MEID-EUIMID Operator Test Plan

Version **1.3**

11 January 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

Contents

Figures

1

Revision History

Date	Version	Description
22 December 2008	1.2	Initial CDG release
11 January 2010	1.3	Minor revision

2

1. Introduction

With the impending exhaust of the ESN/UIMID resource, the CDMA2000 industry is moving towards MEID/EUIMID implementation. This test plan provides a generic set of high-level test cases for verifying the functionality of MEID/EUIMID-based handsets in commercial CDMA networks, and providing assurance that an operator's migration will proceed smoothly.

Depending on the operator's device type (e.g., R-UIM-based or integrated) and migration choice (e.g., SF_EUIMID vs. LF_EUIMID), not all tests may be applicable to all operators. It is expected that only a subset of this test plan would actually be performed by any given operator.

The tests are loosely ordered by priority and logical test order (e.g., provisioning is tested before making calls).

1.1 Acronyms and Abbreviations

Abbreviation	*Definition*
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
AC	Authentication Center
AN	Access Network
ANSI	American National Standards Institute
AT	Access Terminal
BSC	Base Station Controller
BCD	Binary Coded Decimal
CAVE	Cellular Authentication and Voice Encryption
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CIBER	Cellular Intercarrier Billing Exchange Roamer
CSR	Customer Service Representative

Abbreviation	***Definition***
ESN	Electronic Serial Number. In this document, “ESN” (with quotation marks) denotes the value of a signaling protocol field named ESN.
EUIMID	Expanded UIMID
EVDO	Evolution – Data Optimized
GDA	Global Decimal Administrator
GHA	Global Hexadecimal Administrator
HLR	Home Location Register
HRPD	High Rate Packet Data
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOS	Inter-Operability Specification
IS	Information Services
IVR	Interactive Voice Response
LF_EUIMID	Long Form EUIMID
ME	Mobile Equipment
MEID	Mobile Equipment Identifier
MIN	Mobile Identification Number
MS	Mobile Station
MSC	Mobile Switching Center
NAI	Network Access Identifier
NAM	Number Assignment Module
OTA	Over-The-Air
OTAF	Over-The-Air Function
OTASP	Over-The-Air Service Provisioning
PCF	Packet Control Function
PDSN	Packet Data Serving Node
pESN	Pseudo-ESN
PLCM	Public Long Code Mask
PRL	Preferred Roaming List
pUIMID	Pseudo-UIMID

Abbreviation	*Definition*
QXDM	Qualcomm eXtensible Diagnostic Monitor
RAN	Radio Access Network
RNC	Radio Network Controller
R-UIM	Removable User Identity Module
SF_EUIMID	Short-Form EUIMID
SHA	Secure Hash Algorithm
SMS	Short Message Service
SPC	Service Programming Code
UIMID	User Identity Module Identifier
USGIND	Usage Indicator
VLR	Visitor Location Register

1.2 Referenced Documents

1. 3GPP2 C.S0072 v1.0, MEID Support for CDMA Spread Spectrum System
2. 3CPP2 C.S0024-A, CDMA 2000 HRPD Air Interface Specification
3. 3GPP2 C.S0066-0 v2.0, OTASP for MEID Equipped Mobile Stations in Spread Spectrum
4. 3GPP2 X.S0008, IS-41 MAP Support for the MEID
5. 3GPP2 A.S001x v5.0.1, IOS for CDMA2000 Access Network Interfaces
6. 3GPP2 v.S0008-C v1.0, IOS for HRPD RAN Interfaces
7. 3GPP2 C.S0023-C v2.0, RUIM for Spread Spectrum System
8. White Paper on Pseudo-ESN Collisions, available at http://www.tiaonline.org/standards/resources/esn/documents/Collisions_pESN_wp.pdf
9. CDG Reference Document #137, Mobile Equipment Identifier Roaming Recommendations, Ver 1.0

2. Mobile Hardware Identifiers

Several identifiers may be used to identify the handset and/or R-UIM. This set of identifiers is collectively and informally referred to in this document as the “hardware identifiers.” Note that this general term is not necessarily equivalent to the Hardware Identifier used in EVDO.

The different identifiers are briefly described below.

2.1 Electronic Serial Number

The Electronic Serial Number (ESN) is a 32-bit number assigned by the mobile station (MS) manufacturer, uniquely identifying the mobile station equipment. ESNs are typically represented as an eight-character hexadecimal string, or as an 11-digit decimal number. A 32-bit address space gives a maximum pool of $2^{32} \approx 4.3$ billion unique ESNs. These ESNs are used in CDMA systems in a variety of places. In some cases, this usage is based on an assumption that the ESN is unique; in most cases, it is not. Generous allocation, inefficient usage, and the huge number of cellular devices manufactured since the 1980s has led to the current shortage.

Two different structures of the ESN (both in use) are shown in the figure below:

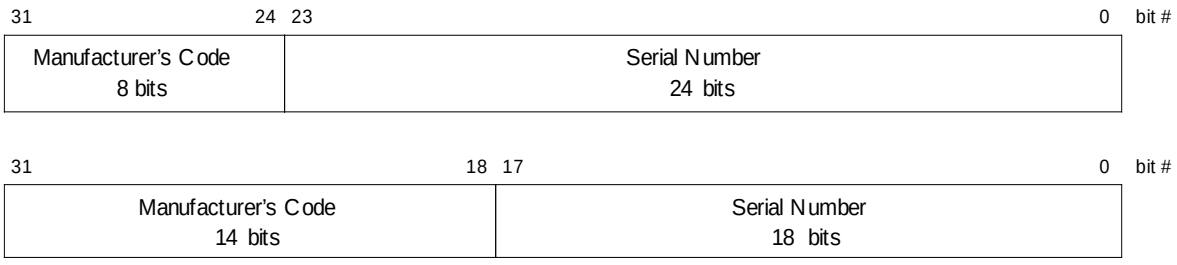

Figure 2-1 ESN Structure

In this document, “ESN” (with quotation marks) may be used to denote the value of a signaling protocol field named ESN. This 32-bit field may be filled with the value of the ESN, pESN, UIMID, or pUIMID as appropriate.

2.2 Mobile Equipment Identifier

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

The structure of the MEID is specified in Figure 2-2:

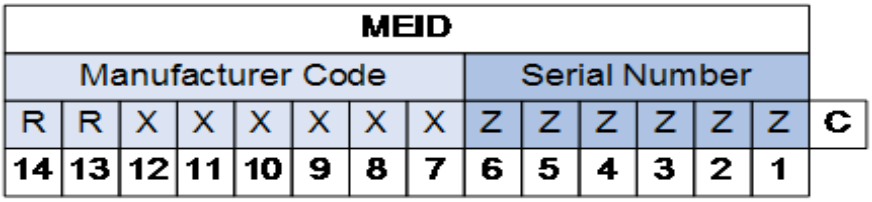

Figure 2-2 MEID Structure

RR: Reporting body identifier. Restricted to the range A0–FF. This ensures separation from the GSM International Mobile Equipment Identity (IMEI), which also uses a 56-bit space, but is restricted to BCD values only (i.e., 14 decimal digit representation). The RR values 99 (and below, if necessary) are reserved for use by dual-mode devices; in this case, the IMEI and MEID will be the same value (the remaining digits of the MEID are also restricted to BCD values). Because these values are both legitimate MEID codes and IMEI codes, assignment requires coordination between the GHA and GDA and may take longer.

