



# MEID and EUIMID Migration

*CDG Document 158*

*Version 2.0*

30 September 2008

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](mailto:cdg@cdg.org)

## **Notice**

Each CDG member acknowledges that CDG does not review the disclosures or contributions of any CDG member nor does CDG verify the status of the ownership of any of the intellectual property rights associated with any such disclosures or contributions. Accordingly, each CDG member should consider all disclosures and contributions as being made solely on an as-is basis. If any CDG member makes any use of any disclosure or contribution, then such use is at such CDG member's sole risk. Each CDG member agrees that CDG shall not be liable to any person or entity (including any CDG member) arising out of any use of any disclosure or contribution, including any liability arising out of infringement of intellectual property rights.

# 1. Executive Summary

- 1  
2  
3 • **Issue.** It has been known for several years that the ESN numbering resource,  
4 used for both the handset's Electronic Serial Number and for R-UIM UIMID  
5 codes, is close to exhaustion. Due to stringent conservation and reclamation of  
6 codes the life of the resource was extended several years beyond the first  
7 predictions. However, the last virgin (never before assigned) ESN code is  
8 expected to be assigned later in 2008 and reclaimed codes are expected to last  
9 only a few months longer (perhaps through 2009).
- 10 • **Industry Response.** In response to these events, the CDMA2000<sup>®</sup> industry is  
11 migrating handsets from ESN to MEID-based addressing, and R-UIMs from  
12 UIMID- to EUIMID-based addressing.
  - 13 ○ **Non-unique values, known as pESN (pseudo-ESN) or pUIMID**  
14 **(pseudo-UIMID), will be used in ESN/UIMID fields, previously**  
15 **depended upon to be unique**
- 16 • **Potential Impact.** If there are no steps taken in the network and back-end  
17 systems to accommodate this change, possible impacts include:
  - 18 ○ Crosstalk, interference, blocked and dropped calls
  - 19 ○ Misaddressed air interface messaging (e.g. SMS received by wrong  
20 user)
  - 21 ○ Inability to provision and/or bill some subscribers
  - 22 ○ Spurious Fraud Detection alerts
- 23 • **Migration Status.** The migrations have already started
  - 24 ○ Several major CDMA2000<sup>®</sup> operators have already upgraded their  
25 network and deployed MEID-based handsets
  - 26 ○ EUIMID-based R-UIMs have already been deployed by several R-UIM  
27 vendors
- 28 • **Recommended Actions.** All CDMA2000<sup>®</sup> operators are recommended to
  - 29 ○ Upgrade their network to support C.S0072 to minimize PLCM collisions
  - 30 ○ Remove any requirement in their back-end systems for a unique  
31 ESN/UIMID value
  - 32 ○ Use MEID-equipped devices
  - 33 ○ Choose either Long or Short EUIMID format and be prepared to  
34 provision them in R-UIMs when UIMID codes exhaust



# Contents

---

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

<b>1. Executive Summary .....</b>	<b>ii</b>
<b>2. The Need for Migration .....</b>	<b>9</b>
2.1 Exhaust Impacts – Consequences of Inaction .....	10
2.1.1 ESN Usage .....	10
2.1.2 Duplication Impact.....	11
2.1.3 Collision Impact.....	12
2.1.4 MEID/EUIMID Support.....	13
2.2 Resource Utilization and Timelines.....	15
2.2.1 Predicted Timelines .....	15
2.2.2 Current Resource Utilization .....	15
2.2.3 Migration Activities .....	16
2.3 Likelihood of Impacts.....	16
2.3.1 Basic Duplication Probability.....	16
2.3.2 Duplications in a group of cards/devices.....	16
2.3.3 PLCM Collision Probability .....	17
<b>3. Hardware Identifiers Involved.....</b>	<b>19</b>
3.1 Identifier Relationships.....	19
3.2 Existing Identifiers .....	20
3.2.1 Electronic Serial Number (ESN) .....	20
3.2.2 User Identity Module Identifier (UIMID) .....	21
3.2.3 Integrated Circuit Card Identifier (ICCID) .....	23
3.3 New Identifiers .....	24
3.3.1 Mobile Equipment Identifier (MEID).....	24
3.3.2 Expanded UIMID (EUIMID).....	26
3.4 Derived Identifiers.....	27
3.4.1 Secure Hash Algorithm 1 (SHA-1).....	27
3.4.2 Pseudo-ESN (pESN) .....	27
3.4.3 Pseudo-UIMID (pUIMID) .....	29
<b>4. Standards Involved .....</b>	<b>31</b>
4.1 MEID.....	31

1	4.1.1 Requirements .....	31
2	4.1.2 Administration .....	31
3	4.1.3 Billing .....	31
4	4.1.4 Air Interface .....	31
5	4.1.5 ANSI-41 MAP Updates .....	33
6	4.1.6 Over-the-Air Activation .....	34
7	4.1.7 Interoperability and Testing .....	35
8	4.2 Expanded UIMID (EUIMID) .....	36
9	4.2.1 Requirements .....	36
10	4.2.2 Administration .....	36
11	4.2.3 CDMA R-UIM .....	36
12	4.2.4 CDMA SIM Application .....	36
13	<b>5. EUIMID Migration Options .....</b>	<b>37</b>
14	5.1 Long-Form EUIMID .....	37
15	5.2 Short-Form EUIMID .....	38
16	5.3 CDMA Card Application Toolkit (CCAT) .....	39
17	5.4 Device Compatibility with EUIMID .....	40
18	<b>6. Recommendations .....</b>	<b>41</b>
19	6.1 Operators with non-R-UIM-equipped handsets .....	41
20	6.2 Operators with R-UIM-equipped handsets .....	44
21	<b>7. Scenarios .....</b>	<b>48</b>
22	7.1 Device / R-UIM Combinations of Interest .....	49
23	7.2 Non-R-UIM Operator .....	50
24	7.2.1 Basic Operation .....	50
25	7.2.2 Data Services .....	56
26	7.2.3 Lost/Stolen Phone .....	57
27	7.2.4 Over the Air Service Provisioning .....	58
28	7.2.5 Roaming .....	61
29	7.3 R-UIM Operator – existing R-UIM in MEID device .....	63
30	7.3.1 Basic Operation .....	63
31	7.3.2 Data Services .....	67
32	7.3.3 Lost/Stolen Phone .....	67
33	7.3.4 Over the Air Service Provisioning .....	69
34	7.3.5 Roaming .....	70
35	7.4 R-UIM Operator – Short-Form EUIMID .....	71
36	7.4.1 Basic Operation .....	71

1	7.4.2 Data Services .....	74
2	7.4.3 Lost/Stolen Phone .....	75
3	7.4.4 Over the Air Service Provisioning .....	76
4	7.4.5 Roaming.....	77
5	7.5 R-UIM Operator – Long-Form EUIMID .....	78
6	7.5.1 Basic Operation.....	78
7	7.5.2 Data Services .....	79
8	7.5.3 Lost/Stolen Phone.....	80
9	7.5.4 Over the Air Service Provisioning .....	80
10	7.5.5 Roaming.....	81
11	<b>8. Terminology .....</b>	<b>82</b>
12	<b>9. References .....</b>	<b>86</b>
13		
14		
15		

**Figures**

1

2     Figure 3-1: Identifier Relationships ..... 19

3     Figure 3-2 - ESN Manufacturer's code allocation ..... 21

4     Figure 3-3 - Usage Indicator Function ..... 22

5     Figure 3-4 - Structure of ICCID ..... 23

6     Figure 3-5 - MEID Structure (Hexadecimal) ..... 24

7     Figure 3-6 - Derivation of the pESN ..... 28

8     Figure 3-7 - Derivation of the pUIMID ..... 29

9     Figure 7-1 - Device & Card Combinations ..... 49

10    Figure 7-2 - MEID MS Registration - no X.S0008 support ..... 50

11    Figure 7-3 - MEID MS Registration - X.S0008 supported ..... 51

12    Figure 7-4 - Authentication of MEID device ..... 52

13    Figure 7-5 - MEID Origination/Termination ..... 53

14    Figure 7-6 - ESN-based addressing conflict ..... 54

15    Figure 7-7 - MEID Handoff ..... 55

16    Figure 7-8 - OTASP Data Flow ..... 59

17    Figure 7-9 - UIMID Registration - no X.S0008 support ..... 63

18    Figure 7-10 - UIMID Registration - X.S0008 supported ..... 64

19    Figure 7-11 - CheckMEID Operation ..... 68

20    Figure 7-12 - SF\_EUIMID Registration with X.S0008 support ..... 72

21

**Tables**

1

2 Table 3-1 - Sample duplicate pESNs (Hexadecimal format) .....28

3 Table 3-2 - Sample duplicate pUIMIDs .....30

4 Table 3-3 - Sample pESN to pUIMID duplications .....30

5 Table 4-1 - EVDO HardwareIDType values .....33

6 Table 7-1 - Handoff matrix for C.S0072 support levels .....55

7



## ***Revision History***

1

2

<b>Date</b>	<b>Version</b>	<b>Description</b>
2007-05-08	0.1	Document Outline
2007-05-22	0.2	(Incomplete) Draft for comments
2007-06-22	0.3	Update following internal review
2007-10-12	0.4	Draft for use in CDG MEID/EUIMID Seminars
2007-11-12	0.5	Updated draft for CDG website
2007-11-30	1.0	Formatted for posting as CDG White Paper
2008-04-02	1.1	Added band class issue
2008-09-30	2.0	Updated with the latest information from operators, vendors and standards organizations

3



## 2. The Need for Migration

This section describes the impacts of the exhaust of the Electronic Serial Number (ESN) and (Removable) User Identity Module Identifier (UIMID) resource, the likelihood of these impacts occurring, and estimates of the dates of total depletion of these resources.

The specific identifiers are described in further detail in Section 3. . For the purposes of understanding the discussion in this section, the following brief definitions may be used:

- **ESN.** Existing 32-bit identifier for a mobile station. Nearing exhaust.
- **UIMID.** 32 bit card identifier, typically replaces ESN wherever it is used<sup>1</sup>. Nearing exhaust. Allocated from the same numbering space as the ESN. It is also nearing exhaust.
- **MEID.** Replacement<sup>2</sup> 56-bit identifier for the ESN
- **EUIMID.** Replacement<sup>2</sup> identifier for the UIMID
- **pESN.** Non-unique identifier used in place of the ESN, derived from MEID.
- **pUIMID.** Non-unique identifier used in place of the UIMID, derived from the EUIMID.

In this document, “ESN” can refer to a unique, “true” ESN assigned to a mobile station, and also to the “ESN” field in a particular protocol message, which may be populated by a (true) ESN, or another 32-bit identifier, e.g. UIMID, pESN, or pUIMID.

---

<sup>1</sup> UIMID does not replace ESN as the HardwareID parameter in EVDO.

<sup>2</sup> Although the MEID is a replacement for the ESN in the sense that a mobile station will be assigned a MEID instead of a (unique) ESN, this is not to say that the MEID is used in messaging everywhere an ESN-assigned mobile would use its ESN. Likewise for EUIMID and UIMID.

## 2.1 Exhaust Impacts – Consequences of Inaction

At the most simplistic level, the immediate impact of the exhaust of a required, unique identifier like the ESN or UIMID would be a halt to CDMA2000® mobile manufacturing unless some form of re-use, expansion or other relaxation of the uniqueness requirement were implemented.

To enable the industry to proceed, new, longer identifiers have been defined in various standards - see Sections 3. - 4. **To maintain backwards compatibility, non-unique “pseudo” values derived from these new identifiers are used wherever the protocols require an ESN or UIMID value.**

This subsection describes the network impacts arising from the fact that a value that was previously reliably known to be unique to a particular handset or card can now be used by multiple handsets or cards. Additional impacts relating to the way a handset advertises that it uses the new identifier are discussed in Section 2.1.4 .

Section 6. describes recommended actions to avoid or mitigate the impacts listed here – those actions involve changes to various parts of the network and supporting systems. The current section assumes that those actions have *not* been carried out.

### 2.1.1 ESN Usage

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. The bullets below list the major standardized uses of ESN. (Note: The UIMID, if present, may override the ESN. All ESN usage listed below can also apply to the UIMID, except the final bullet – see Section 3.2.2 )

- **Layer 2 Link Access Control (LAC) Addressing.** The ESN forms an optional part of the LAC addressing fields used to identify mobiles over the air. Most operators use the “IMSI + ESN” addressing option on the access channel (more strictly known as the reverse common signaling channel, r-csch). On the paging channel (or forward common signaling channel, f-csch), either IMSI- (or Temporary Mobile Station Identity, TMSI) or ESN-based addressing can be used, but not the combination of both as on the access channel.
- **Public Long Code Mask (PLCM).** The ESN is used to generate the PLCM, which distinguishes one call from another. PLCM “collision” is a key concern when duplicate ESN or UIMID are present in a network.
- **Non-programmed IMSI.** Part of the ESN is used to form the default IMSI of a mobile when an IMSI value has not been explicitly programmed. This value is non-unique today, and no impact is expected from the resource exhaust.

