Set Up Call command
- Send SMS command
- Send USSD command
- Refresh
- Launch Browser command
- BIP commands (Open Channel / Close Channel / Send Data / Receive Data)
- Call Control by SIM envelope
- SMS MO Control by SIM envelope
- Set Up Event List command
- Timer Management
- And in other commands like Play Tone, Set Up Menu, Run AT Command, Send DTMF.

To avoid confusing the end-user (the message will not be seen), when receiving an Envelope SMS-PP Download with TP-PID=7Fh, the device SHALL NOT notify the end-user (no text displayed, no ring) of the reception of this message.

The events related to the Set Up Event List command SHALL be sent by the device to the UICC in a transparent way for the end user.

7.4 Basic Commands

All commands below are defined in the first release of the Toolkit specification and are quite well implemented in devices. This chapter only mentions specific modes and parameters that were either included later in the specification or that are currently requested by the market and are not always well supported.

- Display Text
  - » Sustained text (or Immediate Response) shall be supported
  - » Duration (variable timeout) should be supported
  - » Maximum number of characters that can be displayed: 200 characters
  - » Displayed on top of other applications (browser for instance)
- Get Inkey
  - » Binary Choice (Yes or No Response) shall be supported
  - » Duration (variable timeout) should be supported
  - » Help Information should be supported
- Get Input

  - Maximum number of characters displayed (for the question): 60 characters
  - Maximum number of characters that can be used: 100 Characters
  - Help Information should be supported
- Select Item
  - Order given by the SIM shall be supported
  - Maximum number of characters (for title or for each item): 60 characters
  - Number of items supported: at least 10 items
  - Help Information should be supported
  - SoftKey should be supported
- Set Up Menu
  - Quick access to the SIM Menu (3 click max) and first position
  - Help Information should be supported
  - SoftKey should be supported
- Send Short Message
  - Management of concatenated SMS shall be supported
  - No user confirmation
  - Support of "Packing by ME required"
- Set Up Call
- More Time
- Play Tone
  - Audible (via speaker)
  - Not blocking in case of "Silent mode" (ex Terminal Response "09" instead of TR 2x or 3x)
- Envelope Menu Selection
- SMS Point to Point Data Download (PID = 0x7F & DCS = 0xF6)
- Send SS

7.5 Terminal Profile

The Terminal Profile gives the capabilities of the device. It is very important to have accurate information in this command as several Toolkit applications are using it to define the way they behave and to assess whether or not they are able to run on the targeted device.

All supported commands and parameters SHALL be indicated in the Terminal Profile command. If a feature is not supported it SHALL NOT be indicated as supported in the Terminal Profile.

7.6 Terminal Response

The device SHALL provide the appropriated Terminal Response answer for all proactive commands requested by the UICC. The maximum delay for a "TR=12; No Response from user" SHALL NOT exceed 2 minutes.

7.7 Refresh command

The REFRESH command is used by Toolkit applications whenever it is important to have the device re-reading a file or repeating a specific action (like a network attachment). The following parameters/qualifiers are requested:

- Refresh Init + Full File Change Notification shall be supported

- Refresh File Change Notification shall be supported
- Refresh Init + File Change Notification shall be supported
- Refresh Init shall be supported
- Refresh Reset shall be supported
- Refresh NAA Reset, only applicable for 3G platform shall be supported
- Refresh Session Reset, only applicable for 3G platform shall be supported
- Refresh Steering of Roaming should be supported

Thanks to remote administration, UICC behavior can be modified Over the Air. It is thus very important that the device respects the following recommendations when applicable.

In the case of a UICC REFRESH request in "reset" mode, the network attachment parameters may have changed, so it is mandatory to set-up new connections (voice and data) according to these parameters:

- Check again all the "SIM" capabilities (2G/3G, etc.)
- If applicable ask for a PIN code presentation from the end-user, not using a "stored" one
- Perform a network de-attachment and full attachment (using freshly read PLMN files, EF_{Loci} and EF_{IMSI})
- Cut all data connections (internet, BIP, etc.) and DO NOT answer with "Terminal busy" or similar Terminal Response to active Toolkit applications

In the case of a UICC REFRESH request with parameters other than "reset" mode, the device shall:

- Cut all data connections (internet, BIP, etc.) and DO NOT answer with "Terminal busy" or similar Terminal Response to active Toolkit applications
- Based on the Command Qualifier perform a network de-attachment and full attachment (using freshly read PLMN files,EF_{Loci} and EF_{IMSI})
- Shall not send a TERMINAL PROFILE while executing the REFRESH procedure; not before and not after sending the TERMINAL RESPONSE to the REFRESH command
- Shall not update any Files on the UICC between reception of the REFRESH command and executing the REFRESH procedure (e.g. to avoid updating of network related EFs)
- Send a Terminal-Response to indicate a successful REFRESH procedure

7.8 Send USSD command

Send USSD is used for mobile network operator services relying on dynamic Toolkit application.

The Data Coding Scheme used in the USSD String field is coded as for Cell Broadcast Data Download command defined in ETSI TS 23.038. The coding of DCS for 7 bits and 8 bit is different from DCS commonly used for SMS. Most of application using USSD server from mobile network operator uses a packet message with the associated DCS=0x0F.

Some USSD services request the network to send back some data, within the Terminal Response. This data SHALL be forwarded to the UICC and SHALL NOT be displayed on the screen by the device.

