Migrating Network Elements to MEID and Expanded UIMID (E-UIMID)

David Crowe
CDMA Development Group
Version 3.6 – June, 2012
www.cdg.org/meid
The Issue
The Issue

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.
The Issue

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.

- The original 32 bit hardware identifiers known as ESN and UIMID are almost entirely depleted—no new assignments since 2010.
Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.

The original 32 bit hardware identifiers known as ESN and UIMID are almost entirely depleted—no new assignments since 2010.

Replacement hardware identifiers for cdma2000® are standardized and available—
- MEID: Mobile Equipment Identifier
- EUIMID: Expanded UIM Identifier
The Issue

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.

- The original 32 bit hardware identifiers known as ESN and UIMID are almost entirely depleted—no new assignments since 2010.

- Replacement hardware identifiers for cdma2000® are standardized and available –
  - MEID: Mobile Equipment Identifier
  - EUIMID: Expanded UIM Identifier

- Operators must evaluate the impact on all network components and may need software upgrades for some.
The Issue

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.

- The original 32 bit hardware identifiers known as ESN and UIMID are almost entirely depleted—no new assignments since 2010.

- Replacement hardware identifiers for cdma2000® are standardized and available –
  - MEID: Mobile Equipment Identifier
  - EUIMID: Expanded UIM Identifier

- Operators must evaluate the impact on all network components and may need software upgrades for some.

- MEID devices and EUIMID cards are now accepted by all major CDMA2000 networks.
The Issue

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a permanent and unique code for a variety of reasons.

- The original 32 bit hardware identifiers known as ESN and UIMID are almost entirely depleted—no new assignments since 2010.

- Replacement hardware identifiers for cdma2000® are standardized and available –
  - MEID: Mobile Equipment Identifier
  - EUIMID: Expanded UIM Identifier

- Operators must evaluate the impact on all network components and may need software upgrades for some.

- MEID devices and EUIMID cards are now accepted by all major CDMA2000 networks.
Definitions

- **MEID – Mobile Equipment ID**
  - 14 digit/56 bit identifier like IMEI.
  - Differs from IMEI in allowing hexadecimal digits (‘A’–’F’).
  - Single ‘check’ digit on labels, bar codes, etc.

- **EUIMID – Expanded UIM ID**
  - Short Form (SF_EUIMID) comes from MEID numbering space.
  - Long Form is the pre-existing ICCID (18 decimal digits/72 bits)

- **pESN/pUIMID**
  - ‘Pseudo’ 32-bit identifier is calculated from MEID or EUIMID using SHA-1 hash algorithm.
  - MEID mobiles also have pESN.
  - EUIMID cards also have pUIMID.
Your Network
Your Network

R-UIM
Your Network
Your Network
Your Network

- R-UIM
- ME
- BSC
- MSC/VLR
- PDN
- AAA
- www.cdg.org
Your Network

- OTAF
- MSC/VLR
- BSC
- PDN
- AAA
- R-UIM
- ME
Your Network

OTAF

MSC/VLR

BSC

PDN

AAA

HLR

ME

R-UIM

CDMA2000 www.cdg.org
Your Network

- OTAF
- MSC/VLR
- BSC
- PDN
- AAA
- Other
- HLR
- ME
- R-UIM
R-UIM – Removable UIM

- Operators must choose SF_EUIMID or LF_EUIMID.
- EF(UIMID) provisioned with pUIMID.
- SF_EUIMID requires 3GPP2 C.S0023-C (TIA-820-C) support for:
  - EF(SF_EUIMID) – Storage for identifier allocated by TIA.
  - Service n8 – Provides access to SF_EUIMID.
  - EF(USGIND) – Set bit 2 to ‘1’ for SF_EUIMID to displace MEID in signaling.
  - Service n9 is optional. It stores MEID, allowing the card to determine when it has been moved to another phone.
- LF_EUIMID requires:
  - Correct provisioning of a properly allocated unique identifier in existing EF(ICCID).
  - Benefits from modified OTASP, R-UIM and CSIM standards.
- MEID/EUIMID testing provided by 3GPP2 C.S0073-B.
ME – Mobile Equipment (Handset)

