MEID and EUIMID Migration

CDG Document 158

Version 2.1

February, 2011

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

1. Executive Summary

- **Issue**. It has been known for several years that the ESN numbering resource, used for both the handset's Electronic Serial Number and for R-UIM UIMID codes, is close to exhaustion. Due to stringent conservation and reclamation of codes the life of the resource was extended several years beyond the first predictions. However, the last virgin (never before assigned) ESN code was assigned in 2008 and the last applications for assignments using reclaimed codes were accepted by the administrator (TIA) on June 30th 2010.
- **Industry Response**. In response to these events, the CDMA2000® industry has been migrating handsets from ESN to MEID-based addressing, and R-UIMs from UIMID- to EUIMID-based addressing, and several operators have completed this transition.
    - **Non-unique values, known as pESN (pseudo-ESN) or pUIMID (pseudo-UIMID), will be used in ESN/UIMID fields, previously depended upon to be unique.**
- **Potential Impact**. If there are no steps taken in the network and back-end systems to accommodate this change, possible impacts include:
    - Crosstalk, interference, blocked and dropped calls.
    - Misaddressed air interface messaging (e.g. SMS received by wrong user).
    - Inability to provision and/or bill some subscribers.
    - Spurious Fraud Detection alerts.
- **Migration Status**. The migrations have already started
    - Several major CDMA2000® operators have already upgraded their network and deployed MEID-based handsets.
    - EUIMID-based R-UIMs have already been deployed by several operators.
- **Recommended Actions**. All CDMA2000® operators are recommended to
    - Upgrade their network to support C.S0072 to minimize PLCM collisions.
    - Remove any requirement in their back-end systems (e.g. HLR, VLR, billing, provisioning) for a unique ESN/UIMID value.
    - Use MEID-equipped devices.
    - Choose either Long or Short EUIMID format and provision future R-UIM or CSIM cards with this identifier.

Contents

Figures

Tables

Revision History

Date	Version	Description
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
2010-11-30	2.1	Updated to reflect the latest status of the resources and the migration.

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 definitions are used:

- **ESN**. Existing 32-bit identifier for a mobile station. Essentially exhausted and assignment applications no longer being accepted.
- **UIMID**. 32-bit card identifier that typically replaces the handset ESN (ESN_ME) in ESN protocol fields[1]. Essentially exhausted and assignment applications are no longer being accepted. Allocated from the same numbering space as the ESN.
- **MEID**. Replacement[2] 56-bit identifier for the ESN.
- **EUIMID**. Replacement[2] identifier for the UIMID. This can be the SF_EUIMID (which may substitute for the handset MEID (MEID_ME) in MEID protocol fields) or LF_EUIMID (ICCID).
- **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”, when unqualified, 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. The term “ESN_ME” is used to explicitly refer to the value stored in the mobile station.

---

[1] UIMID does not replace ESN as the HardwareID parameter in EVDO.

[2] 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. In both cases a pseudo-ESN or pseudo-UIMID is calculated for backwards compatibility with signaling.

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 because a value that was previously reliably known to be uniquely assigned 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. recommends 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.

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

2.1.2 Duplication Impact

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

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

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

[3] See http://www.3gpp2.org/Public_html/specs/C.S0003-0_v3.0.pdf

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

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

2.1.3 Collision Impact

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

When messages are addressed by ESN to one of multiple duplicate-ESN mobiles in the same area[4] the messages may be processed by two or more mobiles. See the [Collisions WP] for a listing of the impact of each message that may be addressed in this way, and Section 7.2.1.6 for a particular example where a mobile can receive an SMS intended for someone else.

Note that the alternative addressing method (via IMSI) may be susceptible to similar effects if a non-subscribed mobile were programmed with the IMSI of a legitimate mobile in the same area. However, the likelihood of this occurring is much less. This is because a mobile with a duplicate IMSI could not get any other services (it would fail authentication) and it would only cause interference if it stayed in the vicinity of the legitimate phone. The most likely scenario where this could occur is when a subscriber gets a new phone and the IMSI is transferred to that phone.

[4] i.e. the area over which the message is sent

The impact of collisions derives from the fact that in current networks, the Public Long Code Mask (PLCM[5]) is derived from the mobile's ESN.

2.1.3.1 What is a PLCM?

The PLCM is a 42-bit number used to generate the public long code, a pseudonoise sequence used for scrambling on the forward CDMA traffic channel and spreading on the reverse CDMA traffic channel[6]. On the forward traffic channel, distinct Walsh codes further distinguish individual users' traffic. However on the reverse traffic channel, only the ESN-derived portion of the PLCM differentiated users' traffic until Release D and 3GPP2 C.S0072 provided other derivation methods.

In CDMA2000® networks, the PLCM comprises a channel-specific header plus a permutation of the mobile's ESN.

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

2.1.3.2 Impact of PLCM collision

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

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

2.1.4 MEID/EUIMID Support

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

In EV-DO Revision 0 networks that include the Hardware Identifier in the A12 interface, access authentication failures may result for MEID-equipped mobiles on a

---

[5] 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

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

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

Some R-UIM handsets in the market do not support EUIMID-equipped R-UIMs (see 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. Virgin ESN code blocks were completely exhausted by the end of 2008. Assignments continued beyond that date using reclaimed codes but the TIA stopped accepting new applications for assignments on June 30th 2010.

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 also stopped accepting applications for new UIMID code blocks on June 30th 2010 although assignments will continue for some time with previously received applications as need for codes is demonstrated and as reclaimed codes become available.

2.2.2 Current Resource Utilization

An overview of the ESN manufacturer code assignments is available on the TIA website[7].

Usage of pESNs and pUIMIDs removed one 8-bit manufacturer code (~16.8 million codes) from assignment but otherwise did 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.

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).

[7] http://www.tiaonline.org/standards/resources/esn/codes.cfm

EUIMID assignment commenced in 2007, with several major R-UIM manufacturers supplying millions of EUIMID-equipped cards to their operator customers. The SF_EUIMID is assigned by the MEID administrator (TIA) and the LF_EUIMID is assigned nationally.

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

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

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[8]. The value is calculated as follows for a group of *n* cards/devices:

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

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

or, using the factorial notation, "!":

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

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

[8] 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

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

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

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

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

2.3.3 PLCM Collision Probability

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

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

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

where:

- U: the total number of carrier sectors in the operator's network.
- λ: expected number of calls made per hour in an average sector.
- $1/\mu$: average call holding time (in fractions of an hour).
- f: fraction of the calls that use pESN based handsets or pUIMID R-UIMs
- I: number of neighboring sectors that interfere with an average sector.
- N: the possible values for the public long code mask (PLCM): 2^{24}.

One scenario in this document estimated daily collisions in a large system with 60,000 sectors, each of which had 6 neighboring sectors. It estimated that they would rise from zero with no pESNs or pUIMIDs to almost 600 per day (throughout the entire system) if all mobiles transmitted a pESN or pUIMID. This is a rate of just

[9] See http://mathworld.wolfram.com/StirlingNumberoftheSecondKind.html

under 4 collisions per million calls over the day or just under 6 collisions per million calls during busy hour. Obviously this problem is eliminated if precautions against pESN/pUIMID collisions are taken.

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

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

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

m (number of potentially colliding users)	**E (expected number of calls before collision occurs)**
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

[10] http://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.

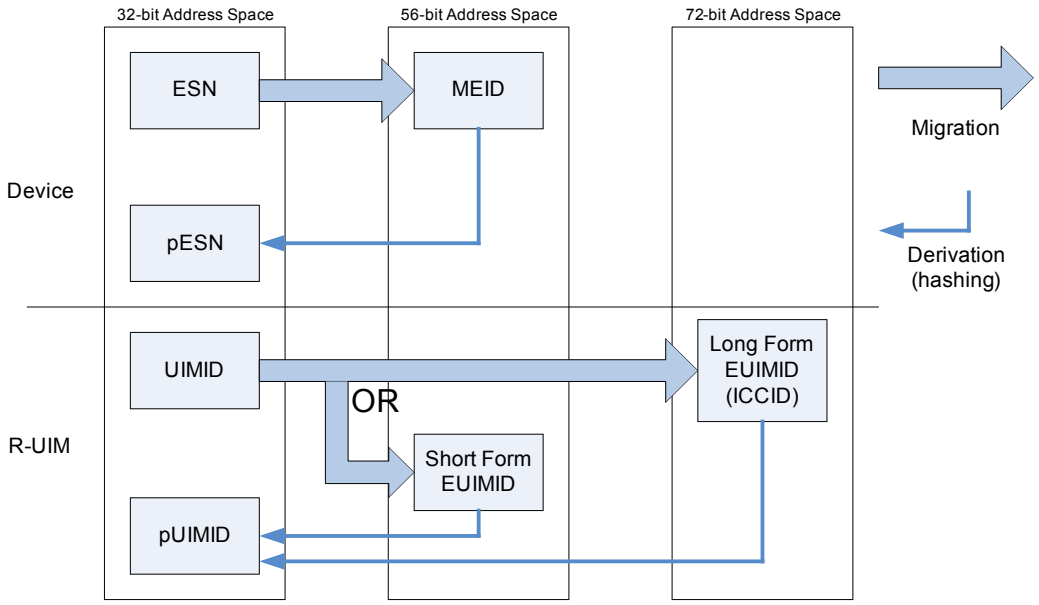

Figure 3-1: Identifier Relationships

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[11]. 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 have 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 up to approximately 16.7 million wireless devices[12] although many manufacturers produced far fewer devices leaving many codes stranded. 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.

