Open Market Handsets (OMH) Device Specification

CDG Document 167

Version 3.0

July 2010

CDMA Development Group
575 Anton Boulevard, Suite 560
Costa Mesa, California 92626
PHONE +1 888 800-CDMA
+1 714 545-5211
FAX +1 714 545-4601
http://www.cdg.org
cdg@cdg.org

<page left blank intentionally>

Contents

1. Introduction 1
2. R-UIM Compatibility 3
2.1 OMH Device Using a Legacy R-UIM (D1) 4
3. Mechanisms 5
3.1 R-UIM Commands (D5) 5
3.2 Subsidy Lock (D10) 5
3.3 Carrier Customization (D15) 5
3.4 CDMA Card Application Toolkit (D20) 6
3.5 Device and Model Identification (D25) 10
3.6 Over-the-Air (OTA) Provisioning and Firmware 10
3.6.1 CCAT / UTK Data Download (D30) 10
3.6.2 OTASP / OTAPA (D35) 11
3.7 Root Certificates (D40) 11
3.8 Configuration Data Sources (D45) 11
3.9 cdma2000 (D50) 12
4. Voice (D55) 13
4.1 General and R-UIM 13
4.2 Protocols 14
5. SMS (D60) 17
5.1 General and R-UIM 17
5.2 Protocols 17
6. 3G Packet Data (D65) 21
6.1 General and R-UIM 21
6.2 Multiple Profiles 22
6.3 Protocols 22
7. HRPD (1xEV-DO) (D70) 25
7.1 General and R-UIM 25
7.2 Protocols 25
7.3 HRPD Rev A Specific 26

7.4 1x and HRPD Interworking 26
8. WAP Browser (D75) 29
8.1 General, R-UIM, and User Interface (UI) 29
8.2 Protocols 30
8.3 Download 31
8.4 Media 32
9. MMS (D80) 35
9.1 General, R-UIM, and UI 35
9.2 Protocols 36
9.3 Media Types 38
10. Java (D85) 43
11. BREW (D90) 45
12. LBS (D95) 47
13. Mapping of Requirements to Acceptance Testing [Informative] 49
14. Terminology 53
15. References 57
16. Appendix: MEID/EUIMID Support 63
16.1 Overview 63
16.2 MEID 63
16.3 EUIMID 64
16.3.1 Long Form EUIMID (LF_EUIMID) 64
16.4 Short Form EUIMID (SF_EUIMID) 65
16.5 Network Support of MEID/EUIMID 65
16.6 OTASP Systems and MEID/EUIMID 67
17. Appendix: Concatenated PRL Usage 69
17.1 Overview 69
17.2 cPRL Format and Parsing 70

Tables

Table 2-1 Device and R-UIM Compatibility Matrix [Informative] 3
Table 13-1 Mapping of Requirements to Acceptance Test Plans 49

Revision History

Date	Version	Description
Jan. 2008	1.0	Initial release version; included in OMH Enabler Package v1
May 2008	2.0	Updated R-UIM Compatibility requirements Updated carrier customization requirements Clarified CCAT and SMS-PP download requirements Clarified usage of Device Model on the R-UIM by the network Clarified sources of configuration data: R-UIM, device or user inputs Clarified emergency number handling Recommended network support of SO68 4GV-NB for voice services Updated SMS requirements for usage of access channel and traffic channel Updated requirements of Broadcast SMS and Flash SMS Updated Long SMS and EMS requirements Clarified that Simple IP authentication algorithm fields on the R-UIM will be ignored by the device Added requirement of multiple user profiles for 3GPD Clarified optional 3GPD requirements for low-end devices Added special 3GPD requirements for LBS Updated User Agent Profiles for WAP/Browser Clarified HTTP implementation of MMS Updated BREW requirements Updated LBS requirements Added reference [OWPVC] Editorial changes Included in OMH Enabler Package v2

Date	Version	Description
July 2010	3.0	Separated the network requirements into a new document CDG197 so that this document (CDG167) only contains the device requirements Added the new requirement numbering system so that each requirement has a requirement number for easy referencing Added OMH logo to the cover page and first page of each chapter Changed “Open Market Handset” to “Open Market Handsets” Changed requirement to inform user to upgrade their legacy card as optional Added encoding requirement to service provider name, application labels and device model Expanded requirements for CCAT Added cdma2000 requirements including cPRL Updated voice requirements for supplementary services Updated SMS requirements to make some requirements optional Updated 3GPD requirements for multiple profiles so that SIP and MIP share the same profile extension information Added information on the behavior of data dormant timers Expanded HRPD requirements Added optional requirement on bookmark saving Clarified requirements for WAP download and media types Added requirements on MMS User Preferences Added requirements on MMS Notifications Updated MMS media types Clarified BREW requirements Clarified LBS requirements Added a mapping table to map device requirements to device test plans for information purpose Updated information for EVDO HardwareID and MEID Added an appendix on cPRL usage Editorial changes

1. Introduction

The Open Market Handsets (OMH) initiative is a strategic effort to benefit the CDMA ecosystem by enabling open distribution of devices across networks and regions by expanding Removable User Identity Module (R-UIM) capabilities to support a full set of competitive features and standardizing a uniform device implementation for each feature.

The R-UIM-enabled OMH feature set includes support for the following:

- Voice Services and Device Operation
- Short Message Service (SMS)
- 3G Packet Data (3GPD)
- Wireless Application Protocol (WAP) Browser
- Multimedia Message Service (MMS)
- Java
- Binary Runtime Environment for Wireless (BREW)
- Applications residing on OMH R-UIMs
- High Rate Packet Data (HRPD) (1xEV-DO)
- Location Based Services (LBS)

This document contains the requirements for OMH devices. Each requirement has a requirement number in this format: **Dn-m**, where **D** represents the device, **n** represents the feature set or functional area and **m** represents the requirement number within that feature set or functional area. These requirements are also formatted in blue, as an aid to the reader.

1

2 <page left blank intentionally>

2. R-UIM Compatibility

The following table provides a high-level view of behavior for different combinations of OMH- and non-OMH-compliant R-UIMs and devices.

Table 2-1 Device and R-UIM Compatibility Matrix [Informative]

User Puts…	Into...	Result
Legacy RUIM[1]	Legacy Device[2]	Existing behavior, i.e., Voice and SMS based on provisioning in the RUIM and all other features based on provisioning in the device.
OMH R-UIM	Legacy Device	Same as above.
Legacy R-UIM	OMH Device	Voice and SMS based on provisioning in the R-UIM. User may need to upgrade the R-UIM to access data services.
OMH R-UIM	OMH Device	Voice, SMS, data, and OMH enabled features based on provisioning in the R-UIM.

Legacy devices operate exactly the same with OMH and legacy R-UIMs, since the software in these devices is not aware of the additional capabilities of the R-UIM.

OMH devices used with legacy R-UIMs will support voice, SMS, and tethered-mode data calls. To access other data services, subscribers with OMH devices may need to upgrade their legacy R-UIMs.

OMH devices used with OMH R-UIMs allow subscribers to access the full set of data-oriented, OMH-enabled features supported by the device and network, with all of these features enabled by configuration data residing in the R-UIM.

[1] If an R-UIM is based on a 3GPP2 R-UIM specification version prior to C.S0023-D, it is referred to as a legacy R-UIM.

[2] If a device does not support C.S0023-D R-UIM, it is a legacy device.

2.1 OMH Device Using a Legacy R-UIM (D1)

D1-1 When a legacy R-UIM is inserted into an OMH device, the device should inform the user that he/she needs to upgrade the R-UIM in order to obtain data services.

D1-5 If the device informs the user when a legacy R-UIM is inserted into an OMH device, the device should detect the insertion of the same legacy card that was last inserted so that it does not need to prompt the user again.

D1-10 When a legacy R-UIM is used in an OMH device and the user attempts to access any type of data service, the device ***shall*** inform the user that he/she needs to upgrade the R-UIM to an OMH R-UIM in order to obtain data services.

D1-15 If an OMH device informs the user to upgrade the R-UIM when a legacy R-UIM is used, the device ***shall*** keep the display text on the screen until the user acknowledges it.

D1-20 When a legacy R-UIM is inserted into an OMH device, the device ***shall*** still support voice calls.

D1-25 When a legacy R-UIM is inserted into an OMH device, the device ***shall*** still support SMS.

D1-30 When an OMH device using a legacy card sets up a tethered data call using Password Authentication Protocol (PAP) authentication in Relay Model, it ***shall*** perform PAP authentication using credentials from the terminal.[3]

D1-35 When an OMH device using a legacy card sets up a tethered data call using PAP authentication in Network Model, it ***shall*** perform PAP authentication using credentials from the terminal.

D1-40 When an OMH device using a legacy card sets up a tethered data call using the Challenge Handshaking Authentication Protocol (CHAP) authentication in Relay Model, it ***shall*** perform CHAP authentication using credentials from the terminal.

D1-45 When an OMH device using a legacy card sets up a tethered data call using CHAP authentication in Network Model, it ***shall*** perform CHAP authentication using credentials from the terminal.

[3] In this document, Terminal means a laptop or some other computing device that is connected to the OMH device in tethered mode.

3. Mechanisms

3.1 R-UIM Commands (D5)

D5-1 The device ***shall*** support all the R-UIM commands, as defined in [CDG166].

D5-5 The device ***shall*** support the security-related R-UIM commands identified in the *R-UIM Commands* section of [CDG166].

3.2 Subsidy Lock (D10)

OMH devices are designed to be open devices that do not contain any operator-specific information so that they may be used in multiple networks. Because subsidy lock mechanisms inherently require devices to maintain operator-specific information to enforce personalization (e.g., table of IMSI_M or IMSI_T ranges belonging to that operator), a subsidy locked OMH device would no longer be considered an OMH device.

If an operator desires to subsidize a particular OMH device, they could do so by working with the device Original Equipment Manufacturer (OEM) to implement their desired personalization mechanism on the device. At that point, however, it would no longer be considered an OMH device.

D10-1 The device ***shall not*** have subsidy locks.

3.3 Carrier Customization (D15)

D15-1 If the service provider name is provisioned in EF_{SPN} on the R-UIM, the device ***shall*** display that information on the idle screen.

D15-5 The device ***shall*** support decoding of the following encoding types defined in [CR1001] for the character string data present in EF_{SPN}:

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters[4]
- "Unicode"[5]

[4] The characters are encoded the same way when the encoding type is Octet, Unspecified, or 7-bit ASCII.

[5] Per Clause D98, Section 3.10 "Unicode Encoding Schemes" in [UNICODE], if BOM (byte order mark) is not present, the bytes for each character are in big-endian order. Otherwise, BOM indicates the byte order explicitly.

D15-10 If an application label has been provisioned for a particular application in $EF_{AppLabels}$, the device's user interface ***shall*** display this text label with the associated icon or menu item used to launch that application (e.g., "Content World").

D15-15 The device ***shall*** support decoding of the following encoding types defined in [CR1001] for the character string data present in $EF_{AppLables}$ (see footnotes in **D15-5** for notes on encoding):

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters[6]
- "Unicode"

D15-20 If an application label has not been provisioned for a particular application in $EF_{AppLabels}$, the device's default label ***shall*** be displayed (e.g., "MMS").