- 1       • **Access Probe Timing.** The ESN (as RN\_HASH\_KEY) is used to compute a  
2       delay applied to mobile access sub-attempts<sup>3</sup>. As there are only 512  
3       possible values, collisions occur today and are resolved by existing  
4       procedures. No impact is expected from the resource exhaust.
- 5       • **Authentication input.** The ESN is used as one of the inputs to compute the  
6       Authentication Response value in the Cellular Authentication and Voice  
7       Encryption (CAVE) algorithm. Since CAVE was designed to combat cloning,  
8       where a subscriber's IMSI and ESN is copied by a fraudster, its security is  
9       not compromised by a non-unique ESN value.
- 10      • **Registration Timer Pseudorandom Number Generator.** The ESN is one  
11      of the inputs to the pseudorandom number generator used in some cases in  
12      timer-based registration. Collisions are currently possible with this generator,  
13      and no impacts are expected due to the resource exhaust.
- 14      • **Back-end systems.** Individual operators may have used the ESN as a  
15      “unique key” for any number of internal systems. Although not subject to  
16      standardization, ESN usage could typically include: an index into a device  
17      information/capabilities database; a uniqueness check at provisioning time;  
18      or a billing integrity check. This is most likely for applications where IMSI is  
19      not available, such as initial service provisioning or pre-sale logistics  
20      tracking.
- 21      • **EVDO Hardware ID.** The ESN is used in EVDO and associated network  
22      protocols as the HardwareID parameter. The UIMID will **not** be transmitted  
23      as HardwareID in R-UIM equipped EVDO devices.

### 24      **2.1.2 Duplication Impact**

25      In this document, “duplication” refers to two mobile stations sharing the same pESN  
26      or pUIMID value, used whenever the signaling protocol (or other scenario) calls for  
27      an ESN. Without any other changes in the network or mobiles, these mobiles  
28      function as if they have a duplicate ESN. The mobiles may in general be located  
29      anywhere within an operator's network or that of their roaming partners. Note that  
30      the mobiles may (and should) have different IMSIs.

31      Impacts of duplication are generally felt in back-end systems. While the exact  
32      impacts are operator specific, some of the more likely impacts are listed below:

- 33      • **No Provisioning.** The provisioning system may reject attempts to provision  
34      mobiles that share the same ESN value.

---

<sup>3</sup> See [http://www.3gpp2.org/Public\\_html/specs/C.S0003-0\\_v3.0.pdf](http://www.3gpp2.org/Public_html/specs/C.S0003-0_v3.0.pdf)

- 1     • **Incorrect Provisioning.** The provisioning system may retrieve a record for the  
2       wrong device when a database is indexed by a (non-unique) ESN, resulting in  
3       the incorrect provisioning of a mobile or R-UIM.
- 4     • **Billing errors.** A billing system or clearinghouse may generate errors for Call  
5       Detail Records (CDRs) received with one ESN but with different MINs/IMSI.
- 6     • **Fraud alerts.** A fraud system might generate multiple false alarms on seeing  
7       call attempts or CDRs from the same ESN with different MINs/IMSI.
- 8     • **No Service.** Some core network elements (such as HLRs and VLRs) may not  
9       allow multiple mobiles to be registered with the same ESN preventing two or  
10      more subscribers presenting the same pESN or pUIMID from obtaining  
11      service.
- 12    • **Duplicate NAIs.** If an ESN- or UIMID-based NAI is used today, this will  
13      become non-unique with the use of pseudo-identifiers, potentially leading to  
14      authentication failures and denial of data service.

15    In most cases equipment vendors can supply patches or upgrades to eliminate  
16    these problems.

### 17    **2.1.3 Collision Impact**

18    In this document, “collision” refers to two duplicate-ESN mobiles that are active in  
19    the same carrier-sector or in two or more interfering sectors. The mobiles may be  
20    active for several reasons including attempting to make (or receive) calls at about  
21    the same time. Collision is thus a specific case of duplication.

22    When messages are addressed by ESN to one of multiple duplicate-ESN mobiles in  
23    the same area<sup>4</sup>, the messages may be processed by both mobiles. See the  
24    [Collisions WP] for a listing of the impact of each message that may be addressed in  
25    this way, and Section 7.2.1.6 for a particular example where a mobile can receive  
26    an SMS intended for someone else.

27    Note that the alternative addressing method (via IMSI) may be susceptible to similar  
28    effects if a mobile were programmed with the IMSI of a legitimate mobile in the  
29    same area. However, the likelihood of this occurring is much less. This is because a  
30    mobile with a duplicate IMSI could not get any other services (it would fail  
31    authentication) and it would only cause interference if it stayed in the vicinity of the  
32    legitimate phone.

---

<sup>4</sup> i.e. the area over which the message is sent

1 The impact of collisions derives from the fact that in current networks, the Public  
2 Long Code Mask (PLCM<sup>5</sup>) is derived from the mobile's ESN.

### 3 **2.1.3.1 What is a PLCM?**

4 The PLCM is a 42-bit number used to generate the public long code, a pseudonoise  
5 sequence used for scrambling on the forward CDMA traffic channel and spreading  
6 on the reverse CDMA traffic channel<sup>6</sup>. On the forward traffic channel, distinct Walsh  
7 codes further distinguish individual users' traffic. However on the reverse traffic  
8 channel, only the PLCM differentiated users' traffic until Release D and 3GPP2  
9 C.S0072 provided other derivation methods.

10 In CDMA2000<sup>®</sup> networks, the PLCM comprises a channel-specific header plus a  
11 permutation of the mobile's ESN.

12 (Note by contrast that for CDMA 1xEV-DO networks, the PLCM is *not* derived from  
13 a hardware identifier permanently associated with the Access Terminal.)

### 14 **2.1.3.2 Impact of PLCM collision**

15 The [Collisions WP] describes in detail the effects of PLCM collisions. In brief, the  
16 effects may include:

- 17 • **Cross-talk.** Both parties engaged in calls using the same PLCM may hear the  
18 reverse audio from only one mobile (the one whose traffic arrives at the base  
19 station with greater power)
- 20 • **Interference and call drops.** If the signals from both mobiles arrive at similar  
21 power, they will interfere destructively resulting in a high frame error rate and  
22 the possibility of both calls dropping.

## 23 **2.1.4 MEID/EUMID Support**

24 A particular situation not directly related to non-unique ESN values has been  
25 encountered in some network configurations. In this instance, the way in which the  
26 mobile advertises that it uses one of the new identifiers results in an illegal  
27 parameter value being generated on a particular interface. The impact is that none  
28 of these mobiles can receive service. Investigations to date suggest that the issue  
29 *may* be confined to a single operator. For more information, see the [MEID Failure  
30 Bulletin].

31 In EV-DO networks that include the Hardware Identifier in the A12 interface, access  
32 authentication failures may result for MEID-equipped mobiles on a non-upgraded

---

<sup>5</sup> Not to be confused with the Private Long Code Mask. Private Long Code Masks are rarely used in current networks, and are not discussed in this document. See [Collisions WP] for a brief treatment

<sup>6</sup> For (much) more detail, see [http://www.3gpp2.org/Public\\_html/specs/C.S0002-0\\_v3.0.pdf](http://www.3gpp2.org/Public_html/specs/C.S0002-0_v3.0.pdf)

1 network. See Section 7.2.2.2 for more information. Failures may also be observed  
2 in non-upgraded EV-DO networks where the MEID cannot be sent in the airlink  
3 record by the PCF, or is not expected/supported at the PDSN or AAA.

4 Some R-UIM handsets in the market do not support EUIMID-equipped R-UIMs (see  
5 section 5.4 ).

## 2.2 Resource Utilization and Timelines

### 2.2.1 Predicted Timelines

The Telecommunications Industry Association (TIA) administers the ESN and UIMID manufacturer code space, and publishes regular reports on utilization. At the time of writing it was expected that virgin ESN codes would exhaust completely within a few weeks. In July 2008, at a TIA TR-45 meeting, industry representatives decided that about 30 million reclaimed codes would be reassigned for future ESN needs, to be assigned before December 31, 2009.

The UIMID manufacturer code space for R-UIMs (a subset of the same resource) has actually already been exhausted, with assignments continuing only because the ESN administrator has been able to continue to reclaim codes from older technologies (AMPS analog and TDMA digital) and transfer them to the UIMID administrator where they are allocated efficiently in blocks of ~260,000 codes with 14 bit manufacturer code prefixes. The TIA has not issued a predicted exhaust date for UIMIDs because reusing codes requires considerable investigation and it cannot be known until the investigation is complete whether the codes are reclaimable. Therefore, it cannot be known how many more codes will be available through this TIA effort. It is expected that the UIMID resource will last somewhat longer than ESN, but this cannot be guaranteed.

### 2.2.2 Current Resource Utilization

An overview of the ESN manufacturer code assignments is available on the TIA website<sup>7</sup>.

As of July 2008 the virgin ESN resource was essentially completely utilized with the newly approved reclaimed blocks totalling approximately 30 million codes available for assignment through December 31, 2009.

The June 2008 UIMID Administrator's report shows that pending requests for codes currently exceed the remaining available resource – requests are being only partially filled at this time and future assignments relied on further code reclamations.

Usage of pESNs and pUIMIDs removed one 8-bit manufacturer code (~16.8 million codes) from assignment but otherwise does not negatively impact the ESN/UIMID resource space – these pseudo values always use a pre-allocated manufacturer code (0x80) that does not conflict with other assignments. The use of MEID and EUIMID has a positive impact in that every device manufactured with one of these codes is one less ESN or UIMID that needs to be allocated from the rapidly diminishing pool.

---

<sup>7</sup> <http://www.tiaonline.org/standards/resources/esn/codes.cfm>

### 2.2.3 Migration Activities

MEID assignment commenced in October, 2005 (also under administration by the TIA). MEID-equipped devices have already been commercially deployed by several large operators, who have also upgraded their networks to support many/all of the recommendations in Section 6. . (In this document however, “current” or “existing” networks refer to non-upgraded networks).

EUIMID assignment commenced in 2007, with several major R-UIM manufacturers supplying millions of EUIMID-equipped cards to their operator customers.

## 2.3 Likelihood of Impacts

An important question for operators to understand is “how likely is a problem to occur?”, related to the non-uniqueness of the ESN parameter. As a general comment, it is important to note that the probability of duplication or collision cannot be given without considering other inputs, e.g. the size of the sample group, call arrival rate in the busy hour, etc. Several different calculations are available, and are shown in the subsections below.

### 2.3.1 Basic Duplication Probability

Since there are  $2^{24}$  different pESN/pUIMID code values, the probability of any two pESNs/pUIMIDs chosen at random being the same is

$$P(\text{any 2 pUIMIDs/pESNs same}) = \frac{1}{2^{24}} = \frac{1}{16,777,216}$$

### 2.3.2 Duplications in a group of cards/devices

As the number of cards or devices in a group grows, the probability of duplication rises faster than might be intuitively thought, due to a phenomenon known as the Birthday Problem<sup>8</sup>. The value is calculated as follows for a group of  $n$  cards/devices:

$$P(\geq 1 \text{ duplication in } n) = 1 - P(\text{no duplications})$$

$$= 1 - \left( \frac{2^{24} - 1}{2^{24}} \times \frac{2^{24} - 2}{2^{24}} \times \dots \times \frac{2^{24} - (n - 1)}{2^{24}} \right)$$

---

<sup>8</sup> Named for the surprising fact that with a group of only 23 people, there is a 50% chance of a common birthday. See <http://mathworld.wolfram.com/BirthdayProblem.html>



1 or, using the factorial notation, “!”:

$$2 = 1 - \left( \frac{2^{24}!}{2^{24n} \bullet (2^{24} - n)!} \right)$$

3 When  $n$  reaches approximately 4800, the probability of at least one duplication  
4 reaches 50%. With  $n = 10000$ , the probability is approximately 95%.

5 Although these numbers are not realistic for users in a single sector, they can be  
6 significant at the network-wide level – back-end systems will very likely have to deal  
7 with duplicate pESNs/pUIMIDs as the number of deployed MEIDs and EUIMIDs  
8 grows.

9 The probability of a specific number of duplications is given by:

$$10 \quad P(\text{exactly } x \text{ duplications in group of } n) = \frac{1}{N^n} S(n, n-x) \frac{N!}{(N-n+x)!},$$

11 where  $N = 2^{24}$ , and  $S(n, k)$  is the Stirling number of the second kind<sup>9</sup>. This formula  
12 can in theory be used to derive the expected number of duplications within a batch  
13 of R-UIMs or MEID phones, although the numbers involved in the calculations  
14 quickly become unwieldy.

### 15 **2.3.3 PLCM Collision Probability**

16 Several documents aim to provide a sense of how often PLCM collisions might be  
17 expected to occur in a network (assuming the upgrade steps described in Section 6.  
18 are not implemented).

19 The primary reference is the [Collisions WP] document, which derives an expected  
20 number of collisions in a day for the network. This is the sum of the expected  
21 collisions per hour, which is given by:

$$22 \quad E(\text{hourly collisions in the network}) \approx \frac{2f^2(I+1)}{N\mu} U\lambda^2,$$

23 where:

- 24 •  $U$ : the total number of carrier sectors in the operator’s universe.
- 25 •  $\lambda$ : expected number of calls made per hour  $h$  in an average sector.
- 26 •  $1/\mu$ : average call holding time.
- 27 •  $f$ : fraction of the calls that use pESN based handsets or pUIMID R-UIMs

---

<sup>9</sup> See <http://mathworld.wolfram.com/StirlingNumberoftheSecondKind.html>

- 1       •  $l$ : number of neighboring sectors that interfere with the current sector.
- 2       •  $N$ : the possible values for the public long code mask (PLCM):  $2^{24}$ .

