Open Market Handset (OMH) Device and Network Specification

CDG Document 167

Submitted to CDG OMH SIG
by Reliance, Tata, and Qualcomm

January 2008

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

Reviewed By

Company	Area	Name	Contact
Reliance	Handset	Bhakti Nimkar	bhakti.nimkar@relianceada.com
Reliance	Handset	Trishala Nambiar	trishala.nambiar@relianceada.com
Reliance	VAS	Debasis Das	debasis.das@relianceada.com
Reliance	Testing	Ajay Mathur	ajay.a.mathur@relianceada.com
Tata	Technology	Kshitij Keote	kshitij.keote@tatatel.co.in
Tata	Technology	Santoshi Rana	santoshi.rana@tatatel.co.in
Tata	VAS	Vikram Karandikar	vikram.karandikar@tatatel.co.in
Qualcomm	CDMA Initiatives	Bryan Gurganus	bryang@qualcomm.com
Qualcomm	BREW	David Park	dpark@qualcomm.com
Qualcomm	LBS	Kirk Burroughs	kirkb@qualcomm.com
Qualcomm	CDMA Initiatives	Bryan Cook	bcook@qualcomm.com

Update History

Version	Date	Description of changes
0	*OCT07*	• *Initial draft for review*
A	*NOV07*	• *Significant update of text*
B	*JAN08*	• *Significant update of text*
1.0	**JAN08**	• **Initial release version**

Contents

1. Overview

The Open Market Handset (OMH) initiative is a strategic effort to benefit the CDMA ecosystem by enabling open distribution of handsets across networks and regions by expanding R-UIM capabilities to support a full set of competitive features and standardizing a uniform device and network 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)
- WAP/Browser Functionality
- Multimedia Message Service (MMS)
- JAVA
- BREW
- R-UIM based Applications
- High Rate Packet Data (1xEV-DO)
- Location Based Services (LBS)

This document contains the guidelines for OMH devices and networks. It is a complementary document to [CDG166].

2. R-UIM Compatibility

Below is a high-level view of behavior for different combinations of OMH and non-OMH compliant R-UIMs and devices.

User Puts…	Into...	Result
Legacy R-UIM	Legacy Device	Existing behavior.
OMH R-UIM	Legacy Device	Voice and SMS based on R-UIM, but additional features must be provisioned in the device.
Legacy R-UIM	OMH Device	Voice and SMS based on provisioning in R-UIM. User must upgrade R-UIM to access data services.
OMH- R-UIM	OMH Device	User accesses new OMH features. Configuration data missing in the R-UIM may be entered manually or OEM provisioned in the device.

Figure 2-1: Device and R-UIM Compatibility Matrix

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 only support voice and SMS. To access data services, subscribers with OMH devices must upgrade their legacy R-UIMs[1].

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

---

[1] The option of allowing the user to use a legacy R-UIM and manually configure data on the device was explored. However, this option introduces undesirable behavior. Namely, if the device were later sold on the secondary market and the purchaser also used a legacy R-UIM, the device would continue to use the manually configured data from the previous owner.

2.1.1 Device

- When a legacy R-UIM is inserted into an OMH device, the device should inform the user that they need to upgrade their R-UIM in order to obtain data services
- 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 user that they need to upgrade their R-UIM in order to obtain data services.
- An OMH device ***shall*** prohibit the manual provisioning of the extended OMH configuration parameters. This is required because the use of two different legacy cards can create unwanted behavior.

2.1.2 Network

- None

3. Mechanisms

3.1 R-UIM Commands

For a list of R-UIM Commands that ***shall*** be supported by both the device and R-UIM, refer to the "R-UIM Commands" section of [CDG166]

3.2 Authentication

OMH supports standard voice and data authentication mechanisms defined in [CDG90].

3.2.1 Device

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

3.2.2 Network

- The network ***shall*** support CAVE-based authentication defined in [CDG90].
- The network may support packet data authentication mechanisms

3.3 Subsidy Lock

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 may do so by working with the device OEM to implement their desired personalization mechanism on the device. At that point, however, it would no longer be considered an OMH device.

3.3.1 Device

- If a device has OMH branding on it, it ***shall not*** have subsidy locks.