3.4 CDMA Card Application Toolkit (D20)

The CDMA Card Application Toolkit (CCAT) provides the interface between the device and the R-UIM. CCAT is defined in [CS0035]. The intention of the following CCAT requirements is to provide sufficient CCAT support to enable operators to provision lightweight applications (e.g., wireless banking, personal information collection for pre-paid subscribers, tracking of device ID and model information, etc.) that run on the R-UIM card.

D20-1 The device ***shall*** provide an icon and/or a menu item for the user to select so that the user will be able to access the CCAT menus from the applications on the R-UIM.

D20-5 The device ***shall not*** provide users with the ability to block outgoing SMS messages initiated by a CCAT SEND SHORT MESSAGE proactive command.[7]

D20-10 The device ***shall*** support SET UP MENU and MENU SELECTION, without Help Request, Replace Menu, and Remove Menu, and with next action indicators "Send SM," "Set Up Call," "Launch Browser," and "Provide Local Information."

D20-15 The device ***shall*** support SET UP MENU, allowing Large Menu with many items, with large items, or with Large Alpha Identifier.

D20-20 The device ***shall*** support SET UP MENU with soft keys.

D20-25 The device ***shall*** support DISPLAY TEXT with the following parameters and scenarios:

- Normal priority, Unpacked 8 bit data for Text String
- Normal priority, Unpacked 8 bit data for Text String, screen busy

[6] The characters are encoded the same way when the encoding type is Octet, Unspecified or 7-bit ASCII.

[7] CCAT applications on the R-UIM using SEND SHORT MESSAGE would have been approved and loaded on the R-UIM by the operator.

- High priority, Unpacked 8 bit data for Text String
- Packed, SMS default alphabet
- Clear message after delay
- Text string with 160 bytes
- Backward move in card session
- Session terminated by user
- Icon and text to be displayed, no text string given, not understood by the device
- No response from user
- Display of the extension text
- Variable timeout

D20-30 The device ***shall*** support GET INPUT with the following parameters and scenarios:

- Digits only, SMS default alphabet, device to echo text, device supporting 8 bit data Message
- Digits only, SMS default alphabet, device to echo text, packing SMS Point-to-point required by device
- Character set, SMS Default Alphabet, device to echo text, device supporting 8 bit data Message
- Digits only, SMS default alphabet, device to hide text, device supporting 8 bit data Message
- Backwards move
- Abort
- Null length for the text string
- No response from the user
- Default text for the input
- Default text for the input with max length

D20-35 The device ***shall*** support MORE TIME.

D20-40 The device ***shall*** support POLL INTERVAL.

D20-45 The device ***shall*** support PROVIDE LOCAL INFORMATION with Language Setting.

D20-50 The device should support PROVIDE LOCAL INFORMATION with Battery State.

D20-55 The device ***shall*** support REFRESH with the following parameters and scenarios:

- Card Initialization and File Change Notification
- Card Reset
- Card reset after Short Message Service Point to Point (SMS-PP) data download

D20-60 The device ***shall*** support SELECT ITEM with the following parameters and scenarios:

- Mandatory features
- Large menu
- Backward move by user
- Default item
- No response from user
- Soft keys

D20-65 The device ***shall*** support TERMINAL PROFILE.

D20-70 The device ***shall*** support SEND SHORT MESSAGE with the following parameters and scenarios:

- Packing not required, 8-bit data
- Packing required, 8-bit data
- Packing not required, SMS default alphabet
- Alpha identifier length '00', packing not required, 8-bit data
- Packing not required, 8-bit data, no alpha identifier

D20-75 The device ***shall*** support SET UP CALL with the following parameters and scenarios:

- Call confirmed by the user and connected
- Call rejected by the user

D20-80 The device should support GET INKEY with the following parameters and scenarios:

- Digits only for character, Unpacked 8 bit data for Text String
- Digits only for character set, SMS default Alphabet for Text String
- Backward move
- Abort
- SMS default alphabet for character set, Unpacked 8 bit data for Text String
- Max length for the Text String
- No response from the user
- Help information available
- Variable timeout

D20-85 The device should support TIMER MANAGEMENT with the following parameters and scenarios:

- Start a timer several times, get the current value of the timer, and deactivate the timer
- Try to get the current value of a timer that is not started: action in contradiction with the current timer state

- Try to deactivate a timer which is not started: action in contradiction with the current timer state
- Start all 8 timers

D20-90 The device should support TIMER EXPIRATION with the following parameters and scenarios:

- Pending proactive command
- Card application toolkit busy

D20-95 The device should support EVENT DOWNLOAD – IDLE SCREEN AVAILABLE.

D20-100 The device should support POLLING OFF.

D20-105 The device should support SET UP EVENT LIST with the following parameters and scenarios:

- Set Up Call Connect Event
- Replace Event
- Remove Event
- Remove Event on ME Power Cycle

D20-110 The device should support SET UP IDLE MODE TEXT with the following parameters and scenarios:

- Display idle mode text
- Replace idle mode text
- Remove idle mode text
- Competing information on device display
- Device power cycled
- REFRESH with card Initialization

D20-115 The device should support EVENT DOWNLOAD with the following parameters and scenarios:

- Browser termination
- CALL CONNECTED [Mobile Terminated (MT) and Mobile Originated (MO)]
- CALL CONNECTED, Device supporting SET UP CALL
- CALL DISCONNECTED
- MT Call event

D20-120 The device should support LAUNCH BROWSER with the following parameters and scenarios:

- Connect to the default URL
- Connect to the specified URL, alpha identifier length=0
- Browser identity, no alpha identifier
- Use the existing browser, connect to the default URL

- Close the existing browser session and launch new browser session, connect to the default URL
- If not already launched

3.5 Device and Model Identification (D25)

Device identification refers to the Electronic Serial Number/Mobile Equipment Identifier (ESN/MEID) of the device and the UIM Identifier/Expanded UIM Identifier (UIMID/EUIMID) of the card. Requirements are provided below for the device, but more detailed information regarding OMH and device identification can be found in the *Appendix: MEID/EUIMID Support* section of this document.

In addition to device identification information, requirements are also provided below for storing the model information of the device on the R-UIM.

D25-1 The device ***shall*** support MEID.[8]

D25-5 The device ***shall*** be provisioned with a properly formed MEID.

D25-10 The device ***shall*** be provisioned with an ESN containing the pESN value derived from the device's MEID.

D25-15 If service n8 (SF_EUIMID-based EUIMID) is activated in EF_{CST} (CDMA Service Table), the device ***shall*** use EF_{USGIND} (Usage Indicator) to determine whether to use the Short Form Expanded UIM Identifier (SF_EUMID) or MEID for network identification, as defined in [CDG166].

D25-20 Just as the device writes its ESN/MEID to the R-UIM during power-up, it ***shall*** also write its manufacturer information, model information, and software version information to EF_{Model} on the R-UIM.

D25-25 The device ***shall*** support the following encoding types defined in [CR1001] for the character string data present in EF_{Model} (see footnotes in **D15-5** for notes on encoding):

- "Octet, unspecified": Containing unpacked ASCII characters
- "7-bit ASCII": Containing unpacked ASCII characters
- "Unicode"

3.6 Over-the-Air (OTA) Provisioning and Firmware

3.6.1 CCAT / UTK Data Download (D30)

D30-1 The device ***shall*** support the CCAT SMS-PP data download mechanism as defined in [CS0035].

D30-5 The device ***shall*** support the UIM Toolkit (UTK) SMS-PP data download mechanism.[9]

[8] MEID is still required when Short Form EUIMID (SF_EUIMID) is used for device identification by the network.

3.6.2 OTASP / OTAPA (D35)

Since OMH R-UIMs are expected to be provisioned with all necessary information before reaching the subscriber, OTA provisioning mechanisms are generally only needed to modify provisioning information on R-UIMs already in the field.

Note: While current OTASP/OTAPA functionality defined in 3GPP2 [CS0016] is maintained, OMH does not extend OTASP/OTAPA functionality to support new Elementary Files (EFs) defined in [CDG166].

D35-1 The device ***shall*** support OTASP/OTAPA commands identified in the *R-UIM Commands* section of [CDG166] to support existing OTASP/OTAPA systems.

D35-5 The device ***shall*** support the download of Concatenated Preferred Roaming List (cPRL) over OTASP/OTAPA.

3.7 Root Certificates (D40)

D40-1 If the operator has provisioned root certificates on the R-UIM, the device ***shall*** use these certificates in addition to default certificates present on the device. For details, see the *EF_{RC} (Root Certificates)* section of [CDG166].

3.8 Configuration Data Sources (D45)

When an operator introduces a new OMH data service, configuration data for this new service may not yet be provisioned in OMH R-UIMs already being used by subscribers. In order to update these deployed R-UIMs, operators would ideally use an OTA provisioning technique to update these data. However, recognizing that not all operators have deployed such techniques, OMH devices provide an option for users to manually enter configuration data, such as server addresses.

D45-1 Manual entry of configuration data may be supported for:

- WAP Browser
- MMS
- Java
- LBS

D45-5 Manual entry of configuration data ***shall not*** be supported for:

- Voice
- SMS

[9] Rather than using the Card Application Toolkit Protocol Teleservice (CATPT) teleservice ID, as is done with the CCAT version of SMS-PP data download, the UTK version uses the regular SMS teleservice ID and sets the message display mode to indicate that the message is a data download. Supporting this mechanism on the device essentially means that the device must look at the message display mode of received SMS messages to determine whether they should be displayed before passing them to the R-UIM. Otherwise, the mechanism is basically between the network server and the R-UIM.

- 3GPD
- HRPD
- BREW

D45-10 If manually entered configuration data is supported, it ***shall*** be stored locally on the device to protect the integrity of the R-UIM.

3.9 cdma2000 (D50)

D50-1 The device ***shall*** support cdma2000 Release 0 as defined in [CS0001], [CS0002], [CS0003], [CS0004], and [CS0005].

D50-5 The device may support cdma2000 releases after Release 0.

D50-10 The device ***shall*** satisfy the conformance requirements defined in [CS0031].

D50-15 The device ***shall*** satisfy the performance requirements defined in [CS0011].

D50-20 The device ***shall*** support cPRL stored in EF_{PRL} on the R-UIM.

D50-25 The device should support Enhanced PRL stored in EF_{PRL} on the R-UIM.

4. Voice (D55)

4.1 General and R-UIM

D55-1 Voice services on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the *Basic Voice Services and Device Operation* section of [CDG166].

D55-5 The device should support Abbreviated Dialing Numbers (i.e., phonebook) stored on the R-UIM.

D55-10 The device may support Fixed Dialing Numbers stored on the R-UIM.

D55-15 The device should have the capability to store and retrieve internationally formatted numbers to and from the R-UIM.

D55-20 The device ***shall*** read all applicable calling feature codes from the R-UIM and display them to the user.

D55-25 The device ***shall not*** allow the user to enable or disable any calling features if the calling feature codes are not defined on the RUIM. Alternatively the device may fall back to the default set of calling feature codes valid for the respective operator.

D55-30 The device should be provisioned with a list of all emergency numbers used in OMH markets.

D55-35 The device ***shall*** always permit calls to emergency numbers, even if no R-UIM is inserted.[10]

D55-40 The device should allow the user to dial emergency numbers stored on the R-UIM and device when R-UIM is present.

