Open Market Handsets (OMH) Minimum Network Test Plan

CDG Document 173

Version 2.1

February 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

Revision History

Date	Version	Description
Unreleased	1.0	Not included in OMH Enabler Package v1
May 2008	2.0	Initial release; included in OMH Enabler Package v2
May 2009	2.1	• OMH Device with Legacy R-UIM: changed “will not allow data calls” to “may not allow data calls” • UTK SMS-PP Download: added Service n26 • SMS: removed “receive SMS” from Objectives • Added test case for cPRL download via UTK SMS-PP • Added test case for cPRL download via OTAPA/OTASP • Changed “Browser” to “WAP Browser” throughout

<page left blank intentionally>

1. *Introduction*

1.1 Purpose

This document provides sufficient test cases to allow an operator to validate a minimum level of adherence to Open Market Handset (OMH) network requirements. The test cases provided herein are intended to accomplish the following:

1. Validate that the operator provisioning process supports OMH Removable User Identity Module (R-UIM) provisioning.
2. Confirm which OMH-supported mechanisms and features are offered by the operator.
3. Demonstrate that basic functionality such as voice calls and Short Messaging Service (SMS) function properly with OMH devices.
4. Demonstrate that, if implemented by the network, OMH-supported mechanisms such as SMS Point-to-Point (SMS-PP) data download, Multimedia Messaging Service (MMS), WAP Browser, Binary Runtime Environment for Wireless (BREW), Java, SMS, etc., function properly with OMH devices.

1.2 Usage

Details of each test case are provided in this document. This document is intended to be used in conjunction with [CDG174], which provides a consolidated spreadsheet for reporting the result of each test case.

All OMH operators must perform the tests described in this test plan and submit a completed [CDG174] document to OMHinfo@cdg.org in order to be identified as an OMH operator.

If infrastructure equipment from multiple vendors is used in the network under test, relevant tests must be repeated and results recorded with each vendor's equipment. Refer to individual test cases for details.

For those cases requiring logging tools, several options are available to the operator (QXDM, CAIT, Ethereal, etc.).

1.3 Conventions Used

References cited in this document are identified using an abbreviated document number, e.g., [CDG166], and are summarized in *Section 14.*

<page left blank intentionally>

2. *Compatibility*

2.1 OMH Device with Legacy R-UIM

This is a required test case for all operator networks.

2.1.1 Objective

Verify that OMH devices work with legacy cards per [CDG167] Section 2 on the operator's infrastructure.

2.1.2 Setup Notes

- OMH device.
- The device does <u>not</u> contain provisioning for data. (Note: It never should.)
- Legacy (non-OMH) R-UIM; i.e., the R-UIM does not contain service n15 ("Messaging and 3GPD Extensions") in the CDMA service table.
- The R-UIM contains valid provisioning for voice and SMS services.
- The R-UIM does <u>not</u> contain provisioning for data or WAP Browser.

2.1.3 Expected Results

- The OMH device will send and receive voice calls.
- The OMH device will send and receive SMS messages.
- The OMH device may allow data calls.
- When attempting to make a data call, the OMH device may inform the user that he/she needs to upgrade the R-UIM in order to obtain data services.

2.1.4 Procedure

1. Insert the legacy R-UIM card into the device.
2. Power on the device.
3. Place a voice call from the device.
4. Verify that the call is successful.
5. Tear down the voice call.
6. Place a voice call to the device.
7. Verify that the call is successful.

8. Tear down the voice call.
9. Send an SMS message from the device.
10. Verify that the message was sent successfully.
11. Send an SMS message to the device.
12. View the message on the device to verify that it was received successfully.

2.2 Legacy Device with OMH R-UIM

This is a required test case for all operator networks.

2.2.1 Objective

The objective of this test case is to verify that legacy devices work with OMH cards per [CDG167] Section 2 on the operator's infrastructure.

2.2.2 Setup Notes

- Legacy (non-OMH) device.
- The device contains valid provisioning for data and WAP Browser.
- OMH R-UIM.
- The OMH R-UIM contains valid provisioning for voice and SMS.
- The OMH R-UIM contains valid provisioning for data parameters.

2.2.3 Expected Results

- The legacy device will send and receive voice calls.
- The legacy device will send and receive SMS messages.
- The legacy device is able to make a data call.

