FAQ for ESN and UIM_ID Transition from ESN to MEID & EUIMID

Note: The resource used for UIM_IDs (i.e., a 32-bit identifier associated with a SIM or smart card) is compatible with and derived from the ESN pool of Manufacturer Code-Serial numbers. Therefore UIM_ID exhaust is directly impacted by ESN exhaust.

Q. 1: **Does ESN and UIM_ID administration of existing assignments cease to be required ?**

    A Once the Mobile Equipment IDentifier (MEID) is implemented, the administrators are anticipated to continue to support the Electronic Serial Number (ESN) and User Identity Module IDentifier (UIM_ID) administration process for a reasonable limited time. At this time we see no change in the UIM_ID administration process.

Q. 2: **Will a query of ESN requirements or notification of MEID status be provided to the FCC ?**

    A Yes. The ESN Administrator will continue to update the FCC on ESN exhaust and the status of migration efforts to MEID.

Q. 3: **How will we learn of applications need for MEID instead of ESN to Manufacturers and Industry ?**

    A If a Manufacturer, you will be contacted at your last known point of contact. If a new applicant, please see the procedures at the TIA website http://www.tiaonline.org/standards/resources/esn or http://www.tiaonline.org/standards/resources/meid . If an interested entity, an outreach program provides information found at the TIA website.

Q. 4: **What if I do nothing as an operator ?**

    A Doing nothing is not an option as some functions may not always work, e.g., Over the air Activation (OTA) and basic calling with "conflict of ESNs" collision. Collision probability between two Code Division Multiple Access (CDMA) mobiles using the same pseudo-ESN is currently under study, see question 4b. The minimum needed is for the serving system to recognize and provide service to an MEID capable mobile.

Depending on implementations, home/roaming anomalies may or may not occur. Although it is anticipated that the ESN assignment and MEID assignment process will be done in parallel for a short time, once ESNs exhaust, only MEIDs will be assigned.

The pseudo-ESN (0x80 as its 'Manufacturer Code', followed by the 24 least significant bits of the SHA-1 hash of the 56 bit MEID) is used when MEID isn't implemented in a system.

It is not recommended to delay MEID implementation.

Q.4a: **When MEID capable phones roam into networks that don't support MEID, what happens ?**

    A The phone uses its pseudo-ESN if the system doesn't support MEID yet. While the probability is minimal, this can create conflict of ESNs and would become more acute as more phones with MEID are deployed.

Q.4b: **What are the potential implications of a "conflict of ESNs" ?**

    A If more than one mobile derive the same pseudo-ESN from their MEIDs, then there is the potential for several types of collisions: the Public Long Code Mask (PLCM) generated for each mobile will be the same, there may be impacts to fraud detection mechanisms that rely on Mobile Identification Number (MIN)-ESN pairs instead of authentication, there may be collisions with respect to generated call-back numbers for 911 calls, and there may be difficulties within billing systems that utilize ESN as their subscription identifier. See also the "Whitepaper on Pseudo-ESN Collisions" on the ESN MEID section of the TIA website.

Q. 5: **Are 911 calls affected ?**

    A When an MEID-based Mobile Station (MS) lacking a valid callback number places a 911 call, the non-dialable "callback number" provided to the Public Service Answering Point (PSAP) will be derived from the 24 least significant bits of the pseudo-ESN (in the same way that the non-dialable "callback number" is currently derived from the 24 least significant bits of the ESN).

    When an uninitialized MEID-based MS places a 911 call, the MEID may be used to address the channel assignment message to the MS if an IS-2000-D (or later) or ANS TIA-136/TIA-136-E/TIA-943 air interface is in use. The pseudo-ESN may be used for this purpose if the air interface in use is an analog interface or an older CDMA air interface.