3.4 Carrier Customization

3.4.1 Device

- If present, the device ***shall*** display the operator name provisioned in $\mathbf{EF_{SPN}}$
- If present, the device should display home screen and logo images provisioned on the R-UIM ($\mathbf{EF_{IMG}}$)
    - The device ***shall*** scale images provisioned on the R-UIM to the resolution/capabilities of the device's screen before displaying them
    - On the RUIM; IMG gone from R-UIM (We'll get rid of it here too)
- If an application label has been provisioned for a particular application in $\mathbf{EF_{AppLabels}}$, the device's user interface should display this text label with the associated icon or menu item used to launch that application
- None

3.5 CDMA Card Application Toolkit (CCAT)

CCAT provides the interface between the device and the R-UIM. CCAT is defined in [CS0035].

3.5.1 Device

- The device ***shall*** support all CCAT items identified in [CDG166]
  The intention is 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.

3.5.2 Network

- The network may support the CCAT SMS-PP Download mechanism.
  This mechanism provides the ability to modify provisioning data on the R-UIM using SMS messaging. Note that CCAT SMS-PP allows the provisioning of new data elements defined in [CDG166], whereas OTASP/OTAPA does not.

3.6 Device and Model Identification

Device identification refers to the ESN/MEID of the device and the UIMID/EUIMID of the card. Requirements are provided below for the device and network, but more detailed information regarding OMH and device identification can be found in the *Appendix: MEID/EUIMD 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.

3.6.1 Device

- The device ***shall*** support MEID[2] as defined in [CDG90].
- The device ***shall*** be provisioned with a properly formed MEID
- The device ***shall*** be provisioned with an ESN containing the pESN value derived from the device's MEID.
- If SF_EUIMID is being used, the device ***shall*** use EF$_{USGIND}$ (Usage Indicator) to determine whether to use SF_EUMID or MEID for network identification as defined in [CDG166]
- Operators may use either Short Form (SF_EUIMID) or Long Form (LF_EUIMID) EUIMIDs. The advantages and disadvantages of each are captured in the *Appendix: MEID/EUIMD Support* section of this document
- Just as the device writes its ESN/MEID to the R-UIM during power up, it ***shall*** also write its model information to the R-UIM

3.6.2 Network

- The network ***shall*** support the 3GPP2 C.S0072 standard.
- Additional network recommendations regarding MEID and EUIMID, as well as the advantages and disadvantages of Short Form (SF_EUIMID) or Long Form (LF_EUIMID) EUIMIDs, are provided in the *Appendix: MEID/EUIMD Support* section of this document.

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

3.7.1 CCAT / UTK Data Download

3.7.1.1 Device

- The device ***shall*** support CCAT SMS-PP data download mechanism as defined in 3GPP2 C.S0035.
- All EFs on the R-UIM ***shall*** be updateable via SMS-PP data download mechanism.

---

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

- The device ***shall*** support UTK SMS-PP data download mechanism
  Note: Rather than using the 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.

3.7.1.2 Network

- The network may support CCAT SMS-PP data download mechanism.
- All EFs on the R-UIM may be updateable via SMS-PP data download mechanism.
- Following an SMS PP data download, the network may send an SMS message asking the user to power cycle in order for changes to take effect.
- The network may support UTK SMS-PP data download mechanism

3.7.2 OTASP/OTAPA

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 that while current OTASP/OTAPA functionality defined in [3GPP2 CS0016] is maintained, the first phase of OMH does not extend OTASP/OTAPA functionality to support new EFs defined in [CDG166].

3.7.2.1 Device

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

3.7.2.2 Network

- The network may support OTASP/OTAPA currently defined in [3GPP2 CS0016]

3.8 Root Certificates

- 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].

3.9 Manual Entry of Application Configuration Data

3.9.1 Device

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 over-the-air provisioning technique to update these data. However, recognizing that not all operators have deployed such techniques, OMH devices provide an option for users to manual enter configuration data such as server addresses.

- Manual entry of configuration data may be supported for:
    - Browser
    - MMS
    - Java
    - LBS
- Manual entry of configuration data ***shall not*** be supported for:
    - Voice
    - SMS
    - 3GPD
    - HRPD
    - BREW
- If manually entered configuration data is supported, it ***shall*** be stored locally on the device to protect the integrity of the R-UIM
- If such data is stored in NV memory on the device, this memory ***shall*** be reset when a new R-UIM is inserted.