---

[11] 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.

[12] 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).

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

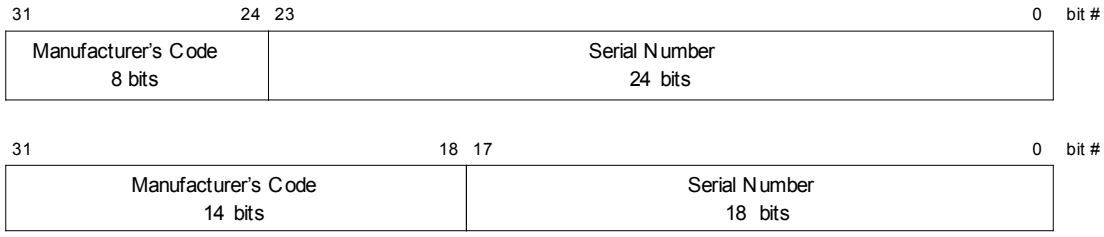

Figure 3-2 - ESN Manufacturer's code allocation

For more information, see the TIA website[13], and the definition in [C.S0005]. The TIA also produces a regular ESN Administrator's Report, available from Gary Pellegrino, the TIA TR-45 EUMAG chair (Gary@CommFlowResources.com), or the ESN administrator, John Derr (JDerr@tiaonline.org).

3.2.2 User Identity Module Identifier (UIMID)

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

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

The TIA currently administers the UIMID space.

In 1x voice and data modes the UIMID can be used instead of the ESN from the device wherever the ESN is signaled over the air or used in calculations (e.g. CAVE authentication).[15] This behavior is controlled by a variable on the R-UIM, the Usage

---

[13] http://www.tiaonline.org/standards/resources/esn/

[14] http://www.tiaonline.org/standards/resources/esn/codes.cfm

[15] Some signaling messages defined in C.S0066-0 v2.0, C.S0016-C v2.0 and CDMA 2000 Release E explicitly call for the use of ESN_ME and will not substitute UIMID.

Indicator (EF_{USGIND}). Figure 3-3 shows the function of the usage indicator (only bit 1 is relevant here – the function of bit 2 is discussed in Section 3.3.2). Note that the value of this indicator is not explicitly available to the network. This is not true in EV-DO where the HardwareID is sourced from the ME identifier (ESN or MEID) regardless of the value of EF_{USGIND}.

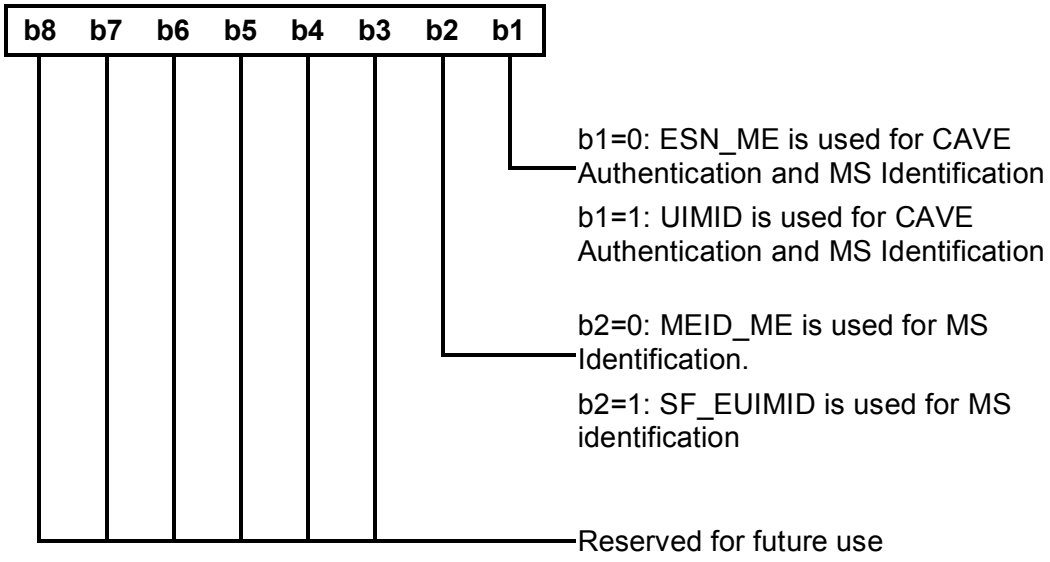

Figure 3-3 - Usage Indicator Function

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

For more information, see [C.S0023]. The TIA produces a regular UIM Administrator's Report, available via email and by distribution to various 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_{ICCID}) is 80 bits (room for 20 digits) 3GPP2 C.S0023-C v2.0 recommends that the check digit is also included as the nineteenth digit along with a single filler digit (0xf) as the twentieth. 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)[16], 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:

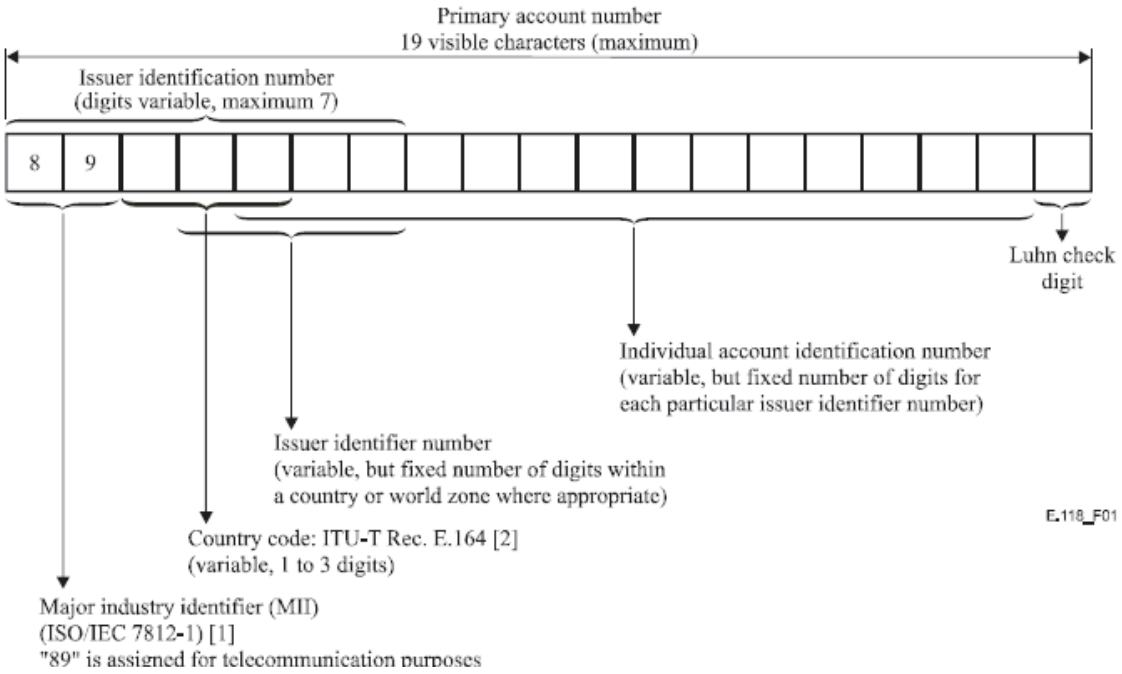

Figure 3-4 - Structure of ICCID

[16] The ability to query for these identifiers is added in C.S0066 v2, in C.S0016-C v2 and via Status Request messages in Revisions D and E of C.S0005 (CDMA2000 radio interface level 3).

3.3 New Identifiers

3.3.1 Mobile Equipment Identifier (MEID)

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

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

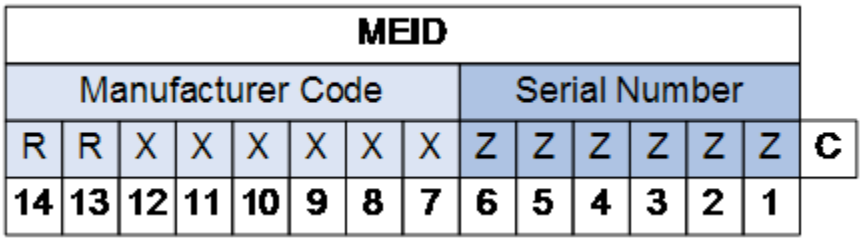

Figure 3-5 - MEID Structure (Hexadecimal)

The subfields are defined as follows:

RR: Reporting Body Identifier. Currently restricted to the range A0 – FF. This ensures separation from the GSM International Mobile Equipment Identity (IMEI), which also uses a 56-bit space, but is restricted to BCD values only (i.e. 14 decimal digit representation). The RR values 00-99 can be used by dual-mode devices – in this case the IMEI and MEID will be the same value (the remaining digits of the MEID are also restricted to BCD values).