7.9 Provide Local Information command

The Provide Local Information command is one of the most used commands by many Toolkit applications. It provides a huge amount of information about the device (terminal identity, date & time) or about the network (location, network measurement) to the application running in the UICC by using various command qualifiers.

The following qualifiers SHALL be supported:

- Location Information (MCC, MNC, LAC, Cell Identity and Extended Cell Identity)
- IMEI of the device
- Network Measurement results & BCCH
- Date, Time & Time Zone
- Language setting
- Timing Advance
- Access Technology
- IMEISV of the device
- Search Mode Change
- MEID of the terminal
- NMR UTRAN
- Battery Status

The device SHALL make sure that information provided in the Provide Local Information commands is consistent with network related information written into the EFs (e.g. EF_LOCI, EF_FPLMN, etc.).

7.10 Set Up Idle Mode Text command

The Idle mode text SHALL be displayed in a way ensuring that neither the network name nor the service providers name is affected.

If some other high priority information is showed in the screen, the previous Idle Mode Text SHALL be restored as soon as this information is no longer displayed.

When an Idle Mode Text is displayed, the device shall not alter the display until either:

- a new Set Up idle Mode Text is requested (even with a NULL length)

or

- other information is temporarily using the screen

The terminal SHALL support up to 240 bytes, with sufficient time to read it and the associated scrolling mechanism if needed.

7.11 Timer Management / Timer Expiration

Timers are used to allow a UICC Toolkit application to start at a specific moment or to wake-up at regular timing to check if a specific condition is triggered. The device SHALL support up to 8 timers at the same time and the following commands SHALL be supported:

- Start Timer shall be supported
- Deactivate Timer shall be supported
- Get Current Value of Timer shall be supported
- Envelope Timer Expiration shall be supported

7.12 Set Up Event List command

The UICC uses the Set Up Event List command to provide the list of events used by its applications. When an event occurs and if this event is part of the list requested by the UICC, the device SHALL inform the UICC with the corresponding envelope. It is important that the device notifies the UICC as soon as possible (less than 1 second) in order to ensure the requested behaviors of the Toolkit application are met.

The following events SHALL be supported by devices:

- MT Call event
- Call Connected event
- Call Disconnected event
- Location Status event
- User Activity event
- Idle Screen Available event
- Language Selection Status event
- Browser Termination event
- Data Available event
- Channel Status event
- HCI Connectivity event (in case of NFC device)
- Access Technology Change event
- Network Search Mode Change event

7.13 Call Control by SIM

The Call Control command is used to allow a Toolkit application to provide an additional service (like modifying a number to take into account specific numbering change) or an additional control (like prohibiting some special numbers with additional charges).

The following commands/parameters SHALL be supported:

- Call Control allowed shall be supported
- Call Control allowed with modification shall be supported
- Call Control not allowed shall be supported
- USSD string Data Object supported in Call Control shall be supported
- Env Call Control always sent to the SIM during automatic redial mode shall be supported

The device SHALL be able to manage the command in a full transparent mode for the end-user depending on the Alpha Identifier used.

USSD service can be used in conjunction with the Call Control command so a device SHALL support a Call Control mechanism in the case of a Send USSD proactive command.

The device SHALL send the call control command for any Mobile Originated calls (except emergency) even in case of redial mode.

7.14 MO Short Message Control by SIM

This mechanism is equivalent to the previous mechanism (Call Control) but adapted to Short Message Originated from the device or UICC.

The following parameters SHALL be supported:

- Short Message allowed
- Short Message allowed with modification
- Short Message not allowed

7.15 Bearer Independent Protocol

The Bearer Independent Protocol is based on the following commands and events that shall be supported:

- Open channel
- Close channel
- Send data
- Receive data
- Get channel status
- Channel status event
- Data available event

BIP Client in UDP and TCP mode SHALL be supported.

In all cases, the device SHALL support the transparent mode in case of Alpha ID = NULL or no Alpha ID.

The device SHALL also support several BIP channels, at least 2.

7.16 Launch browser command

It shall be possible either to launch the browser with the default URL or to provide a specific URL. Such URL can be either on the network or hosted locally in a SCWS. The key parameters that SHALL be supported are:

- Default URL support shall be supported
- Launch browser on a specific URL shall be supported
- No user confirmation step

Launch Browser SHALL also work correctly (still both with a remote or local server) when issued after a specific event or command. For example, it shall be possible to trigger a Toolkit application after a Call Control and use the Launch Browser command on local URL (SCWS) in the UICC.

8. Secure Element Access API & Access Control

In line with the growth in growth smartphones, mobile device application numbers are also increasing. Some applications leverage UICC access to provide additional services and/or security to the end-user. This is especially the case for mobile NFC, where device applications (like a wallet or transport UI) will interact with UICC applets, but applications intended to provide additional security (like Secure VoIP, strong authentication, etc.) may also leverage UICC applets. It is thus mandatory for OS platforms to provide access to UICC applets by supporting an API available for 3rd party developers (e.g. SIMalliance Open Mobile API).

This API will enable the interaction between device applications and the applets running in the UICC. The requirements are the same for all the mobile OS platforms, but the implementation and standards applicable may differ depending on the platform targeted.