3.9.2 Network

- None

4. Voice

No changes should be required to support voice service for R-UIM equipped devices.

4.1 Device

- The device shall comply with voice requirements as defined in [CDG90]
- Voice services on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the Voice section of [CDG166].
- The device ***shall*** support all mandatory service options identified in [CDG90]
- The device ***shall*** also support Service option 68 (4GV-NB)
- The device may Service option 70 (4GV-WB).
- The device ***shall*** be provisioned with a list of all emergency numbers used in OMH markets
- The device ***shall*** allow users to add emergency numbers, but ***shall not*** allow users to delete emergency numbers provisioned by the manufacturer. *(Note that operators can prohibit abuse by blocking emergency calls to invalid emergency numbers at the MSC).*
- The device ***shall*** always permit calls to emergency numbers, even if no R-UIM is inserted.
- The device ***shall*** support enhanced PRLs, described in [CDG86]
- The device ***shall*** be able to receive voice mail notifications via SMS Voicemail Notifications and by Feature Notification Messages as described in [CDG 135].
- The devices ***shall*** support service in the following frequency bands:
    - Bandclass 0, 800 MHz (A and B bands)
- Devices may support service in the following frequency bands:
    - Bandclass 1, 1900 MHz
    - Bandclass 5/11, 450 MHz
    - Bandclass 6, 2100 MHz
    - AMPS, 800 MHz (A and B bands)

- The device ***shall*** support the standard network-based "+" code dialing solution described in [CDG145]
- The device should also provide the user with an option to use a handset-based "+" code dialing solution (e.g. manual programming of the "+" code key)

4.2 Network

The operator's network configuration for voice service ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the Voice section of [CDG166].

- The network ***shall*** support Service option 3 (EVRC)
- The network may support additional service options (e.g. 68 (4GV-NB), 70 (4GV-WB), etc…)
- The network should support "+" code dialing as described in [CDG145]

5. Short Message Service (SMS)

5.1 Device

- The SMS client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM as defined in [CDG90]. For details on this information, see the SMS section of [CDG166].
- The device ***shall*** support MO SMS over access channel
- The device ***shall*** support MO SMS over traffic channel
- The device ***shall*** support service option 6
- The device ***shall*** support service option 14
- The device ***shall*** support MT SMS over paging channel
- The device ***shall*** support MT SMS over traffic channel
- The SMS client on the device should support a device-based long SMS functionality for mobile originated SMS messages that does not depend on network or terminating device support
  (i.e. automatically segment the long SMS message into multiple smaller SMS messages, each with '(x of y)' prepended to the start of the message body)
- The device ***shall not*** send an SMS message that exceeds 140 bytes.
- Devices that perform local segmentation of long SMS messages ***shall*** ensure that no individual segment exceeds 140 bytes.
- The SMS client on the device may support enhanced SMS (EMS)
- The device ***shall*** support Broadcast SMS for receiving information updates and emergency alerts from the network
- The device ***shall*** handle an SMS message received with relative time value of 246 (Immediate) as a Flash SMS
- Multilingual devices ***shall*** encode mobile originated SMS messages with Unicode
- English devices ***shall*** encode mobile originated SMS messages with ASCII
- The device ***shall*** support Unicode, UTF-8, and ASCII for mobile terminated SMS messages
-

5.2 Network

- The operator's network configuration for SMS service ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the SMS section of [CDG166].
- The network ***shall*** support MO SMS over access or traffic channel. It may support both.
  Note: a configuration item on the R-UIM allows the operator to indicate whether their network supports MO SMS over access channel, traffic channel, or both.
- The network ***shall*** support service option 6 or 14. It may support both.
  Note: $\mathbf{EF_{SMSCAP}}$ *on the R-UIM allows the operator to indicate which service option is supported by their network.*
- The network ***shall*** support MT SMS delivery over paging the channel or traffic channel. It may support both.
- The network may support EMS / concatenated SMS
- The network may support Broadcast SMS
- The network may support Flash SMS
- The SMSC ***shall*** ensure that all MT SMS messages are no larger than 140 bytes in length.