XXXXXX: Manufacturer code. In practice, this value has been segmented across multiple manufacturers for some existing assignments by treating the leftmost digit of the Serial Number as an additional digit.[17]

ZZZZZZ: Serial Number, assigned by the manufacturer (possibly within segmented range as above, in which the leftmost digit is treated as part of the Manufacturer code).

[17] Current assignment practices allow the identifier to be treated as if the Manufacturer Code was 9 (or more) digits long and the Serial Number only 5 (or fewer) digits long. This makes allocation more efficient for smaller manufacturers, with only one million (or fewer) numbers being assigned at a time instead of close to 17 million.

C: Check Digit for use when an MEID is printed (e.g. on packaging or on the exterior of an MS). The check digit is not part of the MEID and is not transmitted when the MEID is transmitted. It is calculated using the Luhn algorithm modified to use base-16 arithmetic when the MEID is in the hexadecimal range (RR=A0 – FF).

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

MEID administration is performed by the Global Hexadecimal Administrator (GHA). TIA currently serves as the GHA. Assignment of MEIDs with decimal RR codes is performed by administrators approved by the GSMA, including TIA in the range RR=99 and BABT in the range RR=35.

For more information, see the TIA website[18]. See [X.S0008] for information on the decimal representation of MEID, as well as checksum calculation details. The TIA produces a regular MEID Administrator's Report, available from the TIA EUMAG chair (Gary@CommFlowResources.com) and also on the 3GPP2 TSG-S FTP site.

3.3.2 Expanded UIMID (EUIMID)

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

- Short Form EUIMID (SF_EUIMID): The SF_EUIMID shares the same address space as the MEID. R-UIM card manufacturers are allocated MEID manufacturer codes in the same manner, and from the same range, as handset manufacturers. No identifier will be allocated as both an MEID and an SF_EUIMID.
- Long Form EUIMID (LF_EUIMID): This is equal to the value of the ICCID of the card. In practice this is the 20 digit/80 bit contents of EF_{ICCID} which will probably include a check digit and filler digit (0xf) as well as the ICCID which is probably 18 digits/72 bits in size.

When the SF_EUIMID is used, bit 2 of the Usage Indicator describes whether the SF_EUIMID of the card replaces the MEID of the device wherever it is used (see Figure 3-3).[19]

---

[18] http://www.tiaonline.org/standards/resources/meid/

[19] Strictly speaking, the Usage Indicator is only described in the standard as denoting MEID override in C.S0004 (radio interface), not C.S0016 (OTA). 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

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

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[20]) 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” of 0x80 to give the required 32-bit identifier and to ensure that there cannot be a conflict with any assigned codes that will never use the 0x80 prefix).

For more information, see RFC3174 (http://www.ietf.org/rfc/rfc3174.txt). Implementations of the SHA-1 hashing algorithm are freely available on the internet (e.g. http://www.slavasoft.com).

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_p 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.

---

[20] 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_{ICCID}, usually including the check digit and a filler digit (0xf).

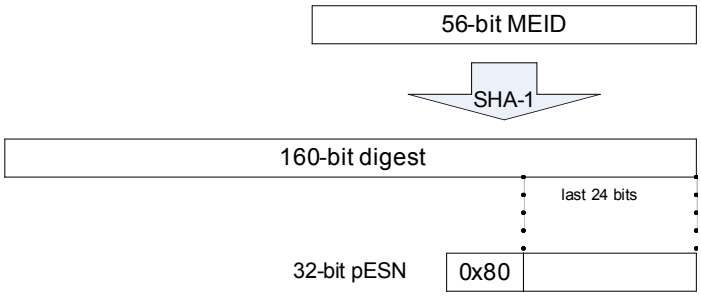

Figure 3-6 - Derivation of the pESN

Since there are more possible MEIDs than pESNs, more than one MEID will map to the same pESN[21]. By way of example, Table 3-1 below shows several pairs of MEIDs with a common pESN. It is this lack of uniqueness in the pESN that represents the main impact to operator networks and business processes. The likelihood of this kind of duplication occurring is discussed in Section 2.3 .

MEID1	MEID2	pESN
A0000000001BC2	A0000000003472	80003C21
A00000000000A6	A0000000003422	80066CDE
A0000000002277	A0000000003584	80270ABB

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

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

For more information, see [C.S0072]. A calculator including a pESN-generator and other related functions is available on the CDG website[22].

[21] Simple division, and an assumption of uniformity in the hashing function yields each pESN value being shared by ~1.6 billion MEIDs.

[22] http://www.cdg.org/devices/meid/meid_euimid_calculator.asp

3.4.3 Pseudo-UIMID (pUIMID)

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

The pUIMID is derived from the EUIMID in the same manner as the pESN is derived from the MEID (and therefore shares the same space as the pESN), as shown below:

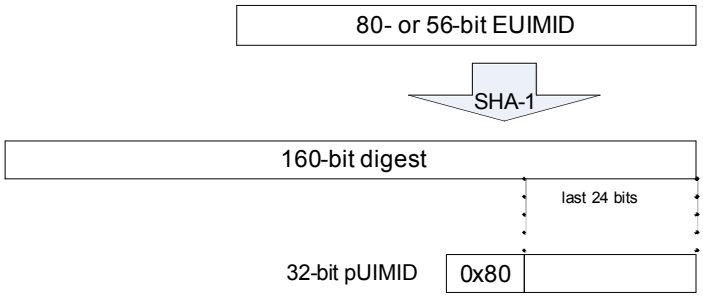

Figure 3-7 - Derivation of the pUIMID

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

LF_EUIMID-1[23]	LF_EUIMID-2[23]	pUIMID
89910010000000021981f	89910010000000081654f	80E7F275
89910010000000037789f	89910010000000116740f	809F9406
89910010000000087735f	89910010000000088642f	8059659C

Table 3-2 - Sample duplicate pUIMIDs

The pUIMID space is not segmented or administered in any way. Due to the behavior of the hash function, pUIMIDs derived from a specific EUMID range may occupy any part of the pUIMID address space. pUIMIDs and pESNs share the same address space: a pESN may clash with another pESN or a pUIMID. Table 3-3 below shows three examples of pESN – pUIMID clashes. The specific manufacturer code (0x80) ensures that a pUIMID will not clash with any true (unique) ESN or UIMID.

MEID	LF_EUIMID[23]	pESN/pUIMID
A0000000000D00	899100100000000 5182f	80B270AD
A0000000002559	899100100000008 1878f	802E9C53
A0000000002A85	899100100000003 9298f	808840E4

Table 3-3 - Sample pESN to pUIMID duplications

[23] Values are shown as stored in the R-UIM card with the 19th digit the check digit and the 20th digit the 0xf filler.

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 *MEID GHA Assignment Guidelines and Procedures*[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 the *Global Wireless Equipment Numbering Administration Procedures* [SC.R4001].

4.1.3 Billing

The Cellular Intercarrier 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.[24]

[24] CIBER is a proprietary protocol owned by MACH.

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.

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

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

Release E (September, 2009) was designed in a modular fashion (with some features not requiring P_REV changes) and allows access to the full range of hardware identifiers (MEID_ME and ESN_ME) and card identifiers (SF_EUIMID, LF_EUIMID and ICCID) via new record types in Status Request messages. These new capabilities can be safely implemented in devices otherwise conforming to older specifications.

4.1.4.2 Updates to earlier releases of IS-2000

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

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

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

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

- PLCM specified by the Base Station (BS-assigned)

- PLCM derived from IMSI (2-types)
- PLCM derived from MEID

Of these types, IMSI-based PLCMs have limitations on their use for roamers from other networks, and MEID-based PLCMs require extra messaging (to retrieve the MEID from the MS before the PLCM can be assigned) and are not guaranteed to be unique (as the MEID length is greater than that of the PLCM). Therefore the recommended approach, and the one assumed throughout this document, is BS-assigned PLCM. The IMSI and MEID PLCM types may be useful on system borders the complexity of synchronizing the PLCM usage with BSs of another operator may be greater than the tiny risk of collisions.

All MEID-equipped devices are expected to support C.S0072 (i.e. there should be no devices launched with MEIDs that do not support the new messaging in C.S0072). Some R-UIM capable devices are known to exist which have MEIDs, but set SCM bit 4 to 0. This behavior is not recommended, and can lead to PLCM collisions when EUIMID-equipped R-UIMs are used that cannot be resolved even when all base stations are upgraded to support C.S0072.

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

4.1.4.3 1xEV-DO Revision A

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

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

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

Table 4-1 - EVDO HardwareIDType values

Note that only the ESN and MEID are defined for inclusion in the HardwareID field. C.S0024-B v3.0 (September, 2009) clarifies that even when an R-UIM or CSIM is inserted in an EV-DO device that the ESN or MEID should continue to be transmitted, not the UIMID or EUIMID. There is no concept of a pESN in EV-DO – an MEID device will return the MEID as its HardwareID.