The mandatory requirements for such API are:

- Allow sending APDU commands to UICC applications. It is not possible to provide high level APIs as the APDU used by specific applications may not be standardized. This is why a generic APDU access is mandatory
- Manage logical channels on the device to avoid any interference between UICC applications
- Forbid the use of the logical channel 0 which is reserved for the device's telecom application
- Send back any error code happening during the execution of command by a UICC applet. Error codes SHALL not be modified or grouped in a generic error
- Manage specific warning codes (such as 9F xx, 61 xx, 62 xx and 63 xx) coming from the UICC. Such warning codes SHALL never been considered as an error code by the device, nor replaced by another error code (like the 6F 00 error code). Note that the management may be different depending on the code but in all cases, the device SHALL either retrieve all the data from the UICC and deliver it to the application together with a correct execution code (90 00), or the device SHALL deliver the warning code back to the application without automatically issuing any further command. In this instance, it is then up to the application to retrieve the data
- Manage an access control policy that will restrict the access to a given UICC applet to explicitly authorized device applications only

For J2ME platform, the specifications applicable are:

- JSR-177 APDU package for the Secure Element Access API
- JSR-177 Access Control List (rules stored in a PKCS#15 file system)
- JSR-118 Recommended Security practice for MIDlet signing

For other Open OS platforms, the specifications applicable are:

- SIMalliance Open Mobile API
- GlobalPlatform Secure Element Access Control. The whole specification SHALL be implemented including the support of the ARA-M applet and as backward mechanism the support of the ARF file system (PKCS#15) if the ARA-M is not present in the UICC

9. NFC device implementation guidelines

This chapter provides more information on the features requested for a NFC device using a SWP-UICC.

Such a device is embedding the following components and main physical adaptations: a NFC controller connected to the UICC (CLF) coupled to a RF antenna integrated in the device, a connection between the UICC and the NFC controller (SWP line) and a standard ISO 7816 interface.

These NFC guidelines are split in two parts, a reminder of the functional requirements defined by the GSMA and a second part focused on deeper technical implementation guidelines.

9.1 GSMA requirements

The main requirements are described in the GSMA document "NFC Handset APIs & Requirements – version 3.0 October 2012" and are referenced in below table. For more information on the implementation, refer to the GSMA document.

Feature	GSMA document reference
Terminal shall support ISO/IEC 14443 RF type A & B	NFC Handset APIs & Requirements – chapter 7.1: NFC_REQ_08 to NFC_REQ_10 Compliancy with test specifications ISO 10373
Terminal shall support ETSI SWP & HCI	NFC Handset APIs & Requirements – chapter 7.1: NFC_REQ_20 to NFC_REQ_24 Compliancy with test specifications ETSI 102 694-1 & 102 695-1
Terminal shall support CLT mode	NFC Handset APIs & Requirements – chapter 7.1: NFC_REQ_19
Terminal shall support reader mode by UICC	NFC Handset APIs & Requirements – chapter 7.1: NFC_REQ_15 to NFC_REQ_17
Terminal shall provide a Secure Element Access API	NFC Handset APIs & Requirements: - chapter 7.2 for all devices; NFC_MOD-25 & NFC_MOD_26 - chapter 6.5 for Java devices; API_J2ME_01 to NFC_REQ_05 - chapter 7.3 for Open OS devices: API_REQ_27 to API_REQ_30
Terminal shall support Access Control for Secure Element Access API	NFC Handset APIs & Requirements – chapter 7.11: API_REQ_51, API_REQ_52, and UIApp_REQ_53
Terminal shall support reading NFC tags	NFC Handset APIs & Requirements – chapter 7.1: NFC_REQ_11 to NFC_REQ_14
Terminal shall support UI application triggering (HCI EVT_TRANSACTION)	NFC Handset APIs & Requirements – chapter 7.6: UIApp_REQ_33 & UIApp_REQ_34
Terminal shall support Bearer Independent Protocol	NFC Handset APIs & Requirements – chapter 7.7: RemMan_REQ_35 to RemMan_REQ_38

Terminal shall support Smart Card Web Server	NFC Handset APIs & Requirements – chapter 7.10: SCWS_REQ_50
Terminal shall be able to manage several SEs (one SE active at a time)	NFC Handset APIs & Requirements – chapter 7.9: MultiSE_REQ_46 to MultiSE_REQ_49
Terminal/CLF shall support both full power mode and low power mode (ETSI 102 613)	NFC Handset APIs & Requirements – Annex 3; item 2 & 3
Terminal/CLF shall both support a Windows size of 3 and 4 (ETSI 102 613)	NFC Handset APIs & Requirements – Annex 3; item 7 & 8
Terminal shall support proactive command ACTIVATE (ETSI 102 223)	NFC Handset APIs & Requirements – Annex 2
Terminal shall support proactive HCI connectivity event (ETSI 102 223)	NFC Handset APIs & Requirements – Annex 2

9.2 Additional requirements for NFC devices

To complete the GSMA document, this chapter details additional requirements and describes important recommendations for device implementation.

SWP interface & boot procedure

During the hardware boot procedure, some devices are powering the CLF which in turn powers the SWP UICC interface, starting the SWP activation.
In some cases, when the device software layers are initializing, the SWP line may be deactivated and then reactivated. This deactivation/reactivation can happen while the SWP protocol initialization is not fully completed (e.g. only some gates were opened by the UICC but not yet all the needed gates) thus leading to an incorrect initialization. Furthermore, there is no way to resume again a correct initialization until the next UICC boot (i.e. after the VCC is powered off and on again).