3       One scenario in this document estimated daily collisions in a large system with  
 4       60,000 sectors, each of which had 6 neighboring sectors. It estimated that they  
 5       would rise from zero with no pESNs or pUIMIDs to almost 600 per day (throughout  
 6       the entire system) if all mobiles transmitted a pESN or pUIMID. Obviously this  
 7       problem is eliminated if precautions against pESN/pUIMID collisions are taken.

8       Alternatively, a Lucent standards contribution from 2003<sup>10</sup> calculated the expected  
 9       number of call replacements (i.e. an existing call finishing to be replaced by a new  
 10       call on the sector) until a collision occurs, as:

$$11 \qquad \qquad \qquad E(\text{replacements until collision}) = \frac{N}{m-1},$$

12       where  $N$  is  $2^{24}$  as before, and  $m$  is the number of potentially colliding users, i.e. the  
 13       number of active calls on the sector and interfering sectors.

<b>m (number of potentially colliding users)</b>	<b>E (expected number of calls before collision occurs)</b>
10	1,864,135
20	883,011
30	578,524
40	430,185
50	342,392
60	284,359
70	243,148
80	212,369
90	188,508
100	169,466

14

<sup>10</sup> [ftp://ftp.3gpp2.org/TSGC/Working/2003/2003-03-Vancouver/TSG-C-2003-03-Vancouver/WG2/C20-20030317-018A\\_\(LU\)SHA\\_Response.pdf](ftp://ftp.3gpp2.org/TSGC/Working/2003/2003-03-Vancouver/TSG-C-2003-03-Vancouver/WG2/C20-20030317-018A_(LU)SHA_Response.pdf)

# 3. Hardware Identifiers Involved

This section presents the formats and characteristics of the existing and new hardware identifiers for CDMA2000® devices and R-UIMs.

## 3.1 Identifier Relationships

Figure 3-1 below shows a summary of the relationships between the various identifiers possible for the device and the R-UIM. The following subsections describe each identifier in more detail.

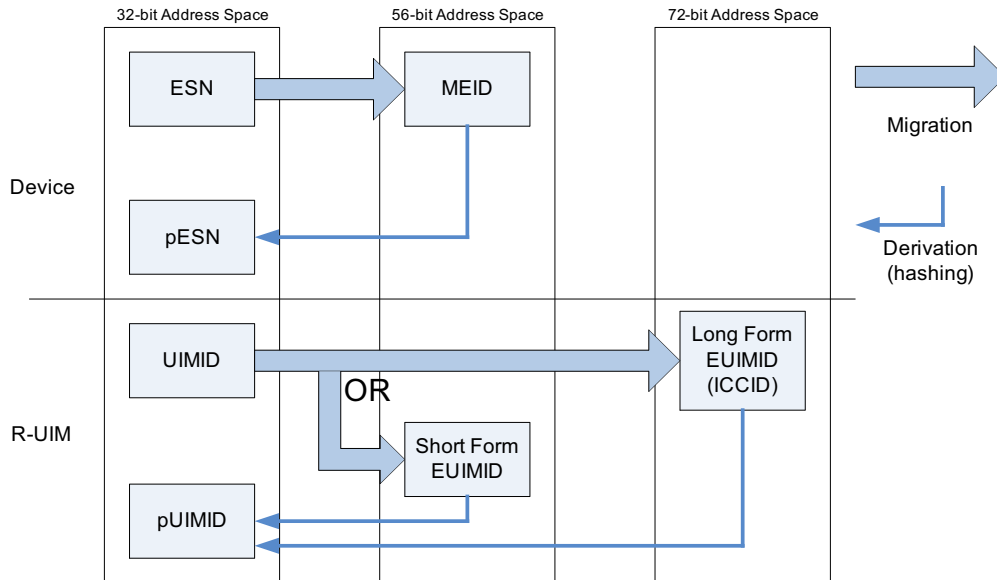


Figure 3-1: Identifier Relationships

## 3.2 Existing Identifiers

### 3.2.1 Electronic Serial Number (ESN)

The Electronic Serial Number (ESN) is a 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment. ESNs are typically represented as an eight-character hexadecimal string, or as an 11-digit decimal number<sup>11</sup>. ESNs are used by AMPS, TDMA and CDMA air interface protocols. In CDMA and related standards, the ESN is used for a variety of functions (see Section 2.1.1 for more detail).

A 32-bit address space gives a maximum pool of  $2^{32} \approx 4.3$  billion unique ESNs. Generous allocation, inefficient usage and the huge number of cellular devices manufactured since the 1980s has led to the current shortage.

ESNs were initially allocated by assigning an 8-bit manufacturer's code to a cellular phone manufacturer. The manufacturer would allocate the remaining 24-bits as unique serial numbers to approximately 16.7 million wireless devices<sup>12</sup>. This could be repeated for each of the 256 manufacturer codes. More recently, in an attempt to allocate the rapidly diminishing resource more efficiently, 14-bit manufacturer codes have been assigned (~260,000 values per code). These two allocation schemes represent administrative approaches to assigning the 32-bit number range, and do not change the way the ESN is transmitted over the air or carried in other network signaling. Although the CIBER manual describes three different ways to construct a decimal representation of an ESN, in practice only one method is in common use, which assumes an 8-bit manufacturer code and converts this and the remaining 24-bits separately to decimal before concatenation.

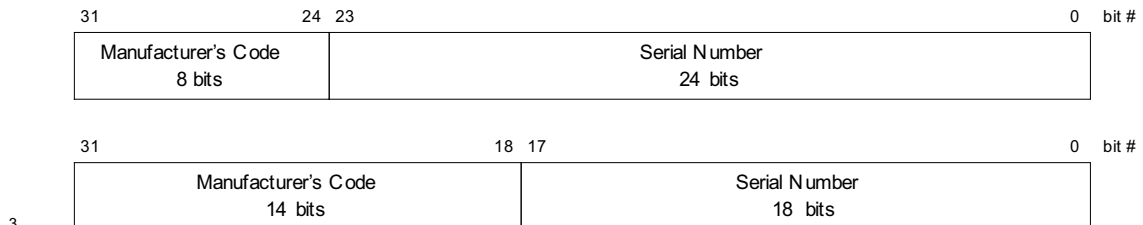
ESN manufacturer codes are currently administered by the Telecommunications Industry Association (TIA). The serial number portion of the ESN is administered by the manufacturer.

---

<sup>11</sup> The decimal representation is formed by concatenation of the decimal representation of the first 2, and last 6 hex characters, rather than direct hex-to-decimal conversion of the entire value. Thus hex ESN 9D124886 is written as 15701198214, not 02635221126. This corresponds to the Manufacturer's Code and Serial Number for 8 bit Manufacturer Codes, but not for 14 bit codes.

<sup>12</sup> Technically the ESN was divided into an 8 bit manufacturer's code, 6 reserved bits, followed by an 18 bit serial number (~262 thousand codes). However, most manufacturers used the reserved bits to bring the serial number to 24 bits (~16.8 million codes).

1 Figure 3-2 below shows the two methods used for segmenting the ESN allocation  
2 space.



3  
4  
5 **Figure 3-2 - ESN Manufacturer's code allocation**

6 **i** For more information, see the TIA website<sup>13</sup>, and the definition in [C.S0005]. The  
7 TIA also produces a monthly ESN Administrator's Report, available from Gary  
8 Pellegrino, the TIA TR-45 EUMAG chair ([Gary@CommFlowResources.com](mailto:Gary@CommFlowResources.com)), or  
9 the ESN administrator, John Derr ([JDerr@tiaonline.org](mailto:JDerr@tiaonline.org)).

### 10 3.2.2 User Identity Module Identifier (UIMID)

11 The UIM Identifier (UIMID) is a unique 32-bit number assigned to an R-UIM. It is  
12 defined in [C.S0023] (including earlier versions than the one referenced in this  
13 document). Earlier versions allowed the UIMID to be up to 56 bits in length to  
14 anticipate future evolution. This size change has been superseded by the migration  
15 to EUIMID described in the latest standard revision and in this document, and the  
16 UIMID is now understood to be a unique 32-bit number only. It may also be written  
17 as UIM\_ID.

18 The UIMID shares a 32-bit addressing space with the ESN. UIMID allocations  
19 include both "virgin" codes (codes that have never been assigned as ESNs –  
20 identifiable by "(not currently available for other CDMA technology use)" in the on-  
21 line ESN assignment table<sup>14</sup>), and "reclaimed" codes, that were previously allocated  
22 as ESNs, but have been identified as unused, or used for older (e.g. AMPS-only)  
23 devices (and thus unlikely to clash with CDMA-only devices using these R-UIMs).

24 The TIA currently administers the UIMID space.

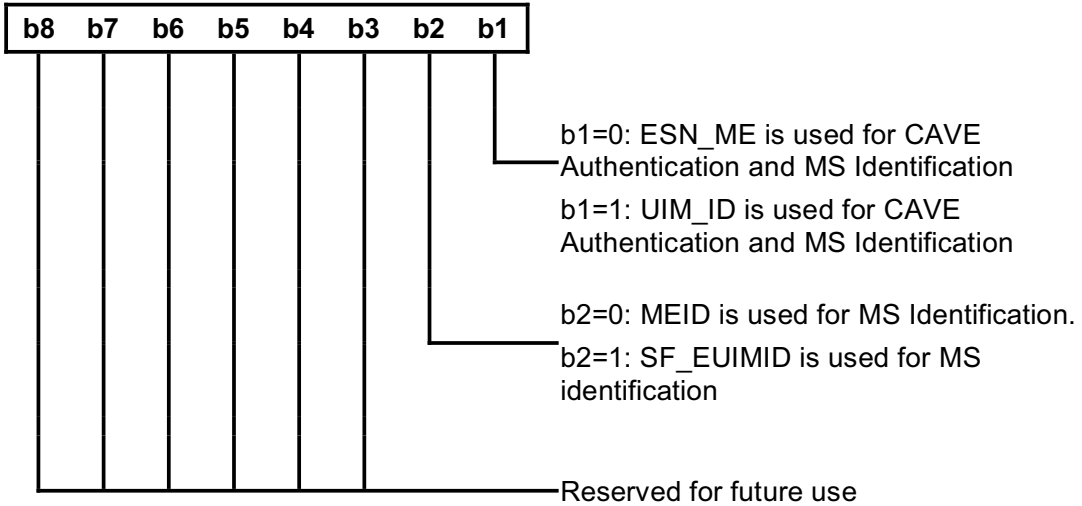
25 In 1x voice and data modes the UIMID can be used instead of the ESN from the  
26 device wherever the ESN is signaled over the air or used in calculations (e.g. CAVE  
27 authentication). This behavior is controlled by a variable on the R-UIM, the Usage  
28 Indicator (EF<sub>USGIND</sub>). Figure 3-3 shows the function of the usage indicator (only bit 1  
29 is relevant here – the function of bit 2 is discussed in Section 3.3.2 ). Note that the  
30 value of this indicator is not explicitly available to the network. This is not true in EV-

<sup>13</sup> <http://www.tiaonline.org/standards/resources/esn/>

<sup>14</sup> <http://www.tiaonline.org/standards/resources/esn/codes.cfm>

1 DO where the HardwareID is sourced from the ME identifier (ESN or MEID)  
 2 regardless of the value of EF<sub>USGIND</sub>.

3



4

**Figure 3-3 - Usage Indicator Function**

5 In practice, all operators using R-UIM are believed to set b1 to 1, i.e. the UIMID  
 6 replaces the ESN wherever it is used in a 1X mode. This is for compatibility with  
 7 ANSI-41 mobility management protocols that rely on each IMSI/MIN being  
 8 associated with a single ESN. Moving a UIM from one phone to another will  
 9 associate the IMSI/MIN with a different hardware ESN, but the UIMID will remain the  
 10 same.

11 **i** For more information, see [C.S0023]. The TIA produces a monthly UIM  
 12 Administrator's Report, available via email and by distribution to various  
 13 standards organizations.

### 3.2.3 Integrated Circuit Card Identifier (ICCID)

The Integrated Circuit Card Identifier (ICCID) is an 18-digit BCD (72-bit) identifier assigned to the physical R-UIM card. Since the storage on the R-UIM (EF<sub>ICCID</sub>) is 80 bits (room for 20 digits) 3GPP2 C.S0023-C v2.0 recommends that the check digit is also included along with a single filler digit (0xf). Since there is no demarcation within this field to distinguish the portions, and some non-standard identifiers are known to exist, the entire 80 bit field will be returned in response to an OTASP query for the ICCID or EXT\_UIM\_ID (if LF\_EUIMID is used)<sup>15</sup>, and will be used as an input to the hash function to compute the pUIMID if LF\_EUIMID is used (see section 3.4.2 ).

The ICCID is currently present on all R-UIM cards (as well as GSM SIM cards). It is defined in [E.118] (which is referenced indirectly from [C.S0023]). The ICCID is typically printed on the card, and is also stored electronically.

Figure 3-4 below shows the structure of the ICCID.