2.2.4 Procedure

1. Insert the R-UIM card into the legacy device.
2. Power on the device.
3. Place a voice call from the device.
4. Verify that the call is successful.
5. Tear down the voice call.
6. Place a voice call to the device.
7. Verify that the call is successful.
8. Tear down the voice call.
9. Send an SMS message from the device.
10. Verify that the message was sent successfully.

11. Send an SMS message to the device.
12. View the message on the device to verify that it was received successfully.
13. Initiate a WAP Browser session.
14. Verify that a data call is set up by browsing to a couple of pages.
15. Close the WAP Browser.

<page left blank intentionally>

3. *Mechanisms*

3.1 MEID / SF_EUIMID Support

This test case applies only to operator networks that support Mobile Equipment Identifier (MEID)/Short Form Expandable UIM Identifier (SF_EUIMID).

This test case should be performed for each unique combination of Base Station Controller (BSC) and Mobile Switching Center (MSC) vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

3.1.1 Objective

The objective of this test case is to verify that Cellular Authentication and Voice Encryption (CAVE) authentication works successfully on the networks that support MEID.

3.1.2 Setup Notes

- OMH device.
- The device supports both MEID and SF_EUIMID.
- The device is provisioned with an MEID.
- OMH R-UIM.
- Service n8 (SF_EUIMID-based EUIMID) is allocated and activated in the CDMA service table.
- Bits b1 and b2 of the UIM ID/SF_EUIMID Usage Indicator in EF_{USGIND} are set per [CS0023] Section 3.4.32 to indicate the following:
  - b1=1: UIM_ID is used for CAVE authentication and Mobile Station (MS) identification.
  - b2=1: SF_EUIMID is used for MS identification.
- EF_{USGIND} file ID is 3F00/7F25/6F42 per [CS0023].
- The network supports MEID and is provisioned accordingly.
- The network requires CAVE authentication (i.e., sends AUTH=1 and a RAND challenge in the overhead message train).
- Call logging is needed to verify values sent between the device and the network.

- MEID support is indicated by bit 4 of the Station Class Mark (SCM) in the Origination message being set. Normally, if this bit is set, the SCM value seen in the log will be 0x3A.
- The MEID value can be read from NV Item 1943.

Note: The device only sends the MEID value to the network in the extended status response message if it receives a status request message containing RECORD_TYPE 0x27(MEID) from the network.

3.1.3 Expected Results

- CAVE authentication is being used successfully.
- The MEID field sent by the device to the network contains the SF_EUIMID.

3.1.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Place a voice call from the device.
4. Verify that the call is successful.
5. Tear down the voice call.
6. Review the log file to verify that the network is sending AUTH=1 and a RAND challenge value in the overhead message train.
7. Review the log file to verify that the device includes an authentication response (AUTHR) in system access attempts.
8. Review the log file to verify that the MEID field sent by the device to the network contains the SF_EUIMID.

   Note: The device only sends the MEID value to the network in the Extended Status Response message if it receives a Status Request message containing RECORD_TYPE 0x27 (MEID) from the network.

3.2 CCAT SMS-PP Data Download

This test case only applies to operator networks that support the standard CDMA Card Application Toolkit (CCAT) SMS-PP data download mechanism.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

Note that this mechanism can be used to update any Elementary File (EF) on the R-UIM. However, for the purposes of verifying the mechanism, EF_{SPN} will be used. There is no significance to the choice of this particular EF.

3.2.1 Objective

The objective of this test case is to verify that the CCAT SMS-PP data download mechanism functions as expected.

3.2.2 Setup Notes

- OMH device.
- OMH R-UIM.
- Service n26 (Data Download via SMS-PP) is allocated and activated in the CDMA service table.
- Network must prepare two CCAT SMS-PP data download messages:

  <*Message1*> overwrites EF_{SPN} with the text "Test Name."

  <*Message2*> overwrites EF_{SPN} with the original operator name.

3.2.3 Expected Results

- The receipt of <*Message1*> should change the service provider name displayed by the device (after it is power cycled) to "Test Name."
- The receipt of <*Message2*> should change the service provider name displayed by the device (after it is power cycled) back to the original name.

3.2.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Verify that the service provider name displayed by the device is the text provisioned in EF_{SPN} on this R-UIM.
4. Send <*Message1>.*
5. After the message has been received, power off the device.
6. Power the device back on.
7. Verify that the service provider name displayed by the device is "Test Name."
8. Send <*Message2>.*
9. After the message has been received, power off the device.
10. Power the device back on.
11. Verify that the original operator name is now displayed by the device.

