"Frequently Asked Questions" (FAQ)

on

MEID and Expanded UIMID (E-UIMID)

Version 4.0

March 15, 2010

Further information can be found at http://cdg.org/meid or by contacting meid@cdg.org

Hardware Identifier Transitions
From ESN and UIMID to MEID and EUIMID
"Frequently Asked Questions"

Existing Identifiers: ESN and UIMID

1. When are ESN and UIMID numbers expected to be fully depleted?

Applications for assignments of ESN and UIMID have not been accepted since June 30, 2010 and assignments of codes for previously received applications are continuing as codes come available through reclamation of earlier assignments that were not used for CDMA devices and as manufacturer records document a need.

2. Why can't all ESN codes assigned to analog and TDMA be reused?

ESN codes were never allocated for specific technologies. Manufacturers assigned ESN codes when analog was the only technology may have later gone on to manufacture TDMA and then CDMA mobiles with the same allocation. There has never been a requirement to use ESN codes only for a particular technology. Codes can be re-used when manufacturer records clearly record that the codes were not used or were used for older technologies. UIMID codes cannot be reclaimed unless a manufacturer obtained one and did not use it because they are already at the minimum block size and were only assigned for CDMA usage.

3. When were ESN and UIMID assignments no longer accepted by the TIA?

Applications for assignments of ESN and UIMID were no longer accepted by the TIA after June 30, 2010.

4. How do I get information on ESN and UIMID assignments?

Resource administrators, such as the TIA, normally produce regular reports. A summary of ESN assignments is produced monthly. UIMID assignments are reported quarterly. Contact the TIA (meidadmin@tiaonline.org) for more information.

5. What if I don't do anything or simply re-use ESN codes?

This will result in ESN duplications and collisions that, although rare, can cause service-affecting problems, which are described below.

6. What is the PLCM and how is it affected by non-unique ESN codes?

The PLCM is the Public Long Code Mask that distinguishes communications on the reverse traffic channel. In systems that do not support new PLCM assignment types it is derived from the ESN (or UIMID in a card-based phone) and thus reverse traffic channel *communications from mobiles using the same ESN/UIMID code are indistinguishable. This can cause cross-talk, dropped calls, etc.*

7. Is Over-the-Air-Service-Provisioning (OTASP) affected?

OTASP databases may be indexed by ESN (or UIMID in card-based systems) because phones or cards are often not shipped with a pre-programmed IMSI. Thus the ESN or UIMID was traditionally the only unique identifier available for provisioning. In situations where the ESN or UIMID is not unique, the OTASP database may fail to provision a mobile. A solution is to implement C.S0066 or Revision E of the CDMA2000 air interface which can allow the retrieval of the MEID by the OTAF. Note that some scenarios (e.g. use of LF_EUIMID, EUIMID card in ESN phone, SF_EUIMID in non-IS-820-C compliant phone) may still not allow the retrieval of a unique identifier for the card, even with C.S0066 support in the network. In addition, OTASP protocols (designed before EUIMID standardization) use the 0x80 prefix to indicate that the mobile is MEID capable. An EUIMID R-UIM in an ESN-capable phone will normally transmit a pUIMID (i.e. having a 0x80 prefix), and the OTAF will conclude that the mobile is MEID capable. This needs to be taken into account when designing or upgrading an OTAF.

8. How is Billing Affected?

Call detail record and billing record formats will continue to accept a 32-bit identifier. Some may allow an additional identifier to be specified (e.g. MEID) while others (specifically the CIBER inter-carrier billing format) do not allow both identifiers, but do allow MEID (or SF_EUIMID) to replace the 32-bit identifier (e.g. pESN or pUIMID). We are unaware of any billing systems that assume that the 32-bit identifier is unique so the presence of duplicate pseudo identifiers should not be a problem. Some systems that process call detail or billing records also include fraud-monitoring capabilities, discussed below. Many systems perform MIN/ESN validation at the home system (as authentication is not available) and the MEID, since it is associated with the hardware, not the subscription, cannot help filter out billing records calls made with, for example, unsubscribed phones. The 32-bit identifier, even when not unique, is still useful for MIN-'ESN' validation. For maximum compatibility with roaming partners it is recommended that billing systems continue to include the 32-bit identifier, even when only a pseudo-ESN or pseudo-UIMID is available.