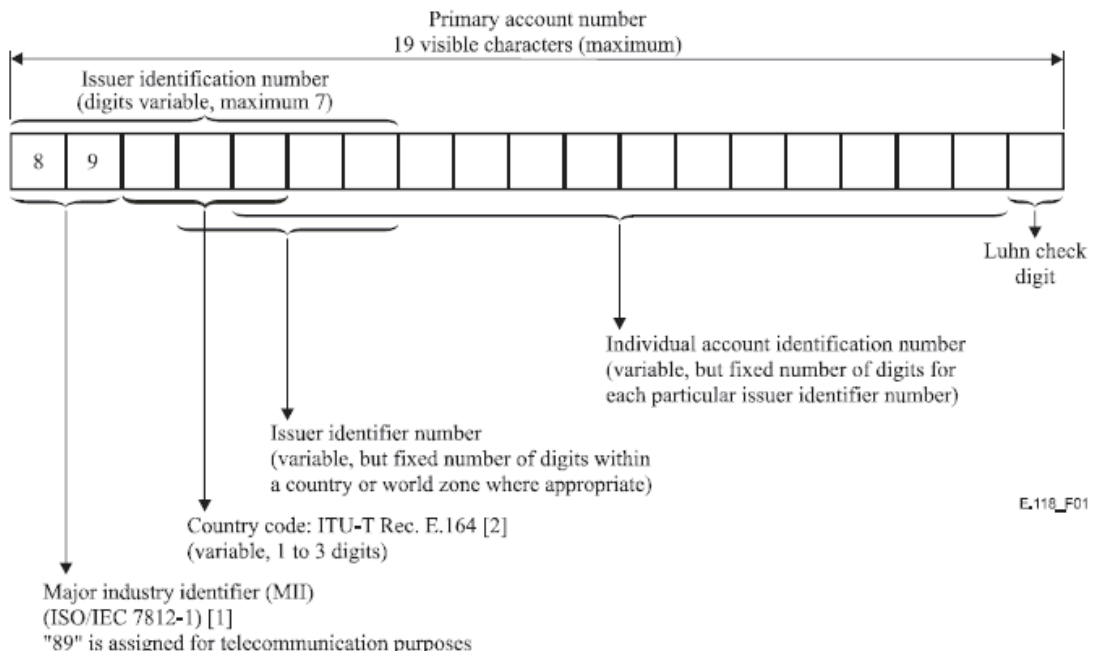


Figure 3-4 - Structure of ICCID

<sup>15</sup> The ability to query for these identifiers is added in C.S0066 v2, and in the expected C.S0016-C v2.

1 **3.3 New Identifiers**

2 **3.3.1 Mobile Equipment Identifier (MEID)**

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

8 The structure of the MEID is shown in Figure 3-5 below (using hexadecimal format).

MEID														
Manufacturer Code							Serial Number							
R	R	X	X	X	X	X	X	Z	Z	Z	Z	Z	Z	C
14	13	12	11	10	9	8	7	6	5	4	3	2	1	

9  
10 **Figure 3-5 - MEID Structure (Hexadecimal)**

11 The subfields are defined as follows:


12 RR: Reporting Body Identifier. Restricted to the range A0 – FF. This  
 13 ensures separation from the GSM International Mobile Equipment  
 14 Identity (IMEI), which also uses a 56-bit space, but is restricted to  
 15 BCD values only (i.e. 14 decimal digit representation). The RR values  
 16 99 (and below, if necessary) are reserved for use by dual-mode  
 17 devices – in this case the IMEI and MEID will be the same value (the  
 18 remaining digits of the MEID are also restricted to BCD values).  
 19 Because these values are both legitimate MEID codes and IMEI  
 20 codes, assignment requires coordination between the GHA and GDA  
 21 and may take longer.<sup>16</sup>

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

---

<sup>16</sup> These restrictions are for the purposes of administrative separation from IMEI only. Nothing in the signaling standards explicitly prohibits any 56-bit value from being used as an MEID.



- 1 treating the leftmost digit of the Serial Number as an additional  
2 digit.<sup>17</sup>
- 3 **ZZZZZZ:** Serial Number, assigned by the manufacturer (possibly within  
4 segmented range as above, in which the leftmost digit is treated as  
5 part of the Manufacturer code).
- 6 **C:** Check Digit for use when an MEID is printed (e.g. on packaging or on  
7 the exterior of an MS). The check digit is not part of the MEID and is  
8 not transmitted when the MEID is transmitted. It is calculated using  
9 the Luhn algorithm modified to use base 16 arithmetic.
- 10 With RR in the range A0 – FF, the available pool of MEIDs is  $96 \times 2^{48} \approx 27$  thousand  
11 trillion, or approximately 6.3 million times the size of the ESN address space.
- 12 MEID administration is performed by the Global Hexadecimal Administrator (GHA).  
13 TIA currently serves as the GHA. Assignment of MEIDs with decimal RR codes  
14 requires coordination with the GDA.
- 15  For more information, see the TIA website<sup>18</sup>. See [X.S0008] for information on  
16 the decimal representation of MEID, as well as checksum calculation details.  
17 The TIA produces a monthly MEID Administrator's Report, available from the  
18 TIA EUMAG chair ([Gary@CommFlowResources.com](mailto:Gary@CommFlowResources.com)) and also on the 3GPP2  
19 TSG-S FTP site.

---

<sup>17</sup> Current assignment practices treat the identifier as if the Manufacturer Code was 9 digits long and the Serial Number only 5 digits long. This makes allocation more efficient, with only one million numbers being assigned at a time instead of close to 17 million.

<sup>18</sup> <http://www.tiaonline.org/standards/resources/meid/>

### 1 **3.3.2 Expanded UIMID (EUIMID)**

2 The Expanded UIMID (EUIMID) is a new identifier designed to address the exhaust  
3 of the UIMID resource. It is defined in [C.S0023], where two different forms of  
4 EUIMID are described:

- 5 • Short Form EUIMID (SF\_EUIMID): The SF\_EUIMID shares the same  
6 address space as the MEID. R-UIM card manufacturers are allocated MEID  
7 manufacturer codes in the same manner, and from the same range, as  
8 handset manufacturers.
- 9 • Long Form EUIMID (LF\_EUIMID): This is equal to the value of the ICCID of  
10 the card. In practice this is the 20 digit/80 bit contents of EF<sub>ICCID</sub> which will  
11 probably include a check digit and filler digit (0xf) as well as the ICCID which  
12 is probably 18 digits/72 bits in size.

13 When the SF\_EUIMID is used, bit 2 of the Usage Indicator describes whether the  
14 SF\_EUIMID of the card replaces the MEID of the device wherever it is used (see  
15 Figure 3-3).<sup>19</sup>

16 The relative merits of the two approaches are discussed in Section 5. . Note that the  
17 EUIMID may be variously referred to as the Extended UIMID, Expanded R-UIM  
18 Identifier, EXT\_UIM\_ID, EUIM-ID or E-UIMID in some sources.

---

<sup>19</sup> Strictly speaking, the Usage Indicator is only described in the standard as denoting MEID override in IS-2000, not IS-683. Nevertheless, handset manufacturers have interpreted this as a total override of MEID, consistent with the behavior of UIMID with respect to ESN, and facilitates OTASP provisioning of SF\_EUIMID-equipped R-UIMs

## 3.4 Derived Identifiers


With the use of new, longer identifiers, devices and cards no longer have a true (i.e. unique) ESN or UIMID. However, “ESN” is a required field in many messages. Therefore there is a need to derive a 32-bit identifier to populate this field.

### 3.4.1 Secure Hash Algorithm 1 (SHA-1)

The Secure Hash Algorithm 1 (SHA-1) is used to produce a condensed, 160-bit digest of an input number or text string. Although not important for this application, this process is intended to be one-way only, i.e. given a particular digest (or “hash”), it is not easy to work out what the input message might have been.

More importantly, like all well-designed hash functions, SHA-1 spreads its results uniformly across its result space, regardless of the relationship between input messages (i.e. inputs differing only slightly, perhaps by one bit, do not produce outputs that are more similar than two very different inputs).

SHA-1 is the algorithm used in CDMA standards to derive a digest from the (56- or 80-bit<sup>20</sup>) input. In this case, the complete SHA-1 output (160 bits) is actually longer than the input message – as a result only the 24 least-significant bits of the output are used (combined with an 8-bit “manufacturer code” to give the required 32-bit identifier).

 For more information, see RFC3174<sup>21</sup>. Implementations of the SHA-1 hashing algorithm are freely available on the internet<sup>22</sup>

### 3.4.2 Pseudo-ESN (pESN)

The Pseudo-ESN (pESN) is a 32-bit identifier derived from the MEID, used in place of the ESN. It 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 Mobile Station as the value of the ESN<sub>p</sub> Permanent Mobile Station Indicator (the variable that otherwise stores the (true) ESN).

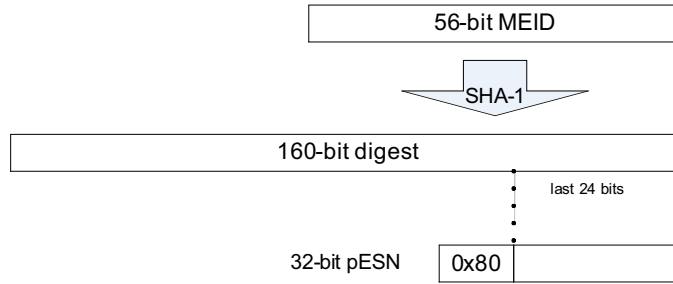
Figure 3-6 below shows the derivation of the pESN. Since there is a defined (albeit one-way) relationship between MEID and pESN, it is possible to derive the pESN even if only the MEID is received by any particular entity.

---

<sup>20</sup> 3GPP2 C.S0023-C v2.0 clarifies that the input to the SHA-1 algorithm for LF\_EUIMID is the entire 80 bits of the EF<sub>ICCID</sub>, usually including the check digit and a filler digit (0xf).

<sup>21</sup> <ftp://ftp.rfc-editor.org/in-notes/rfc3174.txt>

<sup>22</sup> E.g. <http://www.slavasoft.com/>



1

2

**Figure 3-6 - Derivation of the pESN**

3 Since there are more possible MEIDs than pESNs, more than one MEID will map to  
 4 the same pESN<sup>23</sup>. By way of example, Table 3-1 below shows several pairs of  
 5 MEIDs with a common pESN. It is this lack of uniqueness in the pESN that  
 6 represents the main impact to operator networks and business processes. The  
 7 likelihood of this kind of duplication occurring is discussed in Section 2.3 .

MEID1	MEID2	pESN
A00000000001BC2	A00000000003472	80003C21
A000000000000A6	A00000000003422	80066CDE
A00000000002277	A00000000003584	80270ABB

8

**Table 3-1 - Sample duplicate pESNs (Hexadecimal format)**

9 The pESN space is not segmented or administered in any way. Due to the behavior  
 10 of the hash function, pESNs derived from a specific MEID range may occupy any  
 11 part of the pESN address space. The specific manufacturer code (0x80) ensures  
 12 that a pESN will not clash with any true (unique) ESN or UIMID.

13 **i** For more information, see [C.S0072]. A pESN-generator is available on the  
 14 internet<sup>24</sup>.

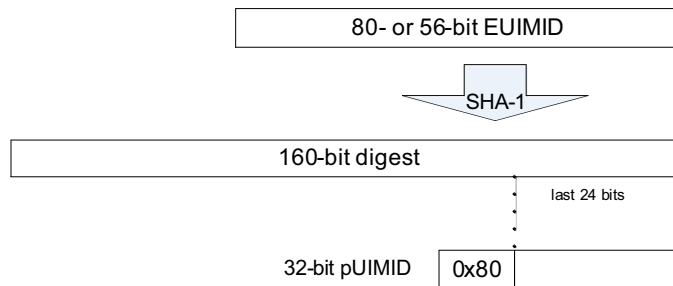
<sup>23</sup> Simple division, and an assumption of uniformity in the hashing function yields each pESN value being shared by ~1.6 billion MEIDs.

<sup>24</sup> <http://www.neolineas.com/pesn.yaws>

1 **3.4.3 Pseudo-UIMID (pUIMID)**

2 The Pseudo-UIMID (pUIMID) is a 32-bit identifier derived from the EUIMID (either  
3 Short or Long Form), and used in place of the UIMID (which itself typically replaces  
4 the ESN).

5 The pUIMID is derived from the EUIMID in the same manner as the pESN is derived  
6 from the MEID (and therefore shares the same space as the pESN), as shown in  
7 Figure 3-7 below:



8  
9

**Figure 3-7 - Derivation of the pUIMID**

1 Since there are more possible EUIMIDs than pUIMIDs, more than one EUIMID will  
 2 map to the same pESN. By way of example, Table 3-2 below shows three pairs of  
 3 (in this case, Long Form) EUIMIDs with a common pUIMID. (Note that the hash  
 4 function is computed over the LF\_EUIMID as a BCD number, not simple decimal,  
 5 and includes the check digit and Hex 'F' filler).

LF_EUIMID1	LF_EUIMID2	pUIMID
8991001000000021981f	89910010000000081654f	80E7F275
8991001000000037789f	89910010000000116740f	809F9406
8991001000000087735f	89910010000000088642f	8059659C

6 **Table 3-2 - Sample duplicate pUIMIDs**

7 The pUIMID space is not segmented or administered in any way. Due to the  
 8 behavior of the hash function, pUIMIDs derived from a specific EUMID range may  
 9 occupy any part of the pUIMID address space. pUIMIDs and pESNs share the same  
 10 address space: a pESN may clash with another pESN or a pUIMID. Table 3-3 below  
 11 shows three examples of pESN – pUIMID clashes.