XXXXXX: Manufacturer code. In practice, this value has been segmented across multiple manufacturers for some existing assignments.

ZZZZZZ: Serial number. Assigned by the manufacturer (possibly within segmented range as above).

C: Check digit for use when an MEID is printed (e.g., on packaging or on the exterior of an MS). The check digit is not part of the MEID and is not transmitted when the MEID is transmitted.

With RR in the range A0–FF, the available pool of MEIDs is $96 \times 2^{48} \approx 27$ thousand trillion, or approximately 6.3 million times the size of the ESN address space.

2.3 Pseudo-ESN

To maintain backward compatibility, non-unique “Pseudo-ESN” values derived from this new identifier MEID are used wherever the protocols require an ESN (see Figure 2-3).

Pseudo-ESN is constructed by concatenating the ESN 8-bit manufacturer code 0x80 (reserved for this purpose) with the least significant 24 bits of the SHA-1 digest of the MEID. The pESN is stored in the MS as the value of the ESN_p Permanent Mobile Station Indicator [the variable that otherwise stores the (true) ESN].

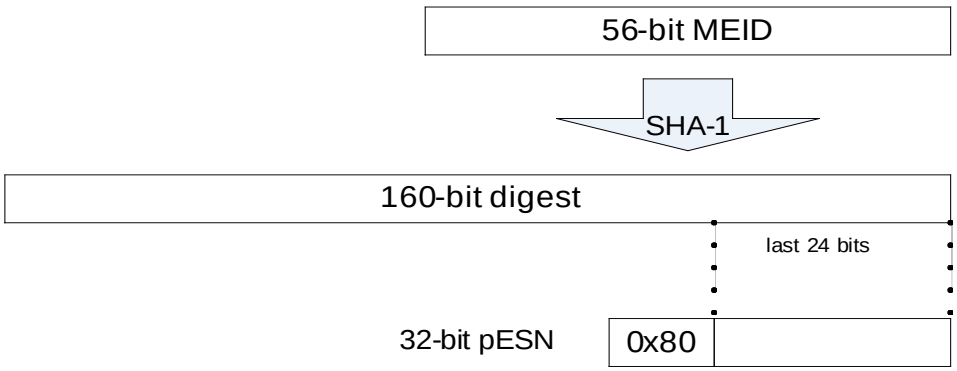

Figure 2-3 Derivation of Pseudo-ESN

Pseudo ESNs generated from MEID are not unique in nature (whereas True ESNs are unique). Because of the non-unique nature of Pseudo-ESNs, there exists the *possibility* of various issues with network and back-end systems, such as: Short Message Service (SMS) getting delivered to wrong mobiles, incorrect paging, crosstalk, interference, dropped calls, billing errors, incorrect database queries in the network, Over-The-Air-Service-Provisioning (OTASP) failures, etc.

2.4 User Identification Module Identifier

The UIM Identifier (UIMID) is a unique 32-bit number assigned to an R-UIM. The UIMID shares a 32-bit addressing space with the ESN. The UIMID can be used instead of the ESN from the device wherever the ESN is signaled over the air or used in other calculations (e.g., CAVE authentication). This behavior is controlled by a variable on the R-UIM, the Usage Indicator (EF_{USGIND}). Figure 2.4 shows the function of the usage indicator. Note that the value of this indicator is not explicitly available to the network. In practice, all operators using R-UIM are believed to set b1 to 1 (i.e., the UIMID replaces the ESN wherever it is used in CDMA 1X). This is done to ensure compatibility with ANSI-41 mobility management protocols that rely on each IMSI/MIN being associated with a single ESN. Moving a UIM from one phone to another will associate the IMSI/MIN with a different hardware ESN, but the UIMID will remain the same.

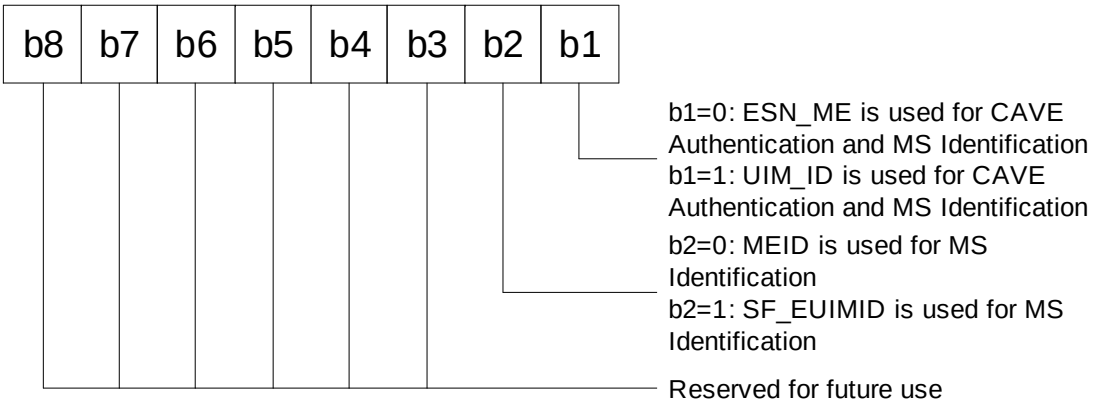

Figure 2-4 Usage Indicator (USGIND) Structure

In EVDO networks, even though an R-UIM card is used for services, the access terminal (AT) only provides either ESN or MEID to the access network (AN) through a HardwareID Response Message.

2.4.1 Expanded UIMID

The Expanded UIMID (EUIMID) is a new identifier designed to address the exhaust of the UIMID resource. There are two different formats of EUIMID:

- Short Form EUIMID (SF_EUIMID): The SF_EUIMID shares the same address space as the MEID. R-UIM card manufacturers are allocated MEID manufacturer codes in the same manner, and from the same range, as handset manufacturers.
- Long Form EUIMID (LF_EUIMID): This is equal to the value of the ICCID (Integrated Circuit Card Identifier) of the card.

When the SF_EUIMID is used, bit 2 of the Usage Indicator describes whether the SF_EUIMID of the card replaces the MEID of the device wherever it is used.

2.4.2 Pseudo-UIMID

To maintain backward compatibility, a 32-bit Pseudo-UIMID is derived from EUIMID. The pUIMID is derived from the EUIMID in the same manner as the pESN is derived from the MEID (and therefore shares the same space as the pESN). The use of Pseudo-UIMID instead of EUIMID has the same consequences as using the Pseudo-ESN instead of MEID.

MEID was originally intended to be introduced in conjunction with IS-2000 Release D. Because of the urgency associated with the feature and the uncertainty of IS-2000 Revision D commercialization, the necessary changes for MEID have been retrofitted into earlier releases of IS-2000. Various standards related to MEID network migration are given below and listed in Section 1.2, Referenced Documents, on page 3.