3.3 UTK SMS-PP Data Download

This test case applies only to operator networks that support the UIM Toolkit (UTK) version of the SMS-PP data download mechanism.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

Note: Unlike the standard CCAT version, the UTK version of this mechanism only allows for the updating of Preferred Roaming List (PRL) information on the R-UIM.

3.3.1 Objective

The objective of this test case is to verify that the UTK SMS-PP data download mechanism functions as expected.

3.3.2 Setup Notes

- OMH device.
- OMH R-UIM.
- Service n26 (Data Download via SMS-PP) is allocated and activated in the CDMA service table.
- A card reader is needed to read the PRL on the R-UIM.
- The network must prepare two UTK SMS-PP data download messages:

  <*Message*1> modifies the PRL. Note that the modified PRL must still allow the user to acquire the network.

  <Message*2*> restores the original PRL.

3.3.3 Expected Results

- The receipt of <*Message1*> should modify the PRL.
- The receipt of <*Message2*> should restore the original PRL.

3.3.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device and acquire the network.
3. Send <*Message1>.*
4. After the message has been received, power off the device.
5. Remove the R-UIM.
6. Use a card reader to verify that the PRL was modified.
7. Insert the R-UIM back into the device.
8. Power on the device and acquire the network.
9. Send <*Message2>.*
10. After the message has been received, power off the device.
11. Remove the R-UIM.
12. Use a card reader to verify that the original PRL was restored.

4. *Basic Voice Service and Device Operation*

While the behavior of basic voice services is not impacted by OMH, a minimal set of voice services testing is defined as a “sanity test” to ensure that such services are still functioning as expected on the operator’s network.

4.1 Voice Call

This is a required test case for all operator networks.

4.1.1 Objective

The objective of this test case is to verify that the International Mobile Subscriber Identities (IMSIs) are provisioned correctly and the voice call functions as expected.

4.1.2 Setup Notes

- OMH device.
- OMH R-UIM.
- Card reader.

4.1.3 Expected Results

- The voice call is set up.

4.1.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Ensure that the device acquires the network.
4. Originate a mobile-to-land or mobile-to-mobile voice call.
5. Verify the voice path between the two parties.
6. Hang up the call.

<page left blank intentionally>

5. *Short Messaging Service*

5.1 SMS

This test case should be performed for each unique combination of MSC and Message Center (MC) vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

5.1.1 Objective

The objective of this test case is to verify that the OMH devices can send SMS messages and the network can deliver them to the recipient successfully.

5.1.2 Setup Notes

- OMH device.
- OMH R-UIM.
- EF_{SMSCAP} file ID is 3F00/7F25/6F76 per [CDG166].
- Card reader.

5.1.3 Expected Results

- The network should successfully deliver SMS messages to the intended recipient.

5.1.4 Test Method

1. Use the card reader to set the SMS flags field in EF_{SMSCAP} as follows to ensure that SMS messages can be sent on Traffic and/or Access Channel (depending on the size of the SMS):

   bit 1 = 1 (Send on Access enabled)

   bit 2 = 1 (Send on Traffic enabled)

2. Use the card reader to set the SMS Default Service option field in EF_{SMSCAP} to a byte value of 1 (service option 6).
3. Create and send an SMS message.
4. Verify that the operator’s network sends the SMS message to the intended recipient successfully.

5.2 Enhanced Short Messaging Service

This test case applies only to operator networks that support Enhanced Short Messaging Service (EMS) functionality.

This test case should be performed for each unique combination of MSC and MC vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

5.2.1 Objective

The objective of this test case is to verify that EMS functionality works correctly on the network and that the EMS message is sent by the device and forwarded by the network.

5.2.2 Setup Notes

- OMH device.
- EMS device (not necessarily OMH).
- OMH R-UIM.
- EF_{SMSCAP} file ID is 3F00/7F25/6F76 per [CDG166].
- Card reader.

5.2.3 Expected Results

- The EMS message sent should be received completely by the EMS-compliant recipient.

5.2.4 Test Method

1. Use the card reader to set the SMS flag field bit 3 (EMS) = 1 to enable the EMS messages.
2. Create and send a SMS message that exceeds 140 bytes.
3. Verify that the EMS message is sent by the device and delivered by the network to the EMS-capable device.

6. *3G Packet Data*

6.1 Mobile IP Data Call

This test case applies only to operator networks that support 3G packet data and mobile IP (MIP).

This test case should be performed for each Packet Data Serving Node (PDSN) vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

6.1.1 Objective

The objective of this test case is to verify that the mobile IP data call works on a network provider that supports MIP functionality.