MEID	LF_EUIMID	pESN/pUIMID
A0000000000D00	8991001000000000518	80B270AD
A0000000002559	8991001000000008187	802E9C53
A0000000002A85	8991001000000003929	808840E4

12 **Table 3-3 - Sample pESN to pUIMID duplications**

13

## 4. Standards Involved

---

Since the ESN is a fundamental identifier in a CDMA system, many standards are impacted by the migration to MEID (and the corresponding UIMID to EUIMID migration). The following subsections provide a brief overview of the function of the various standards documents. The categorization into subsections is purely an editorial convenience, and does not reflect any official designation.

### 4.1 MEID

#### 4.1.1 Requirements

[S.R0048] is a brief document from 3GPP2 TSG-S that provides the Stage 1 requirements for MEID.

#### 4.1.2 Administration

3GPP2 Steering Committee document [SC.R4002] describes the role of the MEID Global Hexadecimal Administrator (GHA) in assigning manufacturer codes for MEIDs, and ensuring that assigned resources are utilized efficiently. The allocation of responsibility between the GHA and the Global Decimal Administrator (GDA) for IMEIs is further described in SC.R4001.

#### 4.1.3 Billing

The Cellular Inter-carrier Billing Exchange for Roamer (CIBER) record specification includes an ESN field in many of its defined record types. The meaning of this field has been expanded to include MEID as an alternate identifier, and a new value signifying MEID has been defined for the associated indicator field. It is not possible to include both a pESN or pUIMID and an MEID in a single CIBER record.<sup>25</sup>

#### 4.1.4 Air Interface

##### 4.1.4.1 IS-2000 Release D and E

MEID was originally intended to be introduced in conjunction with IS-2000 Release D. In this standard, MEID can *replace* the ESN as the device identifier used over the air in the Link Access Control (LAC) layer.

---

<sup>25</sup> CIBER is a proprietary protocol owned by MACH.

1 Release D also allows the use (first added in Release C) of Public Long Code Mask  
2 (PLCM) types not based on the ESN.

3 At present, there are no plans to commercialize IS-2000 releases beyond Release  
4 A. Because of this, the necessary changes for MEID (not including LAC address  
5 modifications) have been retrofitted into earlier releases of IS-2000 (see Section  
6 4.1.4.2 ). Capabilities provided only by Release D are not discussed further in this  
7 document, and should not be anticipated by operators.

8 A new version under development, known as Release E, will take some features  
9 from Release D, but current plans do not include MEID in LAC addressing.

#### 10 **4.1.4.2 Updates to earlier releases of IS-2000**

11 [C.S0072] (TIA-1082) retrofits MEID into pre-Release D versions of IS-2000. It  
12 provides the following capabilities:

- 13 • A Mobile Station (MS) can be equipped with an MEID, and can indicate this  
14 by setting bit 4 of the Station Class Mark (SCM) to 1. Previously this bit had  
15 the meaning of "IS-54 Power Class" and was always 0 for CDMA devices.  
16 The SCM is already included by the MS in various messages.  
17 *Note:* The Base Station (BS) does not advertise its support for MEID usage.
- 18 • New messages for the BS to assign a PLCM that is not derived from the  
19 ESN (or pESN), and to manage handoffs with this new PLCM
- 20 • A new record type allowing the BS to retrieve the MEID from the MS via the  
21 Status Request Message.

22 **Note that the MEID is not used to form the MS LAC address used on the**  
23 **access or paging channels. The address continues to use the ESN (or pESN,**  
24 **in the case of a MEID-equipped MS).**

25 C.S0072 uses the new PLCM types defined in IS-2000 Release D:

- 26 • PLCM specified by the Base Station (BS-assigned)
- 27 • PLCM derived from IMSI (2-types)
- 28 • PLCM derived from MEID

29 Of these types, IMSI-based PLCMs have limitations on their use for roamers from  
30 other networks, and MEID-based PLCMs require extra messaging (to retrieve the  
31 MEID from the MS before the PLCM can be assigned) and are not guaranteed to be  
32 unique (as the MEID length is greater than that of the PLCM). Therefore the  
33 recommended approach, and the one assumed throughout this document, is  
34 BS-assigned PLCM.

35 All MEID-equipped devices are expected to support C.S0072 (i.e. there should be  
36 no devices launched with MEIDs that do not support the new messaging in  
37 C.S0072). Some R-UIM capable devices are known to exist which have MEIDs, but



1 set SCM bit 4 to 0. This behavior is not recommended, and can lead to PLCM  
 2 collisions when EUIMID-equipped R-UIMs are used that cannot be resolved even  
 3 when all base stations are upgraded to support C.S0072.

4 Base stations should support at least the BS-assigned PLCM type.

#### 5 **4.1.4.3 1xEV-DO Revision A**

6 Revision A of [C.S0024] adds support for an Access Terminal (AT) to use MEID as  
 7 its Hardware Identifier (HardwareID). HardwareID is optionally used in EVDO – it is  
 8 sent by the AT only if the Access Network (AN) explicitly requests it via the  
 9 HardwareIDRequest message. Most commercial networks are believed to request  
 10 the HardwareID from the AT (e.g. as a way to identify and tear down hung  
 11 sessions).

12 MEID support is defined in such a way (modifying the Default Address Management  
 13 Protocol, and using a HardwareIDType value for MEID from a range previously  
 14 allowed in Release 0) that a MEID-equipped AT can also return MEID as its  
 15 HardwareID to an EVDO Release 0 network. The possible values are shown in  
 16 Table 4-1:

HardwareIDType field value	Meaning
0x010000	ESN
0x00ffff	MEID
0x00NNNN, where NNNN is in the range 0x0000 to 0xffff, inclusive.	See 3GPP2 C.R1001
0xfffff	Null
All other values	Invalid

17 **Table 4-1 - EVDO HardwareIDType values**

18 Note that only the ESN and MEID are defined for inclusion in the HardwareID field.  
 19 This implies that even when an R-UIM is inserted in an EV-DO device that the ESN  
 20 or MEID should continue to be transmitted, not the UIMID or EUIMID. There is no  
 21 concept of a pESN in EV-DO – an MEID device will return the MEID as its  
 22 HardwareID.

#### 23 **4.1.5 ANSI-41 MAP Updates**

24 ANSI-41 MAP provides a number of mobility management functions. Most of its  
 25 signaling messages include ESN as a mandatory parameter. The protocol does not  
 26 itself require uniqueness, but applications based on the protocol may make this  
 27 assumption. ANSI-41 does assume a fixed relationship between a MIN/IMSI and an  
 28 ESN or UIMID. It is this assumption that forces R-UIM equipped mobiles to transmit  
 29 UIMID or pUIMID rather than ESN or pESN.

1 [X.S0008] adds support for MEID into ANSI-41. It adds MEID as an optional  
2 parameter in many messages that contain the ESN. Note that the  
3 mandatory/optional status of the ESN parameter remains unchanged. The UIMID,  
4 pESN or pUIMID can be used instead of ESN, transparently to ANSI-41.

5 X.S0008 also adds messaging to enable Equipment Identity Register (EIR)  
6 functionality, which provides functions such as combating device theft by checking  
7 the MEID against a list of known stolen devices or comparing with a list of  
8 problematic devices. A generic request message that can be used to order retrieval  
9 of the MEID from the MS is also added. This capability is effectively disabled if the  
10 Short Form EUIMID replaces the hardware MEID in air interface signaling.

11 X.S0008 network modifications provide additional capabilities but are not considered  
12 essential elements in MEID or EUIMID support.

### 13 **4.1.6 Over-the-Air Activation**

14 Over-the-Air activation is affected by the migration away from ESN, because ESN is  
15 often used as the only unique identifier for an unprovisioned mobile. When a non-  
16 unique ESN is provided there needs to be some mechanism to obtain a unique  
17 identifier to ensure the correct device is being provisioned.

18 [C.S0066] is a modification to C.S0016 / IS-683 that adds a mechanism for the  
19 Over-the-Air Function (OTAF) platform to retrieve the MEID from a device, via the  
20 Extended Protocol Capability Response Message. As with other OTAF messaging,  
21 the information is carried back to the OTAF inside the SMS\_BearerData parameter  
22 of an ANSI-41 SMSDeliveryPointToPoint (SMDPP) message. This means that it is  
23 possible to transmit MEID within the OTA protocol layer even when lower layers  
24 (e.g. ANSI-41) do not support MEID.

25 [C.S0066] provides equivalent MEID handling capabilities to C.S0016-C/TIA-683-D  
26 (with the exception of MEID LAC addressing), but it allows these capabilities to be  
27 used with earlier revisions of C.S0016.

28 A negative interaction was discovered between MEID and band-class information in  
29 both [C.S0016] and [C.S0066] that meant that information on band classes other  
30 than 0 (Cellular 800 MHz), 1 (US PCS 1900), 3 (Japan 800 MHz) and 6 (IMT2000,  
31 2.1 GHz) is only available during provisioning for mobiles that have been  
32 provisioned with an MEID. 3GPP2 has addressed this issue in C.S0016-C v2.0 (to  
33 be published soon) and C.S0066-0 v2.0 (July, 2008).

34 The same new versions of C.S0016 and C.S0066 will also allow the MEID, ICCID  
35 and EUIMID to be transmitted from a mobile equipped with R-UIM to the OTAF.  
36 Previous versions only allowed the MEID to be transmitted (or the SF\_EUIMID if  
37 UsgInd bit 2 was set to '1').

38 [X.S0033][X.S0033] is a modification to 3GPP2 N.S0011 / TIA IS-725 to support  
39 MEID. It adds MEID as an optional parameter to various OTASP- and OTAPA-  
40 related messages. Some of the content overlaps with X.S0008.

## 1 **4.1.7 Interoperability and Testing**

### 2 **4.1.7.1 CDMA2000<sup>®</sup> Access Network Interoperability**

3 The interoperability Specification (IOS) suite of standards ([A.S001x]) has been  
4 updated (as of Version 5.0) to include support for MEID. MEID is added as an  
5 optional parameter in many messages. Support is also added for the new PLCM  
6 types. IOS Version 5.0.1 is compatible with C.S0072.

7 The MEID capabilities of this standard revision are primarily designed to support the  
8 MEID handling as defined in IS-2000 Release D (i.e. MEID in the LAC address).  
9 The transport options for MEID allowed by C.S0072 (Status Request Message) and  
10 C.S0066 (Extended Protocol Capability Response Message) may be encapsulated  
11 unchanged even by earlier revisions of IOS. Transport of the new PLCM types may  
12 be necessary for inter-BSC soft handoff.

13 See [MEID Failure Bulletin] for a potential service-affecting issue related to the  
14 interpretation of SCM bit 4 on this interface.

15 These standards also define transport of the MEID over the A8/9 and A10/11  
16 interfaces for packet data sessions.

### 17 **4.1.7.2 HRPD Access Network Interoperability**

18 [A.S0008] provides (in Revision A and later) support for MEID in the various “A”  
19 interfaces for 1xEV-DO. Among other changes, Hardware-ID is added as an  
20 optional parameter for A12 authentication, and MEID is listed as a possible  
21 HardwareIDType.

### 22 **4.1.7.3 CDMA2000<sup>®</sup> Signaling Testing for MEID**

23 [C.S0073] provides a signaling test specification for MEID equipped CDMA2000<sup>®</sup>  
24 mobile stations. Revision A of this specification is being developed and will include  
25 test sequences for MEID mobile stations with an R-UIM inserted, when EUIMID is  
26 the card identifier.

### 27 **4.1.7.4 CDMA2000<sup>®</sup> Wireless IP Network Standard**

28 [X.S0011] defines requirements for support of wireless packet data networking  
29 capability on a third generation wireless system based on CDMA2000<sup>®</sup>. Revision D  
30 includes modifications to allow MEID to be carried on the various network interfaces,  
31 and particularly for its inclusion in the “airlink record” and in Usage Data Records  
32 (UDRs)

33

## 1 **4.2 Expanded UIMID (EUIMID)**

### 2 **4.2.1 Requirements**

3 3GPP2 TSG-S report [S.R0111] provides the Stage 1 requirements for the EUIMID.  
4 Note that only C.S0016-C v2.0 and C.S0066-0 v2.0 contain the capabilities to fully  
5 satisfy all its requirements.

### 6 **4.2.2 Administration**

7 3GPP2 Steering Committee report [SC.R4003] describes the administration  
8 procedures of the EUIMID, both short-and long-form. The document essentially  
9 devolves LF\_EUIMID administration to the existing ICCID process, and SF\_EUIMID  
10 administration to the MEID administration process.

### 11 **4.2.3 CDMA R-UIM**

12 [C.S0023] defines the capabilities of the CDMA Removable User Identity Module  
13 (R-UIM). Revision C adds, among other things, a description of the Long Form (LF)  
14 and Short Form (SF) EUIMID (see Section 3.3.2 ). This specification is currently  
15 being updated to clarify the storage order of the SF\_EUIMID and describe how the  
16 pUIMID is calculated from the LF\_EUIMID (to be published as C.S0023-C v2.0).

### 17 **4.2.4 CDMA SIM Application**

18 [C.S0065] describes the CDMA Subscriber Identity Module (CSIM), an application  
19 residing on the Universal Integrated Circuit Card (UICC). UICC provides a generic  
20 platform for applications such as CSIM, and the UMTS Subscriber Identity Module  
21 (USIM) used in GSM-evolved 3G systems. CSIM represents an evolution from the  
22 existing R-UIM standard, however C.S0065 provides equivalent capabilities to  
23 C.S0023 with respect to EUIMID.