- MEID Support for CDMA Spread Spectrum System (3GPP2 C.S0072 v1.0)
- CDMA2000 HRPD Air Interface Specification (3GPP2 C.S0024-A)

- OTASP for MEID Equipped Mobile Stations in Spread Spectrum (3GPP2 C.S0066-0 v2.0)
- IS-41 MAP Support for the MEID (3GPP2 X.S0008)
- IOS for CDMA2000 Access Network Interfaces (3GPP2 A.S001x v5.0.1)
- IOS for HRPD RAN Interfaces (3GPP2 v.S0008-C v1.0)
- RUIM for Spread Spectrum System (3GPP2 C.S0023-C v2.0)

Even if the network is not able to support the MEID and EUIMID, these handsets should work in a non-MEID/EUIMID network through the use of Pseudo-ESNs/Pseudo-UIMIDs. MEID/EUIMID handsets do not know the capabilities of the network. (The network does not advertise its MEID/EUIMID capabilities to its handsets.) When a R-UIM card with EUIMID is inserted in an ESN-based MS, actual EUIMID may not be available to the network.

Note: In this test plan, it is assumed that usage indicator bit B1 is set to 1 for a UIMID card and B2 is set to 1 for an SF_EUIMID card.

3. Operator Logistics and Sales Process

Several of the tests in this document are designed to test the operator's back-end systems and processes for dependence on a unique ESN/UIMID. Unless uniqueness-dependent systems and processes are modified to either ignore pESN/pUIMID duplications, or to use the MEID/EUIMID as an alternative unique key, problems may result.

The exact steps in the supply and sales processes will vary from operator to operator. For that reason, a generic process is described below and illustrated in Figure 3-1 and forms the basis for several test cases. In a specific operator's case, parts of this process may be absent or combined into a single step. Other functions may also be performed that are not captured here. A close examination of the real process followed should be made to determine the appropriate tests to perform.

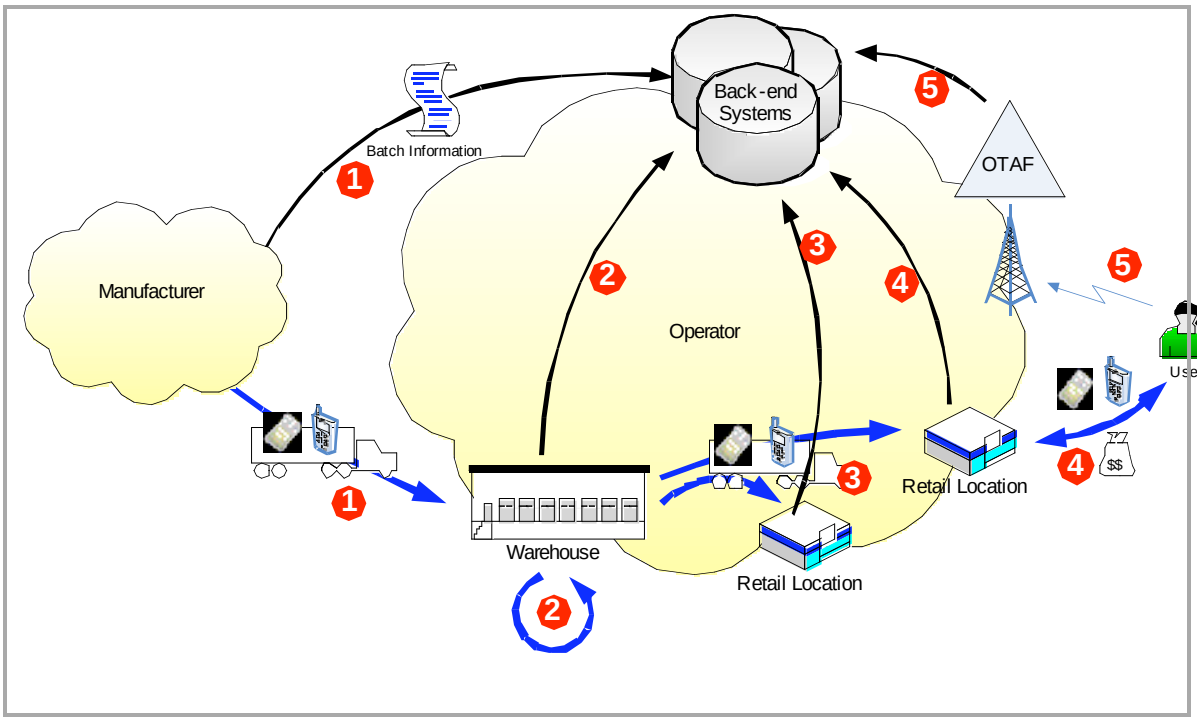

Figure 3-1 Generic Operator Sales Process

Steps are as follows:

1. Manufacturer delivers a batch of cards or devices to the operator. The units may or may not contain IMSIs and/or A-keys at this stage. Batch information listing the individual units (e.g., by ESN/MEID/UIMID/EUIMID) and the associated A-key/IMSI (if present) is provided to the operator at the same time.
2. Programming/personalization may take place at the operator's warehouse. An example would be prepaid devices that are sold fully programmed [and provisioned at the Home Location Register (HLR)] through non-specialist retail locations. This step may be performed by a third party on the operator's behalf. Provisioning information may be added to the operator's customer care systems, or generic batch information may be updated with specific IMSIs, etc.
3. The units are distributed to the retail locations. Logistics systems are updated to track stock location.
4. A new/repeat subscriber purchases a card/device. Programming may take place in the store with associated network system updates, or the unit may be simply marked as "sold" to allow a successful OTASP session to occur later.
5. The subscriber initiates an OTASP session to complete programming and provisioning.

4. Operator Receives Batch of SF_EUIMID/LF_EUIMID R-UIMs

4.1 Objective

This test verifies that the operator's back-end systems can accommodate receipt of a batch of SF_EUIMID/LF_EUIMID R-UIMs.

4.2 Rationale

Operator systems may not accept loading of batch information (e.g., into an authentication-provisioning database) that contains duplicate pUIMIDs.

4.3 Entry Requirements

- The operator uses SF_EUIMID or LF_EUIMID.
- Normal business processes for supplying R-UIM batch from the card vendor to the operator are documented, known, and understood.
- The file format for card batch information (e.g., UIMID□A-key mapping) is available.
- Dummy batch information has been created for SF_EUIMID/LF_EUIMID R-UIMs that contains at least one pUIMID duplication. Depending on the exact system requirements, corresponding physical R-UIMs may not be necessary, but may be useful for follow-on tests.

4.4 Test Procedure

1. Working with the card vendor and operator Information Services (IS) staff as necessary, simulate delivery of a duplicate-pUIMID card batch from the vendor to the operator. Load necessary information in all systems that are populated prior to actual retail sale of the card.
2. Check for any errors during the load process (e.g., "UIMID already in use").
3. When the test is complete, back out the batch to return all systems to their pre-test state. (But note that this test may be a prerequisite to later tests.)

4.5 Test Result

Successful result:

- The batch information is loaded successfully in all necessary systems.

Unsuccessful result:

- The batch information cannot be loaded in one or more necessary systems.

4.6 Comments

- Individual operators' systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.
- Problems with pUIMID duplication could be avoided either by changing the "primary key" field for a database to accommodate the unique SF_EUIMID/LF_EUIMID, or by removing the requirement for UIMID uniqueness if the value begins with 0x80 (i.e., a pseudo value).
- Note that, if LF_EUIMID is used, this identifier can only be remotely retrieved from the card by the network using procedures defined in the most recent version of C.S0066-0 (v2.0).
- Depending on an operator's business processes, the card manufacturer may pre-provision the cards with unique IMSI values and provide these values in the batch information. In this case, less importance may be placed on the pUIMID value.