D55-45 The device should allow the user to add emergency numbers, but should not allow the user to delete emergency numbers provisioned by the manufacturer.[11]

[10] The emergency numbers on the R-UIM are applicable to the user's home networks and might not be applicable to the networks that the user has roamed to in a different country. That is why the device should allow the user to enter, modify, and delete emergency numbers on the device as needed, depending on the network or country the user has roamed to.

[11] Operators can prohibit abuse by blocking emergency calls to invalid emergency numbers at the Mobile Switching Center (MSC).

4.2 Protocols

D55-200 The device should support Voice Privacy and allow the user to activate it when a voice call is set up and during a voice call.

D55-205 The device should support the following call forwarding types:

- Call forwarding Unconditional – Land Line Number
- Call forwarding: Unconditional – Voice Mail Number
- Call forwarding: Busy – Land Line Number
- Call forwarding: Busy – Voice Mail Number
- Call forwarding: Default – Land Line Number
- Call forwarding: Default – Voice Mail Number
- Call forwarding: No Answer – Land Line Number
- Call forwarding: No Answer – Voice Mail Number

D55-210 The device should support Three-Way Calling.

D55-215 The device should support Call Waiting.

D55-220 The device should support Caller ID.

D55-225 The device should support Message Waiting Indication.

D55-230 The device ***shall*** also support EVRC-B service option 68 (4GV-NB).

D55-235 The device should support the standard network-based "+" code dialing.

D55-240 The device should provide a plus key or equivalent user interface convention to allow "+" code dialing.

D55-245 The device should support phonebook storage and subsequent retrieval of digits with a "+" code, regardless of the source of the digits (e.g., user entry, caller display, and Device Origination Address).

D55-250 The device should support transmission of the dialed digits in ASCII mode for internationally dialed voice calls in the Origination Message using the International NUMBER_TYPE without using the "+" character.

D55-255 The device should support setting the NUMBER_PLAN to either "ISDN/Telephony" or "Unknown" for internationally dialed voice calls.

D55-260 The device should accept an internationally formatted Calling Party Number information record for an incoming voice call with NUMBER_TYPE = "International number" and NUMBER_PLAN set to either "Unknown" or "ISDN/Telephony."

D55-265 The device should present a received internationally formatted Calling Party Number to the subscriber with a leading "+" symbol.

D55-270 The device should match a received internationally formatted Calling Party Number to a corresponding phonebook entry.

D55-275 The device ***shall*** support Display Records that are sent from the network using Feature Notification Message, Flash with Information Message, and Alert with Info Message.

D55-280 The device ***shall*** support Burst Dual Tone Multi Frequency (DTMF).

D55-285 The device should support Continuous DTMF.

<page left blank intentionally>

5. SMS (D60)

5.1 General and R-UIM

D60-1 The SMS client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the *Short Message Service (SMS)* section of [CDG166].

D60-5 The device should perform SMS retries using the retry parameters provisioned on the R-UIM.

D60-10 The device should allow the user to store SMS messages to the R-UIM.

D60-15 The device should automatically store received SMS messages to R-UIM.

D60-20 The device should allow the user to modify the messages on the R-UIM.

D60-25 The device should allow the user to delete the messages from the R-UIM.

D60-30 The device should allow the user to store SMS Parameters to the R-UIM.

D60-35 The device should allow the user to modify SMS Parameters on the R-UIM.

D60-40 The device should allow the user to delete SMS Parameters from the R-UIM.

D60-45 The device should use SMS Parameters from the R-UIM when sending MO SMS messages.

D60-50 The device should allow the user to choose one of the SMS Preferences records for use with SMS.

D60-55 The device should use MESSAGE_ID from the R-UIM when sending MO SMS messages and increment it by 1.

D60-60 The device ***shall*** support the following encoding types defined in [CR1001] for the character string data present in $EF_{BCSMStable}$ (see footnotes in **D15-5** for notes on encoding):

- "Octet, unspecified": Containing unpacked ASCII characters.
- "7-bit ASCII": Containing unpacked ASCII characters.
- "Unicode"

5.2 Protocols

D60-200 The device ***shall*** support MO SMS over access channel.

D60-205 The device ***shall*** support MO SMS over traffic channel.

D60-210 The device ***shall*** support MT SMS over paging channel.

D60-215 The device ***shall*** support MT SMS over traffic channel.

D60-220 The device ***shall*** support service option 6.

D60-225 The device ***shall*** support service option 14.

D60-230 The device ***shall*** support Voice Mail Notification over SMS.

D60-235 If the device supports HRPD, the device should support sending and receiving of SMS while the device is in 1x and HRPD hybrid mode.

D60-240 The device ***shall*** support the sending and receiving of messages with empty text.

D60-245 The device ***shall*** support the sending and receiving of messages with an Internet email address.

D60-250 The device ***shall*** allow the user to forward a message.

D60-255 The device ***shall*** allow the user to send a message to multiple addresses.

D60-260 If the device's user interface allows users to enter an SMS message that exceeds 140 bytes, it ***shall*** ensure that no individual segment exceeds 140 bytes when it segments the long messages.

D60-265 The device should support transmission of the Destination Address parameter in ASCII mode for internationally addressed messages.

D60-270 The device should support setting the Destination Address NUMBER_TYPE to "International number" for internationally addressed messages.

D60-275 The device should accept an Originating Address parameter coded in ASCII mode when receiving internationally addressed messages.

D60-280 The device should accept an Originating Address parameter with NUMBER_TYPE = "International number" when receiving internationally addressed messages.

D60-290 The device should present a received internationally formatted Originating Address parameter to the subscriber with a leading "+" symbol.

D60-295 The device should match a received internationally formatted Originating Address parameter to a corresponding phonebook entry.

D60-300 The device may support Broadcast SMS for receiving information updates and emergency alerts from the network.

D60-305 The device should handle an SMS message meeting all of the following conditions as a Flash SMS message:

- Relative Validity Period value is 246 (Immediate) and/or Display Mode is 0 (Immediate).
- No other message parameters indicate that the message is a special message not intended for the end user (e.g., an SMS-PP download message).

D60-310 If the device supports Flash SMS, it ***shall*** process a Flash SMS message as follows:

- The message ***shall*** be presented to the user directly.

- The message ***shall*** not be automatically stored by the device.
- The device may allow the user to clear the message or to manually save the message to the device or the R-UIM.

<page left blank intentionally>

6. 3G Packet Data (D65)

6.1 General and R-UIM

D65-1 3GPD services on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the *3GPD* section of [CDG166].

D65-5 The device ***shall*** support both PAP and CHAP authentication for Simple IP using credentials and authentication algorithms on the R-UIM.

D65-10 If the device supports Mobile IP, the device ***shall*** support Mobile IP authentication using credentials and authentication algorithms on the R-UIM.

D65-15 The device ***shall*** support Mobile IP to Simple IP fallback based on the flag in $EF_{3GPDOPM}$.[12]

D65-20 The device should support the following features based on the parameters on the R-UIM:

- Extended Packet Zone Identifiers (EPZID)
- Hysteresis Activation Timer (HAT)
- TCP Keep-alive Idle Timer

D65-25 The device ***shall*** restore the dormant timer to the value contained in EF_{DGC} when an application exits. This prevents an application from changing the dormant timer to a value that may be inappropriate for other applications.

D65-30 The device ***shall*** support tethered-mode data calls in Relay Model using PAP credentials from the terminal.

D65-35 The device ***shall*** support tethered-mode data calls in Relay Model using CHAP credentials from the terminal.

D65-40 The device ***shall*** support tethered-mode data calls in Network Model using PAP credentials from the R-UIM.

D65-45 The device ***shall*** support tethered-mode data calls in Network Model using CHAP credentials from the R-UIM.

[12] This EF is provisioned by the operator, and the device should not change it unless for debugging purposes.

6.2 Multiple Profiles

D65-200 The device ***shall*** support Multiple User Profiles for Simple IP based on provisioning information in $EF_{3GPDUPPExt}$[13], as well as EF_{SIPUPP}.

D65-205 The device ***shall*** support Multiple User Profiles for Mobile IP based on provisioning information in $EF_{3GPDUPPExt}$[14], as well as EF_{MIPUPP}.

D65-210 When performing Mobile IP to Simple IP fallback, the device ***shall*** fall back from a Mobile IP profile to a corresponding Simple IP profile that has the same Network Address Identifier (NAI) index.

D65-215 For Multiple User Profiles, the device ***shall*** reuse the existing data session if the application to be launched uses the same profile as the existing application does (hence, they have the same priority).

D65-220 For Multiple User Profiles, the device ***shall*** preempt the existing application and set up a new data session if the application to be launched resides in a profile that has a higher priority than the profile for the existing application.

D65-225 For Multiple User Profiles, the device ***shall*** reject the application to be launched if its profile has a lower priority than the profile for the existing application.

D65-230 Since LBS can be present in multiple profiles, as defined in the *3GPD* section of [CDG166], it ***shall*** share data sessions with one, many, or all the other applications on the device based on the provisioning of the R-UIM.

D65-235 If there are multiple profiles containing LBS in the APPLICATIONS bit mask, the one having the lowest priority ***shall*** be used as the default LBS profile.

D65-240 When an LBS data session needs to be established but there is no existing data session active, the default LBS profile ***shall*** be used for establishing a data session.

D65-245 If an LBS data session is active and a new application is launched that has a higher priority, the current data session ***shall*** be released and a new data session ***shall*** be established by using this higher priority profile; and then, if the new profile also contains LBS, the LBS application shall be launched again, which will share the same data session with the new application.

6.3 Protocols

D65-400 The device ***shall*** support [CS0017].

D65-405 The device ***shall*** support service option 33.

D65-410 The device ***shall*** support IPv4.[15]

---

[13] $EF_{SIPUPPExt}$ has been renamed to $EF_{3GPDUPPExt}$.

[14] $EF_{MIPUPPExt}$ has been removed. Instead, the extension block in $EF_{3GPDUPPExt}$ is used for both Mobile IP profiles and SIP profiles.

[15] IPv6 will be addressed in a later phase.

D65-415 The device ***shall*** support Simple IP operation.

D65-420 The device ***shall*** support Simple IP establishment without authentication.

D65-425 The device ***shall*** support Simple IP establishment with PAP authentication.

D65-430 The device ***shall*** support Simple IP establishment with CHAP authentication.

D65-435 The device should support Mobile IP operation.

D65-440 If the device supports Mobile IP, the device ***shall*** support Mobile IP Inter-PDSN Handoff in Active State.

D65-445 If the device supports Mobile IP, the device ***shall*** support Mobile IP Inter-PDSN Handoff in Dormant State.

D65-450 If the device supports Mobile IP, the device ***shall*** support Mobile IP Intra-PDSN Handoff in Active State.

D65-455 If the device supports Mobile IP, the device ***shall*** support Mobile IP Intra-PDSN Handoff in Dormant State.

D65-460 The device ***shall*** support Simple IP Inter-PDSN Idle Handoff.

D65-465 The device ***shall*** support Simple IP Intra-PDSN Handoff in Dormant State.

D65-470 If the device supports Mobile IP, the device ***shall*** support successful Mobile IP Point-to-Point (PPP) negotiation and termination.

D65-475 If the device supports Mobile IP, the device ***shall*** support Agent Discovery and Registration using dynamic Home Address assignment.

D65-480 If the device supports Mobile IP, the device ***shall*** support Agent Discovery and Registration using static Home Address assignment.

D65-485 If the device supports Mobile IP, the device ***shall*** support Router Advertisement lifetime expiry.