To ensure a correct SWP initialization, in case of a first activation with a full initialization (i.e. first boot of the device with a new SWP UICC), the device/CLF SHALL either:

- Wait to receive the SESSION_ID (SET_PARAMETER command) from the UICC and then EVT_HCI_END_of_OPERATION event
- Wait to receive the SESSION_ID (SET_PARAMETER command) from the UICC and then it is recommended to wait for at least 2 seconds without any activity on the SWP line before deactivating the line

To ensure a correct SWP initialization, in the case of a first activation with a light initialization (i.e. boot of the device with a known SWP UICC), the device/CLF SHALL either:

- Wait to receive the GET_SESSION_ID (GET_PARAMETER command) from the UICC and then EVT_HCI_END_of_OPERATION event
- Wait to receive the GET_SESSION_ID (GET_PARAMETER command) from the UICC and then it is recommended to wait for at least 2 seconds without any activity on the SWP line before deactivating the line

SWP interface deactivation

After a NFC transaction, the device or the CLF can decide to deactivate SWP line to limit the power consumption. However, only the NFC application and the UICC know whether a NFC transaction has ended, or if there is still processing to complete. The terminal shall thus only deactivate SWP protocol:

- After receiving a FIELD OFF information and the explicit notification from the UICC all processing is terminated through the standardized EVT_HCI_END_of_OPERATION event
- After receiving a FIELD OFF information and the expiration of a recommended time out set to a least 1s of inactivity on the SWP line if the UICC is not supporting the event EVT_HCI_END_of_OPERATION

SWP interface retry policy

In the case of a protocol error, an IFrame sent by the CLF over the SWP interface may not be acknowledged by the UICC (due to some other activities on UICC side). In order to improve the robustness of the NFC implementation and thus avoid NFC transaction errors, it is strongly recommended that CLF/device implements the support of a retransmission mechanism, supporting the retry/resend of the IFrame during at least 100 ms before deactivating the line.

SWP UICC detection (retry mechanism)

The ETSI SWP standard specifies that if a device is detecting that the UICC is not a SWP UICC, the SWP line shall be deactivated. This mechanism is important to save power if the CLF is not deactivating the SWP line and also to set the C6 pin at a ground level if the UICC is not SWP. UICC support of the SWP is indicated in the UICC ATR.

In the case of when the UICC has indicated SWP support and has already performed one successful initialization, it is highly recommended for the CLF to again activate the SWP line each time the device is entering a RF field, even if for any reason one of the next SWP activations is not successful.

This is mandatory to avoid waiting until the next device boot to do this check: end-users are rebooting their devices less and less. Thus, if an error occurs during one of the UICC activation, or if the UICC NFC feature was updated over the air, it will improve the user experience and the robustness of the NFC feature.

NFC parameters management

Legacy NFC infrastructures were designed to work with plastic cards or NFC tokens dedicated to a single card emulation application. Some of these NFC infrastructures are thus expecting to have the exact NFC parameters matching their specification (SAK, FWT, WTX, RF speed, etc.).
With mobile NFC, the device is able to manage multiple applications and to behave in different modes, for example both in card emulation mode and peer to peer mode.

If the NFC parameters provided by a UICC for a NFC application are overwritten by the device, they may be rejected by existing NFC infrastructures, blocking completely their use of the application. Such an issue was already faced in the field with contactless transportation readers when the device is supporting Peer to Peer mode and is thus overwriting the SAK value provided by the UICC application. The terminal and the CLF shall thus avoid overwriting NFC parameters set by the UICC.

SWP baud rate

NFC transactions, especially when considering access control or transport infrastructures, have very strong timing constraints. It is thus very important to optimize their performance whenever possible and to use a high baud rate in the communication between the CLF and the UICC. In several field cases, a higher baud rate will make the difference between a successful transaction and good user experience and a disappointing failure when using a NFC device.
It is strongly recommended to enable a SWP baud rate of at least 1Mb/s and it is mandatory to at least support 848Kb/s.

Power mode - battery assisted

The SWP specification defines two different power modes: the full power mode where the UICC is able to draw up to 10 mA on the SWP interface and the low power mode limiting the UICC power mode to 5 mA.

The objective of the low power mode is to enable NFC transaction while the CLF and UICC are only powered thanks to the RF magnetic field of a NFC reader. An important use case associated to the low power mode for Mobile NFC is the possibility for the end-user to exit from a transport system even if there is not enough energy to power the device.

In practice many devices are not implementing a real "power by the field" mode but are rather using a "battery assisted" mode. Even if there is no energy in the device battery to power the device CPU and screen, there is still enough energy to power the UICC/CLF system and perform many contactless transactions. In case of a battery assisted transaction, it is highly recommended to also enable the "full power" mode described in the ETSI SWP specification in order to improve the performance of the transaction and avoid issues with NFC readers that are too constraining on transaction timings, like some MIFARE readers. The impact on the battery is very limited (UICC will draw up to 10 mA instead of 5 mA for a couple of ms).

Note related to UICC application implementations: EMVCo AAUI specification (requirement B 3.1.18) is mandating the availability of the device screen to authorize the processing of a banking transaction. Some field implementations for banking applications are using the power mode as a way to detect the availability of the device's screen: if the UICC is in full power mode, the implementation assumes that the device screen is available, while if the UICC is in low power mode, the implementation assumes that the device screen is not available.