5. Operator Receives Batch of MEID Phones

5.1 Objective

This test verifies that the operator's back-end systems can accommodate receipt of a batch of MEID phones.

5.2 Rationale

Operator systems may not accept loading of batch information (e.g., into an authentication-provisioning database) that contains duplicate pESNs.

5.3 Entry Requirements

- The operator uses MEID phones.
- Normal business processes for supplying a MEID batch from the device vendor to the operator are documented, known, and understood.
- The file format for device batch information (e.g., MEID□A-key mapping) is available.
- Dummy batch information has been created for MEID devices that contains at least one pESN duplication. Depending on the exact system requirements, corresponding physical MEID phones may not be necessary, but may be useful for follow-on tests.

5.4 Test Procedure

1. Working with the device vendor and operator IS staff as necessary, simulate delivery of a duplicate-pESN device batch from the vendor to the operator. Load necessary information in all systems that are populated prior to actual retail sale of the device.
2. Check for any errors during the load process (e.g., “MEID already in use”).
3. When the test is complete, back out the batch to return all systems to their pre-test state. (But note that this test may be a prerequisite to later tests.)

5.5 Test Result

Successful result:

- The batch information is loaded successfully in all necessary systems.

Unsuccessful result:

- The batch information cannot be loaded in one or more necessary systems.

5.6 Comments

- Individual operators' systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.
- Problems with pESN duplication could be avoided either by changing the "primary key" field for a database to accommodate the unique MEID, or by removing the requirement for MEID uniqueness if the value begins with 0x80 (i.e., a pseudo value).
- Depending on an operator business processes, the device manufacturer may pre-provision the devices with unique IMSI values and provide these values in the batch information. In this case, less importance may be placed on the pESN value.

6. Personalization/Programming of Cards / Devices

6.1 Objective

This test verifies that any personalization/programming performed by or on behalf of the operator before the units are distributed for sale can proceed in a duplicate pESN/pUIMID environment.

6.2 Rationale

If systems and processes only track the 32-bit ESN/UIMID, problems may be encountered when this identifier is no longer unique.

6.3 Entry Requirements

- Either the “Operator receives batch of EUIMID cards” or “Operator receives batch of MEID phones” test is successfully completed (as appropriate to operator device types).
- Normal business processes for personalization or programming of cards/phones in the operator’s warehouse are documented, known, and understood.
- Physical cards/devices corresponding to the batch information (or at least a subset including a duplicate pseudo-identifier) are available at the operator’s warehouse or simulated environment.
- A dummy range of IMSIs is identified, if necessary, together with any other information required to be entered during the personalization process.

6.4 Test Procedure

1. Perform personalization/programming steps on the duplicate pESN/pUIMID devices/cards according to the operator’s normal business processes.
2. Update all necessary systems with the results.
3. Perform a database read to verify that the systems were updated successfully and that distinct records are present for the duplicate pESN/pUIMID units.

6.5 Test Result

Successful result:

- Personalization/programming is successfully completed according to the operator's requirements, and all necessary systems are updated.

Unsuccessful result:

- Systems update cannot be completed due to primary key duplication.

6.6 Comments

Individual operators' systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.

7. Distribution of Devices/Cards to Retail Locations

7.1 Objective

This test verifies that the operator's stock tracking systems can function in a duplicate pseudo-identifier environment.

7.2 Rationale

If systems and processes only track the 32-bit ESN/UIMID, problems may be encountered when this identifier is no longer unique.

7.3 Entry Requirements

- The "Personalization/Programming of Cards/Devices" test is successfully completed.
- Normal business processes for distribution of units to retail locations are documented, known, and understood.
- A subset of batch information containing duplicate pseudo-identifiers is available.

7.4 Test Procedure

1. Via updates to logistics systems, simulate distribution of cards/devices to retail locations. In particular, "send" units with duplicate pseudo-identifiers to different physical locations.
2. Perform a database read to verify that the systems were updated successfully and that distinct records are present for the duplicate pESN/pUIMID units.

7.5 Test Result

Successful result:

- The logistics system is correctly updated to indicate distribution of all units.

Unsuccessful result:

- Systems update cannot be completed due to primary key duplication.

7.6 Comments

Individual operators' systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.

8. Subscriber Purchase Device / Card – No OTASP

8.1 Objective

This test verifies that a subscriber can purchase a device/card and have it provisioned in-store.

8.2 Rationale

Back-end provisioning systems must not require the 32-bit identifier to be unique.

8.3 Entry Requirements

- The “Distribution of Cards/Devices to Retail Locations” test is successfully completed.
- The operator does not use OTASP, or allows in-store programming and provisioning of devices/cards as an option.
- Normal business processes for end-user retail sale are documented, known, and understood.
- Two unprogrammed, unprovisioned MEID devices or EUIMID R-UIMs are available for simulated sale, with duplicated pESN/pUIMID.

8.4 Test Procedure

1. Simulate subscriber purchase of the first card/device in the retail location.
2. Program the phone/card with necessary information as per normal business practice (e.g., keypad NAMing sequence, terminal card/phone programming, etc.).
3. Submit a network provisioning request via the normal operator process (e.g., fax a provisioning request or enter information at premises terminal).
4. After an appropriate delay, check that information was successfully entered and that a call can be made/received.
5. Repeat these steps for a second (duplicate pseudo-identifier) card/device.

8.5 Test Result

Successful result:

- Both devices/cards are successfully programmed and provisioned, and can make/receive calls.

Unsuccessful result:

- One or both cards/devices cannot be provisioned and programmed through normal processes, e.g., a “duplicate ESN detected” error results.

8.6 Comments

Individual operators’ systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.

9. Subscriber Purchase Device / Card – OTASP to Follow

9.1 Objective

This test verifies that a subscriber can purchase a device/card and have it marked as open for later OTASP.

9.2 Rationale

If the back-end system tracks only the 32-bit identifier, problems may arise if more than one pseudo-value is open for OTASP at the same time.

9.3 Entry Requirements

- The “Distribution of Cards/Devices to Retail Locations” test is successfully completed.
- The operator uses OTASP.
- Normal business processes for end-user retail sale are documented, known, and understood.
- Two unprogrammed, unprovisioned MEID devices or EUIMID R-UIMs (as appropriate for operator device types) are available for simulated sale, with duplicated pESN/pUIMID.

9.4 Test Procedure

1. Simulate subscriber purchase of the first card/device in the retail location.
2. Update back-end systems as appropriate (e.g., card/device marked sold, ready for OTASP, credit check passed, etc.).
3. Repeat these steps for the second (duplicate pseudo-identifier) card/device.

9.5 Test Result

Successful result:

- Both devices/cards are successfully marked ready for programming.

Unsuccessful result:

- One or both cards/devices cannot complete the post-purchase status update (e.g., “duplicate record found,” “device already sold,” etc.).

9.6 Comments

Individual operators’ systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.

10. OTASP of MEID Device

10.1 Objective

This test verifies that OTASP of an MEID-equipped device can proceed successfully.