6. 3GPD Packet Data

6.1 Device

- Packet data services on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM as defined in [CDG90]. For details on this information, see the 3G Packet Data section of [CDG166].
- The device ***shall*** support service option 33
- The device ***shall*** support Simple IP operation
- The device ***shall*** support both PAP and CHAP authentication
  Note: CHAP authentication algorithms are run on the R-UIM
- The device ***shall*** support Mobile IP operation.
- The device ***shall*** support Mobile IP to Simple IP fallback when Mobile IP is supported.
- The device ***shall*** support IPv4
  Note: IPv6 will be addressed in a later phase

6.2 Network

- The operator's network configuration for 3G Packet Data ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the 3G Packet Data section of [CDG166].
- The network ***shall*** support service option 33
- The network ***shall*** support Simple IP operation
- The network should support Mobile IP operation. The importance of network support of Mobile IP for inbound roaming is discussed in [CDG140].
- The network ***shall*** support IPv4
  Note: IPv6 will be addressed in a later phase

7. HRPD (1xEV-DO)

This section is to be viewed additional requirements to the 3GPD section to support HRPD.

7.1 Device

- The device may support EV-DO service as defined in [CDG143]
- For HRPD, the device ***shall*** perform A12 (AN-AAA) authentication for EV-DO access using access credentials on the R-UIM.

7.2 Network

- The network ***shall*** perform A12 authentication on mobiles accessing EV-DO service

8. WAP/Browser

8.1 Device – General Requirements

- The device OEM ***shall*** be responsible for integrating the browser client
- The browser client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the Browser section of [CDG166].
- If the operator provisions bookmarks on the R-UIM, the browser client on the device ***shall*** present these bookmarks to the user. For details on these bookmarks, see the Browser section of [CDG166].
- The device ***shall*** provide UAProf information to the network.
- The device ***shall*** send its IMSI to the network in the WAP Client ID header
- The device ***shall*** send its MDN to the network in the WAP MSISDN header
- The device should implement the same IP caching and aging support provided by the chipset (e.g. support the same number of DNS retries implemented by the chipset)
- Devices that support both WAP/browser and BREW should support integration of mobile shop and browser (*i.e. basically allows a browser portal to provide a link to the mobile shop to support cross promotion)*
- The device ***shall*** support the following minimum requirements which have been restated, summarized, and/or clarified from [CDG91]. Note that all requirements listed below are mandatory for OMH, regardless of whether they are listed as mandatory in [CDG91].

[CDG91]	***Bearer and Connection Requirements***
2.1.1	The priority data bearer for WAP sessions ***shall*** be EV-DO (service option 59) or CDMA2000 1x-RTT Packet Data (Service Option 33)
2.1.3	The secondary data bearer for WAP sessions ***shall*** be Circuit-Switched Data (Service Option 15).
2.1.3	Switching from the priority to secondary data bearer ***shall*** be

	automatic in cases where there is no CDMA2000 1xRTT Packet Data coverage.
2.1.4	When using the secondary data bearer, the Circuit-Switched Data call ***shall*** be terminated automatically when the user ends the WAP session as defined in [CDG91].
2.5.1, 2.5.3	The device ***shall*** support the provisioning of a list of at least two WAP gateways. If the device cannot connect to the first WAP gateway on the list, the device shall try the next one on the list.
[CDG91]	***WAP 2.0 Support Required by Client***
2.3.1-30	HTTP 1.1 headers, responses, and status codes
2.3.31-34	HTTP 1.1 methods GET, POST, CONNECT, and OPTIONS
2.2.11	HTTP 1.1 basic authentication
2.2.9	HTTP 1.1 caching model
2.2.12	HTTP state management (local cookie storage)
2.2.1	XHTML Mobile Profile
2.2.2-3	WML 1.3 binary and textual forms
2.2.10	Languages supported by the device
2.2.13	Wireless Cascading Style Sheet (WCSS) v1.1
2.2.18	Public WTA function – “Make Call”
2.2.21	User Agent Profile (UAProf) – “Profile URI” header
2.2.24	TLS server authentication for transport layer security
2.2.27	Loading of root certificates in support of Wireless PKI
2.2.28	WAP certificate profiles
2.4.1	Connection-less WAP push of both text and binary using SMS
[CDG91]	***Content Handling Required by Client***
2.2.7-8	MIME content type including multipart/mixed, multipart/related, and multipart/form-data

2.10.1-3 Display of the WBMP, PNG, and JPEG image contents.