9. Are Fraud Detection Systems Affected?

Until ANSI-41 was widely implemented, around 1990, fraud detection systems were primitive and some would monitor for a single ESN being associated with multiple MIN or IMSI codes. Some fraud detection systems have maintained this check, even though it has little value in modern networks. If it is present, carriers may need to contact their fraud equipment or service providers to ensure that pESN and pUIMID values (easily recognized by their 0x80 prefix) are never added to this database.

10. Is Authentication Affected?

CAVE authentication does use the ESN, or 32-bit equivalent (such as pESN or pUIMID), as an input to CAVE. However, the algorithm does not rely on the uniqueness of the value, therefore remains secure. CAVE authentication relies most heavily on the secret input (A-Key/SSD). In contrast, ESN is transmitted in the clear, and thus must always be assumed to be known to attackers. AKA authentication, which is not yet widely used, does not use ESN as an input.

11. Is ANSI-41 Validation Affected?

*ANSI-41 validation ensures that a single IMSI is always associated with the same ESN or UIMID (at least until the HLR is updated with a new value). It does **not**, however, check that a single ESN or UIMID is used only with a single IMSI. Therefore the presence of duplicate pESNs or pUIMIDs will **not** cause validation failures. Some HLRs are known to have a uniqueness check even though this is not required by ANSI-41. A patch must be installed to remove this check.*

12. Are Provisioning Systems affected?

No specific standards govern provisioning systems, so the exact behavior will be implementation specific. Today, some systems may be configured to disallow provisioning of different subscriptions with the same ESN or UIMID. These would need to either have this check disabled, or use the new identifiers (e.g. MEID/EUIMID) for their uniqueness check instead.

13. How frequently will collisions occur?

The actual rate of collisions will depend on the number of mobiles using pESN or pUIMID on your network, the number of users within interfering range, and the frequency of call attempts. At worst, the rate is expected to be not much more than one out of a million calls. See the White Paper for more information.

Duplications within a batch of phones/R-UIMs are more likely. When there are more than 5,000 devices/cards, there is a greater than 50% probability that somewhere within that group there will be at least one duplicated pESN/pUIMID

New Identifiers: MEID and EUIMID

14. What replaces ESN?

The 56-bit MEID (Mobile Equipment Identifier) combined with the 32-bit pESN will supersede the current unique ESN.

15. How does a Phone Indicate MEID Support?

Phones that support MEID (i.e. support TIA-1082/C.S0072) and are provisioned with an MEID will set SCM bit four (previously not used in CDMA systems) to "1". This indicates that a StatusRequest for MEID will be accepted, that MECAM and MUHDM *messages types are supported, and that PLCM can be assigned by the Base Station or derived from MEID or IMSI instead of being derived from the ESN.*

16. What is the SCM setting for a mobile that supports MEID but does not have one provisioned?

Setting SCM bit 4 indicates that an MEID is available. It should be set to "0" if the mobile is not provisioned with an MEID, but a true ESN is included instead – even if the phone is capable of supporting MEID and BS-assigned PLCM.

17. What does "MEID capable" mean?

"MEID capable" refers to a device that has the necessary software to enable operation with an MEID, even if it is not actually provisioned with an MEID. Some operators and manufacturers have chosen to use a common software build even when some of the devices have an ESN, and others have an MEID. Except for certain isolated edge cases (see FAQ#28 – Have any problems been discovered with MEID or EUIMID?), this distinction should not affect actual operation – a phone is either ESN-equipped (and MEID capability is irrelevant) or MEID-equipped (and MEID capability is assumed).

18. Will a Phone with true ESN always set SCM bit 4 set to 0?

Yes. A mobile provisioned with ESN will set SCM bit 4 to 0. If it contains an R-UIM including EUIMID and UsgInd bit 1 is set to '1' it will transmit a pUIMID instead of ESN. It will not, however, support Status Request or OTASP messaging carrying MEID, nor the MECAM and MUHDM messages supporting the new PLCM types. The combination of mobile station with SCM bit 4 set to 0 and R-UIM card with EUIMID should be minimized due to these limitations. Note that SCM bit 4 is set to 0 even if the R-UIM is SF_EUIMID-based with both bits of the usage indicator set to 1, and the phone has the necessary software to support MEID requests.

19. What will replace UIMID?

The EUIMID (Expanded UIMID) combined with the 32-bit pUIMID will supersede the current unique UIMID. The EUIMID may either be the Short Form (SF_EUIMID) based on the 56 bit/14 hex digit MEID format or the Long Form (LF_EUIMID) based on the 18 decimal digit/72 bit ICCID.