4.1.5 ANSI-41 MAP Updates

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

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

X.S0008 also adds messaging to enable Equipment Identity Register (EIR) functionality, which provides functions such as combating device theft by checking the MEID against a list of known stolen devices or comparing with a list of problematic devices. A generic request message that can be used to order retrieval of the MEID from the MS is also added. This capability is effectively disabled if the Short Form EUIMID replaces the hardware MEID in air interface signaling unless the MEID_ME Status Request information record from CDMA2000 Release E is implemented.

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

4.1.6 Over-the-Air Activation

Over-the-Air activation is affected by the migration away from ESN, because ESN is often used as the only unique identifier for an unprovisioned mobile. When a non-unique pESN is provided a mechanism to obtain a unique identifier to ensure the correct device is being provisioned is needed.

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

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

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

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

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

4.1.7 Interoperability and Testing

4.1.7.1 CDMA2000® Access Network Interoperability

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

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

See [MEID Failure Bulletin] for a potential service-affecting issue related to the interpretation of SCM bit 4 on this interface. The only known occurrence of this problem was resolved in 2010.

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

4.1.7.2 HRPD Access Network Interoperability

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

4.1.7.3 CDMA2000® Signaling Testing for MEID

[C.S0073] provides a signaling test specification for MEID equipped CDMA2000® mobile stations. Revision A of this specification (April, 2008) included test sequences for MEID mobile stations with an R-UIM inserted, when EUIMID is the card identifier.

4.1.7.4 CDMA2000® Wireless IP Network Standard

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

4.2 Expanded UIMID (EUIMID)

4.2.1 Requirements

3GPP2 TSG-S report **Error! Reference source not found.** provides the Stage 1 requirements for the EUIMID. Note that only C.S0016-C v2.0 and C.S0066-0 v2.0 contain the capabilities to fully satisfy all the requirements for OTAPA/OTASP and CDMA2000 Release E contains all the capabilities to fully satisfy all the air interface protocol requirements.

4.2.2 Administration

3GPP2 Steering Committee report [SC.R4003] describes the administration procedures of the EUIMID, both short-and long-form. The document essentially devolves LF_EUIMID administration to the existing ITU-T ICCID process, and SF_EUIMID administration to the MEID administration process.

4.2.3 CDMA R-UIM

[C.S0023] defines the capabilities of the CDMA Removable User Identity Module (R-UIM). Revision C added, among other things, a description of the Long Form (LF) and Short Form (SF) EUIMID (see Section 3.3.2). This specification was updated in C.S0023-C v2.0 to clarify the storage order of the SF_EUIMID and describe how the pUIMID is calculated from the LF_EUIMID (ICCID).

4.2.4 CDMA SIM Application

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

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

[C.S0065] was updated in July 2008 (C.S0065-0 v2.0) to clarify the storage order of 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, and is equal to the existing ICCID of the card[25]. 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_{RUIMID} file on the card, and operate as LF_EUIMID cards[26]. There are no new requirements on devices to support LF_EUIMID unless access to the identifier is required. PLCM collisions are possible if the device in which the card is inserted does not support C.S0072.
- **EIR Support**. Since the device MEID (if present) remains available to the network, use of LF_EUIMID allows easier implementation of an EIR to track/block lost/stolen devices.
- **Retrievable During Provisioning.** If C.S0016-C v2.0 or C.S0066-0 v2.0 is implemented in mobiles and in the OTAF the LF_EUIMID will be available during provisioning with OTASP.

---

[25] In practice the full 80 bit value contained in the R-UIM field EF_{ICCID} is used, which includes a check digit and filler digit (0xf) in addition to the ICCID.

[26] 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.

- **Retrievable At Other Times.** If the appropriate components of the CDMA2000 Release E air interface are implemented by both the RAN and the ME it is possible to retrieve the LF_EUIMID using a Status Request message.

Disadvantages:

- **Not retrievable**. The LF_EUIMID is only retrievable from the card via messaging in C.S0016-C v2.0 (October, 2008), C.S0066-0 v2.0 (July, 2008) and CDMA2000 Release E (September, 2009). It may also be accessible through the CDMA Card Application Toolkit (CCAT, see Section 5.3 below). If not available, there may be an impact on OTASP sessions, where (depending on operator implementation) a unique card identifier may be needed to access card-specific information.
- **Long Identifier**. The 72-bit ICCID, if used to track the card (e.g. from a logistics perspective), will require separate handling from the device MEID. As a longer identifier it is also arguably more prone to keying errors (although a check digit mechanism is also defined for ICCIDs).
- **Issuer Identifier Number (IIN) Limitations**. Countries with 3 digit telephony country codes (as defined in ITU-T E.164) are restricted to only 100 unique IINs. Countries with 2 digit country codes have 1000 unique IINs and those with 1 digit country codes (e.g. North America and the Caribbean) have 10,000 IINs available. This is only a minor limitation because the IIN is generally assigned to an operator, which then assigns arbitrary sized subsets to their R-UIM suppliers.

5.2 Short-Form EUIMID

The SF_EUIMID is a 56-bit identifier, sharing address space with the MEID. An R-UIM indicates its use of SF_EUIMID via service n8 in the CDMA Service Table[27]. An additional option is available with use of the SF_EUIMID, namely the setting of bit 2 of the Usage Indicator octet. When the bit is set to 0 (SF_EUIMID does not override the ME's MEID), use of the SF_EUIMID shares the disadvantages but not the advantages of the LF_EUIMID – it is not retrievable from the card without support for C.S0066-0 v2.0, C.S0016-C v2.0 or CDMA2000 Release E, yet it requires new storage and handling capabilities. One benefit – that of using a common identifier size to track both cards and devices – does not seem sufficient to warrant the use of this configuration. Accordingly, the advantages and

[27] See C.S0023-C Section 3.4.18

disadvantages listed below assume the Usage Indicator bit 2 is set to 1 – i.e. the SF_EUIMID is used in place of the ME MEID.[28]

Advantages:

- **Familiarity**. Use of the SF_EUIMID represents a minimum change from current operation, where the UIMID overrides the device ESN.
- **Retrievable**. The unique SF_EUIMID is available from the MS in either the *Status Response Message*, or the *Extended Protocol Capability Response Message* (both methods require the device itself to have an MEID).
- **Common Identifier**. Both the card and the device can be managed by a commonly formatted and administered 56-bit identifier. (Although both the MEID of the device and the SF_EUIMID of the R-UIM are only available via air interface signaling if C.S0016-C v2.0. C.S0066-C v2.0 or CDMA2000 Release E is implemented.)

Disadvantages:

- **Card/device requirements**. The SF_EUIMID is defined in C.S0023-C v2.0 and C.S0065-0 v2.0. Cards and devices which do not support this level of either standard (or at least, this aspect of this level of the standard) will not be able to override the device MEID. Many R-UIM-based devices in commercial use today do not support C.S0023-C v2.0.
- **No EIR**. Since the device MEID is unlikely to be transmitted to the network by legacy mobiles, it may not be feasible to take advantage of the new X.S0008 CheckMEID operation to track lost, stolen or malfunctioning phones through communications with an EIR.

5.3 CDMA Card Application Toolkit (CCAT)

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

[28] 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.

Similarly, the ME's MEID could be sent to the network even if normally overwritten by the SF_EUIMID[29]. The equivalent note applies to other references in this document to the inaccessibility of this value to the network.

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

5.4 Device Compatibility with EUIMID

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

[29] 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.

6. Recommendations

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

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

6.1 Operators with non-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 pESN-based PLCM, and also allows the MEID to be retrieved from the device.
- **Do not hash check at the BS/MSC.** Hash checking implies verifying that the received “MEID” value will hash to the received “ESN” value. While this may be a valid assumption for the operator’s own subscribers, it may not hold true for inbound roamers present on the operator’s network (e.g. if they use LF_EUIMID, or a unique UIMID, the UIMID/pUIMID will not be hash-related to the ME MEID). Although such checking is not believed to be common, if implemented it may erroneously deny service to a valid subscriber.
- **Stop ESN-based addressing on paging channel**. Duplicated pESNs 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.
- **Remove network element and back-end dependency on unique ESN**. The specific actions will depend on the operator’s systems, and may apply to HLR, VLR, billing, provisioning, fraud systems etc. Either the uniqueness check may be relaxed, or the check may be applied to the MEID instead (assuming MEID is reliably available at the necessary location).

- **Support C.S0066 for OTASP**. If OTASP is used in the operator's network, and there is a need to reference device-specific information (e.g. A-key, SPC) during the OTASP process, then C.S0066-0 v2.0 should be supported to allow the MEID to be transferred to the OTAF.
- **Index OTASPCallEntry by Activation_MIN**. The use of Activation_MIN allows concurrent OTASP sessions for mobiles with the same pESN.
- **Evaluate X.S0008 support**. Operators may choose to implement X.S0008 (MEID for ANSI-41) in their networks. This can be of use for stolen phone scenarios, and in general allows a unique device identifier to be stored in the HLR.
- **Evaluate MEID inclusion in CDRs**. Operators may choose to include MEID in their MSC billing records, with associated upgrades to the billing.