10.2 Rationale

Before an MS has an IMSI provisioned, the only unique identifier available is the hardware identifier (i.e., ESN/MEID). Special messaging is needed to retrieve the MEID from a device during an OTASP session. The requirement to uniquely identify a device during provisioning is dependent on the operator's business processes.

10.3 Entry Requirements

- The operator uses integrated devices.
- The operator sells devices without IMSI, and the end-user completes the provisioning via OTASP.
- The "Subscriber purchase device/card – OTASP to follow" test is successfully completed.
- An unprovisioned, IMSI-less, MEID-equipped test MS is available. The test MS has at least one duplicate pESN in the batch information, and has previously been marked as "sold."

10.4 Test Procedure

1. The subscriber dials *228 (or the equivalent operator OTASP code) to initiate the OTASP session.
2. Proceed with Interactive Voice Response/Customer Service Representative (IVR/CSR) to provision the device.
3. Complete the OTASP session, and make/receive calls to verify that provisioning is successful.

10.5 Test Result

Successful result:

- The OTASP session proceeds successfully, and the device can make/receive calls.

Unsuccessful result:

- The OTASP session fails. Potential reasons include: cannot unlock device [Service Programming Code (SPC) mismatch] and authentication failure [incorrect A-key provisioned into the Authentication Center (AC)].

10.6 Comments

- For standards updates to allow retrieval of MEID during an OTASP session, refer to 3GPP2 C.S0066.
- If authentication is not used, or if the A-key is dynamically generated during the OTASP session, there may be no need to uniquely identify the device. However, if the A-key is pre-provisioned in the device (and the key must therefore be retrieved from the corresponding batch information database for population into the AC), or if the SPC is randomly set for each device, or if logistics/fraud processes require handsets to be marked as “sold” before they can be OTASPed, then unique identification will be required.
- Alternative, nonstandard processes to identify the device are possible, but are outside the scope of this document. For further information contact meid@cdg.org.

11. OTASP of SF_EUIMID Card

11.1 Objective

This test verifies that OTASP of a SF_EUIMID R-UIM can proceed successfully in both MEID-equipped and ESN-equipped devices.

11.2 Rationale

Before a card has an IMSI provisioned, the only unique identifier available is the "hardware" identifier (i.e., UIMID/EUIMID). Special messaging is needed to retrieve the SF_EUIMID from a MEID-equipped device during an OTASP session. The requirement to uniquely identify a card during provisioning is dependent on the operator's business processes.

11.3 Entry Requirements

- The operator uses R-UIMs (test assumes that the operator will have a mix of ESN- and MEID-equipped devices in the field).
- The operator uses/will use SF_EUIMID for R-UIM migration.
- The operator sells cards without IMSI, and the end-user completes the provisioning via OTASP.
- The "Subscriber purchase device/card – OTASP to follow" test is successfully completed.
- Point-of-sale procedures for customer retail card purchase are known and can be simulated.
- Two unprovisioned, IMSI-less, SF_EUIMID cards are available. Each card has at least one duplicate pUIMID in the batch information. USG_IND b2b1 is set to "11" (assumed operator normal setting). Cards are marked as "sold" in back-end systems.
- Two test MEs are available:
  - An MEID-equipped, IS-820-C–compliant ME
  - An ESN-equipped ME

11.4 Test Procedure

1. The subscriber inserts the first card in the MEID-equipped ME.

2. The subscriber dials *228 (or the equivalent operator OTASP code) to initiate the OTASP session.
3. Proceed with IVR/CSR to provision the device.
4. Complete the OTASP session, and make/receive calls to verify that provisioning is successful.
5. Repeat the test with the second card in the ESN-equipped ME.

11.5 Test Result

Successful result:

- Both OTASP sessions proceed successfully, and the subscriber can make/receive calls using the newly provisioned R-UIMs.

Unsuccessful result:

- One or both OTASP sessions fail. Potential reasons include: cannot unlock card (SPC mismatch); authentication failure (incorrect A-key provisioned into AC); and the MEID request fails.

11.6 Comments

- For standards updates to allow retrieval of MEID during an OTASP session, refer to 3GPP2 C.S0066. As defined by the usage indicator b2, SF_EUIMID will override MEID.
- C.S0066 support will not be available in an ESN-equipped device. The OTAF platform may not be able to determine which kind of device is in use before attempting to retrieve the “MEID.” Special OTAF logic and/or handset modifications may be required to gracefully ignore the failure of the MEID request in this case.
- If authentication is not used, or if the A-key is dynamically generated during the OTASP session, there may be no need to uniquely identify the card. However, if the A-key is pre-provisioned in the card (and the key must therefore be retrieved from the corresponding batch information database for population into the AC), or if the SPC is randomly set for each card, or if logistics/fraud processes require cards to be marked as “sold” before they can be OTASPed, then unique identification will be required.
- Alternative, nonstandard processes to identify the card are possible, but are outside the scope of this document. For further information contact meid@cdg.org.

12. OTASP of LF_EUIMID Card

12.1 Objective

This test verifies that OTASP of a LF_EUIMID R-UIM can proceed successfully.

12.2 Rationale

Before a card has an IMSI provisioned, the only unique identifier available is the "hardware" identifier (i.e., UIMID/EUIMID). Only the latest version of C.S0066-0 or C.S0016-C (v2.0) contains procedures that allow for the retrieval of LF_EUIMID during an OTASP session. It cannot be retrieved at any other time via the network. The requirement to uniquely identify a card during provisioning is dependent on the operator's business processes.

12.3 Entry Requirements

- The operator uses R-UIMs. (This test assumes that the operator will have a mix of ESN- and MEID-equipped devices in the field.)
- The operator uses/will use LF_EUIMID for R-UIM migration.
- The operator sells cards without IMSI, and the end-user completes the provisioning via OTASP.
- The "Subscriber purchase device/card – OTASP to follow" test is successfully completed.
- Point-of-sale procedures for customer retail card purchase are known and can be simulated.
- Two unprovisioned, preferably IMSI-less LF_EUIMID cards are available. Each card has at least one duplicate pUIMID in the batch information. Cards are marked as "sold" in back-end systems.
- Two test MEs are available:
  - An MEID-equipped ME
  - An ESN-equipped ME

12.4 Test Procedure

1. The subscriber inserts the first card in the MEID-equipped ME.

2. The subscriber dials *228 (or the equivalent operator OTASP code) to initiate the OTASP session.
3. Proceed with IVR/CSR to provision device.
4. Complete the OTASP session, and make/receive calls to verify that provisioning is successful.
5. Repeat the test with the second card in the ESN-equipped ME.

12.5 Test Result

Successful result:

- Both OTASP sessions proceed successfully, and the subscriber can make/receive calls using the newly provisioned R-UIMs.

Unsuccessful result:

- One or both OTASP sessions fail. Potential reasons include: device not marked as “sold,” cannot unlock card (SPC mismatch); authentication failure (incorrect A-key provisioned into AC); MEID request fails; and unexpected MEID received.

12.6 Comments

- C.S0066 support will not be available in an ESN-equipped device. The OTAF platform may not be able to determine which kind of device is in use before attempting to retrieve the “MEID.”
- If authentication is not used, or if the A-key is dynamically generated during the OTASP session, there may be no need to uniquely identify the card. However, if the A-key is pre-provisioned in the card (and the key must therefore be retrieved from the corresponding batch information database for population into the AC), or if the SPC is randomly set for each card, or if logistics/fraud processes require cards to be marked as “sold” before they can be OTASPed, then unique identification will be required.
- Alternative, nonstandard processes to identify the card are possible, but are outside the scope of this document. For further information contact meid@cdg.org.