Q. 6: **What will be the impact of Pseudo ESNs, and in particular duplicate Pseudo ESNs, on Fraud Management systems ?**

    A This depends on the fraud system. If a system relies on every mobile having a unique ESN, and considers the appearance of the same ESN with different Mobile Station Identity's {MIN or IMSI} (MSIDs) to be potentially fraudulent activity, excessive false alarms would be generated.

Q. 7: **When we have duplicate ESNs (old analog and CDMA) can there be billing problems ?**

    A This depends on the billing system, as there are many implementations. The Standards will define the information sent. Most rely on the MSID or directory number as the billing identifier, but some may still use a 'negative' list of ESNs to reject records for message processing and clearinghouse settlement."

Q. 8: **Do operators have to deploy 1xEV-DV to deploy MEID phones ?**
  A No. The MEID support is required in air interface TIA-2000 Release D (1xEV-DV). TIA-1082 allows support for MEID in all previous releases of TIA-2000. MEID equipped phones will also work in legacy networks that do not support TIA-1082, though with a minimal risk of Public Long Code collisions.

Q. 9: **Can an ESN mobile use TIA-2000 Revision D air interface features ?**
  A No.

Q. 10: **Is pseudo-ESN used in authentication ?**
  A When an MEID-equipped MS computes the authentication response AUTHR, computed via the Cellular Authentication and Voice Encryption (CAVE) algorithm, it uses the pseudo-ESN for the computation. For authentication using Authentication and Key Agreement (AKA), neither pseudo-ESN nor MEID are used. R-UIMID equipped phones use UIMID or pseudo-ESN for CAVE computation.

Q. 11: **Since pseudo-ESN is not unique to an MS, is authentication weakened by the use of pseudo-ESN ?**
  A The authentication calculation depends on the strength and secrecy of the Shared Secret Data (SSD), not on the uniqueness of public information such as ESN or pseudo-ESN. The strength of the authentication process therefore would not be affected by the use of pseudo-ESN.

Q. 12: **In TIA-2000 release D, it is possible that only the MEID is sent on the air interface. How can the network perform CAVE authentication if required by the home system ?**
  A Since TIA-2000 release D specifies a fixed SHA-1 algorithm for computing pseudo-ESN from the MEID, any network element that knows MEID can compute the pseudo-ESN and forward pseudo-ESN to the legacy network. In the ultimate case, the Authentication Center could compute the pseudo-ESN just before computing the expected authentication response.

Q. 13: **What are the implications of MEID on TDMA ?**
  A ANS TIA-136/TIA-943 standardized MEID aspects for Time Division Multiple Access (TDMA) and note that TIA-943 defines a mechanism to incorporate MEID into all revisions of ANS TIA-136.

Q.14: **What is the MEID format ?**
  A The MEID is a 14 digit hexadecimal value with the following format:

Manufacturer Code								Serial Number						CD
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z	C

.
The CD is not part of the MEID value and is not transmitted.

Q.14a: **What is the MEID Check Digit used for ?**

A A Check Digit (CD) may be calculated for use when an MEID is printed (e.g., on packaging or on the exterior of an MS). The CD is not part of the MEID value and is not transmitted when the MEID is transmitted. CD calculation details are provided in TIA 928-2 Annex B.

Manufacturer Code								Serial Number						CD
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z	C

.

Q.15: Is there a Hex to Decimal MEID conversion method ?

    A Yes. The 3GPP2 SC.R0048-A Annex 2 references TIA-928-2 [E] where it describes the decimal representation of MEID. This MEID Hex to decimal method is based on the same methodology that the ESN Hex to Decimal uses for representation. Details are provided in TIA-928-2 [E] Annex A.

Q.16: What is an EUIMID ?

    A See 3GPP2 S.R0111-0 Stage 1 Requirements. The 3GPP2 SC.R4003-0 specification defines administrative guidelines and procedures governing allocation of the (EUIMID) Expanded R-UIM Identifier. (note; short form (SF_EUIMID) allocations also use GHA guidelines 3GPP2 S.R4002-0.