D65-490 If the device supports Mobile IP, the device ***shall*** support Mobile IP Registration Request retry.

D65-495 If the device supports Mobile IP, the device ***shall*** support Mobile IP Registration Lifetime processing.

D65-500 If the device supports Mobile IP, the device ***shall*** support Mobile IP De-Registration.

D65-505 If the device supports Mobile IP, the device ***shall*** support RADIUS authentication.

D65-510 If the device supports Mobile IP, the device ***shall*** support IPSec Security with preserving of existing security association.

D65-515 If the device supports Mobile IP, the device ***shall*** support Foreign Agent Reverse Tunnel Registration.

D65-520 If the device supports Mobile IP, the device ***shall*** support Private Network.

D65-525 If the device supports Mobile IP, the device ***shall*** support Successful Authentication using the MN-AAA extension.

D65-530	If the device supports Mobile IP, the device should support simultaneous Mobile IP and Simple IP.
D65-535	The device ***shall*** support soft handoff of fundamental channel and supplemental channel together.
D65-540	The device ***shall*** support soft handoff of fundamental channel only.
D65-545	The device ***shall*** support hard handoff to high-speed packet data capable system.
D65-550	The device ***shall*** support hard handoff to high-speed packet data capable system with a different Radio Configuration if available.
D65-555	The device ***shall*** support high-speed packet data PPP or IP Expiration.
D65-560	The device should support Simultaneous Voice and Data.

7. HRPD (1xEV-DO) (D70)

This section presents additional requirements for the 3G Packet Data section to support HRPD.

7.1 General and R-UIM

D70-1 For HRPD, the device ***shall*** perform A12 (AN-AAA) authentication for HRPD access using access credentials and authentication algorithms on the R-UIM.

D70-5 The device should support HRPD Rev 0.

D70-10 The device should support HRPD Rev A.

D70-15 The device should support 1x and HRPD hybrid operations.

D70-20 The device should support Receive Diversity.

7.2 Protocols

D70-100 The device ***shall*** support the functions defined in [CS0024].

D70-105 The device ***shall*** satisfy the conformance requirements defined in [CS0038].

D70-110 The device ***shall*** satisfy the performance requirements defined in [CS0033].

D70-120 The device ***shall*** support the Forward and Reverse Test Application Protocol specification (FTAP and RTAP) defined in [CS0029].

D70-125 The device ***shall*** support the HRPD band classes defined in [CS0057].

D70-130 The device ***shall*** satisfy the Interoperability Specification for CDMA2000 Air Interface defined in [CS0044].

D70-135 The device ***shall*** support Default Signaling Application.

D70-140 The device ***shall*** support Default Packet Application.

D70-145 The device ***shall*** support Default Stream Protocol.

D70-150 The device ***shall*** support Default Session Management Protocol.

D70-155 The device ***shall*** support Default Address Management Protocol.

D70-160 The device ***shall*** support Default Session Configuration Protocol.

D70-165 The device ***shall*** support Default Air Link Management Protocol.

D70-170 The device ***shall*** support Default Idle State Protocol.

D70-175 The device ***shall*** support Default Connected State Protocol.
D70-180 The device ***shall*** support Default Route Update Protocol.
D70-185 The device ***shall*** support Default Packet Consolidation Protocol.
D70-190 The device ***shall*** support Overhead Messages Protocol.
D70-195 The device ***shall*** support Default Initialization State Protocol.
D70-200 The device ***shall*** support Default Security Protocol.
D70-205 The device ***shall*** support Default Key Exchange Protocol.
D70-210 The device ***shall*** support Default Authentication Protocol.
D70-215 The device ***shall*** support Default Encryption Protocol.
D70-220 The device ***shall*** support Default Control Channel MAC Protocol.
D70-225 The device ***shall*** support Default Access Channel MAC Protocol.
D70-230 The device ***shall*** support Default Forward Traffic Channel MAC Protocol.
D70-235 The device ***shall*** support Default Reverse Traffic MAC Protocol.
D70-240 The device ***shall*** support Default Physical Layer Protocol.

7.3 HRPD Rev A Specific

D70-400 The device ***shall*** support Multi-Flow Packet Application.
D70-415 The device ***shall*** support Enhanced Idle State Protocol.
D70-420 The device ***shall*** support Enhanced Control Channel MAC Protocol.
D70-425 The device ***shall*** support Enhanced Access Channel MAC Protocol.
D70-430 The device ***shall*** support Enhanced Forward Traffic Channel MAC Protocol.

7.4 1x and HRPD Interworking

D70-600 The device ***shall*** support Voice Origination in HRPD Idle Mode.
D70-605 The device ***shall*** support Voice Termination in HRPD Idle Mode.
D70-610 The device ***shall*** support SMS Origination in HRPD Idle Mode.
D70-615 The device ***shall*** support SMS Termination in HRPD Idle Mode.
D70-620 The device ***shall*** support Voice Origination in HRPD Active Mode.
D70-625 The device ***shall*** support Voice Termination in HRPD Active Mode.
D70-630 The device ***shall*** support SMS Origination in HRPD Active Mode.
D70-635 The device ***shall*** support SMS Termination in HRPD Active Mode.
D70-640 The device ***shall*** support Voice Origination in HRPD Dormant Mode.
D70-645 The device ***shall*** support Voice Termination in HRPD Dormant Mode.
D70-650 The device ***shall*** support SMS Origination in HRPD Dormant Mode.
D70-655 The device ***shall*** support SMS Termination in HRPD Dormant Mode.

D70-660 The device ***shall*** support Inter-Technology switching from HRPD to cdma2000 1x in Dormant Mode.

D70-665 The device ***shall*** support Inter-Technology switching from HRPD to cdma2000 1x in Active Mode.

D70-670 The device ***shall*** support Inter-Technology switching from cdma2000 1x to HRPD in Dormant Mode.

<page left blank intentionally>

8. WAP Browser (D75)

8.1 General, R-UIM, and User Interface (UI)

D75-1 The device should support WAP Browser.

D75-5 The device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the *Browser* section of [CDG166].

D75-10 If the operator provisions bookmarks on the R-UIM, the device ***shall*** present these bookmarks to the user.

D75-15 The device should allow the user to save additional bookmarks on the R-UIM.

D75-20 The device ***shall*** be capable of displaying the web pages based on the bookmarks on the R-UIM.

D75-25 The device ***shall*** allow the user to change any bookmark on the R-UIM.

D75-30 The device should have a visual indicator to indicate the sending and receiving of data packets for WAP sessions.

D75-35 The device ***shall*** allow the user to enter a URL directly.

D75-40 The device should allow the user to navigate “Forward” and “Backward” in the history list.

D75-45 The device should allow the user to save a Wireless Markup Language (WML) card or eXtensible Hypertext Markup Language (XHTML) document for offline viewing and to update and delete the snapshot.

D75-50 The device should allow the user to cache user ID and password information on the client.

D75-55 The device should provide an auto-fill capability that assists users in text entry for frequently used fields.

D75-60 The device should allow the user to use predictive text entry, if this capability is supported by the device.

D75-65 The device should provide visual Secured Browser connection indicators.

D75-70 The device should provide visual Error and Warning Dialogs for HTTP errors.

D75-75 The device should provide visual Error and Warning Dialogs for Repost form data warning.

D75-80 The device should provide a single key/touch access to the browser from the idle screen.

D75-85 The device should support languages that are supported by the device in general.

D75-90 The device should display all error messages in the local language.

D75-95 The device should provide browser version information.

8.2 Protocols

D75-300 The device ***shall*** support WAP 2.0.

D75-302 The device should use cdma2000 as the data bearer.

D75-305 The device ***shall*** support HTTP 1.1 basic authentication.

D75-310 The device should support HTTP 1.1 digest authentication.

D75-315 The device should support Transport Layer Security (TLS) server authentication for transport layer security and SSL 3.0.

D75-320 The device should support certificate chaining.

D75-325 The device should support loading of root certificates in support of Wireless Public Key Infrastructure (PKI).

D75-330 The device should support WAP certificate profiles.

D75-335 The device should support WAP 2.0 caching, i.e., the HTTP 1.1 caching model.

D75-340 The device should support HTTP State Management with local cookie storage.

D75-345 The device ***shall*** support Domain Name Server (DNS) Resolution of Host Names for Proxy.

D75-350 The device should support multiple proxies.

D75-355 If the device supports multiple proxies, the device should support HTTP Proxy fail-over.

D75-360 The device should support the “profile URI” header for User Agent Profile.

D75-365 The device should support the “profile diff” header for User Agent Profile.

D75-370 The device’s User Agent Profile ***shall*** successfully pass validation using the Open Mobile Alliance (OMA) Delivery Context Library for CC/PP and UAProf (DELI) UAProf Validator tool at http://validator.openmobilealliance.org/cgi/.

D75-375 The device ***shall*** support both HTTP and HTTPS, which will be routed via the WAP gateway provisioned on the R-UIM.

D75-380 The device should support WML 1.3 in binary form.

D75-385 The device should support WML 1.3 in textual form.

D75-390 The device should support WMLScript, which is the compiled binary form including WMLScript standard libraries.

D75-395 The device should support Make Call for the public Wireless Telephony Application (WTA) function.

D75-400 The device should support Send DTMF for the public WTA function.

D75-405 The device should support Add Phonebook Entry for the public WTA function.

D75-410 The device should notify the user when it is directed to initiate a call.

D75-415 The device should support Connection-Oriented Push over HTTP.

D75-420 If the device supports WAP Push, the device ***shall*** provide a visual message arrival notification.

D75-425 The device should allow the user to view recently received Service Indication or WAP Push notifications without establishing a WAP session.

D75-430 The device should first alert the user that a connection is about to be started for any push that initiates a background connection.

D75-435 The device should turn on an annunciator/icon to allow the user to view unread Service Indication or WAP Push notifications without establishing a WAP session.

D75-440 The device ***shall*** support the HTTP Content-Type header.

D75-445 The device ***shall*** support the HTTP Content-Disposition header.

8.3 Download

D75-600 The device should support OMA Download 1.0.

D75-605 If the device supports OMA Download 1.0, the device ***shall*** support separate delivery of Download Descriptor and Media Object for OMA Download.

D75-610 If the device supports OMA Download 1.0, the device ***shall*** support combined delivery of Download Descriptor and Media Object with status report.

D75-615 If the device supports OMA Download 1.0, the device ***shall*** support combined delivery of Download Descriptor and Media Object without status report.

D75-620 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification, which is to be sent to the network after the Media Object is installed successfully.

D75-625 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (901) Insufficient memory.

D75-630 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (902) User Canceled.

D75-635 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (906) Invalid descriptor.

D75-640 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (951) Invalid DD Version.

D75-645 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (952) Device Aborted.

D75-650 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification for installation failures with (953) Non-Acceptable Content for unknown or unsupported media object types.

D75-655 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification without server reply and make the downloaded media object available for use by the user.

D75-660 If the device supports OMA Download 1.0, the device ***shall*** support Installation Notification with server error and make the downloaded media object not available for use by the user.

D75-665 If the device supports OMA Download 1.0, when the user selects to continue with a browsing operation after a successful download, the device ***shall*** invoke the URL defined in the NextURL attribute in the Download Descriptor.

D75-670 If the device supports OMA Download 1.0, the device ***shall*** ignore the optional attributes that are not supported and ignore unknown attributes when processing Download Descriptor.