13. Simultaneous, Duplicate OTASP Calls

13.1 Objective

This test verifies that the OTASP process can accommodate simultaneous calls from duplicate pESN/pUIMID devices.

13.2 Rationale

As distinct from the potential requirement to uniquely identify a card/device during provisioning for the purposes of looking up stored information (e.g., A-key), OTAF platforms and other network elements involved in the session may index active sessions using the "ESN" value retrieved during the session. If this is the case, problems are expected with simultaneous sessions from duplicate pESN/pUIMID devices/cards.

13.3 Entry Requirements

- The operator uses OTASP.
- Previous OTASP tests appropriate for operator devices are completed successfully.
- Two unprovisioned MEID-equipped devices with common pESN or EUIMID-equipped cards with common pUIMID and associated MEID-equipped MEs are available.
- Air interface logging [e.g., Qualcomm eXtensible Diagnostic Monitor (QXDM)] is available from at least one of the test MSs.

13.4 Test Procedure

1. Simulate a retail purchase of test cards/devices (e.g., cards/devices are marked "sold" in the back-end database, credit check is marked "pass").
2. If necessary, insert cards in MEs.
3. Make simultaneous calls to *228 (or the equivalent operator OTASP code) to initiate OTASP sessions from both MSs.

Note: The test is exercising the *core* network; the MSs should *not* be on the same or interfering sectors, but should be on the same MSC.

4. Proceed with IVR/CSR to provision the devices.

5. Complete the OTASP sessions, and make/receive calls to verify that provisioning is successful.
6. Check the OTAF error log for any relevant messages.

13.5 Test Result

Successful result:

- Both cards/devices are OTASPed successfully.

Unsuccessful result:

- One or both OTASP sessions fail, as they cannot be distinguished by their associated “ESN” value.

13.6 Comments

The session index is referred to in IS-725-A as the OTASPCallEntry, and may be indexed by ESN or by the Activation_MIN temporarily assigned by the OTAF. 3GPP2 X.S0033 adds MEID as a possible index value. Use of Activation_MIN will avoid the collision issues in this case, without requiring X.S0033/X.S0008 support.

14. MEID Registration

14.1 Objective

This test verifies that MEID-based handsets can be registered successfully.

14.2 Rationale

An issue has been encountered in one network where no service is provided to MEID mobiles. Aside from this, HLR validation should be keyed off IMSI and no impacts are expected from pESN duplication.

14.3 Entry Requirements

- The operator uses integrated handsets.
- A MEID-equipped handset is programmed and provisioned on the network. At least one duplicate-pESN entry should exist in the HLR database (with a different MSID).
- Desirable: Air interface logging (e.g., QXDM) is available from the test MS; ANSI-41 logging is available on the MSC-HLR interface; and MSC-BSC interface logging is available.
- The technician has access to the Visitor Location Register (VLR) and the HLR.

14.4 Test Procedure

1. Power on the MS.
2. Capture air interface and network-side registration logs, if possible.
3. Originate a local call to verify that registration has completed.
4. Verify that the subscriber information is present in the VLR and that the location is updated in the HLR.

14.5 Test Result

Successful result:

- The MEID device is successfully registered in the VLR. MEID validation as per X.S0008 is not required for a successful result.

Unsuccessful result:

- The device cannot register. Possible reasons include: Inter-Operability Specification (IOS) error and pESN duplication detected at the HLR.

14.6 Comments

- For information about the incompatibility error discovered, see the CDG Bulletin.
- 3GPP2 X.S0008 adds MEID as an optional parameter in many ANSI-41 messages. The HLR can return MEIDValidated to indicate that the value has been checked against previously stored information. Support for this check is not required for successful test completion.
- The MEID may optionally be retrieved from the device at registration time, using the Status Request mechanism outlined in 3GPP2 C.S0072.

15. EUIMID Registration

15.1 Objective

This test verifies that EUIMID R-UIMs can be registered successfully.

15.2 Rationale

An issue has been encountered in one network where no service is provided to MEID mobiles. This would also affect EUIMID cards in MEID devices. In addition, if the HLR or MSC attempts to validate the hash relationship between the received “ESN” and “MEID” values, it may fail in an R-UIM scenario.

15.3 Entry Requirements

- The operator uses R-UIMs.
- An existing UIMID-based R-UIM is programmed and provisioned on the network.
- An EUIMID R-UIM is programmed and provisioned on the network (SF_ or LF_EUIMID as per the operator’s chosen migration path). At least one duplicate pUIMID should exist in the HLR database (with a different MSID).
- Two MEID-equipped and one ESN-equipped R-UIM-capable MEs are available.
- Desirable: Air interface logging (e.g., QXDM) is available from the test MS; ANSI-41 logging is available on the MSC-HLR interface; and MSC-BSC interface.
- The technician has access to the VLR and the HLR.

15.4 Test Procedure

1. Insert the R-UIM in the ESN-equipped ME.
2. Power on the MS.
3. Capture air interface and network-side registration logs, if possible.
4. Originate a local call to verify that registration has completed.
5. Verify that the subscriber information is present in the VLR and that location is updated in the HLR.
6. Power down the MS.
7. Transfer the card to the first MEID-equipped ME, then power up and repeat the registration checks.

8. Power down the MS, transfer the card to the second MEID-equipped ME, and power up and repeat the registration checks.
9. Without gracefully powering down the MS (i.e., do a battery pull instead), return the card to the first MEID-equipped ME, and repeat the registration checks one more time.

15.5 Test Result

Successful result:

- All registration combinations are successful. MEID validation as per X.S0008 is not required for a successful result.

Unsuccessful result:

- One or more registration steps in the above procedure fail. Possible reasons include: IOS error, pESN duplication detected at HLR, no MEID available, and MEID mismatch at the HLR and/or the VLR.

15.6 Comments

- For information about the incompatibility error discovered, see the CDG Bulletin.
- 3GPP2 X.S0008 adds MEID as an optional parameter in many ANSI-41 messages. The HLR can return MEIDValidated to indicate that the value has been checked against previously stored information. Support for this check is not required for successful test completion. An over-zealous application of this standard could lead an HLR or VLR to determine (in a LF_EUIMID usage scenario) that the MEID received from the MS is not hash-related to the received “ESN” value, or is different from the previously stored MEID value (e.g., if the card has been moved between MEs).
- The MEID may optionally be retrieved from the device at registration time, using the Status Request mechanism outlined in 3GPP2 C.S0072. It is expected that, in the case of SF_EUIMID, the EUIMID will typically override the MEID, but this is not possible for LF_EUIMID.

16. Call Origination/Termination – Duplicate Pseudo-IDs

16.1 Objective

This test verifies that MEID/EUIMID-based handsets can originate/terminate voice/data calls without crosstalk, interference, and dropped calls.

16.2 Rationale

When two devices having same Pseudo-ESN/Pseudo-UIMID originate/terminate calls within the same carrier and same (or an interfering) sector, crosstalk, interference, or dropped calls can result, if the network is not upgraded to assign different Public Long Code Masks (PLCMs).