- Mobiles provisioned with unique MEID and pESN.
- Mobiles must support 3GPP2 C.S0072/TIA-1082:
  - Collision elimination via BS-Assigned, MEID-based or IMSI-based PLCM.
  - Access to MEID (or SF_EUIMID) via Status Request.
  - SCM bit 4 set to ‘1’ to indicate these capabilities to BS.
- Some *MEID-capable* mobiles manufactured 2006/7 and provisioned with ESN will not operate with an EUIMID card.
- If carrier chooses SF_EUIMID for R-UIM identification, mobile must support 3GPP2 C.S0023-C/TIA-820.
- Revisions to OTASP, R-UIM and CSIM specifications published in 2008 and 2009 to better support EUIMID.
- Release E air interface provides access to all hardware identifiers without PREV change – published early 2010.
ME – Mobile Equipment (Handset)

- Mobiles provisioned with unique MEID and pESN.
- Mobiles must support 3GPP2 C.S0072/TIA-1082:
  - Collision elimination via BS-Assigned, MEID-based or IMSI-based PLCM.
  - Access to MEID (or SF_EUIMID) via Status Request.
  - SCM bit 4 set to ‘1’ to indicate these capabilities to BS.

- Some MEID-capable mobiles manufactured 2006/7 and provisioned with ESN will not operate with an EUIMID card.

- If carrier chooses SF_EUIMID for R-UIM identification, mobile must support 3GPP2 C.S0023-C/TIA-820.
- Revisions to OTASP, R-UIM and CSIM specifications published in 2008 and 2009 to better support EUIMID.
- Release E air interface provides access to all hardware identifiers without PREV change – published early 2010.
Mobiles provisioned with unique MEID and pESN.

Mobiles must support 3GPP2 C.S0072/TIA-1082:
- Collision elimination via BS-Assigned, MEID-based or IMSI-based PLCM.
- Access to MEID (or SF_EUIMID) via Status Request.
- SCM bit 4 set to ‘1’ to indicate these capabilities to BS.

Some MEID-capable mobiles manufactured 2006/7 and provisioned with ESN will not operate with an EUIMID card.

If carrier chooses SF_EUIMID for R-UIM identification, mobile must support 3GPP2 C.S0023-C/TIA-820.

Revisions to OTASP, R-UIM and CSIM specifications published in 2008 and 2009 to better support EUIMID.

Release E air interface provides access to all hardware identifiers without PREV change – published early 2010.
ME – Mobile Equipment (Handset)

- Mobiles provisioned with unique MEID and pESN.
- Mobiles must support 3GPP2 C.S0072/TIA-1082:
  - Collision elimination via BS-Assigned, MEID-based or IMSI-based PLCM.
  - Access to MEID (or SF_EUIMID) via Status Request.
  - SCM bit 4 set to ‘1’ to indicate these capabilities to BS.

Some MEID-capable mobiles manufactured 2006/7 and provisioned with ESN will not operate with an EUIMID card.

- If carrier chooses SF_EUIMID for R-UIM identification, mobile must support 3GPP2 C.S0023-C/TIA-820.

- Revisions to OTASP, R-UIM and CSIM specifications published in 2008 and 2009 to better support EUIMID.
- Release E air interface provides access to all hardware identifiers without PREV change – published early 2010.
3GPP2 C.S0072 provides:
- Collision elimination via new PLCM types.
- Access to MEID (or SF_EUIMID) via Status Request.
  - SCM bit 4 set to ’1’ to trigger these capabilities.

3GPP2 A.S0011-17-C (IOS 5.0.1) provides hard handoff with new PLCM types.

Forward paging channel should be configured for IMSI addressing, not ESN.