6.1.2 Setup Notes

- A MIP data call should be set up.
- OMH device.
- OMH R-UIM.
- Service n38 (MIP) is allocated and activated in the CDMA service table.
- Service n21 (WAP Browser) is allocated and activated in the CDMA service table.
- EF_{MIPUPP} file ID is 3F00/7F25/6F4D per [CS0023].
- $EF_{ME3GPDOPC}$ file ID is 3F00/7F25/6F48 per [CS0023].
- $EF_{3GPDOPM}$ file ID is 3F00/7F25/6F49 per [CS0023].
- EF_{MIPCAP} file ID is 3F00/7F25/6F4B per [CS0023].
- $EF_{WAPBrowserCP}$ file ID is 3F00/7F25/6F7B per [CDG166].
- A card reader is needed to provision the EFs defined above.
- Call logging (both diagnostic and Ethereal) is needed to verify that the MIP data call was established successfully.
  - Verify from the Ethereal logs that (1) the Link Control Protocol (LCP) Configure-Request message sent by the PDSN is rejected by the device that should send out the LCP Configure-reject message, and (2) that, upon the PDSN repeating the LCP Configure-Request [without Point-to-Point Protocol (PPP) authentication request], the device should send a LCP Configure-Ack message to PDSN.

- Next verify that the device sends an IPCP Configure-Request to the PDSN/FA that does not include the IP-Address Configuration option. Verify that the PDSN/FA confirms and acknowledges the device request without assigning an IP address to the device.

6.1.3 Expected Results

- A MIP data call should be set up.

6.1.4 Test Method

1. Provision the b2 (Mobile IP) of $EF_{ME3GPDOPC}$ to 1 to indicate that the OMH device is capable of supporting MIP.
2. Provision the fields of EF_{MIPCAP}.
3. Provision the fields of EF_{MIPUPP} (primary home agent, secondary home agent, MN-AAA_Auth_Algorithm, and MN-HA_Auth_Algorithm).
4. Launch a WAP Browser session, and ensure that the web page can be browsed.

7. *HRPD (1xEV-DO)*

7.1 HRPD Service

This test case applies only to operator networks that support EV-DO service.

This test case should be performed for each unique combination of PDSN, Radio Network Controller (RNC), or AAA-A12 vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next test case.

7.1.1 Objective

The objective of this test case is to verify that the EV-DO service functions correctly using an OMH device and OMH R-UIM.

7.1.2 Setup Notes

- OMH device.
- OMH R-UIM.
- Service n5 (HRPD) is allocated and activated in the CDMA service table.
- $EF_{HRPDCAP}$ file ID is 3F00/7F25/6F56 per [CS0023].
- $EF_{HRPDUPP}$ file ID is 3F00/7F25/6F57 per [CS0023].
- Call logging (both diagnostic and Ethereal) is needed to verify that an EV-DO data call was established successfully.
- Card reader.

7.1.3 Expected Results

- The device should successfully pass A12 authentication.
- The device should set up a successful EV-DO call.

7.1.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Provision field $EF_{HRPDCAP}$ per [CS0023]:
    - MAX_NAI_LENGTH and MAX_SS_LENGTH should be provisioned per [CS0023] and operator's requirements.

  - AUTH_ALGORITHM should allow PPP Challenge Handshaking Authentication Protocol (CHAP) authentication.
4. Provision field $EF_{HRPDUPP}$ per [CS0023]:
   - The Network Address Identifier (NAI) should be a valid A12 NAI provisioned on the network.
   - NAI_LENGTH should be the length of the provisioned NAI.
   - AUTH_ALGORITHM should be set to PPP CHAP (‘0001’).
5. Ensure that the device shows EV-DO service as being available.
6. Launch a WAP Browser session and ensure that a web page can be browsed.
   - Verify through Ethereal logs that the data call was made over EV-DO by ensuring that A12 authentication was successfully passed during the data call.

7.2 cPRL Download via UTK SMS PP Data Download

This test case only applies to operator networks that support the UTK version of the SMS PP data download mechanism.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

7.2.1 Objective

The objective of this test case is to verify that the Concatenated Preferred Roaming List (cPRL) can be successfully downloaded via UTK SMS PP data download.