D75-675 If the device supports OMA Download 1.0, when an attribute occurs multiple times in the Download Descriptor, the device ***shall*** process the first occurrence and ignore the remaining occurrences. The exception is the attribute Type, which is allowed to occur multiple times.

8.4 Media

D75-800 The device should support the display of BMP Image content.

D75-805 The device should support the display of PNG Image content.

D75-810 The device should support the display of JPEG Image content.

D75-815 The device should support the display of GIF Image content.

D75-820 The device should support all audio types in browser that are supported by the device in general.

D75-825 The device should support all video types in browser that are supported by the device in general.

D75-830 If the device supports video services, it should support links from the browser to those video services.

D75-835 The device should support application service discovery for video services, BREW, Java, etc.[16]

D75-840 The device ***shall*** support the Service Indication (SI) content type.

D75-845 The device should support the Service Loading (SL) content type.

D75-850 The device should support the Cache Operation (CO) content type.

[16] For example, if the web page displays a link to a streaming video, the device should allow the user to click on it in order to launch the video streaming application.

D75-855 The device should support OMA Digital Rights Management (DRM) 1.0.

D75-860 If the device supports OMA DRM, it ***shall*** support OMA DRM Forward Lock.

D75-865 The device should support OMA DRM Combined Delivery.[17]

D75-870 The device should support OMA DRM Separate Delivery.

D75-875 The device should support the Session Initiation Request (SIR) content type.

D75-880 The device should support the WAP Pictograms.

D75-885 The device should support Unicode and UTF-8 encoding.

[17] If the device supports DRM Separate Delivery, it must support DRM Combined Delivery.

<page left blank intentionally>

9. MMS (D80)

9.1 General, R-UIM, and UI

D80-1 The device should support MMS.

D80-5 The MMS client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details, see the *MMS* section of [CDG166].

D80-7 If the R-UIM does not contain the MMS WAP gateway configuration, the device may use that information from the device memory.

D80-10 The device ***shall*** support MMS WAP gateway provisioned as either a domain name (PXADDR-FQDN) or IP address (PXADDR) on the R-UIM.

D80-15 If there are more than one MMS connectivity parameter sets including the WAP gateway provisioned on the R-UIM, the device should fall back to the next MMS connectivity parameter set if the device fails to connect to the MMS server using the current connectivity parameter set.

D80-20 The device ***shall not*** send MMS messages larger than the Max Message Size provisioned on the R-UIM.[18]

D80-25 The device ***shall*** perform MMS retries based on retry times and retry interval values provisioned on the R-UIM.

D80-30 The device ***shall*** wait for a duration indicated in the Mobile Messaging Service Center (MMSC) timeout value provisioned on the R-UIM before declaring an MMSC timeout.

D80-35 The device should read and use MMS User Preferences, if they are present on the R-UIM.

D80-40 The device should support the capability of updating MMS User Preferences on the R-UIM.

D80-45 The device should provide an option for the user to specify which MMS User Preferences record will be used when there are multiple User Preferences records on the R-UIM.

D80-50 If there are MMS Notifications present on the R-UIM, the device should read them from the R-UIM, present them to the user, and use those notifications to receive MMS messages from the network.

[18] The maximum MMS message size sent by a device should be the lower of the Max Message Size Value in $EF_{MMSConfig}$ and the maximum message size value in the device's User Agent Profile.

D80-55 The device should support the capability of storing MMS Notifications on the R-UIM.

D80-60 If the device supports the capability of storing MMS Notifications on the R-UIM, it should provide an option for the user to specify where the received MMS Notifications are stored (i.e., on the device or on the R-UIM).

D80-65 If the device supports the capability of storing MMS Notifications on the R-UIM, it ***shall*** follow the procedure defined in [XS0016-0] to update the status fields on the R-UIM.

D80-70 If the device supports the capability of storing MMS Notifications on the R-UIM, it ***shall*** record the time it receives the MMS notification into the MMS Notification PDU on the R-UIM using the RFC2822 Date header.

Reason: If the Date header is not added to the MMS Notification PDU, the expiry time displayed to the user would be relative (e.g., "The message will expire in 2 days") and would not be valid when the same notification is read sometime later (e.g. after two days, the user would still see "The message will expire in 2 days").

D80-75 The device should allow the user to preview the message before it is sent.

D80-80 The device should display a progress bar when a message is being submitted.

D80-85 The device should allow the user to access the phonebook when the device displays the MMS application menus.

D80-90 The device should allow the user to distinguish between read and unread messages.

D80-95 The device should allow the user to enter multiple recipient addresses when a message is composed.

D80-100 The device should allow the pictures and audios stored in the device's gallery or downloads folder to be attached while sending a message.

D80-105 The device should use MMS to upload a picture taken by the camera to a server when selected.

9.2 Protocols

D80-200 The device ***shall*** support the 3GPP2 OMA/WAP MM1 implementation of MMS using HTTP as the transport.

D80-205 The device ***shall*** comply with WAP requirements identified in ***Section*** *8. WAP Browser (D75)* of this document.

D80-210 The device ***shall*** comply with the SMS requirements identified in ***Section*** *5. SMS (D60)* of this document.

D80-220 The device should support OMA DRM Forward Lock.

D80-225 The device should support OMA DRM Combined Delivery.[19]

D80-230 The device should support OMA DRM Separate Delivery.

[19] If the device supports DRM Separate Delivery, it must support DRM Combined Delivery.

D80-235	The device ***shall*** provide User Agent Profile information to the MMS Relay/Server.
D80-240	The device ***shall*** support forward, reply to, and delete functionality.
D80-242	The device ***shall*** send and receive images, audios, and videos indicated in the UAProf.
D80-245	The device should support sending messages to email addresses.
D80-250	The device should support receiving messages from an email address.
D80-255	The device should not reject an incoming multimedia message based on the message size indicated in the MM notification.
D80-260	The device ***shall*** correctly receive and reasonably present a message with an unrecognized field in the MMS header.
D80-265	The device ***shall*** correctly receive and reasonably present a message with a recognized field but with an unrecognized value in the MMS header.
D80-270	The device should receive a Delivery Report for a successfully retrieved message.
D80-275	The device should receive a Delivery Report for a rejected message.
D80-280	The device should receive a Delivery Report for an expired message.
D80-285	The device should receive multiple Delivery Reports, each with a different status, for a message sent to multiple recipients.
D80-290	The device should receive a Read-Reply Report with the date that the message is read.
D80-295	The device should send a Read-Reply Report for a received message that requests read reply.
D80-300	The device should receive multiple Read-Reply Reports, each with a different status, for a message sent to multiple recipients.
D80-305	The device should receive a Read-Reply Report with the date that the message is read.
D80-310	The device should support Immediate Retrieval of a message.
D80-315	The device should support Deferred Retrieval of a message.
D80-320	The device should support Rejected Retrieval of a message.
D80-325	The device ***shall*** support the X-Mms-Message-Type field when sending a message.
D80-330	The device ***shall*** support the X-Mms-Transaction-ID field when sending a message.
D80-335	The device should support the Date field when sending a message.
D80-340	The device ***shall*** support the From field when sending a message.
D80-345	The device ***shall*** support the To field when sending a message.
D80-350	The device should support the Cc field when sending a message.
D80-355	The device should support the Bcc field when sending a message.

D80-360 The device ***shall*** support the Subject field when sending a message.

D80-365 The device should support the X-Mms-Expiry field with Relative option when sending a message.

D80-370 The device should support the X-Mms-Delivery-Time field with Relative option when sending a message.

D80-375 The device should support the X-Mms-Priority field with different priorities when sending a message.

D80-380 The device should support the X-Mms-Delivery-Report field when sending a message.

D80-385 The device should support the X-Mms-Read-Report field when sending a message.

D80-390 The device should support all the mandatory message fields, and when none of the mandatory fields among “To,” “Cc,” and “Bcc” are present in the message to be sent, the device should reject the message with an error displayed to the user.

D80-395 The device should support Long Subject field.

D80-400 The device should support Empty text file.

D80-405 The device should support cancellation of a message by using the Cancel PDUs.

D80-410 The device should support the X-Mms-Message-Class field.

D80-415 The device should support the X-Mms-Expiry field – Relative.

D80-420 The device should support the X-Mms-Expiry field – Absolute.

D80-425 The device should support the X-Mms-Delivery-Time field – Relative.

D80-430 The device should support the X-Mms-Delivery-Time field – Absolute.

D80-435 The device should support the X-Mms-Priority field – Low.

D80-440 The device should support the X-Mms-Priority field – Normal.

D80-445 The device should support the X-Mms-Priority field – High.

D80-450 The device should support the X-Mms-Delivery-Report field.

D80-455 The device should support the X-Mms-Read-Report field.

D80-460 The device should support the X-MMS-Adaptation-Allowed field.

D80-465 The device should be able to reject sending of delivery and read-reply reports.

D80-470 The device should support recording of a voice message when composing MMS.

D80-475 The device should gracefully handle MMS concurrently with other activities, such as voice and SMS.

9.3 Media Types

D80-700 The device should support the audio type MIDI.

D80-705	The device should support the audio 3GPP2 13k speech.
D80-710	The device should support the Adaptive Multi-Rate Narrow Band (AMR NB) audio.
D80-715	The device ***shall*** support the Subject field with UTF8 encoding in sent and received messages.
D80-720	The device ***shall*** support the Text field with US-ASCII encoding in sent and received messages.
D80-725	The device ***shall*** support the Text field with UTF-8 encoding in sent and received messages.
D80-730	The device ***shall*** support Text with UTF-16 (LE) encoding in received messages.
D80-735	The device should support JPG Image size 160x120.
D80-740	The device should support JPG Image size 640x480.
D80-745	The device should support GIF Image size 160x120.
D80-750	The device should support GIF Image size 640x480.
D80-755	The device should support Animated GIF Image size 160x120.
D80-760	The device should support Animated GIF Image size 640x480.
D80-765	The device should support Wireless Bitmap (WBMP) Image size 160x120.
D80-770	The device should support WBMP Image size 640x480.
D80-775	The device should support BMP Image.
D80-780	The device should support the Long Content-Location field.
D80-785	The device should support Synchronized Multimedia Integration Language (SMIL) portrait layout with text above the image.
D80-790	The device should support SMIL portrait layout with text below the image.
D80-795	The device should support SMIL landscape layout with text to the left of the image.
D80-800	The device should support SMIL landscape layout with text to the right of the image.
D80-805	The device should support SMIL multiple objects in same page.
D80-810	The device should support SMIL multiple pages.
D80-815	The device should support SMIL multiple pages with page timing and time dependent content.
D80-820	The device may support 3GPP Video QCIF and sub-QCIF.
D80-825	The device may support 3GPP2 Video QCIF (MPEG4+13k).
D80-830	The device may support 3GPP2 Video QCIF (MPEG4+AMR).
D80-835	The device may support 3GPP2 Video QCIF (H.263+13k).
D80-840	The device may support 3GPP2 Video QCIF (H.263+AMR).