  Note: The previous two recommendations both require retrieval of the MEID over the air interface, at some small capacity cost. Some vendors may automatically initiate MEID retrieval whenever the MS indicates it has an MEID.
- **Ensure Uniqueness of NAIs**. Network Access Identifiers (NAIs) derived from the ESN should be replaced with a unique alternative, such as MEID-derived NAIs (e.g. MEID@realm).
- **Check support for MEID in PCF, PDSN and AAA.** The airlink record sent between the PCF and PDSN, and used to form the PDSN UDR that is sent to the AAA, contains either MEID or ESN. While pESN may be used in non-upgraded 1X systems, the pESN is not available in EVDO unless it is calculated from the MEID.
- **Add support for MEID as EVDO** Hardware ID. Operators who use the Hardware ID in A12 authentication should ensure that MEID is supported as per A.S0008-A.
- **Outbound Roaming Support**. Operators should recognize that not all roaming partners will necessarily support the MEID/EUIMID migration to the same degree. MEID inclusion should not be mandatory (from the perspective of the receiving entity and any subsequent processing) on any inter-network interface, including:
  - ANSI-41 Interfaces
  - CIBER Records
  - A12 Authentication

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

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

- **Unique pESNs.** If operators are struggling to accommodate duplicate pESNs in the required timeframe, a potential mitigation approach is to require only unique pESNs be delivered to them from handset manufacturers. This is a last resort action only, and is discouraged for the following reasons:
  - It may distract operators from properly addressing the required updates
  - It may impose an unreasonable management burden on handset manufacturers, and cause them to "waste" large numbers of MEIDs[30].
  - It becomes progressively more difficult to implement as the number of deployed pESNs rises.
  - Only ~16.7 million different pESNs are available – beyond this uniqueness is not possible.
  - Collisions or duplications due to roamers are not addressed – these may still occur beyond the operator's control.
  - It is only possible with handsets purchased by the operator.
- **Authentication.** S.S0053-0 v2.0 specifies that authentication operations specify ESN, including in CAVE calculations and A-Key checksum generation, pESN should be used instead. There is no loss of security even though this input may not be unique.

[30] 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.
- **Do not hash check 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 will not 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).

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

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

  The lack of a unique identifier may also prompt operators to implement PIN-or PRL-based methods to ensure that the activation is completed to the correct operator.
- **Index OTASPCallEntry by Activation_MIN**. The use of Activation_MIN allows concurrent OTASP sessions for mobiles with the same pUIMID.
- **Evaluate X.S0008 support**. Operators may choose to implement X.S0008 (MEID for ANSI-41) in their networks. This can be of use for stolen phone scenarios (with LF_EUIMID), or to allow a unique card identifier to be stored in the HLR (with SF_EUIMID). Implementation of an Equipment Identity Register is at the operator's discretion.
- **Evaluate MEID/SF_EUIMID inclusion in CDRs**. Operators may choose to include MEID/SF_EUIMID in their MSC call detail records, with associated upgrades to the billing system to parse this new record.

  Note: The previous two recommendations both require retrieval of the MEID/SF_EUIMID over the air interface, at some small capacity cost. Some vendors may automatically initiate MEID/SF_EUIMID retrieval whenever the MS indicates it has an MEID and the system has not recently retrieved it.
- **Check support for MEID in PCF, PDSN and AAA.** The airlink record sent between the PCF and PDSN, and used to form the PDSN UDR that is sent to the AAA, contains either MEID or ESN. While pESN may be used in non-

upgraded 1X systems, the pESN is not available in EVDO unless it is calculated from the MEID.

- **Ensure Uniqueness of NAIs**. Network Access Identifiers (NAIs) derived from the UIMID should be replaced with EUIMID-derived NAIs (e.g. EUIMID@realm).
- **Add support for MEID as EVDO Hardware ID**. Operators who use the Hardware ID in A12 authentication should ensure that MEID is supported as per A.S0008-A. The Hardware ID is either ESN_ME or MEID_ME, never UIMID or EUIMID.
- **Outbound Roaming Support**. Operators should recognize that not all roaming partners may support the MEID/EUIMID migration to the same degree. MEID/SF_EUIMID inclusion should not be mandatory (from the perspective of the receiving entity and any subsequent processing) on any inter-network interface, including:
    - ANSI-41 Interfaces
    - CIBER Records
    - A12 Authentication
    - **CIBER Record Population**. Assuming both a 32- and 56-bit identifier are captured in the MSC CDR (which may be either ESN/pESN/UIMID/pUIMID or MEID/SF_EUIMID respectively), it is recommended that the 32-bit identifier be included until it is either verified that all roaming partners support MEID or SF_EUIMID in CIBER records or the system is capable of storing the capability of every roaming partner individually.
- **Unique pUIMIDs.** If operators are struggling to accommodate duplicate pUIMIDs in the required timeframe, a potential mitigation approach is to require only distinct pUIMIDs be delivered to them from R-UIM manufacturers. This is a last resort action only, and is discouraged for the following reasons:
    - It may distract operators from properly addressing the required updates
    - It may impose an unreasonable management burden on R-UIM manufacturers, and cause them to “waste” large numbers of EUIMIDs[31].
    - It becomes progressively more difficult to implement as the number of deployed pUIMIDs rises.
    - Only ~16.7 million different pUIMIDs are available – beyond this uniqueness is not possible.

[31] 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.** S.S0053-0 v2.0 specifies that everywhere that authentication
4 operations specify ESN, including in CAVE calculations and A-Key checksum
5 generation, UIMID should have been used in R-UIM devices. Now, pUIMID
6 should be used instead. There is no loss of security even though this input
7 may not be unique.

8

7. Scenarios

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

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

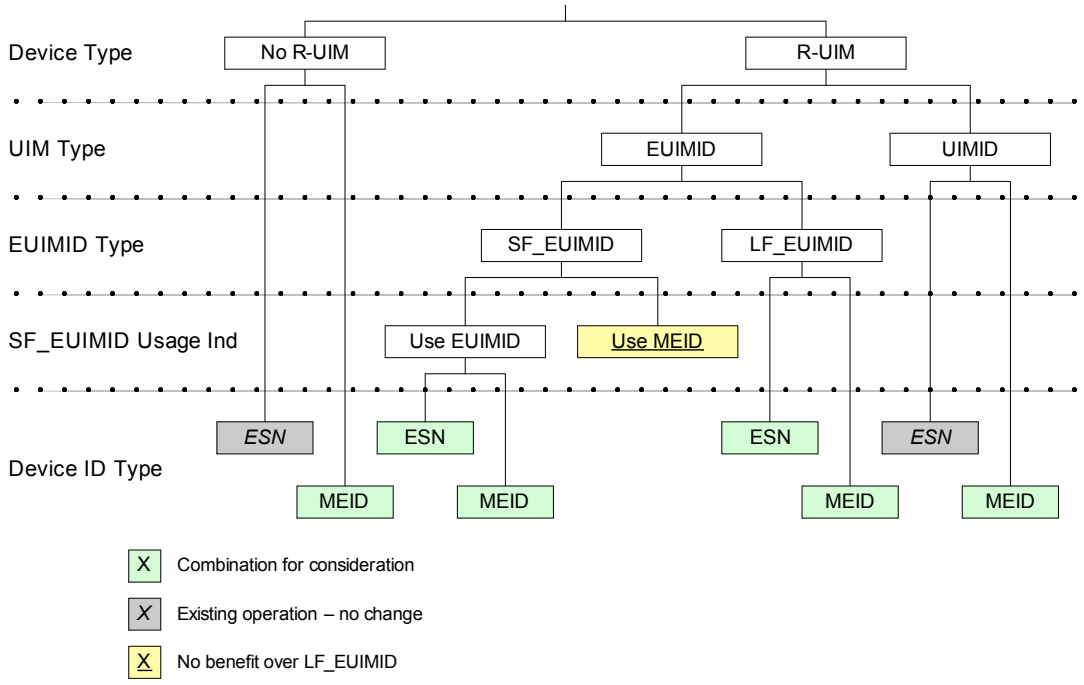

Figure 7-1 - Device & Card Combinations

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:

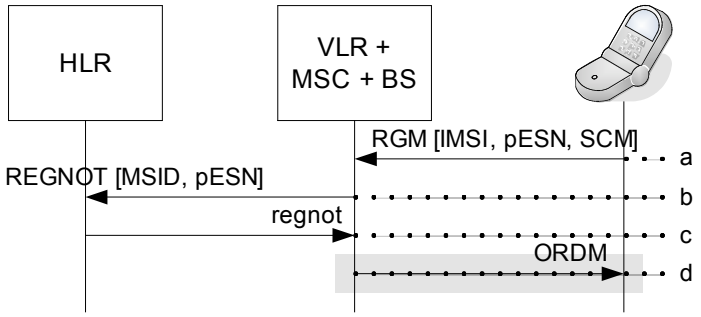

Figure 7-2 - MEID MS Registration - no X.S0008 support

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 although some HLRs are known to reject REGNOT messages with a pESN that matches a pESN that is already stored. The HLR returns the subscriber profile to the MSC.

d) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.2.1.2 Registration – X.S0008 supported