7.2.2 Setup Notes

- OMH 1X only device.
- OMH Hybrid (1x + 1xEV-DO) device.
- OMH R-UIM.
- Service n26 (Data Download via SMS-PP) is allocated and activated in the CDMA service table.
- EF_{PRL} file ID is 3F00/7F25/6F30 per [CS0023].
- The network must support UTK SMS PP data download mechanism and be able to send a cPRL for downloading to the device.

7.2.3 Expected Results

- The 1x only device should be able to download the cPRL and successfully acquire the system based on the IS-683A entries.
- The hybrid device should be able to download the cPRL and successfully acquire the system based on the IS-683C entries.

7.2.4 Test Method

1. Insert the RUIM in the 1x only device.
2. Power up, and wait until it acquires the network.
3. Start logging.
4. Instruct the BS to send a UTK SMS-PP data download message to update EF PRL/6F30 in the RUIM with a cPRL.
5. Analyze the logs to ensure that the SMS PP message is received by the device and transparently passed on to the RUIM.
6. End logging. Analyze the logs to ensure that the SMS-PP message was received.
7. Power down the device and remove the RUIM.
8. Configure the BS now with the system settings as per cPRL in order to match with the entries listed in the cPRL.
9. Insert the RUIM in the phone and power up.
10. Start logging.
11. Wait until the device acquires the system.
12. End logging.
13. Analyze the logs to ensure that the device acquires the system based on the updated cPRL.

7.3 cPRL Download via OTAPA/OTASP

This test case only applies to operator networks that have the capability to download cPRL over the air to devices.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

Note: This mechanism can be used to download the cPRL in EF_{PRL} on the R-UIM.

7.3.1 Objective

The objective of this test case is to verify that the cPRL can be successfully downloaded using OTAPA/OTASP mechanisms.

7.3.2 Setup Notes

- OMH 1X only device.
- OMH Hybrid (1x +EVDO) device.
- OMH R-UIM.
- EF_{PRL} file ID is 3F00/7F25/6F30 per [CS0023].
- The network sends a cPRL for downloading to the device.

7.3.3 Expected Results

- The 1x only device should be able to download the cPRL and successfully acquire the system based on the IS-683A entries.
- The hybrid device should be able to download the cPRL and successfully acquire the system based on the IS-683C entries.

7.3.4 Test Method

1. Insert the RUIM in the 1x only device.
2. Power up, and wait until it acquires the network.
3. Start logging.
4. Initiate an OTASP call from the device. Verify that it connects successfully.
5. Instruct the BS to provision cPRL on the device.
6. Check if the device shows an indication of successful over-the-air provisioning and remains camped to the network.
7. Power down the device and remove the RUIM.
8. Configure the BS now with the system settings as per cPRL in order to match with the entries listed in the cPRL.
9. Insert the RUIM in the phone.
10. Power up.
11. Start logging.
12. Wait until the device acquires the system.
13. End logging.
14. Analyze the logs to ensure that the device acquires the system based on the updated cPRL.
15. Repeat steps above for the hybrid device.

8. *WAP Browser*

8.1 WAP Browser Home Page

This test case applies only to operator networks that support Wireless Application Protocol (WAP) based browsing.

This test case should be performed for each unique WAP gateway server vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

8.1.1 Objectives

The objectives of this test case are:

- To validate 3GPD authentication using RUIM card credentials against the credentials on the operator's network.
- To ensure that the WAP Browser home page and WAP server address provisioning by the network provider is done correctly in order to allow the device to go to the pre-provisioned home page.

8.1.2 Setup Notes

- OMH device.
- OMH R-UIM.
- Service n21 (WAP Browser) is allocated and activated in the CDMA service table.
- $EF_{WAPBrowserCP}$ file ID is 3F00/7F25/6F7B per [CDG166].
- $EF_{SIPPAPSS}$ file ID is 3F00/7F25/6F50 per [CS0023].
- EF_{SIPUPP} file ID is 3F00/7F25/6F4C per [CS0023].
- A card reader is needed to read $EF_{WAPBrowserCP}$ for the Home URL and to provision the EFs defined above. Also make sure that authentication credentials as per the operator's PRI are provisioned.
- Logging (both diagnostic and Ethereal) is required to verify that the IMSI is sent by the device to the network and that, in the diagnostic tool, log mask has Data Link logging and Data Services logging checked, respectively, for PPP logging.

- In the Ethereal logs, view the contents of the first “TCP segment of reassembled PDU” after the Authentication [Password Authentication Protocol/Challenge Handshaking Authentication Protocol (PAP/CHAP)] messages.
- Verify the IMSI information sent in the GET request (HTTP 1.1 method). Normally it is seen in the logs as X-Wap-ClientID.
- In the same logs, ensure that the User Agent Profile URL is present.