An extension of GlobalPlatform Amendment C API is currently under definition to provide a more reliable mechanism and it is strongly recommended that applications rely on this accurate mechanism to identify the availability of the screen rather than using the inappropriate power mode information.

Device RF ON/OFF

Most NFC devices have an option to activate/deactivate the NFC feature. When deactivating the NFC feature, the device is very often powering off the CLF or putting it in idle mode. The UICC remains powered on and able to process ISO commands on the contact interface.

To avoid any de-synchronization between the device/CLF and the UICC:

- When NFC feature is set to "OFF", the device SHALL not reset the CLF
- When NFC feature is set to "OFF", the CLF SHALL keep in its memory all the parameters of the current NFC initialization with the UICC
- When NFC feature is set to "ON", the CLF SHALL reactivate the SWP line

- If the device is booted while the NFC feature is set to "OFF", it SHALL anyway perform a SWP initialization during the boot

UICC NFC configuration update

The CLF SHALL accept an update of the UICC NFC parameters (ANY_SET_PARAMETER) command whenever the SWP line is active, including before and after a NFC transaction when entering or exiting the RF field. Due to timing constraints, these NFC parameters may only be effective for the next transaction.

Global NFC requirement

Except if stated explicitly in a specification, the device SHALL support all the NFC implementation guidelines for all NFC modes: Card Emulation mode, Reader mode and Peer to Peer mode (e.g. the device SHALL NOT implement a mechanism only for Card Emulation without supporting it also for Reader mode by UICC). It is for example the case for:

- HCI_EVT_TRANSACTION
- HCI_EVT_CONNECTIVITY
- Retry policy
- Overwriting of NFC UICC parameters

2G only SIM card & NFC

Contactless technology for UICC cards was defined in the ETSI specifications starting from the release 7. As a consequence, the standardization is well adapted for 2G/3G UICC and further releases but does not cover the case of SIM only cards.

In some cases, mobile network operators are deploying 2G/3G UICC but with specific settings which make the UICC appear as a 2G only SIM card. In this case, the device behavior is not specified and it will be the interpretation of the device manufacturers to decide to whether or not to use the NFC feature.

As stated in the ETSI SWP specification, ISO and SWP interfaces are independent. It is therefore recommended that the device SHALL activate the SWP following the ETSI TS 102 613 specification, whatever the telecom part is (i.e. whether the card is behaving as a SIM or as a USIM).

10. LTE device implementation guidelines

10.1 USIM interface for LTE

LTE authentication is based on the USIM authentication so E-UTRAN technology access SHALL only be granted by a USIM application. Additional features related to LTE data UICC management were added in the standard and are described below.

Extension of the USIM Service Table
The new service n°85 in the EF UST is used for the storage and use of the Evolved Packet System Mobility Management Parameters. It is made of two additional files present under ADF USIM. The device SHALL read the two files EF EPSLOCI and EF EPSNSC (described hereafter) during the USIM initialization and SHALL update them during a 3G session termination.

EPSLOCI (EPS location information):
This file is equivalent to the EPS for EF LOCI (CS domain) or EF PSLOCI (PS domain) files. It is updated by the mobile and holds the following EPS location information:

- Globally Unique Temporary Identifier (GUTI)
- Last visited registered Tracking Area Identity (TAI)
- EPS update status

EPSNSC (EPS NAS Security Context):
The device SHALL manage and update the file according to the last change requests of R8, R9 and R10 of the 3GPP 33.401 that specify the following behavior (extract):

"The full native EPS NAS security context (except for KNASenc and KNASint) shall be stored on the USIM (if the USIM supports EMM parameters storage) or in the non-volatile memory of the ME (if the USIM does not support EMM parameters storage) only during the process of transitioning to EMM-DEREGISTERED state or when an attempt to transition away from EMM-DEREGISTERED state fails, as described in clause 7.2.5. The ME shall under no other circumstances store the EPS NAS security context parameters on the USIM or non-volatile ME memory."

The device SHALL implement the following features:

- Service n°85 in the USIM Service Table (EF UST) which informs the device that the UICC is able to store the E-UTRAN Security Context
- Support the EF EPSLOCI file
- Support the EF EPSNSC (EPS NAS Security Context information) file

10.2 USIM toolkit enhancements

With LTE introduction several USIM Toolkit proactive commands and events have been improved or added to cater for this new technology. These new features allow the evolution of existing applications managing Roaming over network and technologies, access to new devices such as Femtocells and localization of the end user.

The device SHALL support the Toolkit application as described in the following specifications:

- Card Application Toolkit ETSI TS 102 223

- USIM Application Toolkit 3GPP TS 31.111
- CDMA Card Application Toolkit 3GPP2 C.S0035 (for CDMA devices)

This chapter describes the main evolutions and implementation guidelines for LTE and LTE/CDMA devices.