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

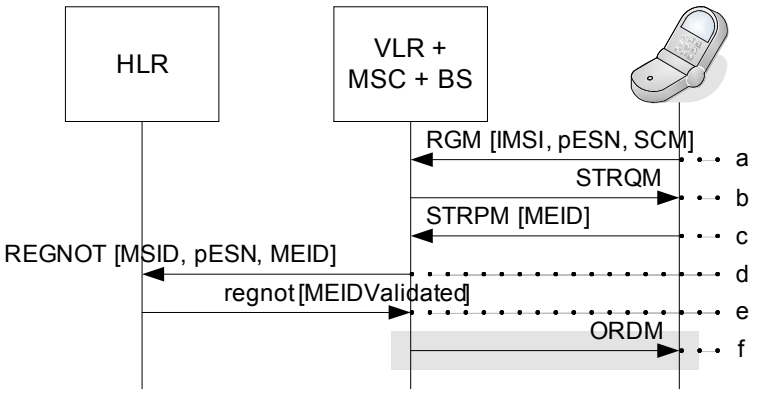

Figure 7-3 - MEID MS Registration - X.S0008 supported

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) Based on the SCM, the MSC recognizes that the mobile has a MEID, and that the MSC does not know this value. It solicits the MEID via the *Status Request Message* (new Information Record in C.S0072).

c) The MS returns its MEID in the *Status Response Message*

d) The MSC sends a RegistrationNotification to the HLR, including the MSID, pESN (required for backwards compatibility) and the MEID.

e) Text extracted from X.S0008: “Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the REGNOT, the HLR includes an MEID comparison in the validation of the subscription. The HLR then registers the indicated MS and returns a regnot to the Serving VLR. The regnot includes the MEIDValidated parameter to inform the Serving VLR/MSC that the MEID associated with the system access has been validated.”

f) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.2.1.3 Authentication

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

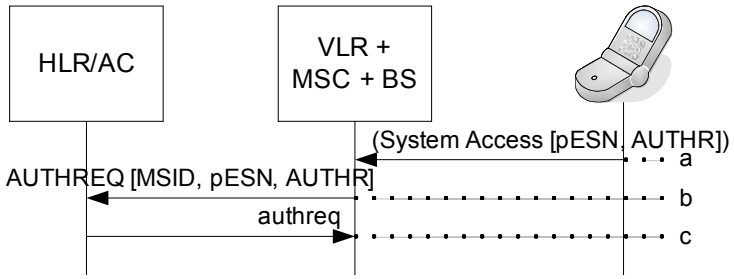

Figure 7-4 - Authentication of MEID device

Steps are as follows:

a) MS makes a system access. It includes its pESN and the Authentication Response parameter (other authentication-related information and SCM not shown).

b) The MSC determines it needs to request authentication at the HLR/AC (e.g. SSD is not shared, or this is the first system access). The MSC sends an AuthenticationRequest to the HLR/AC. MEID may also be requested by the MSC and included in the AUTHREQ.

c) The AC computes the challenge result and compares it with the received response. The pESN is used in the calculation, but not the MEID, even if it is received. The HLR/AC returns an authreq to the MSC to advise that the challenge was successfully passed.

An Authentication scenario not involving signaling is the calculation of the 6-digit checksum used when entering the A-key manually via the handset keypad. The algorithm is defined in S.S0053[32], where the A-key and the ESN are used as inputs. This standard makes no mention of MEID. At least one operator is known to have specified MEID to replace pESN as the input to this algorithm but S.S0053-0 v2.0 clarifies that the same value used for CAVE authentication should be used (i.e. pESN).

[32] http://www.3gpp2.org/Public_html/specs/S.S0053-0_v2.0.pdf

7.2.1.4 Call Origination/Termination

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

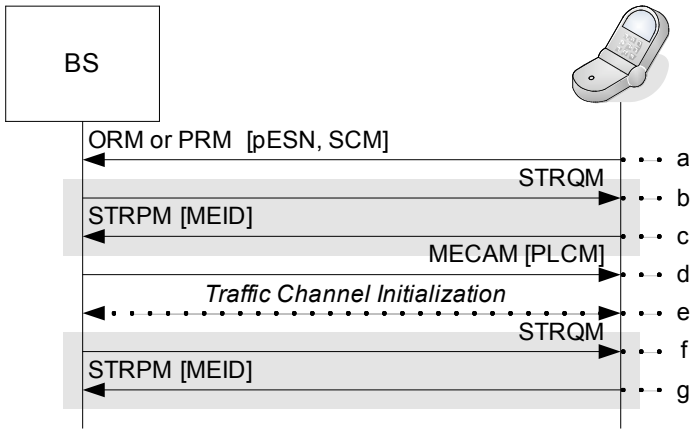

Figure 7-5 - MEID Origination/Termination

Steps are as follows:

a) The MS sends an *Origination Message* or a *Page Response Message*, including its pESN and SCM

b-c) Optionally, the MSC queries the MEID via a *Status Request Message* over the paging channel, and the MS responds. This would be required if the MSC used the MEID-based PLCM type.

d) Since the MS has advertised that it has a MEID via the SCM, the MSC sends an *MEID Enhanced Channel Assignment Message* (new for C.S0072). The message includes the PLCM_TYPE field, and (if the PLCM_TYPE indicates BS-assigned) the PLCM itself.

e) The traffic channel is initialized as normal, using the PLCM as agreed above

f-g) Optionally, the MSC can query the MEID via a *Status Request Message* sent on the traffic channel, and the MS responds.

7.2.1.5 Billing Record Production

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

7.2.1.6 Mobile Terminated SMS

This scenario shows an undesirable result of a message addressed by ESN only. Even with C.S0072 support in the network, this effect can still occur. The *Data Burst Message* used to carry the SMS is only one example of a message that could be addressed in this way – see Section 2.1.3 for more details. The steps are shown in Figure 7-6 below - in this diagram, MS1 and MS2 are both in the same sector:

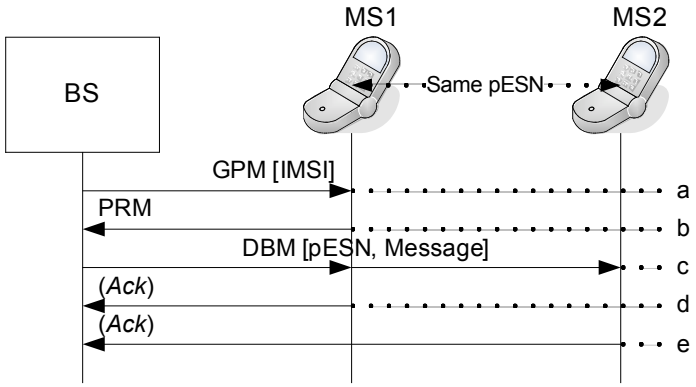

Figure 7-6 - ESN-based addressing conflict

Steps are as follows:

a) The BS sends a *General Page Message* (GPM) to alert the mobile that there is an SMS message for it. The GPM is addressed to the IMSI of the mobile for whom the SMS is intended (MS1). This message is typically sent over a wide area in order to find the mobile.

b) MS1 responds to the page.

c) The BS sends a *Data Burst Message* (DBM) containing the SMS. The DBM is typically sent only on the sector on which the MS responded to the page. In this example, the message length is such that the network chooses to send it on the paging channel, rather than establishing a traffic channel, and the message is addressed using the “ESN” address type. The value in the ESN field is the pESN, which happens to be common to both MS1 & MS2. *Both mobiles receive the text message*.

d-e) Both mobiles send an acknowledgment.

Note that the alternative addressing (IMSI-based) may be susceptible to a similar problem if the operator sends *Data Burst Messages* on the paging channel, but this requires that a mobile is provisioned with the IMSI of a mobile it wishes to receive text messages for and must remain in the vicinity of the target mobile. Legitimate mobiles will not receive IMSI-addressed text messages destined for other mobiles as only one mobile will ever be the legitimate holder of an IMSI at any one time. The most likely scenario where multiple delivery will be found is when a subscriber purchases a new phone and, while the old phone is still powered on and in the vicinity of the new phone, notices that SMS messages are still received by their old phone.

7.2.1.7 Handoff

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

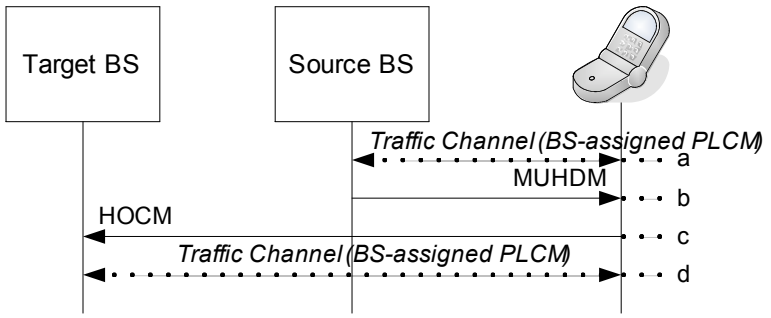

Figure 7-7 - MEID Handoff

Steps are as follows:

a) The MS is operating on a traffic channel in communication with the source BS. AS per Section 7.2.1.4 , the MS uses a BS-assigned PLCM.

b) The source BS sends a MUHDM. This message can include the PLCM type if it is to be changed, or omit it to retain the same PLCM.

c) The MS sends a *Handoff Complete Message* to the Target BS.

d) The traffic channel is established with the new BS.