Q.17: What is a multimode terminal ?

    A An MS designed to operate according to more than one air interface or Network specification (i.e.,3GPP and 3GPP2). The MEID is an International Mobile Equipment Identity (IMEI) for use with a multimode terminal and uses the decimally encoded IMEI range. 3GPP2 S.R0048-A 3G Mobile Equipment IDentifier (MEID) and 3GPP2 SC.R4002-0 MEID Global Hexadecimal Administrator (GHA) Assignment Guidelines and Procedures describe the MEID use in the case of multimode terminals. (note: SF_EUIMID shall use RR=A0-FF regardless if it is a CDMA only or GSM+CDMA card).

Q.18: What is SHA-1 ?

    A The Secure Hash Algorithm (SHA) was developed by NIST, along with the NSA. Information can be found at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf Federal Information Processing Standards Publication (**FIPS) PUB 180-2. FIPS 180-2 superseded FIPS 180-1 as of February 1, 2003.** For a free, downloadable hash calculator program see: http://www.slavasoft.com/hashcalc/ ,where it is important that data be entered in hex format.

Note; The entire SHA-1 generated key isn't used as the pseudo-ESN, see Q4 above. Hashing example: Hexadecimal MEID FF000001123456 has hexadecimal pseudo-ESN 800737E1.

Q.19: What happens to all the "old" ESNs when MEID is rolled out as a standard ?

A The old ESNs will stay assigned to set manufacturers unless they voluntarily return them to the ESN Administrator. This is up to the set manufacturer. It is difficult to say when the last mobile using these old ESNs will be removed from service, it could be many years.

Q.20: Eventually could analog ESNs be reused again since analog is being phased out ?
    A This depends on what the reuse is intended for. Though analog is phasing out in some places, sets in many cases have both analog and digital capabilities. There are already investigations into re-using analog ESNs to derive UIMIDs ('Smart Cards'). The ESN Administrator distributes reports that show the reused ranges.

Q.21: Can the hardware that supports the MEID format use an ESN if one were assigned to it ?
    A This depends on how the hardware/software mobile station (MS) is developed by the set manufacturer. This is an implementation question that should be addressed with your MS manufacturer.

Q.22: Can the hardware have assigned both an MEID and ESN, or is it one and not the other, similar to how a CDMA/GSM phone works ?
    A The standards are specified so that a given mobile will be assigned a true ESN or an MEID but not both.

Q.23: Have any interoperability issues been identified regarding the use of MEID ?
    A Yes. An interoperability issue on the 'A' interface has been discovered between certain BS and MSC implementations,. See CDG Technical Bulletin 070301IRT - publ. March 1, 2007. If any additional questions, please contact- roaming@cdg.org.

Excerpt: Detailed Issue Description. In the failure case, the following behavior is observed:

1. Per C.S0072, MEID-equipped mobiles transmit a '1' in bit 4 of the Station Class Mark (SCM), which is now designated the "MEID support indicator." Prior to this, the bit function was "IS-54 Power Class" and was always set to 0 for CDMA MSs.

2. Following TIA-EIA-136-140, the BS/BSC combines bits 4, 1 & 0 of the SCM to form the IOS "RF Power Capability" field. Note: This is not a CDMA2000® standard, but infrastructure vendors may have shared software between their TDMA and CDMA products, or otherwise decided to use this method for deriving the RF Power Capability value.

3. The RF Power Capability field is included in the Classmark Information Type 2 Information Element, which is a mandatory part of various IOS messages on the A1 interface.

4. When the MSB (i.e., SCM bit 4) is set to 1, the resulting value for the RF Power Capability field is one of the "unused" values as defined in the IOS standard (even in the latest IOS version (v5), which is otherwise updated to handle MEID).

5. Following IOS Message Sending Guidelines, the receiving MSC initiates failure handling, and **the MS does not receive service**.