20. What is the format of the MEID?

The MEID is composed of an 8 hexadecimal digit Manufacturer Code followed by a 6 hexadecimal digit serial number. In practice, many assignments are subdivided resulting in the equivalent of a 9 hex digit Manufacturer Code followed by a 5 hex digit serial number or even smaller subdivisions for smaller manufacturers.

21. Is MEID compatible with IMEI?

*The MEID is identical with the IMEI in size but because it always contains at least one hex digit, and the IMEI is composed solely of decimal digits, it is not compatible for purposes where the digits are interpreted (notably this does **not** include air interface and* *network signaling). For full compatibility a special form of the MEID can be used with all decimal digits. This may be useful in dual-technology phones, but does not affect SF_EUIMID in R-UIMs because GSM SIM cards do not contain an IMEI, so there is nothing to be compatible with. Currently these codes will be assigned with the first two digits set to "99" or lower, assigned by the TIA or any authorized IMEI administrator.*

22. What are the printed formats?

Printed formats of MEID and SF_EUIMID can be either hexadecimal, decimal or 'IMEI'. The hexadecimal format is displayed by printing the hexadecimal representation of each group of 4 bits (0-9, A-F) producing a 14 digit hexadecimal number. The decimal format is produced by converting the manufacturer code (32 bits) to decimal and padding to 10 digits, and following these digits by the serial number (24 bits) after conversion to decimal and padding to 8 digits. This produces an 18-digit number and the 32/24 bit division is used even if the MEID manufacturer code is subdivided. The IMEI format prints each group of four bits as a decimal digit (0-9) producing a 14 digit decimal number. There is no hexadecimal or 18-digit format for IMEI although there are cases where a 14 digit number is treated as an MEID and the 18-digit format generated as if it was a hexadecimal number (which technically it is). Each of these formats may be followed by a single check digit. See 3GPP2 X.S0008 for more details.

The ICCID is represented as an 18 digit decimal number followed by a single check digit. When stored, an additional 'filler' digit (0xf) is included to pad the number to the 10 bytes of storage available in the R-UIM. See ITU-T E.118 and 3GPP2 C.S0023 for more details.

23. What is a check digit?

When providing a human-understandable representation of MEID or EUIMID (e.g. on a computer screen, printed on a phone or read over a phone) a check digit is usually added. This is calculated from the printed digits using the Luhn algorithm and can detect all single digit errors, and most transpositions of two adjacent digits. This is designed to protect against keying errors, not transmission errors. For this reason check digits are not always stored electronically. Check digits are normally calculated using base-10 arithmetic but the check digit for an MEID with one of the first two ("RR") digits between 'A' and 'F' must be calculated using base-16 arithmetic.

24. Who assigns the MEID?

The MEID resource is administered by the GHA (Global Hexadecimal Administrator), which is currently the TIA. This includes the IMEI-compatible form, composed solely of decimal digits (although TIA is not the exclusive administrator of decimal IMEIs). The SF_EUIMID is taken from the MEID address space and administered by the TIA. Specific assignments may be by the TIA or by a designated regional authority.

25. Who assigns the EUIMID?

The SF_EUIMID is assigned from the MEID address space, which is currently assigned by the TIA or a designated regional authority.

The ICCID is administered by the authority in the nation or international organization to which the ITU-T E.164 CC (Country Code) is assigned.

26. What if I support EUIMID and one of my phones roams into a system that doesn't?

The phone will transmit a 32-bit pUIMID, which will be indistinguishable to the system from a pESN. If the phone and base station both support MEID the consequences of collisions is minimized (due to BS-assigned PLCM) but ESN-only addressing on the reverse traffic channel may still cause collisions. If either the phone or the base station does not support MEID, call failures may occur due to PLCM duplication. Some VLRs that have not been upgraded may deny service to two mobiles with the same pESN or pUIMID. Collisions due to OTASP are unlikely because OTASP is not normally supported for roamers.

27. How will I find out about MEID or EUIMID assignments?

Resource administrators, such as the TIA, normally produce regular reports. The MEID (including SF_EUIMID) is administered by the TIA. Contact meidadmin@tiaonline.org for more information. A national authority will administer the ICCID (LF_EUIMID) and reporting requirements will be decided by them.