D80-845	The device may support 3GPP2 Video sub-QCIF (MPEG4 +13k).
D80-850	The device may support 3GPP2 Video sub-QCIF (MPEG4 +AMR).
D80-855	The device may support 3GPP2 Video sub-QCIF (H.263 +13k).
D80-860	The device may support 3GPP2 Video sub-QCIF (H.263 +AMR).
D80-865	The device may support vCard.
D80-870	The device may support vCalendar.
D80-875	The device may support the sending of a Postcard using X-MMS-GREETINGTEXT header.
D80-880	The device may support the sending of a Postcard vCard attachment to multiple recipients.
D80-885	The device may support the sending of a Postcard vCard attachment to multiple recipients with additional vCard properties.
D80-890	The device may support the sending of a Postcard vCard attachment with the ADR field empty.
D80-895	The device should support the sending of full conformance to megapixel class for creation and submission of single object.
D80-900	The device should support Rich Text in various content classes.
D80-902	The device should support XHTML Family User Agent.
D80-905	The device should support full conformance to megapixel class for creation and submission of multiple objects.
D80-910	The device should support the sending and receiving of MMS messages with JPEG containing Huffman table.
D80-915	The device should support the sending of MMS message without defining the duration parameter value (i.e., <par> dur).
D80-920	The device should support the sending of MMS message with a user-specific duration parameter value (i.e., <par> dur).
D80-925	The device should support the retrieval and presentation of the Content Basic content class.
D80-930	The device should support the retrieval and presentation of Content Rich content class.
D80-935	The device should support the retrieval and presentation of Mega-pixel content class.
D80-940	The device should support the EXIF compressed image file format as the JPEG interchange format.
D80-945	The device should handle messages with corrupted content by presenting the content that is not corrupted.
D80-950	The device should handle message with unsupported content (e.g., PDF) by presenting the content that is supported.
D80-955	The device should support 3GPP PSS6 SMIL Language Profile.

D80-960	The device should recognize the hyperlink in the message for launching the browser.
D80-965	The device should support Creation Mode Restricted.
D80-970	The device should support Creation Mode Warning.
D80-975	The device should support Creation Mode Free.
D80-980	The device should support the ability to reduce in size any image taken by the integrated camera to fit into a message of the Core MM Content Domain.
D80-985	The device should support Re-submission Mode Restricted.
D80-990	The device should support Re-submission Mode Free.
D80-995	The device should support Re-submission Mode Warning.
D80-1000	The device should support Message Template functions.

1

2 <page left blank intentionally>

10. Java (D85)

D85-1 The device should support Java Virtual Machine (JVM) required to support Java applications.

D85-5 If the operator has provisioned a Java download URL in EF_{JDL} on the R-UIM, the Java download client on the device ***shall*** use this URL. For details on this URL, see the *Java* section of [CDG166].

D85-10 For Java application download, the 3GPD user profile to be used for establishing a data session for the download ***shall*** be the one having the Java bit enabled in the application bitmask or the one having the Unspecified bit enabled in the application bitmask if the Java bit is not enabled in any profiles.

<page left blank intentionally>

11. BREW (D90)

D90-1 The BREW client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details, see the *BREW* section of [CDG166].

D90-5 The device may support the fallback of BREW configurations from the R-UIM to those on the device when the R-UIM does not have BREW configurations.

D90-10 If the device falls back to NV for BREW configurations, the device ***shall*** delete all applications downloaded from the previous carrier due to Carrier ID mismatch.

D90-15 The device ***shall*** use BREW provisioning data only from the OMH card when BREW service in the EF_{CST} on the R-UIM is enabled.

D90-20 The device ***shall*** allow the user to use a BREW icon or menu item to connect to the BREW download server provisioned on the R-UIM.

D90-25 The device ***shall*** perform BREW download based on BREW Download Flag values provisioned on the R-UIM.

D90-30 The device ***shall*** perform BREW authentication based on the BREW Download Authentication Policy value provisioned on the R-UIM.

D90-35 The device ***shall*** use the BREW Carrier ID, Teleservice ID, Subscriber ID values provisioned on the R-UIM.

D90-40 The device ***shall*** ensure that previously downloaded BREW configuration data and applications are not accessible when an R-UIM with a different BREW Carrier ID value is used.

D90-45 The device ***shall*** perform BREW application execution based on the BREW Application Execution Policy provisioned on the R-UIM.

D90-50 When an R-UIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall*** prevent the applications downloaded by the previous subscriber from being launched.

D90-55 When an R-UIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall not delete*** the applications downloaded by the previous subscriber.

D90-60 When an R-UIM is inserted into the device with the same Carrier ID but a different subscriber ID, the device ***shall*** allow the user to manually delete the applications associated with the previous subscriber ID if the RUIM_DEL_OVERRIDE flag on the R-UIM is enabled.

D90-65 The OEM ***shall*** obtain a single Platform ID for an OMH device that will be used among all OMH operators.

12. LBS (D95)

D95-1	The device ***shall*** retrieve and use the configuration information provisioned on the R-UIM. For details, see the *LBS* section of [CDG166].[20]
D95-5	The device ***shall*** support Standalone GPS.
D95-10	If the device supports Standalone GPS, it ***shall*** support XTRA and use the XTRA parameters from the R-UIM.
D95-15	The device should support V2 User Plane LBS functions.
D95-20	If the device supports V2 User Plane LBS, it ***shall*** support IS-801-1 LBS User Plane call flows.
D95-25	If the device supports V2 User Plane LBS, it ***shall*** support Trusted Mode for Mobile-Resident and Network-Initiated LBS sessions, and use the Position Determination Entity (PDE) addresses from the R-UIM.
D95-30	If the device supports V2 User Plane LBS, it should support Non-Trusted Mode for Network-Initiated LBS sessions, and use the Mobile Positioning Center (MPC) address from the R-UIM.
D95-35	If the device supports V2 User Plane LBS, for Non-Trusted Network-Initiated LBS sessions, the device ***shall*** support SMS Teleservice 65001 for receiving the LBS trigger from the network.
D95-40	If the device supports V2 User Plane LBS, for Non-Trusted Network-Initiated LBS sessions, the device ***shall*** support the notification and verification procedure involving the user's response.
D95-45	If the device supports V2 User Plane LBS, the device ***shall*** support WAP Pull as the trigger from the network to initiate an LBS session.
D95-50	If the device supports V2 User Plane LBS, it ***shall*** support Dynamic Mode as configured on the R-UIM (i.e., falling back to standalone GPS as needed).
D95-55	The device should allow the user to turn on/off all LBS functions.
D95-60	When the device is out of CDMA coverage, the device should continue to support LBS using mechanisms not requiring CDMA service.

[20] See the 3GPD section of this document for the special cases of LBS working with multiple user profiles.

13. Mapping of Requirements to Acceptance Testing [Informative]

The following table contains the mapping from device requirements to device acceptance test plans for ease of reference.

Table 13-1 Mapping of Requirements to Acceptance Test Plans

Device Requirements (this document)	***Acceptance Test Plans [CDG183]***
Using Legacy R-UIMs (D1)	OMH Specific Optional OMH Specific OMH Inter-Operability Test (IOT)
R-UIM Commands (D5)	OMH Specific Optional OMH Specific OMH IOT R-UIM (48)
Subsidy Lock (D10)	OMH Specific Optional OMH Specific
Carrier Customization (D15)	OMH Specific Optional OMH Specific
CCAT (D20) CCAT/UTK Download (D30)	OMH Specific Optional OMH Specific CCAT Optional CCAT
Device and Model Identification (D25)	OMH Specific Optional OMH Specific OMH IOT MEID (73)
OTASP/OTAPA (D35)	OMH Specific Optional OMH Specific OTASP (60)
Root Certificates (D40)	OMH IOT
Configuration Data Sources (D45)	OMH Specific Optional OMH Specific
cdma2000 (D50)	C2K conf (31) C2K conf (43)

Device Requirements (this document)	***Acceptance Test Plans [CDG183]***
Voice (D55)	OMH Specific Optional OMH Specific OMH IOT Audio (56) C2K conf (31) C2K conf (43) Optional PCD
SMS (D60)	OMH Specific Optional OMH Specific OMH IOT SMS (61) C2K conf (31) C2K conf (43) PCD Field IOT
3GPD (D65)	OMH Specific Optional OMH Specific OMH IOT C2K perf (11) C2K conf (31) or C2K conf (43) WIP (37) Field IOT Data Throughput
HRPD (D70)	OMH Specific Optional OMH Specific DO intwk (94) DO rel0 perf (33) DO revA perf (33A) DO revA conf (38A) WIP (37) Field IOT Data Throughput
WAP (D75)	OMH Specific Optional OMH Specific OMH IOT WAP Field Optional WAP Field WAP IOT
MMS (D80)	OMH Specific Optional OMH Specific OMH IOT MMS Conf Optional MMS Conf MMS Field Optional MMS Field
Java (D85)	OMH Specific Optional OMH Specific OMH IOT

Device Requirements (this document)	***Acceptance Test Plans [CDG183]***
BREW (D90)	OMH Specific Optional OMH Specific OMH IOT
LBS (D95)	OMH Specific Optional OMH Specific Field IOT

1

<page left blank intentionally>

14. Terminology

Acronyms	*Meaning*
3GPD	3G Packet Data
AMR NB	Adaptive Multi-Rate Narrow Band
BCD	Binary Coded Decimal
BOM	Byte Order Mark
BREW	Binary Runtime Environment for Wireless
BS	Base Station
CATPT	Card Application Toolkit Protocol Teleservice
CAVE	Cellular Authentication and Voice Encryption
CCAT	CDMA Card Application Toolkit
CDR	Call Detail Records
CHAP	Challenge Handshaking Authentication Protocol
CO	Cache Operation
cPRL	Concatenated PRL
CRC	Cyclical Redundancy Checking
DELI	Delivery Context Library for CC/PP and UAProf
DNS	Domain Name Server
DRM	Digital Rights Management
DTMF	Dual Tone Multi Frequency
EF	Elementary File
EIR	Equipment Identity Register
EPRL	Extended PRL
EPZID	Extended Packet Zone Identifier
ESN	Electronic Serial Number
ESN/MEID	Electronic Serial Number/Mobile Equipment Identifier

Acronyms	***Meaning***
EUMID	Expanded UIM Identifier
FTAP	Forward Test Application Protocol
HAT	Hysteresis Activation Timer
HRPD	High-Rate Packet Data
ICCID	Integrated Circuit Card Identifier
IMSI	International Mobile Subscription Identifier
IOT	Inter-Operability Test
IP	Internet Protocol
JVM	Java Virtual Machine
LBS	Location Based Services
MEID	Mobile Equipment Identifier
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Center
MO	Mobile Originated
MPC	Mobile Positioning Center
MSC	Mobile Switching Center
MT	Mobile Terminated
NAI	Network Address Identifier
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OMH	Open Market Handsets
OTA	Over-the-Air
OTAPA	Over-the-Air Parameter Administration
OTASP	Over-the-Air Service Provisioning
PAP	Password Authentication Protocol
PDE	Position Determination Entity
PDU	Protocol Data Unit
pESN	Pseudo Electronic Serial Number
pUMID	Pseudo UIM Identifier
PKI	Public Key Infrastructure

Acronyms	***Meaning***
PLCM	Public Long Code Mask
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
QCIP	Quarter Common Intermediate Format (176 pixels x 144 pixels)
RTAP	Reverse Test Application Protocol
R-UIM	Removable User Identity Module
SI	Service Indication
SIR	Session Initiation Request
SMIL	Synchronized Multimedia Integration Language
SMS	Short Message Service
SMSC	Short Message Service Center
SMS-PP	Short Message Service Point to Point
TLS	Transport Layer Security
UAProf	User Agent Profile
UI	User Interface
UIMID	UIM Identifier
UTK	UIM Toolkit
WAP	Wireless Application Protocol
WBMP	Wireless Bitmap
WML	Wireless Markup Language
WTA	Wireless Telephony Application
xHTML	eXtensible Hypertext Markup Language