24 In this document, the term R-UIM is used generically to refer to Identity Module card  
25 for CDMA networks, and can include the CSIM as well.

26 [C.S0065] was updated in July 2008 (C.S0065-0 v2.0) to clarify the storage order of  
27 the SF\_EUIMID and describe how the pUIMID is calculated from the LF\_EUIMID.

## 5. EUIMID Migration Options

An important decision for an R-UIM operator is the nature of EUIMID to which the operator will migrate. As discussed in Section 3.3.2, two forms of EUIMID are defined in the standards. This section discusses the advantages and disadvantages of the two approaches. In many cases, examples and call-flows for the specific cases are given in Section 7.

### 5.1 Long-Form EUIMID

The LF\_EUIMID is an identifier that can be up to 72 bits long, equal to the existing ICCID of the card<sup>26</sup>. Advantages and disadvantages are as follows:

Advantages:

- **Simplicity.** The ICCID is an existing identifier for the card. There are no new storage requirements in terms of files on the R-UIM to support LF\_EUIMID. Administration procedures are already established for ICCID.
- **Backward compatibility.** With no new data structures to support, current cards (that may not support C.S0023-C) can simply have the pUIMID programmed into the EF<sub>RUIMID</sub> file on the card, and operate as LF\_EUIMID cards<sup>27</sup>. Similarly, there are no new requirements on devices to support LF\_EUIMID. (Although PLCM collisions are possible if the device does not support C.S0072.)
- **EIR Support.** Since the device MEID (if present) remains available to the network, use of LF\_EUIMID allows the implementation of an Equipment Identity Register to track/block lost/stolen devices.
- **Retrievable During Provisioning.** If C.S0016-C v2.0 or C.S0066-0 v2.0 are implemented in mobiles and in the OTAF the LF\_EUIMID will be available during provisioning with OTASP.

<sup>26</sup> In practice the full 80 bit value contained in the R-UIM field EF<sub>ICCID</sub> is used, which includes a check digit and filler digit (0xf) in addition to the ICCID.

<sup>27</sup> A theoretical problem scenario arises when a TMSI is used (stored on the card), the handset pESN is used for identification (Usage Indicator b1 = 0), and the card is moved between two different MEID handsets that have the same pESN. A non-C.S0023-C-compliant card cannot receive the handset MEID, and can therefore not detect that it has been inserted in a different handset, and that the TMSI must be rebound to the new MEID.

1 Disadvantages:

- 2 • **Not retrievable.** The LF\_EUIMID is only retrievable from the card via the  
3 recently standardized air interface messaging in C.S0016-C v2.0 (to be  
4 published soon) and C.S0066-0 v2.0 (July, 2008). It may also be accessible  
5 through the CDMA Card Application Toolkit (CCAT, see Section 5.3 below).  
6 This can have an impact on OTASP sessions, where (depending on operator  
7 implementation) there may be a need to receive a unique card identifier in  
8 order to access card-specific information.
- 9 • **Long Identifier.** The 72-bit ICCID, if used to track the card (e.g. from a  
10 logistics perspective), will require separate handling from the device MEID. As  
11 a longer identifier it is also arguably more prone to keying errors (although a  
12 check digit mechanism is defined for ICCIDs).
- 13 • **Issuer Identifier Number (IIN) Limitations.** Countries with 3 digit telephony  
14 country codes (as defined in ITU-T E.164) are restricted to only 100 unique  
15 IINs. Countries with 2 digit country codes have 1000 unique IINs and those  
16 with 1 digit country codes (e.g. North America and the Caribbean) have 10,000  
17 IINs available. This is only a minor limitation because the IIN is generally  
18 assigned to an operator, which then assigns arbitrary sized subsets to their R-  
19 UIM suppliers.

## 20 5.2 Short-Form EUIMID

21 The SF\_EUIMID is a 56-bit identifier, sharing address space with the MEID. An  
22 R-UIM indicates its use of SF\_EUIMID via service n8 in the CDMA Service Table<sup>28</sup>.  
23 An additional option is available with use of the SF\_EUIMID, namely the setting of  
24 bit 2 of the Usage Indicator octet. When the bit is set to 0 (SF\_EUIMID does not  
25 override the ME's MEID), use of the SF\_EUIMID shares the disadvantages but not  
26 the advantages of the LF\_EUIMID – it is not retrievable from the card, yet it requires  
27 new storage and handling capabilities. One benefit – that of using a common  
28 identifier size to track both cards and devices – does not seem sufficient to warrant  
29 the use of this configuration. Accordingly, the advantages and disadvantages listed  
30 below assume the Usage Indicator bit 2 is set to 1 – i.e. the SF\_EUIMID is used in  
31 place of the ME MEID.<sup>29</sup>

---

<sup>28</sup> See C.S0023-C Section 3.4.18

<sup>29</sup> A theoretical problem scenario could arise in IS-2000 Release D, if the MSID\_TYPE is IMSI + MEID, but bit 1 and bit 2 of the Usage Indicator are not set to the same value: in this case, the input to the CAVE algorithm may not be available to the network to check the authentication result.

1 Advantages:

- 2 • **Familiarity.** Use of the SF\_EUIMID represents a minimum change from  
3 current operation, where the UIMID overrides the device ESN.
- 4 • **Retrievable.** The unique SF\_EUIMID is available from the MS in either the  
5 *Status Response Message*, or the *Extended Protocol Capability Response*  
6 *Message* (both methods require the device itself to have an MEID).
- 7 • **Common Identifier.** Both the card and the device can be managed by a  
8 commonly formatted and administered 56-bit identifier. (Although both the  
9 device MEID and R-UIM's SF\_EUIMID are only available via air interface  
10 signaling if C.S0016-C v2.0 or C.S0066-C v2.0 are implemented.)

11  
12 Disadvantages:

- 13 • **Card/device requirements.** The SF\_EUIMID is defined in C.S0023-  
14 C/C.S0065. Cards and devices which do not support this level of either  
15 standard (or at least, this aspect of this level of the standard) will not be able to  
16 override the device MEID. Many R-UIM-based devices in commercial use  
17 today do not support C.S0023-C.
- 18 • **No EIR.** Since the device MEID is unlikely to be transmitted to the network in  
19 normal operation, it is not possible to take advantage of the new X.S0008  
20 CheckMEID operation to track lost, stolen or malfunctioning phones through  
21 communications with an EIR.

### 22 **5.3 CDMA Card Application Toolkit (CCAT)**

23 [C.S0035] defines the CDMA Card Application Toolkit (CCAT). CCAT defines the  
24 means by which an application resident on the R-UIM interacts with the ME and can  
25 initiate communication with the network. It may be possible to define a CCAT  
26 application which can retrieve and send the LF\_EUIMID (e.g. inside an SMS to an  
27 address that terminates to a network-based application). Comments elsewhere in  
28 this document to the effect that "LF\_EUIMID cannot be transmitted to the network"  
29 do not reflect this possibility.

30 Similarly, the ME's MEID could be sent to the network even if normally overwritten  
31 by the SF\_EUIMID<sup>30</sup>. The equivalent note applies to other references in this  
32 document to the inaccessibility of this value to the network.

---

<sup>30</sup> R-UIM access to the ME's MEID may depend on the card activating service n9 ("MEID Support"). Some early commercially released EUIMID-equipped did not support n9.

1 The UIM Tool Kit (UTK) is an alternative R-UIM application mechanism to CCAT,  
2 which may provide equivalent opportunities for transfer of otherwise inaccessible  
3 identifiers to the network. UTK is less formally standardized (see CDG reference  
4 Document #76), but may be in wider commercial deployment than CCAT.

#### 5 **5.4 Device Compatibility with EUIMID**

6 An issue has been identified with some devices currently in the field that prevents  
7 them operating when an EUIMID-equipped R-UIM is inserted. These devices  
8 contain the software feature to support MEID but do have an ESN rather than an  
9 MEID provisioned. Operators should check with their handset suppliers for affected  
10 models.



1

2

## 6. Recommendations

---

3 The subsections below list recommended actions for operators as they migrate to  
4 MEID-equipped devices, and (possibly) EUIMID-equipped R-UIMs.

5 The recommendations are divided according to usage of R-UIMs. In several cases  
6 the same recommendation applies to both types of operator.

### 7 **6.1 Operators with non-R-UIM-equipped handsets**

8 The following actions are recommended:

- 9 • **Ensure basic MEID backwards compatibility.** An immediate  
10 recommendation is for operators to ensure that MEID-equipped devices can  
11 receive service. Actions involve investigation, and if necessary patches and/or  
12 upgrades to the MSC/BSC. See the [MEID Failure Bulletin] for more  
13 information.
- 14 • **Add C.S0072 support in the network.** C.S0072 allows BS-assigned PLCMs  
15 to prevent cross-talk and dropped calls due to pESN-based PLCM, and also  
16 allows the MEID to be retrieved from the device.
- 17 • **Ensure no hash checking at the BS/MS.** Hash checking implies verifying  
18 that the received “MEID” value will hash to the received “ESN” value. While  
19 this may be a valid assumption for the operator’s own subscribers, it may not  
20 hold true for inbound roamers present on the operator’s network (e.g. if they  
21 use LF\_EUIMID, or a unique UIMID, the UIMID/pUIMID will not be hash-  
22 related to the ME MEID). Although such checking is not believed to be  
23 common, if implemented it may erroneously deny service to a valid subscriber.
- 24 • **Stop ESN-based addressing on paging channel.** Duplicated pESNs can  
25 cause unpredictable results since more than one mobile may process a  
26 message intended for a single MS. The alternative is to move to IMSI-based  
27 addressing where this problem cannot occur with legitimate mobiles.
- 28 • **Remove network element and back-end dependency on unique ESN.** The  
29 specific actions will depend on the operator’s systems, and may apply to HLR,  
30 VLR, billing, provisioning, fraud systems etc. Either the uniqueness check may  
31 be relaxed, or the check may be applied to the MEID instead (assuming MEID  
32 is reliably available at the necessary location).

- 1       • **Support C.S0066 for OTASP.** If OTASP is used in the operator's network,  
2       and there is a need to reference device-specific information (e.g. A-key, SPC)  
3       during the OTASP process, then C.S0066 should be supported to allow the  
4       MEID to be transferred to the OTAF.
- 5       • **Index OTASPCallEntry by Activation\_MIN.** The use of Activation\_MIN  
6       allows concurrent OTASP sessions for mobiles with the same pESN.
- 7       • **Evaluate X.S0008 support.** Operators may choose to implement X.S0008  
8       (MEID for ANSI-41) in their networks. This can be of use for stolen phone  
9       scenarios, and in general allows a unique device identifier to be stored in the  
10      HLR.
- 11      • **Evaluate MEID inclusion in CDRs.** Operators may choose to include MEID in  
12      their MSC billing records, with associated upgrades to the billing system to  
13      parse this new record.
- 14      **Note:** The previous two recommendations both require retrieval of the MEID  
15      over the air interface, at some small capacity cost. Some vendors may  
16      automatically initiate MEID retrieval whenever the MS indicates it has an  
17      MEID.
- 18      • **Ensure Uniqueness of NAIs.** Network Access Identifiers (NAIs) derived from  
19      the ESN should be replaced with a unique alternative, such as MEID-derived  
20      NAIs (e.g. MEID@realm).
- 21      • **Check support for MEID in PCF, PDSN and AAA.** The airlink record sent  
22      between the PCF and PDSN, and used to form the PDSN UDR that is sent to  
23      the AAA, contains either MEID or ESN. While pESN may be used in non-  
24      upgraded 1X systems, the pESN is not available in EVDO unless it is  
25      calculated from the MEID.
- 26      • **Add support for MEID as EVDO Hardware ID.** Operators who use the  
27      Hardware ID in A12 authentication should ensure that MEID is supported as  
28      per A.S0008-A.
- 29      • **Outbound Roaming Support.** Operators should recognize that not all  
30      roaming partners may support the MEID/EUIMID migration to the same  
31      degree. MEID inclusion should not be mandatory (from the perspective of the  
32      receiving entity and any subsequent processing) on any internetwork interface,  
33      including:
- 34          ○ ANSI-41 Interfaces  
35          ○ CIBER Records  
36          ○ A12 Authentication
- 37

- 1           ○ **CIBER Record Population.** Assuming both a 32- and 56-bit  
2 identifier are captured in the MSC CDR (which may be either  
3 ESN/pESN/UIMID/pUIMID or MEID/SF\_EUIMID respectively), it is  
4 recommended that the 32-bit identifier be included until it is either  
5 verified that all roaming partners support MEID or SF\_EUIMID in  
6 CIBER records or the system is capable of storing the capability of  
7 every roaming partner individually.

8 Note that inbound roamers may use R-UIMs, even if the operator's own  
9 subscribers do not.

- 10 • **Unique pESNs.** If operators are struggling to accommodate duplicate pESNs  
11 in the required timeframe, a potential mitigation approach is to require only  
12 distinct pESNs be delivered to them from handset manufacturers. This is a last  
13 resort action only, and is discouraged for the following reasons:
- 14       ○ It may distract operators from properly addressing the required  
15 updates
  - 16       ○ It may impose an unreasonable management burden on handset  
17 manufacturers, and cause them to “waste” large numbers of  
18 MEIDs<sup>31</sup>.
  - 19       ○ It becomes progressively more difficult to implement as the number  
20 of deployed pESNs rises.
  - 21       ○ Only ~16.7 million different pESNs are available – beyond this  
22 uniqueness is not possible.
  - 23       ○ Collisions or duplications due to roamers are not addressed – these  
24 may still occur beyond the operator's control.
- 25 • **Authentication.** Everywhere that authentication operations specify ESN,  
26 including in CAVE calculations and A-Key checksum generation, pESN should  
27 be used instead. There is no loss of security even though this input may not be  
28 unique.