28. Have any problems been discovered with MEID or EUIMID?

The problems discovered so far with the transitions to MEID and EUIMID are:

1. *Certain base stations did not handle SCM bit 4 correctly and MEID-equipped phones would not receive service. This was believed to be isolated to one equipment type in one carrier's network and has been resolved.*

2. *Some early (circa 2007) MEID-capable and R-UIM capable phone models would not work when not provisioned with an MEID, but used with an R-UIM with an EUIMID. This problem can be fixed in several ways, including provisioning the phone with an MEID, using a card with unique UIMID or updating its software.*

3. *OTASP provisioning (C.S0016/C.S0066) cannot obtain all band class information for non-MEID phones. This problem was resolved in C.S0016-C v2.0 (October, 2008).*

4. *OTASP provisioning (C.S0016/C.S0066 before C.S0016-C v2.0) does not have access to a unique provisioning identifier when an R-UIM with EUIMID is in a phone with ESN. As a workaround it is possible to store the EUIMID in R-UIM files that are not needed until the time of provisioning (such as MDN) but that are accessible via all generations of R-UIM phones.*

5. *Certain HLRs and VLRs will not provide service to mobiles with duplicate pESN or pUIMID values unless upgraded. It is possible that similar problems will be found with other core network equipment although none have been reported so far.*

29. My Vendor Provides “MEID Validation”. Should I activate it?

Some infrastructure vendors provide MEID validation, ensuring that the MEID and MIN or IMSI make a matched pair. This validation is acceptable at the HLR where the status of the mobile is known (i.e. whether it has a R-UIM and, if it does, whether it is SIM-locked) but is not acceptable at the VLR, at least not for roamer, as it will prevent any R-UIM cards from being moved between mobiles.

30. What Standards Changed to Support MEID and EUIMID?

Several specifications were changed to support MEID or EUIMID. 3GPP2 identities are given and specifications can be obtained at no charge from the http://www.3gpp2.org website:

- *A.S0001 through A.X0005, Revision C Version 2.0 support the new PLCM assignment methods on the IOS (BSC–MSC interface).*
- *C.S0005-E provides access to the phone’s ESN and MEID as well as the inserted card’s EUIMID and the UIMID, in all cases regardless of UsgInd bit settings and without a PREV change.*
- *C.S0016-C provides access to the MEID (or SF_EUIMID) during OTASP. Version 2.0 was developed to provide access to both MEID and EUIMID (either type) as well as separating band class access from MEID support.*
- *C.S0023-C supports SF_EUIMID in the R-UIM. C.S0023-C v2.0 was developed to provide important clarifications to SF_EUIMID and LF_EUIMID.*
- *C.S0024-A supports MEID as a form of Hardware ID. This can be supported by C.S0024 Revision 0 systems. C.S0024-A v3.0 (September, 2009) clarifies that card identifiers are never transmitted as Hardware ID.*
- *C.S0065-0 v2.0 contains the same changes as C.S0023-C v2.0.*
- *C.S0066-C provides the same changes as C.S0016-C, but in a way that is compatible with releases of C.S0016 before Revision C.*
- *C.S0072 provides support for transmission of MEID (or SF_EUIMID) in Status Request and several new PLCM assignment methods (including BS-assigned).*
- *C.S0073 provides a test plan for MEID-equipped mobiles and base stations. Revision A and B add tests for MEID-equipped mobiles with an EUIMID equipped R-UIM inserted.*
- *X.S0008 provides support for transmission of MEID through the ANSI-41 network, including to an EIR (Equipment Identity Register). Version 2.0 supports the MEID Validation feature.*
- *X.S0011-005-Dsupports MEID in AAA accounting records.*

- *X.S0033 supports transmission of MEID for OTASP purposes at the ANSI-41 protocol level.*

Compatibility with the ESN and UIMID

31. What is a pseudo-ESN?

A pseudo-ESN (pESN) is a 32-bit replacement for a unique ESN in a mobile that is provisioned with an MEID. The format is the 8 bit 'manufacturer code' 0x80 followed by the 24-bit least significant digits of the SHA-1 hash of the MEID. Since there are many times more MEID codes than 2^{24} *there will be many MEID codes that hash to the same pESN value.*

32. What is a pseudo-UIMID?

A pseudo-UIMID (pUIMID) is a 32-bit replacement for a unique UIMID in a R-UIM that is provisioned with an EUIMID. The format is the 8 bit 'manufacturer code' 0x80 followed by the 24-bit least significant digits of the SHA-1 hash of the EUIMID (either Short or Long Form). Since there are many times more EUIMID codes than 2^{24} *there will be many EUIMID codes that hash to the same pUIMID value.*

33. What is the SHA-1 Hash?

The SHA-1 (Secure Hash Algorithm-1) is a "one-way" algorithm that produces a 160-bit output from any input. A hash algorithm is one that takes a numeric input of a particular size and produces an output value that is evenly spread over a specified range of numbers that is much smaller than the input. The original value can therefore not be determined if only the hash value is known. For the purposes of pESN and pUIMID calculations only the least significant (rightmost) 24 bits are retained. SHA-1 was chosen because it is widely available, relatively efficient and produces output with desirable pseudo-random characteristics. By spreading MEID or EUIMID codes over the entire 2^{24} *numbering space, the risk of collisions is reduced to the minimum.*

34. How does a pESN/pUIMID differ from a normal ESN?

A pESN or pUIMID can be distinguished only by the 0x80 'Manufacturer Code' prefix. pESNs cannot be distinguished from pUIMIDs. No manufacturer information can be deduced from a pESN or pUIMID.