Terminal Profile

The device SHALL support the following new indications in the Terminal Profile command:

- E-UTRAN device capability for BIP services (class e supported) was defined by a specific bit into the ME Terminal Profile: bit 7 of the 17th byte
- Multiple Access Technologies supported in Event Access Technology Change and Provide Local Information command: bit 7 of the 25th byte
- Network Rejection Event:
  - bit 5 of the 25th byte for GERAN/UTRAN network
  - bit 7 of the 25th byte for E-UTRAN network
- CSG Cell Selection Event: bit 1 of the 26th byte
- Support of CSG cell discovery (if class "q" is supported) for the Provide Location Status command: bit 2 of the Thirty-first byte

Provide Local Information command for LTE

Several features of the Provide Local Information command were extended with E-UTRAN technology, including:

- Location information: the Cell Identifier for E-UTRAN is coded on 4 bytes instead of 2 bytes
- Cell ID Network measurement result extended to E-UTRAN
- Current access technology extended to E-UTRAN
- Access Technology integrating 3GPP/3GPP2 Interworking
  - Multiple Access Technologies (with the value "0E") is used to inform that a device is currently connected to several network radios
  - For Multiple Access Technology", the device SHALL include all access technologies effectively available (i.e. currently connected to) and not the list of technologies supported by the device
- Discovery of surrounding CSG cells

The Access Technology TLV of the Terminal Response of the command SHALL be coded as following:

- Tag for the Access Technology: '3F' or 'BF'
- Length: length of the following bytes
- Access Technologies currently available in the device

Set Up Event List

Several events were added or modified to match with new LTE network needs:

- Access Technology Change event has been improved to provide information on E-UTRAN radio network. It was also modified to manage and return several available radio technologies (multiple access technologies)
- Network Rejection Event has been added in the event list: the envelope is different from the GERAN/UTRAN network to the E-UTRAN
- CSG Cell Selection Event has been introduced to inform the UICC on leaving or entering into CSG cell coverage or detecting a change in the current CSG cell selection status

The device SHALL support implement the modifications needed to support the modified event and SHALL support the new events.

Call control by SIM
The device SHALL support and use the Service n°87 in the USIM Service Table (EF UST) related to the procedures and commands for Call control on EPS PDN connection by USIM are defined in 3GPP 31.111.

The device SHALL support Call control on EPS PDN connection by USIM (extension of Call control by USIM for LTE network). Before any EPS PDN connection activation, the device SHALL first pass the corresponding data to USIM.

Geographical Location Request
The device SHALL send geographical GPS information to the UICC providing the device has this capability. Otherwise the other types of geographical information available onto the device SHALL be sent. Geographical Location Request selection mode can be defined as Automatic, Semi-Automatic or Manual.

10.3 LTE Access Technology for network selection management

The "(U)SIM Services; Network files management" chapter of this document specifies how the device SHALL manage the files related to network selection.
Within the context of LTE devices, the device SHALL support the LTE access technology in the EF PLMNwAct, EF OPLMNwAct and EF HPLMNwAct files.

10.4 Bearer Independent Protocol

In LTE, the Bearer Independent Protocol (BIP) will be the data communication pipe over TCP (and UDP) to enable UICC applications communication with OTA servers using RAM over HTTPS. In order to have transparent behavior, transparent mode shall be supported when Alpha ID = NULL. When there is no Alpha ID, transparent mode should be applied by default.

Bearer Type eUTRAN SHALL be supported in addition to legacy modes (GPRS, UTRAN, etc…)

10.5 3GPP/3GPP2 Interworking (for LTE/CDMA devices)

3GPP2 mobile network operators launching LTE networks require having LTE and CDMA network-capable devices. Such devices SHALL support the CSIM application and SHALL also support the selection of the network technology based on multi mode device detection and system selection.

CSIM Application
The CSIM application is a Network Access Application similar to the USIM hosted by the UICC providing access to CDMA2000/EVDO networks. The CSIM application supplies an extensive list of features and functionalities required by the smartcard to operate independently on legacy CDMA and EVDO networks. The following list provides an overview of the features supported:

- Roaming, SID/NID Lists
- Algorithms such as CAVE, Diffie-Hellman, MD5, etc.

- OTA mechanisms
- Akey and SSD (Shared Secret Data)
- AKA related functionalities
- Broadcast and MMS
- Simple IP, Mobile IP and HRPD functions
- Location Control Services

CSIM File System

The following files are included in the CSIM file system:

- EF LI; Language Indication
- EF SMS; Short Messages
- EF SMSP; Short Messages Services Parameters
- EF SSFC; Supplementary Services Features Code Table
- EF SPN; CDMA Home Service Provider Home Name
- EF MDN; Mobile Directory Number
- EF PUZL; Preferred User Zone List
- EF HRPDCAP; HRPD Access Authentication Capability Parameters
- EF HRPDUPP; HRPD Access Authentication User Profile Parameters
- EF CSSPR; Current SSPR P Rev
- EF EPRL; Extended Preferred Roaming List
- EF 3GCIK; 3G Cipher and Integrity Keys
- EF ICI; Incoming Call Information
- EF OCI; Outgoing Call Information

Multi Mode Device Detection and 3GPP/3GPP2 System Selection

UICC parameters take precedence over those present in the device. When multiple systems are available, multi mode device SHALL be able to automatically select the preferred system thanks to the information available in the DF MMSS (Multi Mode and System Selection) described below:

- EF MLPL (MMSS Location Associated Priority List) holding the list of grouping based on location specific information. PLML allows the base station to specify the MSPL to be used in a location grouping
- EF MSPL (MMSS System Priority List) holding the list of prioritized cellular systems that assist the device in the selection process
- EF MMSSMODE (MMSS Mode Settings) defining the selection mode: Automatic, Semi-Automatic or Manual

The device SHALL support:

- CSIM as specified in 3GPP2 C.S0065-B
- OTASP/PA stack to interact with CSIM for PRL and NAM parameters download as described in 3GPP2 C.S0016-D
- CSIM file system, including all mandatory fields and procedures as well as the optional fields and associated procedures described above in the CSIM File System part
- Multi Mode Device Detection and 3GPP/3GPP2 System Selection

10.6 Home eNodeB (HeNB) provisioning

The 3GPP 31.102 specifies the storage of user H(e)NB parameters in the UICC (release 8) and the storage of operator H(e)NB parameters (release 9). UICC information takes precedence over the information stored in the device.