Shall not:
- Assume that a ‘0x80’ prefix ESN indicates MEID support.

3GPP2 C.S0073 provides test sequences (Rev. A includes EUIMID, Rev. B includes OTASP).
BS – Base Station

- 3GPP2 C.S0072 provides:
  - Collision elimination via new PLCM types.
  - Access to MEID (or SF_EUIMID) via Status Request.
  - SCM bit 4 set to ’1’ to trigger these capabilities.

- 3GPP2 A.S0011-17-C (IOS 5.0.1) provides hard handoff with new PLCM types.

- Forward paging channel should be configured for IMSI addressing, not ESN.

- Shall not:
  - Assume that a ‘0x80’ prefix ESN indicates MEID support.

- 3GPP2 C.S0073 provides test sequences (Rev. A includes EUIMID, Rev. B includes OTASP).
BS – Base Station

- 3GPP2 C.S0072 provides:
  - Collision elimination via new PLCM types.
  - Access to MEID (or SF_EUIMID) via Status Request.
    - SCM bit 4 set to ’1’ to trigger these capabilities.

- 3GPP2 A.S0011-17-C (IOS 5.0.1) provides hard handoff with new PLCM types.

- Forward paging channel should be configured for IMSI addressing, not ESN.

- Shall not:
  - Assume that a ‘0x80’ prefix ESN indicates MEID support.

- 3GPP2 C.S0073 provides test sequences (Rev. A includes EUIMID, Rev. B includes OTASP).
PDN – Packet Data Network

○ PDSN:
  ○ Can transmit MEID (or SF_EUIMID) to AAA in accounting records (ref. 3GPP2 X.S0011-005-D)
  ○ *Will* only receive MEID (not pESN) on EVDO.

○ If NAI format is “esn@domain”:
  ○ Replace by “meid@domain” or another unique address format (e.g. IMSI).

○ If HRPD/EVDO Access Network (AN) uses HardwareID it shall:
  ○ accept MEID instead of ESN.
  ○ translate “HardwareIDType” on the air interface to “Hardware ID Type” on the A12 interface.
  ○ not expect to receive R-UIM identifiers as Hardware ID.
PDSN:
- Can transmit MEID (or SF_EUIMID) to AAA in accounting records (ref. 3GPP2 X.S0011-005-D)
- **Will** only receive MEID (not pESN) on EVDO.

If NAI format is “esn@domain”:
- Replace by “meid@domain” or another unique address format (e.g. IMSI).

If HRPD/EVDO Access Network (AN) uses HardwareID it shall:
- accept MEID instead of ESN.
- translate “HardwareIDType” on the air interface to “Hardware ID Type” on the A12 interface.
- not expect to receive R-UIM identifiers as Hardware ID.
PDN – Packet Data Network

- **PDSN:**
  - Can transmit MEID (or SF_EUIMID) to AAA in accounting records (ref. 3GPP2 X.S0011-005-D)
  - *Will* only receive MEID (not pESN) on EVDO.

- If NAI format is “esn@domain”:
  - Replace by “meid@domain” or another unique address format (e.g. IMSI).

- If HRPD/EVDO Access Network (AN) uses HardwareID it shall:
  - accept MEID instead of ESN.
  - translate “HardwareIDType” on the air interface to “Hardware ID Type” on the A12 interface.
  - not expect to receive R-UIM identifiers as Hardware ID.
PDN – Packet Data Network

○ **PDSN:**
  ○ Can transmit MEID (or SF_EUIMID) to AAA in accounting records (ref. 3GPP2 X.S0011-005-D)
  ○ *Will* only receive MEID (not pESN) on EVDO.

○ If NAI format is “esn@domain”:
  ○ Replace by “meid@domain” or another unique address format (e.g. IMSI).