---

<sup>31</sup> With multiple handset manufacturers supplying a single operator, each manufacturer may be restricted to a portion of the pESN address space for that operator, further increasing the wastage of MEIDs.

## 6.2 Operators with R-UIM-equipped handsets

The following actions are recommended:

- **Ensure basic MEID backwards compatibility.** An immediate recommendation is for operators to ensure that MEID-equipped devices can receive service. Actions involve investigation, and if necessary patches and/or upgrades to the MSC/BSC. See the [MEID Failure Bulletin] for more information.
- **Add C.S0072 support in the network.** C.S0072 allows BS-assigned PLCMs to prevent cross-talk and dropped calls due to pUIMID-based PLCM, and also allows the MEID/SF\_EUIMID to be retrieved from the device.
- **Ensure no hash checking at the BS/MSC or HLR.** Hash checking implies verifying that the SHA-1 hash of the received “MEID” matches the received “ESN” value. Use of the LF\_EUIMID, or unique UIMID (or SF\_EUIMID in a MEID-equipped device that does not support C.S0023-C) will result in a 32-bit identifier being sourced from the R-UIM, and a 56-bit identifier from the ME, which are highly unlikely to be hash-related. Any such checking may erroneously deny service to a valid subscriber.
- **Stop ESN-based addressing on the paging channel.** Duplicate pUIMIDs can cause unpredictable results since more than one mobile may process a message intended for a single MS. The alternative is to move to IMSI-based addressing where this problem cannot occur with legitimate mobiles.
- **Decide on EUIMID format.** The operator should consider the characteristics discussed in Section 5. and then choose either Long Form or Short Form EUIMID.
- **Verify handset compatibility with EUIMID.** The operator should check whether any handset models currently in circulation will fail to operate with an EUIMID-equipped R-UIM (see Section 5.4 ).
- **Verify device/card support for EUIMID.** In particular this applies to SF\_EUIMID, which imposes new requirements on the card and device.
- **Deploy MEID-equipped devices.** Even with C.S0072 support in the network, an EUIMID-equipped R-UIM in an ESN-equipped device is susceptible to PLCM collision, and may prove challenging for OTASP without custom handling as discussed below.
- **Remove network element and back-end dependency on unique UIMID and ESN.** The specific actions will depend on the operator’s systems, and may apply to HLR, VLR, billing, provisioning, fraud systems etc. Either the UIMID uniqueness check may be relaxed, or the check may be applied to the EUIMID instead (assuming EUIMID is reliably available at the necessary location).

1 Inventory management etc may also need to move from the ESN to the MEID  
 2 to track/report on devices (even though these identifiers may not be available  
 3 in air interface signaling).

- 4 • **Support OTASP modifications if unique card information required.** If  
 5 OTASP is used in the operator's network, the card does not come pre-  
 6 provisioned with MDN, MIN or IMSI, and there is a need to reference card-  
 7 specific information (e.g. A-key, SPC) during the OTASP process, then  
 8 C.S0066-0 v1.0 should be supported to allow the SF\_EUIMID to be transferred  
 9 to the OTAF or C.S0066-0 v2.0 to allow both the MEID and EUIMID (either  
 10 form) to be transferred. Alternatively, and to achieve the ability to provision  
 11 EUIMID cards in ESN mobiles, the EUIMID can be stored in fields such as  
 12 MDN and IMSI\_T that are accessible to all ESN mobiles and that may not  
 13 need to contain the intended data prior to provisioning.
- 14 • **Avoid static card-specific information in OTASP if unique identifier**  
 15 **unavailable.** If no unique card identifier is retrievable, alternative approaches  
 16 to card-specific information can be used instead of indexing a pre-provisioned  
 17 database. These could include:
  - 18 ○ Secure generation of A-key during OTASP session
  - 19 ○ Cards issued with default SPC (Service Programming Code), set to  
 20 random value during OTASP session

21 The lack of a unique identifier may also prompt operators to implement PIN-or  
 22 PRL-based methods to ensure that the activation is completed to the correct  
 23 operator.

- 24 • **Index OTASPCallEntry by Activation\_MIN.** The use of Activation\_MIN  
 25 allows concurrent OTASP sessions for mobiles with the same pUIMID.
- 26 • **Evaluate X.S0008 support.** Operators may choose to implement X.S0008  
 27 (MEID for ANSI-41) in their networks. This can be of use for stolen phone  
 28 scenarios (with LF\_EUIMID), or to allow a unique card identifier to be stored in  
 29 the HLR (with SF\_EUIMID). Implementation of an Equipment Identity Register  
 30 is at the operator's discretion.
- 31 • **Evaluate MEID/SF\_EUIMID inclusion in CDRs.** Operators may choose to  
 32 include MEID/SF\_EUIMID in their MSC call detail records, with associated  
 33 upgrades to the billing system to parse this new record.

34 **Note:** The previous two recommendations both require retrieval of the  
 35 MEID/SF\_EUIMID over the air interface, at some small capacity cost. Some  
 36 vendors may automatically initiate MEID/SF\_EUIMID retrieval whenever the  
 37 MS indicates it has an MEID and the system has not recently retrieved it.

- 38 • **Check support for MEID in PCF, PDSN and AAA.** The airlink record sent  
 39 between the PCF and PDSN, and used to form the PDSN UDR that is sent to  
 40 the AAA, contains either MEID or ESN. While pESN may be used in non-

- 1 upgraded 1X systems, the pESN is not available in EVDO unless it is  
2 calculated from the MEID.
- 3 • **Ensure Uniqueness of NAIs.** Network Access Identifiers (NAIs) derived from  
4 the UIMID should be replaced with EUIMID-derived NAIs  
5 (e.g. EUIMID@realm).
  - 6 • **Add support for MEID as EVDO Hardware ID.** Operators who use the  
7 Hardware ID in A12 authentication should ensure that MEID is supported as  
8 per A.S0008-A. The Hardware ID is either ESN or MEID, never UIMID or  
9 EUIMID.
  - 10 • **Outbound Roaming Support.** Operators should recognize that not all  
11 roaming partners may support the MEID/EUIMID migration to the same  
12 degree. MEID/SF\_EUIMID inclusion should not be mandatory (from the  
13 perspective of the receiving entity and any subsequent processing) on any  
14 internetwork interface, including:
    - 15 ○ ANSI-41 Interfaces
    - 16 ○ CIBER Records
    - 17 ○ A12 Authentication
    - 18 ○ **CIBER Record Population.** Assuming both a 32- and 56-bit  
19 identifier are captured in the MSC CDR (which may be either  
20 ESN/pESN/UIMID/pUIMID or MEID/SF\_EUIMID respectively), it is  
21 recommended that the 32-bit identifier be included until it is either  
22 verified that all roaming partners support MEID or SF\_EUIMID in  
23 CIBER records or the system is capable of storing the capability of  
24 every roaming partner individually.
  - 25 • **Unique pUIMIDs.** If operators are struggling to accommodate duplicate  
26 pUIMIDs in the required timeframe, a potential mitigation approach is to  
27 require only distinct pUIMIDs be delivered to them from R-UIM manufacturers.  
28 This is a last resort action only, and is discouraged for the following reasons:
    - 29 ○ It may distract operators from properly addressing the required  
30 updates
    - 31 ○ It may impose an unreasonable management burden on R-UIM  
32 manufacturers, and cause them to “waste” large numbers of  
33 EUIMIDs<sup>32</sup>.
    - 34 ○ It becomes progressively more difficult to implement as the number  
35 of deployed pUIMIDs rises.
    - 36 ○ Only ~16.7 million different pUIMIDs are available – beyond this  
37 uniqueness is not possible.

---

<sup>32</sup> With multiple card manufacturers supplying a single operator, each manufacturer may be restricted to a portion of the pUIMID address space for that operator, further increasing the wastage of EUIMIDs.

- 1                   ○ Collisions or duplications due to roamers are not addressed – these
- 2                   may still occur beyond the operator's control.
- 3                   • **Authentication.** Everywhere that authentication operations specify ESN,
- 4                   including in CAVE calculations and A-Key checksum generation, UIMID
- 5                   should have been used in R-UIM devices. Now, pUIMID should be used
- 6                   instead. There is no loss of security even though this input may not be unique.
- 7

1

## **7. Scenarios**

---

2 This section describes specific scenarios, the changes imposed by the migration to  
3 MEID/EUIMID, and/or the impacts caused by duplicate 32-bit identifiers. Note that  
4 the call-flow diagrams presented in this section are intended to highlight relevant  
5 aspects, and may not include all messages/responses for the scenario in question.

6 The scenarios are grouped according to different operator choices about the type of  
7 device and/or R-UIM that their subscribers use. Except when explicitly noted, the  
8 assumption is made that the network supports C.S0072. In some cases, information  
9 may be duplicated, or refer to previously described scenarios.

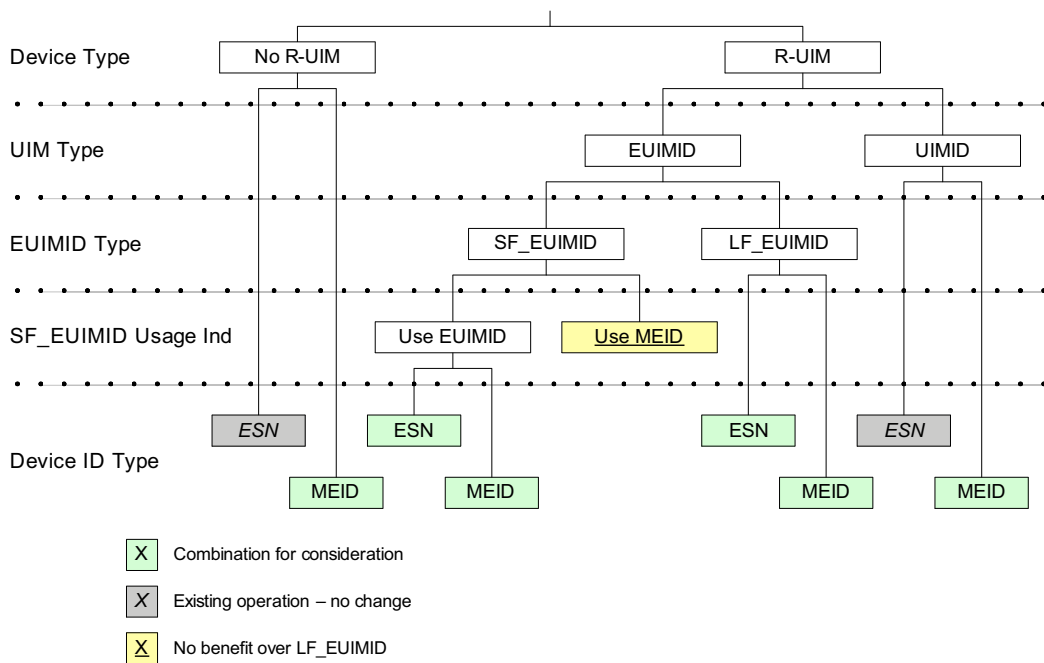


**7.1 Device / R-UIM Combinations of Interest**

Figure 7-1 below shows the expansion of different R-UIM and device combinations, and highlights the ones that will be considered (although potentially found to be problematic) in the scenarios below. For all R-UIM cases, the assumption is made that bit 1 of the usage indicator is set to 1 (i.e. UIMID overrides ESN) – this is consistent with current R-UIM operator practice.

As an example, the branch on the extreme right of the diagram represents the following combination:

- Device Type: R-UIM
- UIM Type: UIMID
- EUIMID Type: N/A
- SF\_EUIMID Usage Indicator: N/A
- Device ID Type: MEID



**Figure 7-1 - Device & Card Combinations**

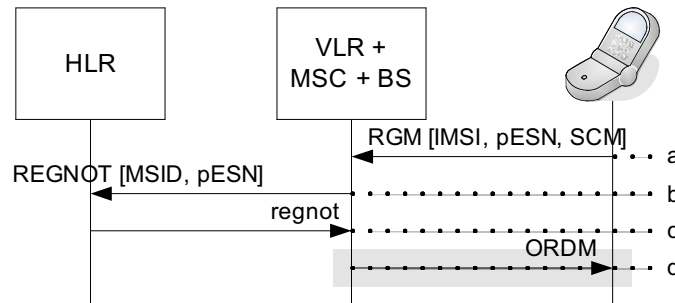
## 7.2 Non-R-UIM Operator

The scenarios in this subsection apply to an operator whose subscribers use devices that do not require an R-UIM. Only new cases (i.e. MS is equipped with MEID) are considered – any new standards impose no changes on present-day operation.