8.1.3 Expected Results

- Upon clicking the WAP Browser’s home page, the user should go to the link as provisioned in the $EF_{WAPBrowserCP}$ home URL information.

8.1.4 Test Method

1. Launch the WAP Browser application.
2. Verify that the home page displayed is the Home URL provisioned in $EF_{WAPBrowserCP}$.
3. Review the log file to verify that the IMSI provisioned on the R-UIM was sent to the network in the WAP-Client-ID header.

9. *Multimedia Messaging Service*

9.1 MMS Messages

This test case applies only to operator networks that support the WAP-based MMS feature.

This test case should be performed for each unique combination of MMSC and WAP gateway server vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

9.1.1 Objective

The objective of this test case is to verify that the OMH devices can send and receive MMS messages and that the network can successfully deliver them to the recipient.

9.1.2 Setup Notes

- OMH device.
- OMH R-UIM.
- $EF_{MMSConfig}$ file ID is 3F00/7F25/6F7E per [CDG166].
- EF_{MMSICP} file ID is 3F00/7F25/6F67 per [CS0023].
- Ensure that the services n40 (MMS) is allocated and activated in the CDMA service table.
- Card reader.
- Ensure that the User Agent Profile for the particular Original Equipment Manufacturer (OEM) model resides on a publicly accessible server.
- In the Ethereal logs, view the contents of the first “TCP segment of reassembled PDU” after the Authentication (PAP/CHAP) messages, and verify that the User Agent Profile is sent in the POST (HTTP 1.1 method).

9.1.3 Expected Results

- The network should successfully deliver MMS messages to the intended recipient.

9.1.4 Test Method

1. Provision the EF_{MMSICP} with Relay/Server Address, Domain Name Address, Port Number, Authentication ID, and Authentication Password as per the PRI provided by the operator.
2. Provision the $EF_{MMSConfig}$ with the parameters as per the PRI.
3. Send an MMS message from the OMH device.
4. Verify that the message is sent successfully from the OMH device.
5. Verify that the operator’s network delivers the MMS message successfully to the intended recipient.

10. *Java*

10.1 Icon or Menu Item to Access a Java Portal

This test case applies only to operator networks that support a Java download service.

This test case should be performed for each unique Java server vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

10.1.1 Objective

The objective of this test case is to verify that OMH devices that provide a Java content portal icon or menu item use the Java download server address provisioned on the OMH R-UIM.

10.1.2 Setup Notes

- An OMH device that provides an icon or menu item for launching a browser to take the user directly to Java content portal is required. This icon or menu item is separate from the browser icon that takes the user to the operator's browser home page.
- OMH R-UIM.
- EF_{JDL} file ID is 3F00/7F25/6F7F per [CDG166].
- Ensure that services n22 (Java) is allocated and activated in the CDMA service table.
- Card reader.

10.1.3 Expected Results

- The device should be able to access the Java download server provisioned in EF_{JDL} on the R-UIM.

10.1.4 Test Method

1. Provision the R-UIM with the carrier-specific URL addresses.
2. Insert the R-UIM into the device and let it acquire the network.
3. Click on the Java application.
4. Verify that the content can be downloaded from the Java content server as provisioned in EF_{JDL}.

10.2 Java and Certificate Usage

This test case applies only to operator networks that provide a Java content portal and act as a signing authority to provide operator-signed applications.

This test case should be performed for each unique Java server vendor equipment deployed in the network. In such cases, the operator will need to provide the root certificate to the device by provisioning it in the EF_{RC} on the R-UIM.

If operator-signed Java applications are not offered for download, mark this test case as N/A in [CDG174] and continue to the next.

10.2.1 Objective

The objective of this test case is to verify that operator-signed applications (i.e., operator acting as the signing authority) can be verified and run on the device using the root certificate provisioned on the R-UIM.

10.2.2 Setup Notes

- OMH device.
- OMH R-UIM.
- A Java content server URL must be provisioned in EF_{JDL} on the R-UIM.
- A root certificate for Java must be provisioned in EF_{RC} on the R-UIM.
- EF_{JDL} file ID is 3F00/7F25/6F7F per [CDG166].
- EF_{RC} file ID is 3F00/7F25/6F91 per [CDG166].
- Ensure that service n16 (Root Certificates) is allocated and activated in the CDMA service table.
- Card reader.
- The network must have a Java content server.
- The Java content server must offer operator-signed applications for download (i.e., the operator is acting as the signing authority for these applications).