○ If HRPD/EVDO Access Network (AN) uses HardwareID it shall:
  ○ accept MEID instead of ESN.
  ○ translate “HardwareIDType” on the air interface to “Hardware ID Type” on the A12 interface.
  ○ not expect to receive R-UIM identifiers as Hardware ID.
AAA – Authentication, Authorization and Accounting entity

- May receive MEID (or SF_EUIMID) in accounting records (3GPP2 X.S0011-005-D).
- For 1X data systems:
  - pESN or pUIMID will replace ESN or UIMID in accounting records.
- For EVDO:
  - Only a phone hardware identifier (MEID or ESN) is sent, not an R-UIM identifier (EUIMID or UIMID).
  - Will not provide pESN if MEID is available.
AAA – Authentication, Authorization and Accounting entity

- May receive MEID (or SF_EUIMID) in accounting records (3GPP2 X.S0011-005-D).

- For 1X data systems:
  - pESN or pUIMID will replace ESN or UIMID in accounting records.

- For EVDO:
  - Only a phone hardware identifier (MEID or ESN) is sent, not an R-UIM identifier (EUIMID or UIMID).
  - Will not provide pESN if MEID is available.
AAA – Authentication, Authorization and Accounting entity

- May receive MEID (or SF_EUIMID) in accounting records (3GPP2 X.S0011-005-D).
- For 1X data systems:
  - pESN or pUIMID will replace ESN or UIMID in accounting records.
- For EVDO:
  - Only a phone hardware identifier (MEID or ESN) is sent, not an R-UIM identifier (EUIMID or UIMID).
  - Will not provide pESN if MEID is available.
OTAF – Over-The-Air Activation Function

- OTASP and other provisioning systems are affected if they currently use ESN or UIMID as unique identifier.
  - Probably not affected if MIN/IMSI is pre-provisioned.
- Should support 3GPP2 C.S0016-C or C.S0066 to access MEID or SF_EUIMID during provisioning.
- SF_EUIMID will be transmitted instead of MEID if UsgInd bit 2 is ‘1’.
- OTAF cannot determine if mobile is MEID capable (SCM bit is not accessible to OTAF).
- 3GPP2 C.S0016-C v2.0 and C.S0066-0 v2.0 (07/2008) provide:
  - Access to both MEID and EUIMID
  - Access to all band class information in ESN mobiles.
- Biggest problem is the provisioning of an EUIMID card in an ESN mobile – no unique provisioning identifier unless cards are pre-provisioned. See next slide for solutions…
OTAF – Over-The-Air Activation Function

- OTASP and other provisioning systems are affected if they currently use ESN or UIMID as unique identifier.
  - Probably *not* affected if MIN/IMSI is pre-provisioned.
- Should support 3GPP2 C.S0016-C or C.S0066 to access MEID or SF_EUIMID during provisioning.
- SF_EUIMID will be transmitted instead of MEID if UsgrInd bit 2 is ‘1’.
- OTAF cannot determine if mobile is MEID capable (SCM bit is not accessible to OTAF).
- 3GPP2 C.S0016-C v2.0 and C.S0066-0 v2.0 (07/2008) provide:
  - Access to both MEID and EUIMID
  - Access to all band class information in ESN mobiles.

- Biggest problem is the provisioning of an EUIMID card in an ESN mobile – no unique provisioning identifier unless cards are pre-provisioned. See next slide for solutions…
OTASP Solution for ESN Mobiles

- An ESN mobile will be unlikely to have the software to transmit EUIMID via C.S0016-C v2.0 or C.S0066-0 v2.0.
- pUIMID will be transmitted but is not unique.
- How can card be uniquely identified?
- There are solutions, including:
  - Pre-provision with MIN, IMSI or MDN:
    » May not be desirable as this can waste numbers and may make inventory management more difficult as cards can only be sold in the region where this number is valid.
  - Keep entirely blank so identification unnecessary:
    » Requires OTA provisioning of A-Key which probably requires a more expensive co-processor card.
    » Does not work for pre-paid where specific card has specific balance.
  - Make EUIMID accessible by putting it in IMSI_T or MDN fields:
    » The EUIMID pre-provisioned in these fields can be replaced by valid data during provisioning. These fields are always accessible.
An ESN mobile will be unlikely to have the software to transmit EUIMID via C.S0016-C v2.0 or C.S0066-0 v2.0.

pUIMID will be transmitted but is not unique.