1

1

2 <page left blank intentionally>

15. References

[CDG166] CDG Reference Document 166, *OMH R-UIM Specification*.

www.cdg.org/omh

[CDG183] CDG Reference Document 183, *OMH Device Test Plan*.

www.cdg.org/omh

[CR1001] 3GPP2 C.R1001-E (TSB-58E), *Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards,* v1.0, September 30, 2005.

www.3gpp2.org/Public_html/specs/C.R1001-E_v1.0_051004.pdf

[CS0002] 3GPP2 C.S0002, *Physical Layer Standard for cdma2000 Spread Spectrum Systems*, June 2010.

http://www.3gpp2.org/Public_html/specs/C.S0002-E_v2.0_cdma2000_1x_PHY.pdf

[CS0003] 3GPP2 C.S0003, *Medium Access Control (MAC) Standard for cdma2000 Spread Spectrum Systems, June 2010.*

http://www.3gpp2.org/Public_html/specs/C.S0003-E_v2.0_cdma2000_1x_MAC.pdf

[CS0004] 3GPP2 C.S0004, *Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems*, June 2010.

http://www.3gpp2.org/Public_html/specs/C.S0004-E_v2.0_cdma2000_1x_LAC.pdf

[CS0005] 3GPP2 C.S0005 (IS-2000), *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*, v3.0, June 15, 2000.

www.3gpp2.org/Public_html/specs/C.S0005-0_v3.0.pdf

[CS0011] 3GPP2 C.S0011-C, *Recommended Minimum Performance Standards for cdma2000 Spread Spectrum Mobile Stations*, March 2006.

http://www.3gpp2.org/Public_html/specs/C.S0011-C_v2.0_060315.pdf

[CS0014] 3GPP2 C.S0014-C, *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems*, v1.0, January 2007.

www.3gpp2.org/Public_html/specs/C.S0014-C_v1.0_070116.pdf

[CS0015] 3GPP2 C.S0015-A (TIA-637B), *Short Message Service (SMS) for Wideband Spread Spectrum Systems*, v2.0, September 30, 2005.

www.3gpp2.org/Public_html/specs/C.S0015-A_v2.0_051006.pdf

[CS0016] 3GPP2 C.S0016-C (TIA-683C), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*, v1.0, October 22, 2004.

www.3gpp2.org/Public_html/specs/C.S0016-C_v1.0_041025.pdf

[CS0017] 3GPP2 C.S0017-001-A, *Data Service Options for Spread Spectrum Systems*, v1.0, June 11, 2004.

www.3gpp2.org/Public_html/specs/C.S0017-001-A_v1.0_040617.pdf

[CS0023] 3GPP2 C.S0023-D, *Removable User Identity Module for Spread Spectrum Systems*, v1.0, June 29, 2009.

http://www.3gpp2.org/Public_html/specs/C.S0023-D_v1.0_R-UIM-090720.pdf

[CS0024] 3GPP2 C.S0024-B, *cdma2000 High Rate Packet Data Air Interface Specification*, v2.0, March 2007.

www.3gpp2.org/Public_html/specs/C.S0024-B_v2.0_070624.pdf

[CS0031] 3GPP2 C.S0031, *Signaling Conformance Tests for cdma2000 Spread Spectrum Systems*

[CS0035] 3GPP2 C.S0035-A, *CDMA Card Application Toolkit (CCAT),* v1.0, February 18, 2005.

www.3gpp2.org/Public_html/specs/C.S0035-A_v1.0_050224.pdf

[CS0038] 3GPP2 C.S0038-0, *Signaling Conformance Specification for High Rate Packet Data Air Interface*, April 2004.

http://www.3gpp2.org/Public_html/specs/C.S0038-B_v1.0_HRPD_SigConf_Spec-090402.pdf

[CS0044] 3GPP2 C.S0044-0, *Interoperability Specification for cdma2000 Air Interface*, October 2004.

http://www.3gpp2.org/Public_html/specs/C.S0044-0_v1.0_040929.pdf

[CS0057] 3GPP2 C.S0057-D, Version 1.0, *Band Class Specification for cdma2000 Spread Spectrum Systems*, September 2009.

http://www.3gpp2.org/Public_html/specs/C.S0057-D_v1.0%20Band%20Class%20.pdf

[CS0066] 3GPP2 C.S0066-0, *Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems*, v2.0, July 25, 2008

www.3gpp2.org/Public_html/specs/C.S0066-0_v2.0_080729.pdf

[CS0068] 3GPP2 C.S0068-0, *ME Personalization for cdma2000 Spread Spectrum Systems*, v1.0, May 26, 2006.

www.3gpp2.org/Public_html/specs/C.S0068-0_v1.0_060530.pdf

[CS0072] 3GPP2 C.S0072-0, *Mobile Station Equipment Identifier (MEID) Support for cdma2000 Spread Spectrum Systems*, v1.0, July 22, 2005.

http://www.3gpp2.org/Public_html/specs/C.S0072-0_v1.0_050727.pdf

[JAVA] JSRs: Java Specification Requests

www.jcp.org/en/jsr/all

[OMARC] OMA-MMS-ARCH-v1_2-20050301-A, *Multimedia Messaging Service Architecture Overview*, v1.2, March 2005.

www.openmobilealliance.org/release_program/docs/MMS/V1_2-20050429-A/OMA-MMS-ARCH-v1_2-20050301-A.pdf

[OMCON] OMA-MMS-CONF-V1_2-20040727-C, *MMS Conformance Document*, v1.2, September 2003.

www.openmobilealliance.org/release_program/docs/MMS/V1_2-20030923-C/OMA-MMS-CONF-V1_2-20030929-C.pdf

[OMCTR] OMA-MMS-CTR-V1_2-20050301-A, *Multimedia Messaging Service Client Transactions*, v1.2, March 2005.

www.openmobilealliance.org/release_program/docs/MMS/V1_2-20050301-A/OMA-MMS-CTR-V1_2-20050301-A.pdf

[OMENC] OMA-MMS-ENC-v1_2-20040323-C, *Multimedia Messaging Service Encapsulation Protocol*, v1.2, March 2004.

http://member.openmobilealliance.org/ftp/Public_documents/MWG/MMS/Permanent_documents/OMA-MMS-ENC-v1_2-20040323-C.zip

[OWAP] *OMA-ERELD-Browser_Protocol_Stack-V2_1-20050204-C, Enabler Release Definition for Browser Protocol Stack Candidate*, v2.1, February 4, 2005.

www.openmobilealliance.org

[OWPVC] *OMA-WAP-ProvCont-v1_1-20050428-C, Provisioning Content,* v1.1, April 2005.

www.openmobilealliance.org

[TS11.11] 3GPP TS11.11, Digital cellular telecommunications system (Phase 2+); *Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface*, v8.14.0 (2007-06).

www.3gpp.org/specs/specs.htm

[TS23.140] 3GPP TS23.140, *MMS Stage 2 Functional Description*, v6.14.0, September 2006.

www.3gpp.org/ftp/Specs/html-info/23140.htm

[UNICODE] *Unicode standard*, version 5.2.0, October 2009.

http://www.unicode.org/versions/Unicode5.2.0/

[XS0008] 3GPP2 X.S0008-0, *MAP Support for the Mobile Equipment Identity (MEID)*, January 2004.

http://www.3gpp2.org/Public_html/specs/X.S0008-0_v3.0_090130.pdf

[XS0016-0] 3GPP2 X.S0016, *MMS Specification Overview, Messaging System Specification*, Rev B, v1.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-000-B_v1.0_040616.pdf

[XS0016-2] 3GPP2 X.S0016-200-0 (TIA-934-200), *MMS Stage 2 Functional Description,* v2.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-200-0_v2.0_040707.pdf

[XS0016-3] 3GPP2 X.S0016-310-0 (TIA-934-310), *MMS MM1 Stage 3 Using OMA/WAP,* v2.0, June 2004.

www.3gpp2.org/Public_html/specs/X.S0016-310-0_v2.0_040617.pdf

[XS0033] 3GPP2 X.S0033-0, Version 2.0, *OTA Support for MEID*, February 2006.

http://www.3gpp2.org/Public_html/specs/X.S0033-0_v2.0_060301.pdf

1

16. Appendix: MEID/EUIMID Support

16.1 Overview

This section describes Mobile Equipment Identifier/Expanded UIM Identifier (MEID/EUIMID) usage as it relates to OMH-compliant devices, R-UIMs, and networks.

The TIA projection in May 2007 shows that ESN manufacturer code address space for handsets will be exhausted in late 2007. The UIMID manufacturer code space for R-UIMs is also expected to be exhausted in the near future. Accordingly, non-unique values will be used in ESN/UIMID fields previously depended upon to be unique.

If no steps are taken in the network and back-end systems to accommodate this change, possible impacts include:

- Crosstalk, interference, and dropped calls due to Public Long Code Mask (PLCM) collision
- Misaddressed air interface messaging (e.g., receive other users' SMS)
- Inability to provision and/or bill some subscribers (fail uniqueness check in back-end)
- Spurious Fraud Detection alerts may occur at the back-end systems, due to the non-uniqueness of pESN/pUIMID

In response to these events, the cdma2000 industry is migrating handsets from ESN- to MEID-based addressing, and R-UIMs from UIMID- to EUIMID-based addressing. These expanded fields will allow for continued unique identification of devices.

As OMH compliant devices will all be new devices, it is imperative that they support the expanded identifiers. Networks used with OMH devices should also support the usage of MEID/EUIMID.

16.2 MEID

The MEID is a new 56-bit identifier assigned by the mobile station manufacturer that uniquely identifies the mobile station equipment. The MEID is intended to address the exhaustion of the ESN resource. It may be represented as a 14-character hexadecimal string, or as an 18-digit decimal number.

OMH-compliant devices ***shall*** all support MEID.

Note: EUIMID cannot be used unless the handset is MEID capable.

In cases where an MEID-capable device is accessing a network that does not support MEID, the device may use pESN to place a call, although there is a risk of collision.

16.3 EUIMID

The EUIMID is a new identifier designed to address the exhaustion of the UIMID resource. It is defined in [CS0023], where two different formats of EUIMID are described: Short Form EUIMID (SF_EUIMID) and Long Form EUIMID (LF_EUIMID). Each of these is described in the following subsections.

The Usage Indicator (EF_{USGIND}) specifies whether the ESN or UIMID should be used for identification and Cellular Authentication and Voice Encryption (CAVE) authentication, and whether MEID or EUIMID should be used for identification.

Operators using OMH handset/cards may choose to use short-form or long-form EUIMIDs to meet their particular needs. Each has advantages and disadvantages, as noted below.

16.3.1 Long Form EUIMID (LF_EUIMID)

The Long Form EUIMID (LF_EUIMID) is equal to the value of Integrated Circuit Card Identifier (ICCID) of the card. The ICCID is an 18-digit Binary Coded Decimal (BCD) (72-bit) identifier assigned to the physical R-UIM card. The ICCID is currently present on all R-UIM cards (as well as GSM SIM cards). The ICCID is typically printed on the card, and is also stored electronically.