10.2.3 Expected Results

- The root certificate provisioned on the R-UIM should allow the operator-signed application to be verified and run.

10.2.4 Test Method

1. Access the operator's Java content portal. Depending on the device, it may be accessed using a Java content portal icon or menu item, or it may be accessed through the operator home page displayed when the Browser icon or menu item is selected.
2. Download an operator-signed application.
3. Verify that the device is able to run this application.

11. BREW

11.1 BREW Behavior When Carrier ID Changes

This test case applies only to operator networks that support the BREW download service.

If not supported, mark this test case as N/A in [CDG174] and continue to the next.

11.1.1 Objective

The objective of this test case is to verify that, when an OMH R-UIM from one BREW operator is replaced by an OMH R-UIM from another BREW operator, the device is able to access and download from the correct BREW server.

11.1.2 Setup Notes

- OMH device.
- Two OMH R-UIMs.
- The R-UIMs are provisioned as follows:

  <*R-UIM-A*> contains BREW parameters for Operator A.

  <*R-UIM-B*> contains BREW parameters for Operator B.
- Service n23 is allocated and activated in the CDMA service table.
- $EF_{BREWDownload}$ file ID is 3F00/7F25/6F81 per [CDG166].
- $EF_{BREWAEP}$ file ID is 3F00/7F25/6F89 per [CDG166].
- $EF_{BREWSID}$ file ID is 3F00/7F25/6F83 per [CDG166].
- Card reader.

11.1.3 Expected Results

- The device should provide access to the correct BREW server for the current R-UIM.
- The device should allow downloads from this BREW server.
- The device should delete applications previously downloaded from a different operator's BREW service when an R-UIM card from a different operator is used.

11.1.4 Test Method

1. Insert the <*R-UIM-A*> into the device.
2. Power on the device.
3. Launch the BREW client and download an application.
4. Verify that the application was downloaded successfully and can be used.
5. Power down the device and remove the R-UIM.
6. Insert the <*R-UIM-B*> into the device and power on the device.
7. Verify that the previously downloaded application is no longer present.
8. Launch the BREW client and download an application.
9. Verify that the application was downloaded successfully and can be used.

12. *Location Based Services*

12.1 XTRA LBS Test

This test case applies only to operator networks that support Global Positioning System (GPS) standalone applications using an eXTended Receiver Assistance (XTRA) server.

This test case should be performed for each XTRA vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next test case.

12.1.1 Objective

The objective of this test case is to verify that standalone GPS using an XTRA server functions correctly using an OMH device and an OMH R-UIM.

12.1.2 Setup Notes

- OMH device with standalone GPS capabilities (including the use of XTRA).
- OMH R-UIM.
- Standalone GPS application on the device.
- $EF_{XTRAConfig}$ file ID is 3F00/7F25/6F84 per [CDG166].
- $EF_{LBSXSURL}$ file ID is 3F00/7F25/6F85 per [CDG166].
- Service n24 (LBS) is allocated and activated in the CDMA service table.
- Call logging (Ethereal) is needed to verify that a data call was made to the XTRA server.
- Card reader.

12.1.3 Expected Results

- The device should successfully obtain a standalone GPS fix using the XTRA server for assistance.

12.1.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Provision field $EF_{LBSEXTRAConfig}$ to default values per [CDG166].

4. Provision field $\text{EF}_{\text{LBSXSURL}}$ to contain the URL(s) of the XTRA server(s) to be used per [CDG166].
5. Launch a GPS standalone application, and verify that it functions correctly.
6. Verify through Ethereal logs that the data call was placed to an XTRA server to help obtain the GPS fix.

12.2 Trusted V2 LBS Test

This test case applies only to operator networks that support trusted V2 Location Based Service (LBS) services.

This test case should be performed for each Position Determination Equipment (PDE) vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next test case.

12.2.1 Objective

The objective of this test case is to verify that trusted V2 LBS services function correctly using an OMH device and an OMH R-UIM.

12.2.2 Setup Notes

- OMH device with V2 LBS capabilities.
- OMH R-UIM.
- LBS application (V2) on the device.
- $\text{EF}_{\text{LBSV2Config}}$ file ID is 3F00/7F25/6F86 per [CDG166].
- $\text{EF}_{\text{LBSV2PDEADDR}}$ file ID is 3F00/7F25/6F87 per [CDG166].
- Service n24 (LBS) is allocated and activated in the CDMA service table.
- Call logging (Ethereal) is needed to verify that a data call was made to the PDE.
- Card reader.