How can card be uniquely identified?

There are solutions, including:

- **Pre-provision with MIN, IMSI or MDN:**
  - May not be desirable as this can waste numbers and may make inventory management more difficult as cards can only be sold in the region where this number is valid.

- **Keep entirely blank so identification unnecessary:**
  - Requires OTA provisioning of A-Key which probably requires a more expensive co-processor card.
  - Does not work for pre-paid where specific card has specific balance.

- **Make EUIMID accessible by putting it in IMSI_T or MDN fields:**
  - The EUIMID pre-provisioned in these fields can be replaced by valid data during provisioning. These fields are always accessible.
MSC and VLR

- Should support 3GPP2 A.S0011-17-C (IOS 5.0.1) for hard handoff.

- May support 3GPP2 X.S0008 for:
  - MEID Validation (use caution with R-UIM systems).
  - MEID (or SF_EUIMID) transmission to VLR, EIR and HLR.

- All operations should continue to work with pESN or pUIMID, however...

- ...some VLRs will not function properly with duplicate ESN codes and must be patched or upgraded.
MSC and VLR

- Should support 3GPP2 A.S0011-17-C (IOS 5.0.1) for hard handoff.

- May support 3GPP2 X.S0008 for:
  - MEID Validation (use caution with R-UIM systems).
  - MEID (or SF_EUIMID) transmission to VLR, EIR and HLR.

- All operations should continue to work with pESN or pUIMID, however...

- ...some VLRs will not function properly with duplicate ESN codes and must be patched or upgraded.
MSC and VLR

- Should support 3GPP2 A.S0011-17-C (IOS 5.0.1) for hard handoff.

- May support 3GPP2 X.S0008 for:
  - MEID Validation (use caution with R-UIM systems).
  - MEID (or SF_EUIMID) transmission to VLR, EIR and HLR

- All operations should continue to work with pESN or pUIMID, however...
  - ...some VLRs will not function properly with duplicate ESN codes and must be patched or upgraded.
HLR - Home Location Register

- HLR usually includes AC (Authentication Center) functions.
- Authentication and other ANSI-41 functions are generally unaffected by the transition to MEID/EUIMID.
  - Where authentication specifies an ESN as input, UIMID, pESN or pUIMID may be used instead, whichever is available.
  - There is no loss of security from non-uniqueness – the ESN has always been transmitted in the clear.
- ANSI-41 upgrades in 3GPP2 X.S0008 to transmit MEID as well as pESN/pUIMID are completely optional.
- Some HLRs insist that all ESN codes are unique. This is not compatible with pESN/pUIMID which are not always unique. These HLRs must be upgraded.
HLR – Home Location Register

- HLR usually includes AC (Authentication Center) functions.

- Authentication and other ANSI-41 functions are generally unaffected by the transition to MEID/EUIMID.
  - Where authentication specifies an ESN as input, UIMID, pESN or pUIMID may be used instead, whichever is available.
  - There is no loss of security from non-uniqueness – the ESN has always been transmitted in the clear.

- ANSI-41 upgrades in 3GPP2 X.S0008 to transmit MEID as well as pESN/pUIMID are completely optional.