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

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

Target BS ➔ Source BS ⬇	No C.S0072 Support	C.S0072 Support
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

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

7.2.2 Data Services

7.2.2.1 CDMA2000® Packet Data

Some operators use a Network Access Identifier (NAI) of the format ESN@realm. Default provisioning of this value should be changed to a unique value, such as MEID@realm.

Origination and PLCM assignment is as for voice.

Either MEID or pESN (or both) is included in the airlink record sent from the PCF to the PDSN[33], and included in the PDSN UDR sent to the AAA. If MEID is sent, the receiving entity must be capable of accepting it (and if the pESN is absent the receiving entity must not consider it required).

7.2.2.2 1xEV-DO Packet Data

An AT can provide its Hardware ID in response to a HardwareIDRequest Message. When the AT is provisioned with an MEID, it will include this value as its Hardware-ID, with a specific HardwareIDType.

In order to include this identifier on the A12 interface, the AN must recode the HardwareIDType to the value specified in A.S0008-A. In other words, the AN cannot simply pass the information received from the AT transparently – it must explicitly understand the “MEID” HardwareIDType, and recode this to the “Type of Identity” coding for MEID, as specified in A.S0016-C (referenced from A.S0008-A Annex E) in order to build a properly formatted A12 message.

Only the MEID is available to be included into an airlink record and subsequently into the PDSN UDR (assuming derivation of the pESN is not performed). The PCF, PDSN and AAA must all be capable of receiving the MEID instead of an ESN field.

7.2.2.3 Other Applications

Any applications (e.g. Java, LBS, MediaPlayer for DRM etc) that today use ESN as a unique equipment identifier should be modified to use MEID instead. In the event that the application uses IMSI, or IMSI+ESN as a unique (subscriber and/or equipment) identifier, this scheme can be retained with the move to MEID.

---

[33] See A.S0017-C v2 sections 2.3 and 4.2.13, and X.S0011-005-D v1 section 3.2.1

7.2.3 Lost/Stolen Phone

A subscriber whose phone has been lost or stolen typically contacts Customer Service from an alternate number. Assuming the subscriber's identity is verified satisfactorily, the HLR subscription may be call-barred to prevent charges to the subscriber's account.

To prevent the stolen phone later being reprogrammed with a new number, the ESN is typically logged as stolen in the provisioning system. For an MEID-equipped device, the MEID should be logged instead (since using the pESN may incorrectly affect other, legitimate phones with the same pESN). This implies that the MEID of the device must be known to the network – possible mechanisms for this include:

- Recording the MEID at the point of sale
- Recording the MEID during an OTASP session (see Section 7.2.4)
- Capturing the MEID in billing records (see Section 7.2.1.5)
- Support of [X.S0008] and provisioning of the MEID in the HLR
- Support of X.S0008 and implementation of an Equipment Identity Register (see Section 7.3.3)

7.2.4 Over the Air Service Provisioning

Over-the-air Service Provisioning (OTASP) is a process by which a prospective subscriber buys a new, unprogrammed device, and has the necessary information (e.g. IMSI) downloaded to the device while making a call to the Customer Service Center (CSC).

At the start of the programming session, the MEID may be the only unique identifier available for the device.

Figure 7-8 shows a simplified typical message flow for an OTASP call. For more detail see IS-725-A[34]. Note that the exact steps are to some extent implementation-dependent, and will depend on the way the operator has integrated the OTAF and the OTASP sales channel into their business processes.

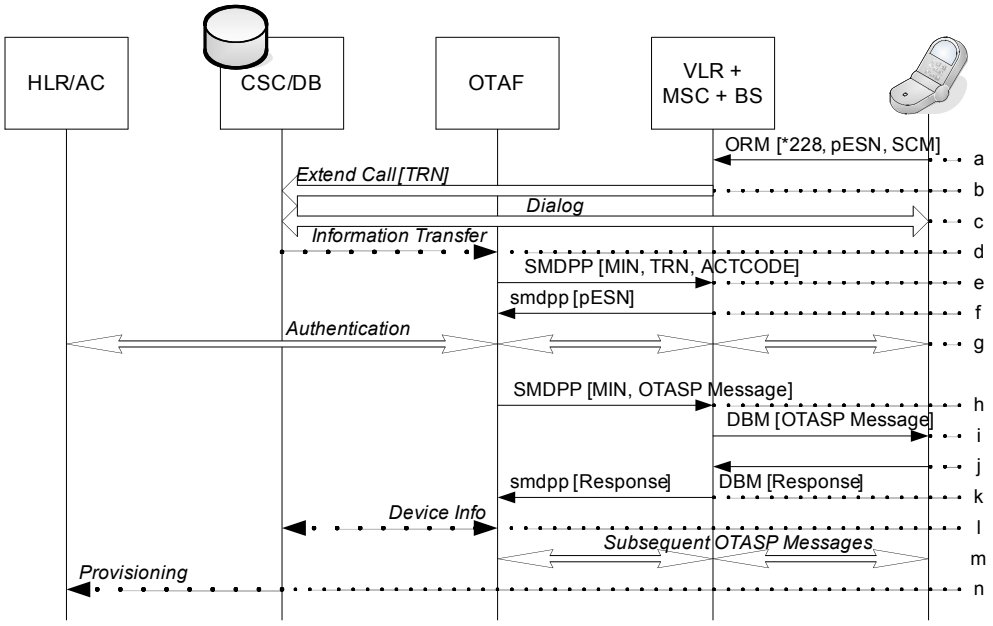

Figure 7-8 - OTASP Data Flow

Steps are as follows:

a) The MS originates a call to the OTASP feature code (typically *228), including its pESN and SCM as with other originations

b) Recognizing the OTASP code, the MSC assigns a Temporary Reference Number (TRN) from a pool and sets this as the Calling Party Number (CgPN). It extends the call to the CSC.

[34] http://www.3gpp2.org/Public_html/specs/N.S0011-0_v1.0.pdf

c) The CSC (shown here co-located with a provisioning database for simplicity) answers the call. The prospective subscriber may enter into a dialog with a Customer Service Representative, or an automated system. Subscribers provide sufficient information (e.g. credit card number, or code allocated at point of sale) to allow the operator to authorize them for service.

d) The CSC provides the TRN to the OTAF.

e) The OTAF sends a SMDPP to the MSC. The message includes the TRN (to identify the call in progress), and a temporary Activation_MIN assigned by the OTAF.
Note: At this point, the OTAF has no knowledge of the device MEID, or even the pESN. If two handsets with the same pESN made simultaneous OTASP calls, the OTAF would still be able to distinguish them based on the TRNs assigned by the MSC, and assign unique Activation_MINs.

f) The MSC returns the pESN of the device. Optionally, if the network requested the device MEID via an earlier STRQM, the MEID could be included here as per X.S0008/X.S0033. Note however that the MEID can be transferred to the OTAF without the need for X.S0008 or X.S0033 (see below). Another SMDPP at this point (not shown) releases the TRN back into the MSC's pool. From this point the Activation_MIN is used to identify the call.

g) Optionally, the OTAF may, in conjunction with the HLR/AC, instruct the MS to generate a new A-key. The same A-key value is securely generated in both the AC and MS so that it does not need to be transferred over the air.

h) The OTAF sends an SMDPP containing an OTASP *Protocol Capability Request Message*. Based on the presence of a pESN (identifiable by its manufacturer code), the OTAF includes in the message a request for the MEID.

i) The MSC passes the message on to the MS encapsulated in a DBM.

j) The MS returns its MEID (together with other capabilities requested)

k) The MSC returns the MEID to the OTAF. The MEID is embedded in the SMS_BearerData of the smdpp and does not explicitly require ANSI-41 / IS-725 modifications.

l) The OTAF may query a database for information about the device, for example the Service Programming Code (SPC). The contents of the database are typically provided by the handset manufacturer, and are indexed by ESN/MEID (but should not be indexed by pESN).

m) Multiple SMDPP/DBM messages may be used to program the desired IMSI, download Preferred Roaming List information, and other tasks. At the conclusion of the OTASP session, the Activation_MIN is released for re-use.

n) The CSC (via the provisioning system) creates an entry in the HLR to match the information in the device just programmed. The entry associates a MIN/IMSI with the pESN and/or MEID. If the A-key has not been generated during the OTASP session, a pre-programmed value may be retrieved from

the device information database. Again, a unique device identifier is required here to ensure the correct record is retrieved.

IS-725-A (3GPP2 N.S0011-0) defines the temporary call record that may exist during an OTASP session at any/all of the MSC, VLR, HLR or AC, and names it the OTASPCallEntry. The standard provides several methods to identify this record, including the Activation MIN and the ESN (extended by X.S0033 to include MEID). The identifier needs to be unique, so ESN is not recommended as a method. Use of MEID requires X.S0008/X.S0033 support in the network.