The USIM Service Table (UST) was extended to indicate the presence of these new services and a new DF, DF HNB (Home eNodeB) was created under the ADF USIM to store these new parameters:

- LTE Home eNodeB: Service n°86 in the EF UST is used for "Allowed Closed-Subscriber-Group Lists as well as the following files under the DF HNB: EF ACSGL (Allowed CSG List), EF CSGI (CSG Indication), EF HNBN (Home eNodeB Name)
- LTE operator Home eNodeB: Service n°90 in the EF UST is used for "Operator CSG List and corresponding indications" as well as the following files under the DF HNB: EF OCSGL (Operator CSG List), EF OCSGT (Operator CSG Type), EF OHNBN (Operator Home eNodeB Name)

The device SHALL support and use these new services and associated EF files in the UICC if available.

11. ISIM (IMS Network Access)

New high bandwidth networks (LTE, HSDPA+, etc.) allow deploying new services (like VoIP, video streaming, etc.) using web-based applications. IMS is the most convenient way to deploy, get access to, maintain and control these applications in an interoperable way.

The 3GPP 31.103 & 31.101 specifications define the ISIM application on UICC for access to IMS services. The ISIM application is requested by many mobile network operators to manage securely data over IP and the authentication to IMS network.

The ISIM support in a device is based on the features described hereafter.

ISIM File System

The ISIM application has a dedicated file system made of several EF files:

- EF IMPI (IMS private user identity) holding the private user identity of the user
- EF IMPU (IMS public user identity) holding one or more public user identity of the user. The device SHALL support at least 10 records (i.e. 10 public identities)
- EF Domain (Home Network Domain Name) holding the home operator's network domain name
- EF AD describing the mode of operation (normal, type approval …)
- EF ARR holding the access rules for files located under the ISIM ADF
- EF P-CSCF (P-CSCF Address): for non 3GPP devices, not able the get the IMS proxy address from the access network procedures (GRPS PDP context activation or DHCP)
- EF GBABP (GBA Bootstrapping parameters) file in the ISIM, holding the AKA random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure
- EF GBANL (GBA NAF List) file in the ISIM, holding the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure
- EF NAFKCA (NAF Key Center Address) holding one or more NAF Key Center Addresses

ISIM Service Table

The ISIM Service Table (EF IST under ADF ISIM) is used to specify the support of different services by the ISIM application:

- Service n°1: P-CSCF @
- Service n°2: Generic Bootstrapping Architecture (GBA)
- Service n°3: HTTP Digest
- Service n°4: GBA-based Local Key Establishment Mechanism
- Service n°5: Support of P-CSCF discovery for IMS Local Break Out. A 3gPP device can now use EFP-CSCF in case of IMS local break out

ISIM authentication

The ISIM application supports different authentication methods, as described below:

- Mutual Authenticate 3G in IMS context; ISIM performs a AKA scheme to access IMS services
- Mutual Authenticate in GBA (Bootstrapping mode) security context; ISIM performs a dedicated AKA for GBA
- Mutual Authenticate in GBA (NAF derivation) security context; ISIM derives results of the bootstrap using IMPI value

- Mutual Authentication HTTP Digest security context; ISIM furnishes response/session key to a realm/nonce/cnonce challenge according RFC2617
- Mutual Authenticate with security context Local Key Establishment (Key derivation mode)" and "(Key availability check mode)" for GBA new key establishment procedure

The device SHALL implement the following features (as described above):

- Support of the ADF ISIM
- Support the ISIM Service Table (EF IST) and associated services
- Support of the ISIM files
- Support of the different authentication methods
- Be able to work with distinct ISIM application (a UICC can hold several ISIM applications)

12. Extended Authentication Protocol (EAP)

EAP (Extensible Authentication Protocol) is a framework for transporting authentication protocols suitable for identifying mobile subscribers over IP networks (ADSL and Wi-Fi).

ETSI 102 310 specifies how the device shall implement the EAP mechanism and retrieve the information from the UICC:

- A UICC application can provide one or more EAP clients
- A UICC EAP client implements one specific EAP method

The device SHALL:

- Use the information in the EF DIR file to present the list of EAP-capable applications to the end-user or to any application needing an EAP authentication according to ETSI 102 310
- Implement EAP AKA according to 3GPP 33.234
- Implement EAP SIM if the device is only using GSM network technology

13. Generic Bootstrapping Architecture (GBA)

Generic Bootstrapping Architecture (GBA) enables the authentication of a user with a valid identity on a Home Location Register (HLR) or a Home Subscriber Server (HSS). The user authentication is instantiated by a shared secret between the Smart Card inserted in the mobile device and the HLR/HSS. The network is checking that the UICC answer to the authentication request is the same as the one computed by the HLR/HSS component.