Note: LF_EUIMID is not used for identification of the mobile by the network; pUIMID as derived by the ICCID is used instead.

Advantages of LF_EUIMID include the following:

- **Simplicity.** The ICCID is an existing identifier for the card. There are no new storage requirements in terms of files on the R-UIM to support LF_EUIMID. Administration procedures are already established for ICCID.
- **Backward compatibility.** With no new data structures to support, current cards (which may not support [CS0023]) can simply have the pUIMID programmed into the EF_{RUIMID} file on the card, and operate as LF_EUIMID cards. Similarly, there are no new requirements on devices to support LF_EUIMID.
- **EIR Support.** Since the device MEID (if present) remains available, use of LF_EUIMID allows the implementation of an Equipment Identity Register (EIR) to track/block lost/stolen devices.

Disadvantages of LF_EUIMID include the following:

- **Not retrievable.** The LF_EUIMID is not retrievable from the card via any currently standardized air interface messaging. This can have an impact on OTASP sessions, where (depending on operator implementation) there can be a need to receive a unique card identifier in order to access card-specific information.

- **Long Identifier.** The 72-bit ICCID, if used to track the card, will require separate handling from the device MEIDs. As a longer identifier, it is also arguably more prone to keying errors (although a check digit mechanism is defined for ICCIDs).

16.4 Short Form EUIMID (SF_EUIMID)

The Short Form EUIMID (SF_EUIMID) is a 56-bit identifier, which shares address space with the MEID. A section of the MEID space would be reserved for EUIMID allocation.

An additional option is available with use of the SF_EUIMID, namely the setting of bit 2 of the Usage Indicator octet. When the bit is set to 0 (SF_EUIMID does not override ME MEID), use of the SF_EUIMID shares the disadvantages but not the advantages of the LF_EUIMID; that is, it is not retrievable from the card, yet it requires new storage and handling capabilities. One benefit of using a common identifier size to track both cards and devices does not seem sufficient to warrant the use of this configuration. Accordingly, the advantages and disadvantages listed below assume the Usage Indicator bit 2 is set to 1 (i.e., the SF_EUIMID is used in place of the ME MEID).

Advantages of SF_EUIMID include the following:

- **Familiarity.** Use of the SF_EUIMID represents a minimal change from current operation, where the UIMID overrides the device ESN.
- **Retrievable.** The unique SF_EUIMID is available from the MS in either the Status Response Message or the Extended Protocol Capability Response Message. (Both methods require the device itself to have an MEID.)
- **Common Identifier.** Both the card and the device can be managed by a commonly formatted and administered 56-bit identifier (although the device MEID is no longer available via air interface signaling).

Disadvantages of SF_EUIMID include the following:

- **Card/device requirements.** The SF_EUIMID is defined in [CS0023]. Cards and devices that do not support this level of the standard (or at least this aspect of this level of the standard) will not be able to override the device MEID.
- **Stolen Phone.** Since the device MEID is not transmitted to the network, it is not possible to take advantage of the newly defined CheckMEID operation to track lost/stolen phones.

16.5 Network Support of MEID/EUIMID

Networks supporting OMH devices should support the usage of MEID/EUIMID. Accordingly, the following network recommendations apply:

- **Add [CS0072] support in the network.** [CS0072] allows Base Station (BS)-assigned PLCMs to prevent cross-talk and dropped calls due to pUIMID-based PLCM, and also allows the MEID/SF_EUIMID to be retrieved from the device.
- **Stop ESN-based addressing on paging channel.** Duplicated pUIMIDs can cause unpredictable results, since more than one mobile may process a message intended

for a single MS. The alternative is to move to International Mobile Subscription Identifier (IMSI) based addressing.

- **Check security impacts of IMSI-addressed messages.** Deliberate reprogramming of a mobile can allow IMSI-addressed messages to be received by multiple mobiles. Avoiding paging channel SMS may mitigate the potential security impacts of the address change.
- **Remove back-end dependency on unique UIMID and ESN.** The specific actions will depend on the operator's systems, and may apply to billing, provisioning, fraud systems, etc. Either the UIMID uniqueness check may be relaxed, or the check may be applied to the EUIMID instead (assuming EUIMID is reliably available at the necessary location). Inventory management, etc., may also need to move from the ESN to the MEID to track/report on devices (even though these identifiers may not be available in air interface signaling).
- **Evaluate [XS0008] support.** Operators may choose to implement X.S0008 (MEID for ANSI-41) in their networks. This decision can be useful in stolen phone scenarios (with LF_EUIMID) to allow a unique card identifier to be stored in the HLR (with SF_EUIMID). Implementation of an Equipment Identity Register is at the operator's discretion.
- **Evaluate MEID/SF_EUIMID inclusion in Call Detail Records (CDRs).** Operators may choose to include MEID/SF_EUIMID in their Mobile Switching Center (MSC) billing records, with associated upgrades to the billing system needed to parse this new record.
- **Ensure Uniqueness of NAIs.** NAIs derived from the UIMID should be replaced with EUIMID-derived NAIs (e.g., EUIMID@realm).
- **Add support for MEID as EVDO HardwareID.** HardwareID is the MEID value on the device, not the SF_EUIMID on the R-UIM.
- **Outbound Roaming Support.** Operators should recognize that not all roaming partners may support the MEID/EUIMID migration to the same degree. MEID/SF_EUIMID inclusion should not be mandatory (from the perspective of the receiving entity and any subsequent processing) on any inter-network interface, including:
  - ANSI-41 Interfaces
  - CIBER Records
  - A12 Authentication
- **CIBER Record Population.** Assuming both a 32- and a 56-bit identifier are captured in the MSC CDR (which may be either ESN/pESN/UIMID/pUIMID or MEID/SF_EUIMID, respectively), the following approach is recommended for population of the single identifier field in the CIBER record:
  - If the identifiers are hash-related, use the 56-bit identifier.
  - If the identifiers are not hash-related, use the 32-bit identifier.
- **Unique pUIMIDs.** If operators are struggling to accommodate duplicate pUIMIDs in the required timeframe, a potential mitigation approach is to require only distinct

pUIMIDs to be delivered to them from R-UIM manufacturers. This is a last resort action only, and is otherwise discouraged, for the following reasons:

- It may distract operators from properly addressing the required updates.
- It may impose an unreasonable management burden on R-UIM manufacturers, and cause them to "waste" large numbers of EUIMIDs.
- It becomes progressively more difficult to implement, as the number of deployed pUIMIDs rises.
- Only ~16.7 million different pUIMIDs are available; beyond this, uniqueness is not possible.
- Collisions or duplications due to roamers are not addressed; they may still occur beyond the operator's control.

16.6 OTASP Systems and MEID/EUIMID

It is also recommended that operators supporting OTASP systems comply with the following recommendations for supporting the provisioning of MEID/EUIMID-capable handsets:

- **Support [CS0066] for OTASP if unique card information is required.** If OTASP is used in the operator's network, and there is a need to reference card-specific information (e.g., A-key, SPC, etc.) during the OTASP process, then [CS0066] should be supported to allow the EUIMID to be transferred to the OTAF. Note that this applies only to SF_EUIMID (LF_EUIMID is not retrievable over the air).
- **Avoid static card-specific information in OTASP if a unique identifier is unavailable.** If no unique card identifier is retrievable (e.g., LF_EUIMID is used), alternative approaches to card-specific information should be used, instead of indexing a pre-provisioned database. These could include:
  - Secure generation of A-key during OTASP session
  - Cards issued with a default SPC, set to a random value during OTASP session

  The lack of a unique identifier may also prompt operators to implement PIN- or PRL-based methods to ensure that the activation is completed to the correct operator.
- **Index OTASPCallEntry by Activation MIN.** Activation MIN provides a unique reference for any element involved in the OTASP process. Indexing on this value allows for pUIMID duplication, and does not require [XS0033] support as would be the case if SF_EUIMID were used as the index value.

<page left blank intentionally>

17. Appendix: Concatenated PRL Usage

17.1 Overview

[IS683C] defines a newer version of PRL called EPRL (Extended Preferred Roaming List) to support 1xEV-DO AT's system selection and acquisition. It includes 1xEV-DO acquisition records and 1xEV-DO system records, in addition to 1x records.

Concatenated PRL (cPRL) accommodates storage of IS-683A PRLs (legacy format) and IS-683C PRLs (the newer EPRL format) together in the existing EF_{PRL} file on the R-UIM. This solution preserves backward compatibility while accommodating forward compatibility.

Usage by device:

The device (1x only or hybrid) reads the cPRL from the EF_{PRL} in the R-UIM and parses it, as described in Section 17.2 below. The device performs 1x or 1xEV-DO system selection based on the IS-683A or IS-683C PRL in the cPRL.

The OTASP/OTAPA download procedures and SMS-PP download procedure for cPRL will be the same as that used for downloading an existing IS-683A PRL.

Usage by network:

If the network is 1xEV-DO capable, it will use the cPRL format to download the cPRL to the devices and R-UIMs for updating the PRL and EPRL information. If the network is not 1xEV-DO capable, it will then use the existing IS-683A PRL format to download to the devices and R-UIMs for updating.

The OTASP/OTAPA download procedure and SMS-PP download procedure used by the network for cPRL will be the same as those used for downloading a normal PRL.

17.2 cPRL Format and Parsing

Below is the format of cPRL, which is defined as a package with a Package CRC at the end after concatenating IS-683A PRL and IS-683C EPRL.

	cPRL Fields	Length (bits)	Comments
PRL: 1x information	PR_LIST_SIZE	16	
	PR_LIST_ID	16	
	PREF_ONLY	1	
	DEF_ROAM_IND	8	
	NUM_ACQ_RECS	9	
	NUM_SYS_RECS	14	
	ACQ_TABLE	Variable	
	SYS_TABLE	Variable	
	RESERVED	0 to 7	
	PR_LIST_CRC	16	CRC of PRL
EPRL: 1x and 1xEV-DO information	PR_LIST_SIZE	16	
	PR_LIST_ID	16	
	CUR_SSPR_P_REV	8	
	PREF_ONLY	1	
	DEF_ROAM_IND	8	
	NUM_ACQ_RECS	9	
	NUM_COMMON_SUBNET_RECS	9	
	NUM_SYS_RECS	14	
	RESERVED	7	
	EXT_ACQ_TABLE	Variable	
	COMMON_SUBNET_TABLE	Variable	
	EXT_SYS_TABLE	Variable	
	RESERVED	As needed	
	PR_LIST_CRC	16	CRC of EPRL
PACKAGE CRC	PACKAGE_CRC	16	CRC for cPRL

The general steps to parse the cPRL are as follows:

1. Parse the PRL part, and use PR_LIST_CRC of the PRL to verify its integrity.
2. Parse the EPRL part, and use PR_LIST_CRC of the EPRL to verify its integrity.
    a. If the CRC check fails, it will be assumed that the whole data block contains PRL only and has no EPRL in it. The parsing stops here.
    b. If the CRC check succeeds, the integrity of the whole data block is verified by checking the PACKAGE_CRC.
        1. If the PACKAGE_CRC check fails, the whole data block is then not valid.
        2. If the PACKAGE_CRC check succeeds, the whole data block is valid with both PRL and EPRL in it. Parsing stops here.

<page left blank intentionally>