35. How can mobiles be distinguished if transmitted ESN is not unique?

Most operations with cdma2000 devices use IMSI as the unique identifier as all subscriptions must have a unique identifier. This leaves only a small problem with phones that are A) unsubscribed; B) retain their previously assigned IMSI; C) are powered on; and D) in the same service area as the subscribed phone that has been assigned the same IMSI. In some circumstances, the IMSI is not used or not available. The most important circumstances are: A) for a new phone or R-UIM that is not pre-provisioned with an IMSI; B) Calculation of the PLCM from the ESN; C) ESN-addressing on the reverse traffic channel.

36. 16 million pESNs/pUIMIDs will last me for a while. Can’t I just make sure they’re unique, then not do anything else?

This is extremely wasteful of the MEID/EUIMID resources. Also it does not address MEID/EUIMID-equipped roamers that appear in your network who may clash with your own subscribers, or clashes that may arise due to your subscribers roaming outside your network. And, since there are only 2^{24} unique pESNs or pUIMIDs (about 16.8 million) this solution will last only until that many mobiles has been added to your network.

37. My provisioning system checks to see if the ESN has been used before when I define a new subscriber. How can this work with MEID/pESN?

Changes will be required to the provisioning system – to either disable the check, or allow the entry of a MEID instead, which will be unique. Depending on the requirements of your network elements (e.g. HLR), the provisioning system can derive the associated (non-unique) pESN, or provide the full MEID to the network element.

38. Which of my currently deployed and upcoming phones, R-UIMs and other devices are compatible with MEID, EUIMID, pESN and pUIMID?

You will need to check with your manufacturers. For the devices that are most common in your network you may wish to perform your own verification testing to ensure that they can function with network support for MEID and EUIMID. For new devices, you may wish to verify from the manufacturer supplemented by your own testing, that they can function both in a network with MEID support and without.

39. What if I upgrade my network before there are any MEID phones?

Upgrading the network early presents no technical problems – the network relies on an indicator from the phone (SCM bit 4) in order to behave differently. Existing base stations should ignore this bit that previously had no meaning in cdma2000 systems.

40. What if I allow MEID or EUIMID devices on the network before there is full support?

Roamers with MEID or EUIMID support may already be on your network. The only problem with this may be a very slightly elevated call failure rate. This is probably too small to detect (probably less than one per million calls).

Providing MEID or EUIMID mobiles without MEID network support is not recommended as a long-term option as the number of these mobiles will be much greater than roamers so the problems of duplication and collisions will be greater. OTASP may not be possible if new devices are not provisioned with an IMSI. Several models of HLR, VLR and other core network equipment will not accept duplicate ESNs unless upgraded.

EVDO/HRPD and Packet Data

41. Is EVDO/HRPD Affected?

An Access Terminal (AT) can respond to a request for Hardware ID with MEID instead of ESN. C.S0024-B v3.0 clarifies that R-UIM identifiers (UIMID and EUIMID) should not be transmitted in this field.

42. Backwards Compatibility

If existing EVDO infrastructure does not accept an access from a mobile based on an unexpected value in the Hardware ID field (i.e. MEID) it will need to be upgraded to either ignore unexpected values or accept MEID.

43. Is the Packet Data Core Network Affected?

The MEID is a new field in cdma2000 packet data accounting (RADIUS) defined in X.S0011-005-D. All core network elements that create, receive or otherwise interpret messages on the RAN-PDSN-AAA interfaces should be capable of at least accepting MEID and possibly also of including it when it is available. This equipment should also be aware that the ESN field will not be populated for EVDO activity with an MEID device.

44. Does the NAI Need to be Changed?

Some systems used esn@domain or uimid@domain as the NAI (Network Access Identifier). This is probably used as a unique identifier at the AAA. This will need to be changed to MEID@domain or EUIMID@domain, or some other identifier that is unique.