12.2.3 Expected Results

- The V2 LBS application should function properly using the network’s PDE.

12.2.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Provision field $\text{EF}_{\text{LBSV2Config}}$ to default values per [CDG166].
4. Provision field $\text{EF}_{\text{LBSV2PDEADDR}}$ to contain the IP address of the PDE per [CDG166].
5. Launch the V2 LBS application.

6. Ensure that the V2 LBS application functions correctly.
7. Verify through Ethereal logs that a data call was placed to the PDE to help provide a location.

12.3 Non-Trusted V2 Test

This test case applies only to operator networks that support non-trusted, network-initiated V2 LBS services.

This test case should be performed for each Mobile Position Center (MPC) vendor equipment deployed in the network.

If not supported, mark this test case as N/A in [CDG174] and continue to the next test case.

12.3.1 Objective

The objective of this test case is to verify that non-trusted, network-initiated V2 LBS services function correctly using an OMH device and OMH R-UIM.

12.3.2 Setup Notes

- OMH device with V2 LBS capabilities.
- OMH R-UIM.
- $EF_{LBSV2Config}$ file ID is 3F00/7F25/6F86 per [CDG166].
- $EF_{LBSV2MPCADDR}$ file ID is 3F00/7F25/6F88 per [CDG166].
- Network-initiated application on the device and network, e.g., “buddy finder.”
- Service n24 (LBS) is allocated and activated in the CDMA service table.
- Call logging (Ethereal) is needed to verify that a data call was made to the MPC.
- Card reader.

12.3.3 Expected Results

- The non-trusted, network-initiated V2 LBS application should function properly using the network’s MPC.

12.3.4 Test Method

1. Insert the R-UIM into the device.
2. Power on the device.
3. Provision field $EF_{LBSV2Config}$ to default values per [CDG166].
4. Provision field $EF_{LBSV2MPCADDR}$ to contain the IP address of the MPC per [CDG166].
5. Launch the network-initiated application, e.g., use the website to access the “buddy finder” application.

6. Verify that the network-initiated application functions correctly in determining the location of the device.
7. If possible, verify through the device UI that the network-initiated application obtained a location.
8. Verify through Ethereal logs that a data call was placed to the MPC to help find the location.

13. *Terminology*

Term	***Meaning***
AAA	Authentication, Authorization, and Accounting
BREW	Binary Runtime Environment for Wireless
BSC	Base Station Controller
CAVE	Cellular Authentication and Voice Encryption
CCAT	CDMA Card Application Toolkit
CHAP	Challenge Handshaking Authentication Protocol
cPRL	Concatenated Preferred Roaming List
EF	Elementary File
EMS	Enhanced Short Messaging Service
GPS	Global Positioning System
IMSI	International Mobile Subscriber Identity
LBS	Location Based Service
LCP	Link Control Protocol
MC	Message Center
MEID	Mobile Equipment Identifier
MIP	Mobile IP
MMS	Multimedia Messaging service
MPC	Mobile Position Center
MS	Mobile Station
MSC	Mobile Switching Center
NAI	Network Address Identifier
OEM	Original Equipment Manufacturer (i.e., the device manufacturer)
OMH	Open Market Handset
OTAPA	Over-the-Air Parameter Administration
OTASP	Over-the-Air Service Provisioning

Term	***Meaning***
PAP	Password Authentication Protocol
PDE	Position Determination Equipment
PDSN	Packet Data Serving Node
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
RNC	Radio Network Controller
R-UIM	Removable User Identity Module
SCM	Station Class Mark
SF_EUIMID	Short Form Expandable UIMID
SIP	Simple IP
SMS	Short Messaging Service
SMS-PP	Short Messaging Service Point-to-Point
UIM	User Identity Module
UTK	UIM Toolkit *(a variant of CCAT used in China and Indonesia)*
WAP	Wireless Application Protocol

14. *References*

[CDG166]	CDG Reference Document 166, *OMH R-UIM Specification*. See OMH Enabler Package v2, available at www.cdg.org/omh.
[CDG167]	CDG Reference Document 167, *OMH Device and Network Specification.* See OMH Enabler Package v2, available at www.cdg.org/omh.
[CR1001]	3GPP2 C.R1001-E (TSB-58-G), *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
[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
[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

<page left blank intentionally>