The 3GPP 33.220 specification describes the features needed on the device to enable Generic Bootstrapping Architecture from UICC.

The device SHALL implement the following features:

- Service n°68 in the USIM Service Table (EF UST)
- Support the EF GBABP (GBA Bootstrapping parameters) file in the UICC. This EF contains the AKA random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure
- Support the EF GBANL (GBA NAF List) file in the UICC. This EF contains the list of NAF_ID and B-TID associated to a GBA NAF derivation procedure
- If the device supports ISIM applications, the device SHALL also be able to manage the security contexts described in 3GPP 31.103: IMS AKA, HTTP Digest, GBA

14. I-WLAN

Wireless LAN may interact with LTE as an untrusted non 3GPP network. In this case, the following guidelines regarding files structure and Card application toolkit commands are applicable.

USIM Service Table

DF WLAN shall be present at the ADF USIM level if either of the services nº59, nº60, nº61, nº62, nº63, nº66, n°81, n°82, n°83, n°84 or n°88 are "available" in the corresponding EF UST (USIM Service Table)

I-WLAN File System

The file system is made of several EF files:

- EF Pseudo: Pseudonym
- EF UPLMNWLAN: User Controlled PLMN Selector for WLAN Access
- EF OPLMNWLAN: Operator Controlled PLMN Selector for WLAN Access
- EF UWSIDL: User Controlled WLAN Specific identifier List
- EF OWSIDL: Operator Controlled WLAN Specific identifier List
- EF WRI: WLAN Re-authentication Identity
- EF HWSIDL: Home I-WLAN Specific Identifier List
- EF WEHPLMNPI: I-WLAN Equivalent HPLMN Presentation Indication
- EF WHPI: I-WLAN HPLMN Priority Indication
- EF WLRPLMN: I-WLAN Last Registered PLMN
- EF HPLMNDAI: HPLMN Direct Access Indicator

Card Application Toolkit extension

The following extensions are needed:

- Terminal Profile
  - » Event I-WLAN Access Status: bit 4 of the Twenty-fifth byte
  - » Provide Local Information with WISD of the current I-WLAN: bit 2 of the Thirtieth byte
  - » Refresh Steering of Roaming for I-WLAN: bit 8 of the Thirtieth byte
- Set Up Event List
  - » I-WLAN Access Status event is introduced for I-WLAN.
  - » EVENT DOWNLOAD FRAMES INFORMATION CHANGED
- BIP – Open Channel
  - » Support of I-WLAN bearer
- REFRESH command
  - » "Steering of Roaming for I-WLAN" REFRESH.
- Provide Local Information
  - » Current WSID is defined: I-WLAN Identifier shall be retrieved

The device SHALL implement the following features (as described above):

- Support of the DF WLAN
- Support of the I-WLAN files
- Support of services associated with WLAN in the USIM Service Table
- Support of the additional qualifiers and parameters for Card Application Toolkit

15. Terminal applications launched from the UICC

ETSI 102 223 class "k" specifies a new BIP mode – Terminal in server mode – allowing the UICC to launch a registered device applications. This feature provides an interesting continuity of service for mobile network operators which are able to perform remote administration activities on the UICC side and, if needed, can trigger a device application.

Terminal application types:

- '00': e-mail application
- '01': synchronization application other than '09'
- '02': network monitoring application
- '03': video streaming application
- '04': audio streaming application
- '05': game application
- '06': browsing application
- '07': device management application as per OMA Device Management V1.2 specifications
- '08': device management application other than '07'
- '09': data synchronization application as per OMA Data Synchronization V1.2.1 specifications

16. Smart Card Web Server

The Smart Card Web Server (SCWS) provides a user friendly technical solution to offer value added services based on the UICC. The SCWS relies on browser technologies and re-uses the browser functionality of the device to enable UICC applications to interact with the user. This enables UICC based applications to be presented in a rich graphical and user friendly environment.

The requirements to support the Smart Card Web Server include:

- Devices SHALL support BIP – UICC in TCP Server mode and Client mode "class e" as specified in the ETSI 102 223
- Device SHALL support at least 4 BIP channels (different than logical channels), 1 for the local communication and 3 additional channels used dynamically for remote management
- Device SHALL support the Access Control Policy Enforcer defined in the OMA TS Smart Card Web Server v1.2

17. High Speed Protocol (HSP)

The High Speed Protocol "USB-IC" is defined in ETSI TS 102 600. It removes the speed limitation of the ISO 7816 interface to improve the communication speed with the UICC, especially for SCWS or high density memory use cases in the UICC. Three classes are defined for USB-IC to address:

- ICCD (Integrate Circuit Card Devices): required for standard APDU exchange with the UICC
- EEM (Ethernet Emulation Mode): Required for SCWS support and to provide remote connectivity to the UICC over HTTP(s) protocol for administrative purposes (SCWS, large files management or application management)
- Mass Storage: Required to access the high density memory in the UICC. Through this class, the UICC will be recognized by the device as a USB memory token.

The EF NCP-IP file holds the network activation parameters to be used by the device for establishing a data channel for UICC remote IP connectivity, using High Speed Protocol (ETSI TS 102 483). The device SHALL read this file during boot sequence.

The device SHALL support the 3 classes described above as well as the EF NCP-IP file in the UICC.