### 7.2.1 Basic Operation

#### 7.2.1.1 Registration – No X.S0008 support

This scenario describes registration for an MEID-equipped MS. The network has not implemented the ANSI-41 changes to support MEID. The steps are shown in Figure 7-2 below:



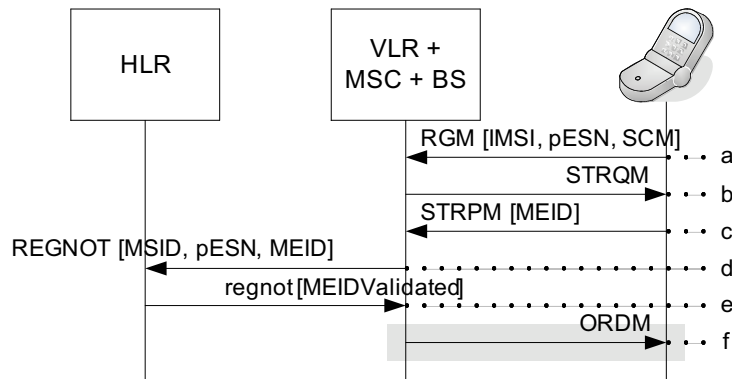
**Figure 7-2 - MEID MS Registration - no X.S0008 support**

Steps are as follows:

- a) MS sends a *Registration Message*, including its IMSI, pESN and Station Class Mark set to indicate MEID support. The MS cannot include its MEID in this message.
- b) Although the MSC is aware that the MS has a MEID, it takes no specific action. It proceeds with the RegistrationNotification INVOKE message, including the pESN and the Mobile Station Identity (MSID – either MIN or IMSI)
- c) The HLR validates the subscription on the basis of MSID-pESN. This combination is unique even though the same pESN value may be used by other MSs with different IMSIs. The HLR returns the subscriber profile to the MSC.
- d) Optionally, the BS sends a *Registration Accepted Order* to the MS

1 **7.2.1.2 Registration – X.S0008 supported**

2 This scenario describes registration for an MEID-equipped MS. The network has  
 3 implemented the ANSI-41 changes to support MEID. The steps are shown in Figure  
 4 7-3 below:



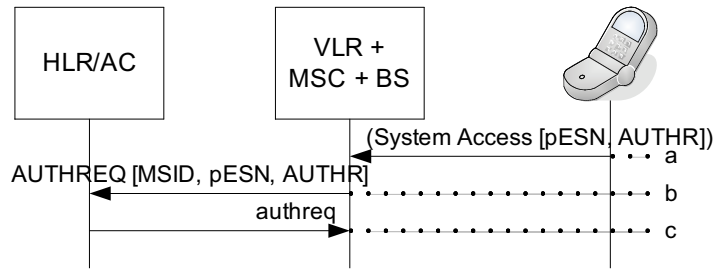
5  
6 **Figure 7-3 - MEID MS Registration - X.S0008 supported**

7 Steps are as follows:

- 8 a) MS sends a *Registration Message*, including its IMSI, pESN and Station  
 9 Class Mark set to indicate MEID support. The MS cannot include its MEID in  
 10 this message.
- 11 b) Based on the SCM, the MSC recognizes that the mobile has a MEID, and  
 12 that the MSC does not know this value. It solicits the MEID via the *Status*  
 13 *Request Message* (new Information Record in C.S0072).
- 14 c) The MS returns its MEID in the *Status Response Message*
- 15 d) The MSC sends a *RegistrationNotification* to the HLR, including the MSID,  
 16 pESN (required for backwards compatibility) and the MEID.
- 17 e) Text extracted from X.S0008: “Based on the existence of a provisioned  
 18 MEID value for this subscription, and the presence of the MEID parameter in  
 19 the REGNOT, the HLR includes an MEID comparison in the validation of the  
 20 subscription. The HLR then registers the indicated MS and returns a regnot  
 21 to the Serving VLR. The regnot includes the MEIDValidated parameter to  
 22 inform the Serving VLR/MS that the MEID associated with the system  
 23 access has been validated.”
- 24 f) Optionally, the BS sends a *Registration Accepted Order* to the MS

1 **7.2.1.3 Authentication**

2 This scenario provides a representative example of the various authentication use  
 3 cases possible. If X.S0008 is supported, MEID may be included in various  
 4 authentication messages, but it is not used in actual authentication computations.  
 5 The steps are shown in Figure 7-4:



6  
7 **Figure 7-4 - Authentication of MEID device**

8 Steps are as follows:

- 9 a) MS makes a system access. It includes its pESN and the Authentication  
 10 Response parameter (other authentication-related information and SCM not  
 11 shown).
- 12 b) The MSC determines it needs to request authentication at the HLR/AC (e.g.  
 13 SSD is not shared, or this is the first system access). The MSC sends an  
 14 AuthenticationRequest to the HLR/AC. MEID may also be requested by the  
 15 MSC and included in the AUTHREQ.
- 16 c) The AC computes the challenge result and compares it with the received  
 17 response. The pESN is used in the calculation, but not the MEID, even if it is  
 18 received. The HLR/AC returns an authreq to the MSC to advise that the  
 19 challenge was successfully passed.

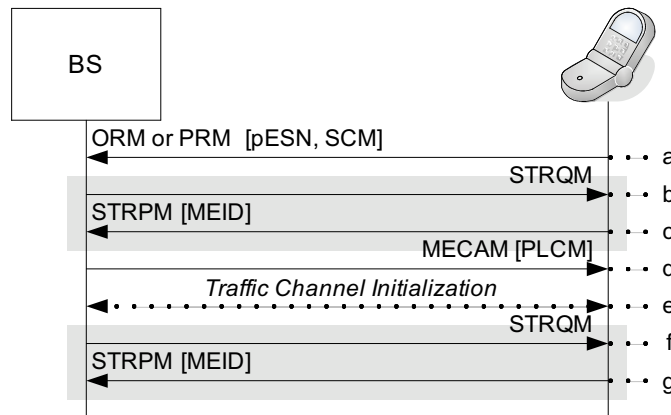
20 An Authentication scenario not involving signaling is the calculation of the 6-digit  
 21 checksum used when entering the A-key manually via the handset keypad. The  
 22 algorithm is defined in S.S0054<sup>33</sup>, where the A-key and the ESN are used as inputs.  
 23 This standard makes no mention of MEID. At least one operator is known to have  
 24 specified MEID to replace pESN as the input to this algorithm. A standards  
 25 contribution from 2004<sup>34</sup> proposes use of the pESN.

33 [http://www.3gpp2.org/Public\\_html/specs/S.S0054-0\\_v1.0.pdf](http://www.3gpp2.org/Public_html/specs/S.S0054-0_v1.0.pdf)

34 [ftp://ftp.3gpp2.org/TSGS/Working/2004/TSG-S\\_2004-12-Kauai/Numbering\\_AHG/S00NUM-20041208-003\\_A-key\\_checksum\\_Nokia.doc](ftp://ftp.3gpp2.org/TSGS/Working/2004/TSG-S_2004-12-Kauai/Numbering_AHG/S00NUM-20041208-003_A-key_checksum_Nokia.doc)

1 **7.2.1.4 Call Origination/Termination**

2 In this scenario, the mobile makes or receives a call. Since the mobile is MEID-  
 3 equipped, the network assigns a PLCM explicitly rather than using one derived from  
 4 the pESN. The steps are shown in Figure 7-5:



5  
6 **Figure 7-5 - MEID Origination/Termination**

7 Steps are as follows:

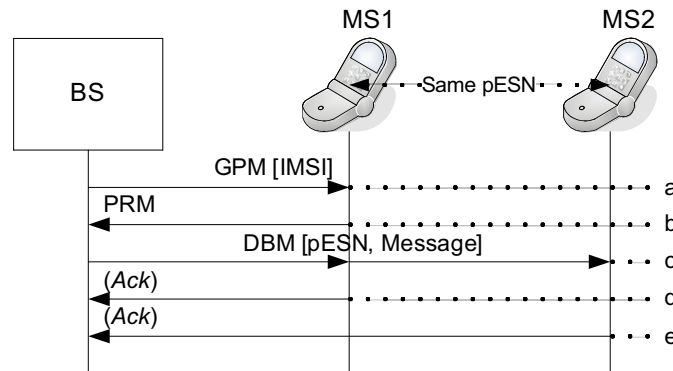
- 8 a) The MS sends an *Origination Message* or a *Page Response Message*,  
 9 including its pESN and SCM
- 10 b-c) Optionally, the MSC queries the MEID via a *Status Request Message* over  
 11 the paging channel, and the MS responds. This would be required if the  
 12 MSC used the MEID-based PLCM type.
- 13 d) Since the MS has advertised that it has a MEID via the SCM, the MSC  
 14 sends an *MEID Enhanced Channel Assignment Message* (new for  
 15 C.S0072). The message includes the PLCM\_TYPE field, and (if the  
 16 PLCM\_TYPE indicates BS-assigned) the PLCM itself.
- 17 e) The traffic channel is initialized as normal, using the PLCM as agreed above
- 18 f-g) Optionally, the MSC can query the MEID via a *Status Request Message* sent  
 19 on the traffic channel, and the MS responds.

20 **7.2.1.5 Billing Record Production**

21 MSC Call Detail Records (CDRs) typically include the MIN/IMSI and ESN of a  
 22 mobile. With the migration to MEID-equipped MSs, operators may wish to retain a  
 23 unique identifier for the mobile hardware in their CDRs. Obtaining this identifier (the  
 24 MEID) will require operators to support the retrieval of the MEID via the Status  
 25 Request Message either at registration time or call time (see Sections 7.2.1.2 and  
 26 7.2.1.4 respectively).

1 **7.2.1.6 Mobile Terminated SMS**

2 This scenario shows an undesirable result of a message addressed by ESN only.  
 3 Even with C.S0072 support in the network, this effect can still occur. The *Data Burst*  
 4 *Message* used to carry the SMS is only one example of a message that could be  
 5 addressed in this way – see Section 0 for more details. The steps are shown in  
 6 Figure 7-6 below - in this diagram, MS1 and MS2 are both in the same sector:



7  
 8 **Figure 7-6 - ESN-based addressing conflict**

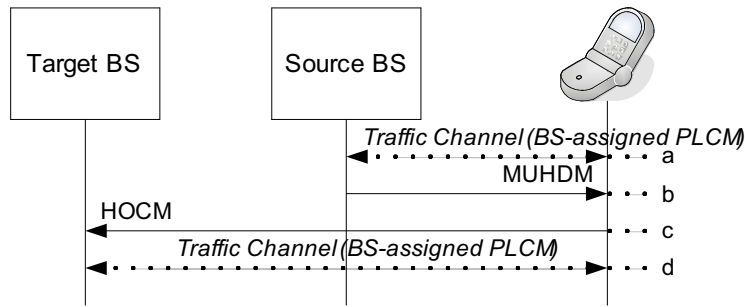
9 Steps are as follows:

- 10 a) The BS sends a *General Page Message* (GPM) to alert the mobile that there  
 11 is an SMS message for it. The GPM is addressed to the IMSI of the mobile  
 12 for whom the SMS is intended (MS1). This message is typically sent over a  
 13 wide area in order to find the mobile.
- 14 b) MS1 responds to the page.
- 15 c) The BS sends a *Data Burst Message* (DBM) containing the SMS. The DBM  
 16 is typically sent only on the sector on which the MS responded to the page.  
 17 In this example, the message length is such that the network chooses to  
 18 send it on the paging channel, rather than establishing a traffic channel. and  
 19 the message is addressed using the “ESN” address type. The value in the  
 20 ESN field is the pESN, which happens to be common to both MS1 & MS2.  
 21 *Both mobiles receive the text message.*
- 22 d-e) Both mobiles send an acknowledgment.

23 Note that the alternative addressing (IMSI-based) may be susceptible to a similar  
 24 problem if the operator sends *Data Burst Messages* on the paging channel, but this  
 25 requires that a mobile is provisioned with the IMSI of a mobile it wishes to receive  
 26 text messages for and must remain in the vicinity of the target mobile. Legitimate  
 27 mobiles will not receive IMSI-addressed text messages destined for other mobiles  
 28 as only one mobile will ever be the legitimate holder of an IMSI at any one time.

1 **7.2.1.7 Handoff**

2 C.S0072 defines the new *MEID Universal Handoff Message* (MUHDM). This  
 3 message allows the PLCM to be specified/modified at handoff time. Figure 7-7  
 4 shows an MEID-equipped mobile handing off between two C.S0072-compliant Base  
 5 Stations:



6  
7 **Figure 7-7 - MEID Handoff**

8 Steps are as follows:

- 9 a) The MS is operating on a traffic channel in communication with the source  
 10 BS. AS per Section 7.2.1.4 , the MS uses a BS-assigned PLCM.
- 11 b) The source BS sends a MUHDM. This message can include the PLCM type  
 12 if it is to be changed, or omit it to retain the same PLCM.
- 13 c) The MS sends a *Handoff Complete Message* to the Target BS.
- 14 d) The traffic channel is established with the new BS.

15 If the handoff requires coordination via the MSC, IOS 5.0.1 (or higher) must be  
 16 implemented on that interface to carry the PLCM information.

17 If the source and target BSs differ in their support of C.S0072 (e.g. during the  
 18 network upgrade process), a PLCM change may be required at handoff. Table 7-1  
 19 lists the various combinations:

Target BS →	No C.S0072 Support	C.S0072 Support
Source BS ↓		
No C.S0072 Support	Continue pESN-based PLCM in UHDM	Continue pESN-based PLCM in UHDM. Subsequent MUHDM could change to a different PLCM
C.S0072 Support	Change to pESN-based PLCM in MUHDM	Could continue with BS-assigned PLCM via MUHDM

20 **Table 7-1 - Handoff matrix for C.S0072 support levels**