16.3 Entry Requirements

- Two programmed, provisioned, MEID-equipped MSs/EUIMID-based RUIM cards inserted in MEID devices, with the same pESN/pUIMIDs, in the same sector, idle on the same channel. Use of a single-channel site is preferable, if possible; otherwise, a careful selection of IMSIs is necessary to achieve the desired hash result (see Section 16.6).
- Air interface logging (e.g., QXDM) is available from at least one of the test MSs.

16.4 Test Procedure

1. Originate/terminate voice calls using two MEID/EUIMID handsets in the same carrier and same sector simultaneously.
2. Capture air interface logs as appropriate.

16.5 Test Result

Successful result:

- Verify that the base station assigns the BS-assigned PLCM to both calls and that calls can be originated or terminated successfully.

Unsuccessful result:

- One or both calls drop or experience crosstalk/interference. A pseudo-ESN/pseudo-UIMID-based PLCM may result in crosstalk, interference, and dropped calls in the same sector and carrier.

16.6 Comments

- When multiple channels are available, mobiles hash to a specific one using an algorithm that takes the MIN as input. Details can be found at 3GPP2 C.S0005-0 §2.6.7.1.
- Air interface upgrades to avoid a PLCM collision are described in 3GPP2 C.S0072.
- Even with C.S0072 implemented, EUIMID R-UIMs in ESN-based MEs will still be subject to collision.

17. Voice Billing Records

17.1 Objective

This test verifies that voice call billing records are correctly identified in the MEID/EUIMID environment.

17.2 Rationale

If a pseudo-identifier is used to “uniquely” identify the billing records for voice calls, pESN/pUIMID duplication can result in ambiguous billing records for mobile subscribers.

17.3 Entry Requirements

- Two MEID-/EUIMID-based handsets having same Pseudo-ESN/Pseudo-UIMID are available.
- Access to billing record processing flow for voice calls is available.

17.4 Test Procedure

1. Originate/terminate voice calls from two MEID/EUIMID-based handsets having the same Pseudo-ESN/Pseudo-UIMID values.
2. Identify the billing records produced for the voice calls made, and verify that the corresponding charges are present on the correct subscriber retail bills.

17.5 Test Result

Successful result:

- Voice billing records are successfully associated with the correct subscriber account.

Unsuccessful result:

- Pseudo-ID duplication leads to ambiguity of record matching, and call records cannot be correctly associated with the subscriber account.

17.6 Comments

- Inclusion of pESN/pUIMID, MEID/SF_EUIMID, or both on the MSC call detail record (CDR) is a matter of operator/vendor choice, and does not preclude a successful test result.
- Provided the subscriber IMSI is the “primary key” for processing, duplicate pseudo-IDs should not present a problem.

18. CDMA2000 Data Call AAA Authentication

18.1 Objective

This test verifies that CDMA2000 data call Authentication, Authorization, and Accounting (AAA) authentication is successful.

18.2 Rationale

Some operators use ESN/UIMID@realm as the NAI during AAA. In a pseudo-identifier environment, this can result in duplication. Additionally, differences in MEID capability between Packet Control Function (PCF), Packet Data Serving Node (PDSN), and AAA may result in problems when receiving accounting records.

18.3 Entry Requirements

- The operator offers cdma2000 data services.
- Provisioned, programmed MEID/EUIMID-based devices/cards, with at least one duplicate pESN/pUIMID, are available in the subscriber database.
- Logging is available at air interface, A10/A11, PDSN-AAA.

18.4 Test Procedure

1. Originate a data call on the CDMA network.
2. Collect appropriate air-interface PPP logs and PDSN AAA logs.

18.5 Test Result

Successful result:

- The data call is authenticated and proceeds successfully.

Unsuccessful result:

- The data call cannot be completed. Possible reasons include: incorrect password and rejected accounting records.

18.6 Comments

3GPP2 A.S0017 describes the airlink record that is passed from the PCF to the PDSN. This can include the ESN, the MEID, or both. If the ESN is required at the PDSN but the MEID is received instead, the record could potentially be rejected.

19. Data Billing Records

19.1 Objective

This test verifies that data billing records are correctly identified in the MEID/EUIMID environment.

19.2 Rationale

If a pseudo-identifier is used to “uniquely” identify the billing records for data calls, pESN/pUIMID duplication can result in ambiguous billing records for mobile subscribers.

19.3 Entry Requirements

- Two MEID-/EUIMID-based handsets having the same Pseudo-ESN/Pseudo-UIMID are available.
- Access to billing record processing flow for data calls is available.

19.4 Test Procedure

1. Originate/terminate data calls from two MEID/EUIMID-based handsets having same Pseudo-ESN/Pseudo-UIMID values are available.
2. Identify the billing records produced for the data calls made, and verify that the corresponding charges are present on the correct subscriber retail bills.

19.5 Test Result

Successful result:

- Data billing records are successfully associated with the correct subscriber account.

Unsuccessful result:

- Pseudo-ID duplication leads to ambiguity of record matching, and call records cannot be correctly associated with the subscriber account.

20. EVDO Authentication (HRPD)

20.1 Objective

This test verifies that EVDO authentication [High Rate Packet Data (HRPD)] is successful.

20.2 Rationale

Equivalent issues to those described for cdma2000 data may apply (e.g., NAI, A10/11 MEID capability mismatch). In addition, for EVDO, there is the option to use HardwareID as a parameter in the A12 authentication messaging. When the AT has an MEID, this is returned to the AN in response to a HardwareIDRequest message. Explicit support at the AN is required in order to be able to include the MEID on the A12 interface. If the HardwareID is a required parameter at the AAA, the authentication may fail if the MEID is not included, or is included but not handled at the AAA.

20.3 Entry Requirements

- The operator supports MEID-based ATs. A provisioned, EVDO-capable AT is available as test device.
- Desirable: Logging on A12 interface.

20.4 Test Procedure

1. Initiate an EVDO connection from the AT.
2. Verify that A12/Radio Access Network (RAN) and PDSN authentication is successfully completed.

20.5 Test Result

Successful result:

- A12 and PSDN authentication complete successfully. HardwareID may or may not be included on A12, depending on operator choice.

Unsuccessful result:

- Authentication fails. Possible reasons include: Radio Network Controller (RNC) not including the MEID in the A12 Access Request Message, and AAA expecting pESN instead; NAI mismatch for PSDN or A12 authentication; and missing expected parameter (ESN) for PDSN accounting start.

21. OTASP of Provisioned MS

21.1 Objective

This test verifies that an OTASP session can be successfully completed for a card/device that already has an IMSI.

21.2 Rationale

Earlier OTASP tests focused on provisioning a card/device, where an IMSI was not available as a unique identifier. These tests may have been safely skipped by operators who do not sell “blank” (i.e., no IMSI) cards/devices. However, these operators may still use OTASP [e.g., for Preferred Roaming List (PRL) download]. Although an IMSI is available and can be used to uniquely identify the subscriber, operator implementations may key off the ESN/UIMID value instead, which could cause problems when these identifiers are no longer unique.

21.3 Entry Requirements

- The operator uses OTASP.
- The operator does not use OTASP for initial device/card provisioning (earlier higher-priority tests should have picked up any issues already).
- A provisioned MEID device/EUIMID card plus MEID and ESN-equipped MEs are available. The device/card has at least one pESN/pUIMID match in the subscription database. The match should be associated with different information for the OTASP session (e.g., a different target PRL).