2.10.5 Playback of all audio codecs supported by the handset device.

[CDG91] ***OMA Download and DRM Support Required by Client***

2.6.1 OMA DRM forward lock.

2.6.3 OMA Generic Content Download Over-the-Air version 1.0.

8.2 Network

- The operator's network configuration for WAP ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the Browser section of [CDG166].
- The WAP server ***shall*** support at least WAP 2.0
- The WAP server ***shall*** support at least HTTP 1.1
- If a WAP server is being used, the WAP server address ***shall*** be locally routable (i.e. reachable by the device)
- The network ***shall*** provide DNS resolution capability for WAP Gateway Domain Name (PXADDR-FQDN) and Home URL (HomeURL) information provisioned on R-UIM.

9. Multimedia Messaging Service (MMS)

9.1 Device – General Requirements

- The device OEM is responsible for integrating the MMS client
- The MMS client on the device ***shall*** retrieve and use configuration information provisioned on the R-UIM. For details on this information, see the MMS section of [CDG166].
- The device ***shall*** support the 3GPP2 OMA/WAP MM1 implementation of MMS
- The device ***shall*** comply with WAP requirements identified in the *WAP/Browser* section of this document.
- The device ***shall*** comply with the SMS requirements identified in the *Short Message Service (SMS)* section of this document.
- Optional (and not currently used) application authentication for MMS[3] is not supported. Support may be added in a later phase, if needed.
- The device ***shall*** support the following minimum requirements which have been restated, summarized, and/or clarified from [CDG92]. Note that all requirements listed below are mandatory for OMH, regardless of whether they are listed as mandatory in [CDG92].

[CDG92]	***Basic Support Required by Client***
2.2.2	Functionality and features per [TS23.140] and [XS0016-0]
2.2.4-6	OMA MMS Client [OMCON], Transactions [OMCTR], and Encapsulation [OMENC] conformance
2.3.1.12	User Agent Profiles (UAProf)
2.4.11.1-10	Error management and exception handling
[CDG92]	***Message Support Required by Client***

[3] *Authentication performed after receipt of a MMS notification with embedded URL but before retrieval of the MMS message using this URL*

2.3.3.5, 2.4.3.2	Able to download messages from a non-provisioned MMSC
2.4.1.17-19	Able to send messages to one or more MDN's or email addresses in the To, Cc, and Bcc fields
2.4.9.3	Support recipient fields (i.e. To, Cc, and Bcc) up to 312 characters each with the mailbox portion, including punctuation ("<>@"), being no longer than 256 characters
2.4.9.11-13	Able to request delivery confirmation, request read confirmation, and set delivery priority on a per message basis
[CDG92]	***Content Handling Required by Client***
2.3.1.13	Multipart mixed messages of the type multipart/mixed and multipart/related
2.3.2.1-3	Text formats: US-ASCII, UTF-8, UTF-16, ISO/Latin1
2.3.2.6-10	Image formats: JPEG, GIF, PNG, WBMP, and BMP
2.3.2.12-13, 2.3.2.15	Audio types: EVRC, QCELP (13k), WAV, MIDI
2.3.1.9, 2.3.2.25	OMA DRM forward lock
2.4.5.1	SMIL profile presentation

9.2 Network

- The operator's network configuration for MMS ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the MMS section of [CDG166].
- The network ***shall*** comply with WAP requirements identified in the *WAP/Browser* section of this document.
- The MMSC address provisioned on the R-UIM ***shall*** be locally routable (i.e. reachable by the device)
- The network ***shall*** provide DNS resolution capability for the MMSC information provisioned on R-UIM.
- The MMSC ***shall*** allow messages with empty subject and/or bodies

- The network ***shall*** use the WAP Push teleservice ID (i.e. 4100) to push MMS notifications

10. Java

10.1 Device

- The device OEM ***shall*** be responsible for integrating the Java Virtual Machine (JVM) required to support Java applications
- If the operator has provisioned a Java download URL on the R-UIM, the Java download browser client on the device ***shall*** use this URL. For details on this URL, see the Java section of [CDG166].