- Some HLRs insist that all ESN codes are unique. This is not compatible with pESN/pUIMID which are not always unique. These HLRs must be upgraded.
Other entities

- Operator networks include other elements, some using proprietary interfaces.
- Most should be unaffected by the ESN to MEID and UIMID to EUIMID transition.
- However, some may have bugs or restrictions that must be corrected, including:
  - Requiring that ESN codes are unique (just like some HLRs and VLRs).
  - Disallowing decimal MEID codes (e.g. RR=99 or lower).
- Verification of all network elements is important.
Other entities

- Operator networks include other elements, some using proprietary interfaces.
- Most should be unaffected by the ESN to MEID and UIMID to EUIMID transition.
- However, some may have bugs or restrictions that must be corrected, including:
  - Requiring that ESN codes are unique (just like some HLRs and VLRs).
  - Disallowing decimal MEID codes (e.g. RR=99 or lower).
- Verification of all network elements is important.
Billing System

- Some billing protocols (e.g. CIBER) allow only one hardware identifier (ESN or pESN or UIMID or pUIMID or MEID or SF_EUIMID) to be transmitted.
- Some billing systems perform MIN/ESN validation (checking that customer record identified by MIN is associated with received ESN).
- This validation is not applicable when MEID is transmitted.
- Carriers can continue to include 32-bit identifier (e.g. pUIMID) or not validate when MEID is received.
- Continued inclusion of the 32-bit identifier is safest.
- Billing systems should accept either 32 or 56 bit formats.
- There is no risk of fraud and only a small risk of billing errors if validation is removed.
Some billing protocols (e.g. CIBER) allow only one hardware identifier (ESN or pESN or UIMID or pUIMID or MEID or SF_EUIMID) to be transmitted.

Some billing systems perform MIN/ESN validation (checking that customer record identified by MIN is associated with received ESN).

This validation is not applicable when MEID is transmitted.

Carriers can continue to include 32-bit identifier (e.g. pUIMID) or not validate when MEID is received.

Continued inclusion of the 32-bit identifier is safest.

Billing systems should accept either 32 or 56 bit formats.

There is no risk of fraud and only a small risk of billing errors if validation is removed.
Operator Status

- The major cdma2000 operators, large and small, have implemented MEID.
- Generally the transition is fairly simple, but some infrastructure upgrades may be required.
- EUIMID has been implemented by most operators ranging from small to very large.
- Remaining operators need to complete the MEID and EUIMID transitions now!
  - No UIMID codes have been assigned since 2010. It may be difficult or impossible to get UIMID cards in the future. EUIMID is a necessity!
Operator Status

- The major cdma2000 operators, large and small, have implemented MEID.
- Generally the transition is fairly simple, but some infrastructure upgrades may be required.
- EUIMID has been implemented by most operators ranging from small to very large.
- Remaining operators need to complete the MEID and EUIMID transitions now!

- No UIMID codes have been assigned since 2010. It may be difficult or impossible to get UIMID cards in the future. EUIMID is a necessity!
Resources

- Glossary.
- Also see http://cdg.org/MEID
- Also see http://tiaonline.org/standards/resources
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP2</td>
<td>Third Generation Partnership Project 2</td>
<td>PLCM</td>
<td>Public Long Code Mask</td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
<td>R-UIM</td>
<td>Removable UIM</td>
</tr>
<tr>
<td>EUIMID</td>
<td>Expanded UIMID</td>
<td>SCM</td>
<td>Station Class Mark</td>
</tr>
<tr>
<td>ICCID</td>
<td>International Charge Card ID</td>
<td>SF_EUIMID</td>
<td>Short form EUIMID using MEID format.</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscription Identity</td>
<td>TIA</td>
<td>Telecommunications Industry Association</td>
</tr>
<tr>
<td>IOS</td>
<td>Inter-Operability Standard (‘A’ Interface)</td>
<td>UIM</td>
<td>User Identification Module</td>
</tr>
<tr>
<td>LF_EUIMID</td>
<td>Long form EUIMID (ICCID of card)</td>
<td>UIMID</td>
<td>R-UIM Identifier</td>
</tr>
<tr>
<td>MEID</td>
<td>Mobile Equipment Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thank You!

Contact
David Crowe
Senior Technical Consultant,
CDG
(dcrowe@cdg.org)