21.4 Test Procedure

1. Dial *228 (or the equivalent operator code) to initiate the OTASP session.
2. Download the PRL, or perform another OTASP task as appropriate.
3. Verify that the correct Over-The-Air function was performed (e.g., correct PRL ID is loaded).
4. If using R-UIM, perform the test in both the ESN- and MEID-equipped MEs.

21.5 Test Result

Successful result:

- The OTASP session completes successfully. The MS is loaded with correct data.

Unsuccessful result:

- The OTASP session cannot complete, or incorrect information is fetched and loaded in the MS.

22. Mobile-Terminated SMS

22.1 Objective

This test verifies that short messages can be successfully delivered to the correct mobile.

22.2 Rationale

Paging channel messages other than the Page message may be addressed using either IMSI or ESN. If an SMS is sent using a Paging Channel *Data Burst Message*, and this message is addressed using the ESN, then duplicate-pESN mobiles in the same sector can both receive a message intended for only one device.

22.3 Entry Requirements

- According to the operator's device type, either:
  - Two provisioned MEID-equipped MSs, with the same pESNs but different IMSIs, idle on the same channel in the same sector, or
  - Two provisioned EUIMID R-UIMs, with the same pUIMID, inserted in MEs (MEID or ESN based), idle on the same channel in the same sector.
- Air interface logging (e.g., QXDM) is available from at least one of the test MSs.

22.4 Test Procedure

1. From a different mobile or a technician interface, send a short (e.g., 1 character) SMS to one of the MEID-equipped MSs.
2. Verify that the message is received correctly on the addressed MS.
3. Check whether the other MS has also received the message.
4. Capture air interface logs as appropriate.

22.5 Test Result

Successful result:

- The message is received correctly at the addressed MS, and at only the addressed MS.

Unsuccessful result:

- The message is not received at the addressed MS (unexpected error potentially unrelated to MEID), or both MSs receive the same message.

22.6 Comments

- A successful result may be obtained if the network uses IMSI addressing rather than ESN, or sends Data Burst Messages exclusively on the traffic channel regardless of message length.
- The Data Burst Message is one example of a non-Page message that may be sent on the paging channel. For a list of other messages and discussion of the potential impact if they are ESN-addressed and received by more than one MS, see the Collisions Whitepaper.

23. Inbound Roaming R-UIM Billing

23.1 Objective

This test verifies that the operator's roaming billing system populates the CIBER record correctly for an R-UIM + MEID combination.

23.2 Rationale

The CIBER record allows only one "hardware identifier" value to be included. This value can be any of the following: ESN, UIMID, pESN, pUIMID, MEID, or SF_EUIMID. When both card- and ME-sourced identifiers are available in the MSC CDR, the card-based identifier should be used in the CIBER record. Use of a ME-derived identifier may cause problems with roaming partners' billing systems.

23.3 Entry Requirements

- Three test R-UIMs are provisioned to be from a valid roaming partner:
  - One regular UIMID card
  - One LF_EUIMID
  - One SF_EUIMID (Multiple roaming partners may be required in order to exercise both EUIMID types. LF_EUIMID is more important to test.)
- An MEID-equipped R-UIM ME is available.
- Access to the operator's CIBER outcollect processing output is available.

23.4 Test Procedure

1. Note and/or calculate the *d*ecimal representation of the UIMID, SF_EUIMID, and pUIMID for the cards, as appropriate, and the pESN and MEID for the test ME.
2. Insert the UIMID R-UIM into the ME, power up, register, and make a local call.
3. Repeat for the other R-UIM types.
4. Capture the resulting CIBER outcollect records.

23.5 Test Result

Successful result:

- In all cases, the CIBER "ESN/IMEI" contains a value derived from the R-UIM, not the ME (e.g., UIMID, pUIMID for UIMID and LF_EUIMID cards, and pUIMID or SF_EUIMID for the SF_EUIMID card).

Unsuccessful result:

- The calls fail, CIBER is not generated, or the ME MEID is included in the CIBER record "ESN/IMEI" field.

23.6 Comments

- For more information on the issue of CIBER population in an R-UIM/MEID environment, see the presentation at the CDG site.
- The CIBER manual has also been updated to indicate the correct population. Contact MACH-Cibernet for a recent copy of the CIBER Data Dictionary.

24. Outbound Voice Roaming

24.1 Objective

This test verifies that the operator's systems can accommodate what may be differing levels of support for MEID/EUIMID in their roaming partners' networks.

24.2 Rationale

Roaming partners' systems may include MEID, when it is not expected by the home operator, or omit this field when it is administratively required.

24.3 Entry Requirements

Note: The entry requirements for an outbound roaming test are onerous, even more so if the tests are to be repeated for every roaming partner. This test is included for completeness in this document, but is not likely to be performed in conjunction with the other in-network test cases.

- One or more provisioned and programmed operator MEID and/or EUIMID devices/cards are located in a roaming partner's network.
- One or more duplicates for the test device pESN/pUIMID exist in the operator's subscriber database.
- Logging on a roaming ANSI-41 interface and technician access to the HLR are available.

24.4 Test Procedure

1. Power on and register roaming devices in the partner network.
2. Verify that registration is successful via traces and HLR access.
3. Make and receive calls on the roaming device(s).
4. Verify that the calls are processed onto the correct subscriber retail bill.
5. Send and receive text messages (if supported by roaming agreements).
6. Verify that text messages are billed correctly.

24.5 Test Result

Successful result:

- Subscriber registration, call origination/termination, and subsequent billing are successful and correct.

Unsuccessful result:

- Any of the test elements cannot be completed successfully, e.g., due to a missing MEID parameter, unexpected MEID parameter, or CIBER “ESN/IMEI” mismatch.

24.6 Comments

- For a general discussion on MEID/EUIMID impacts on roaming, see CDG Ref Doc #137.
- The test case described here is a minimum. Operators are advised to perform a more detailed set of tests, using other test cases from this document adapted for the roaming environment, at their and their roaming partners’ convenience.

25. Customer Service Call

25.1 Objective

This test verifies that customer service applications perform correctly in the MEID/EUIMID environment.

25.2 Rationale

If the tools used by the operator's CSRs key off the 32-bit identifier, they may not locate the correct subscriber record.

25.3 Entry Requirements

- A programmed and provisioned MEID device or a EUIMID-R-UIM with a compatible ME (as determined by operator device types) is available.
- At least one duplicate pESN/pUIMID is present in the operator's provisioning/customer management system for the test MS.

25.4 Test Procedure

1. Originate a call from the MEID/EUIMID MS to customer service.
2. Working together with the operator's customer service staff, exercise the full range of support applications possible for a CSR, particularly those relating to device type (e.g., retrieve programming instructions).
3. Verify that the IMSI retrieved by the CSR matches the phone's IMSI.

25.5 Test Result

Successful result:

- All CSR actions can be completed successfully, particularly those related to information retrieval about the subscriber's device.

Unsuccessful result:

- CSR applications fail (e.g., data retrieval for device type fails or returns incorrect information).

25.6 Comments

Individual operators' systems will vary, and an exact description of the necessary steps cannot be provided in a general test document.