10.2 Network

- The operator's network configuration for Java ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the Java section of [CDG166].
- If the operator has provisioned a Java download URL on the R-UIM, this server ***shall*** be locally routable (i.e. reachable by the device)
- If the operator has provisioned a Java download URL on the R-UIM, the network ***shall*** provide DNS resolution capability for this server

11. BREW

11.1 Device

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

11.2 Network

- The operator's network configuration for BREW ***shall*** be consistent with the provisioning information on the R-UIM. For details on this information, see the BREW section of [CDG166].

12. Location Based Services (LBS)

12.1 Device

- The device may provide LBS services in accordance with [CDG98], [CDG101], and [CDG111].

12.2 Network

- The network may provide LBS services in accordance with [CDG101] and [CDG111].

13. Terminology

4GV	4th Generation Vocoder
4GV-NB	4th Generation Vocoder Narrow Band
4GV-WB	4th Generation Vocoder Wide Band
AAA	Authentication, Authorization, and Accounting
BREW	Binary Runtime Environment for Wireless
CAVE	Cellular Authentication and Voice Encryption
CCAT	CDMA Card Application Toolkit (for R-UIM)
CHAP	Challenge Handshake Authentication Protocol
DF	R-UIM Dedicated File
DM	Device Management (OMA specification)
DNS	Domain Name System
EF	R-UIM Elementary File
EMS	Enhanced Messaging Service
EVRC	Enhanced Variable Rate Codec
HRPD	High Rate Packet Data (i.e. 1xEV-DO)
HTTP	Hypertext Transport Protocol
IOTA	Internet Over the Air
LBS	Location Based Services
ME	Mobile Equipment

MF	R-UIM Master File.
MMS	Multimedia Messaging System
MMSC	MMS Center
MO	Mobile Originated
MT	Mobile Terminated
NAI	Network Access Identifier
NAM	Number Assignment Module. A set of MIN/IMSI-related parameters stored in the mobile station.
OMH	Open Market Handset
OMA	Open Mobile Alliance
OTAF	Over-the-Air Service Provisioning Function. A configuration of network equipment that controls OTASP functionality and messaging protocol.
OTAPA	Over-the-Air Parameter Administration. Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.
OTASP	Over-the-Air Service Provisioning. A process of provisioning mobile station operational parameters over the air interface.
PAP	Password Authentication Protocol
Phase	Revision level of the R-UIM.
RFU	Reserved for future use.
R-UIM	Removable UIM.
SMS	Short Message Services

SMSC	SMS Center
SMS-PP	SMS Point-to-Point
SO	Service Option. A service capability of the system. Service options may be applications such as voice, data, or facsimile.
SIM	Subscriber Identity Module.
UIM	User Identity Module.
WAP	Wireless Application Protocol

14. References

[CDG86] CDG Reference Document #86. *PRL Enhancements for International Roaming,* v1.0, April 1, 2004

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/86_v1.0.zip

[CDG90] CDG Reference Document #90. *Global Handset Requirements for CDMA – CDMA2000 Voice, SMS, and Data.* v2.1. Sept. 28, 2007.

www.cdg.org/members_only/file_download.asp?fn=ref_docs/90.zip

[CDG91] CDG Reference Document #91. *Global Handset Requirements for CDMA Mobile Browser.* v1.08. April 25, 2005.

www.cdg.org/members_only/file_download.asp?fn=ref_docs/91.zip

[CDG92] CDG Reference Document #92. *CDMA Handset Mobile MMS Requirements.* v1.12. April 26, 2005.

www.cdg.org/members_only/file_download.asp?fn=ref_docs/92.zip

[CDG98] CDG Reference Document #98, *CDMA Handset Mobile LBS Requirements* — V1, v1.0, August 22, 2005

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/98.zip

[CDG101] CDG Reference Document #101*, CDMA Mobile Station LBS Requirements - V2*, v1.0, August 22, 2005

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/101.zip

[CDG111] CDG Reference Document #111, *CDMA User Plane LBS IS801-1 Call Flows,* v1.0, August 22, 2005

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/111.zip

[CDG135] CDG Reference Document #135, *Roaming Voice Mail Deposit, Indicator and Access*, v1.0, December 4, 2006

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/135.zip

[CDG140] CDG Reference Document #140, *Mobile IP Resolution*, v1.0, March 3, 2007

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/140.zip

[CDG145] CDG Reference Document #145, *Plus Code Dialing Requirements,* v1.0, September 12, 2007

http://www.cdg.org/members_only/file_download.asp?fn=ref_docs/145.zip

[CDG166] CDG Reference Document #166. *OMH R-UIM Specification*. v1.0. January 2008.

[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

[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

[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 (TIA-820-C). *Removable User Identity Module for Spread Spectrum Systems*. v1.0. May 26, 2006.
www.3gpp2.org/Public_html/specs/C.S0023-C_v1.0_060530.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

[CS0035] 3GPP2 C.S0035-A. *CDMA Card Application Toolkit (CCAT).* 1.0, February 18, 2005.

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

[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.* Version 2.1, February 4 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

[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

15. Appendix: MEID/EUIMID Support

15.1 Overview

This section describes MEID/EUIMID usage as related to the OMH compliant devices, R-UIMs, and networks. This information is a subset of CDG document #158, "MEID and EUIMID Migration", and that document should be consulted for more detailed information.

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

If there are no steps 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
- Mis-addressed 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 backend 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's imperative that they support the expanded identifiers. Also, networks used with OMH devices should support the usage of MEID/EUIMID.

15.2 Mobile Equipment Identifier (MEID)

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

OMH compliant devices should all support MEID. Note that EUIMID can not be used unless the handset is MEID capable.

In cases where an MEID capable device is accessing a network which doesn't support MEID, the device may use pESN to place a call, although there is a risk of collision.

15.3 Expanded UIM Identifier (EUIMID)

The Expanded UIM Identifier (EUIMID) is a new identifier designed to address the exhaust of the UIMID resource. It is defined in [C.S0023], 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}) to specify whether the ESN or UIMID should be used for identification and 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.

15.3.1 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 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, and pUIMID as derived by the ICCID is used instead.

Advantages of LF_EUIMID include:

- **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 (that may not support C.S0023-C) 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 to track/block lost/stolen devices.

Disadvantages of LF_EUIMID include:

- **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).

15.3.2 Short Form EUIMID (SF_EUIMID)

The Short Form EUIMID (SF_EUIMID) is a 56-bit identifier, sharing 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 – it is not retrievable from the card, yet it requires new storage and handling capabilities. One benefit – that 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:

- **Familiarity**. Use of the SF_EUIMID represents a minimum 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:

- **Card/device requirements**. The SF_EUIMID is defined in C.S0023-C/C.S0065. Cards and devices which 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.

15.4 Network support of MEID/EUIMID

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

- **Add C.S0072 support in the network**. C.S0072 allows 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 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 X.S0008 support**. Operators may choose to implement X.S0008 (MEID for ANSI-41) in their networks. This can be of use for stolen phone scenarios (with LF_EUIMID), or 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 CDRs**. Operators may choose to include MEID/SF_EUIMID in their MSC billing records, with associated upgrades to the billing system to parse this new record.
- **Ensure Uniqueness of NAIs**. Network Access Identifiers (NAIs) derived from the UIMID should be replaced with EUIMID-derived NAIs (e.g. EUIMID@realm).
- **Add support for MEID as EVDO H-ID**. Operators who use the HardwareID in A12 authentication should ensure that MEID/SF_EUIMID is supported as per A.S0008-A. The source of the HardwareID (either card or device) should be carefully verified.
- **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 internetwork interface, including:

  - ANSI-41 Interfaces
  - CIBER Records
  - A12 Authentication
- **CIBER Record Population**. Assuming both a 32- and 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[1][1]
  - 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 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 – these may still occur beyond the operator's control.

15.5 OTASP Systems and MEID/EUIMID

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

- **Support C.S0066 for OTASP if unique card information 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) during the OTASP process, then C.S0066 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 unique identifier 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 default SPC, set to random value during OTASP session

  The lack of 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 X.S0033 support as would be the case if SF_EUIMID were used as the index value.