7.2.5 Roaming

The following scenarios describe cases when a device is not in its home network. Due to varying levels of operator readiness, network support for MEID-equipped mobiles may be different in the visited network to that experienced at home, and expected by other elements in the home network. More information is available in [CDG Ref Doc 137].

7.2.5.1 Outbound Roaming

The following scenarios may occur when an operator's MEID-equipped devices roam into another network:

- **No support for MEID devices**. One network was identified which could not serve MEID-equipped mobiles at all. It was upgraded in 2010 but it is possible that other networks with similar problems may exist. See the [MEID Failure Bulletin] for more detail.
- **No C.S0072 support in visited network**. If the visited network does not support C.S0072, the roamer may be at risk of PLCM collisions. Collisions, although very rare, could occur with other roamers, or with the visited network's own subscribers (e.g. if the serving operator had chosen to deploy only unique pESNs for its own subscribers – see Section 6.). Furthermore, the MEID will not be available on any interface.
- **No X.S0008 support in visited network**. Even if C.S0072 is implemented, the visited network may not support the transfer of the MEID in ANSI-41 messages. Alternatively, the home network may not support X.S0008, but the serving network does, and MEID is received unexpectedly in inter-network messages. This should have no consequences as long as unrecognized parameters in ANSI-41 are properly ignored, and as long as MEID-capable networks properly treat MEID as an optional parameter.
- **MEID presence in CIBER.** The CIBER record contains only one field for MEID or pESN. Different roaming partners may populate this field differently. It is therefore recommended that MEID be accepted but that the field is populated with pESN as long as any roaming partners perform MIN/ESN validation.
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pESN) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.
- **MEID in 1X Packet Data UDR.** The MEID may be included in the UDR instead of the ESN, or vice versa, which may differ from the home operator's own network practice.

7.2.5.2 Inbound Roaming

An operator serving roamers from other networks has no control over the deployment timeframe and options implemented by the home operator – the roamers could be using R-UIMs equipped with UIMIDs or EUIMIDs even if the serving operator's own subscribers only use non-R-UIM devices. The relevant issues are addressed in the Outbound Roaming sections of the various operator configurations.

Assuming the serving operator has already deployed MEID-equipped devices and C.S0072 support, inbound roamers with pESN/pUIMID should not cause issues for the serving operator. Communication and negotiation with roaming partners may be useful to address the implementation differences described in Section 7.2.5.1 .

7.3 R-UIM Operator – existing R-UIM in MEID device

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. Here, an existing R-UIM with a unique UIMID has been inserted into a new, MEID-equipped device.

7.3.1 Basic Operation

7.3.1.1 Registration – No X.S0008 support

Without support for X.S0008, this scenario is indistinguishable at the HLR from the existing case (i.e. unique UIMID in unique ESN device). The steps are shown in Figure 7-9:

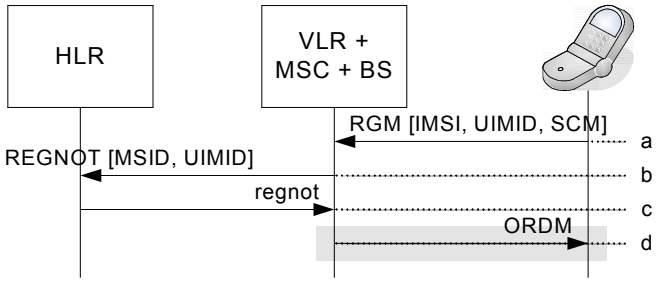

Figure 7-9 - UIMID Registration - no X.S0008 support

Steps are as follows:

a) MS sends a *Registration Message*, including its IMSI, UIMID, 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 UIMID and the Mobile Station Identity (MSID – either MIN or IMSI)

c) The HLR validates the subscription on the basis of MSID-UIMID. This is the same information the HLR receives if the subscriber had inserted their R-UIM in an ESN-equipped device. The HLR returns the subscriber profile to the MSC

d) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.3.1.2 Registration – X.S0008 supported

When the serving network does support X.S0008, the MEID can be included in the REGNOT. The ability to receive information relating both to the card and the device is new: the device ESN is not available to the HLR today. The steps are shown in Figure 7-10:

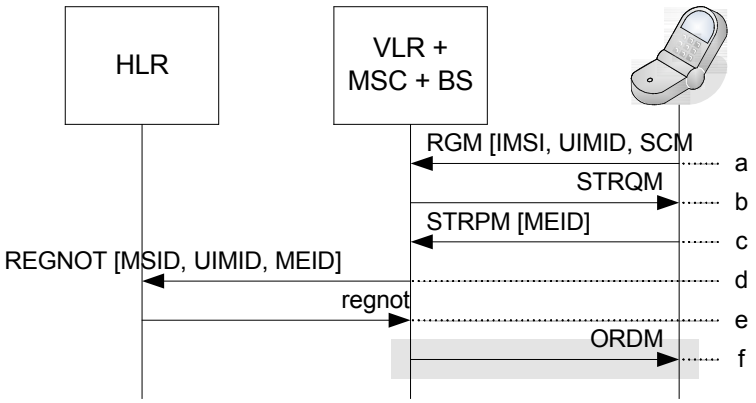

Figure 7-10 - UIMID Registration - X.S0008 supported

Steps are as follows:

a) MS sends a *Registration Message*, including its IMSI, UIMID and Station Class Mark set to indicate MEID support. The MS cannot include its MEID in this message.

b) Based on the SCM, the MSC recognizes that the mobile has a MEID, and that the MSC does not know this value. It solicits the MEID via the *Status Request Message.*

c) The MS returns its MEID in the *Status Response Message.*

d) The MSC sends a RegistrationNotification to the HLR, including the MSID, UIMID, and the MEID. The UIMID is not hash-related to the MEID, so no checking should be performed by the MSC to ensure this.

e) The HLR will presumably not track the MEID value, as the subscriber may transfer the R-UIM to another ME at any time (although it may be recorded to assist in a future lost/stolen report – see Section 7.2.3). In any case, the HLR should not perform a hash-relation check between the two values. Even if the HLR supports X.S0008, it will not include the MEIDValidated parameter in the regnot.

f) Optionally, the BS sends a *Registration Accepted Order* to the MS. Since the MEIDValidated parameter was not present in the regnot, the MEID retrieved from the mobile in step c is not used by the MSC in validating subsequent system accesses.

7.3.1.3 Authentication

Authentication is unchanged from existing operation. The UIMID is used as an input to various CAVE computations. The MEID may be included in various network operations if X.S0008 is supported, but it is not used as an authentication input.

7.3.1.4 Call Origination/Termination

Although the traditional (in this case UIMID-based) PLCM would not be susceptible to collisions, the network is expected to use a BS-assigned PLCM instead, due to the SCM bit 4 being set to 1.

Note: The MSC could in theory examine the first 8 bits of the received ESN to determine whether this was a unique (ESN/UIMID) or non-unique (pESN/pUIMID) value. However the ESN is not a mandatory field in the MSID (as defined in C.S0004), so C.S0072 implies that the decision is made solely on the basis of the SCM. An equipment vendor may choose to require *both* SCM bit 4 = 1 and an "ESN" beginning with 0x80 before assigning a non-UIMID-based PLCM. Similarly, some MEID-equipped handsets have been observed to set the SCM bit 4 to 0 when a unique UIMID-equipped R-UIM is inserted. This behavior is not explicitly covered in existing standards – the "default" behavior expected is that the SCM bit 4 will be set to 1 if the ME has an MEID, irrespective of the type of R-UIM inserted. This custom handset/network behavior will deactivate EIR capabilities for the mobile but will not result in any collision problems as the PLCM derived from the UIMID will be unique.

7.3.1.5 Call Detail Record Production

Similar to the registration case in Section 7.3.1.2 , both the MEID and UIMID may be available in the MSC CDR, a change from current operation where only the UIMID is available and not the handset ESN. Billing system changes would presumably be needed if the operator wished to take advantage of this new information (e.g. for statistical information on handset usage). This does not apply to some billing record formats such as the CIBER inter-carrier format, in which only one hardware identifier can be included. In this case it may be desirable to include the pUIMID instead of the MEID to allow validation of a matched pair of identifiers (the MEID will change if the R-UIM is moved but the pUIMID comes from the card along with the IMSI).

7.3.1.6 Mobile Terminated SMS

MT-SMS and other paging-channel messages are not susceptible to the mis-addressing problem described in Section 7.2.1.6 for this scenario, as message addressed by 'ESN' will actually contain the unique UIMID.

7.3.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM (assuming the SCM bit 4 is set to 1).

7.3.2 Data Services

7.3.2.1 CDMA2000® Packet Data

Operator provisioning using an NAI constructed as UIMID@realm is unaffected by insertion into an MEID-equipped ME.

Origination and PLCM assignment is as for voice.

In 1X mode the UIMID or MEID or both may be included in the airlink record and the subsequent PDSN UDR. For EVDO, the MEID may be included but the UIMID will not be included unless it is calculated from the MEID.

7.3.2.2 1xEV-DO Packet Data

Devices obtain the HardwareID from the device (MEID in this scenario), not the R-UIM.[35] In this scenario the network must be upgraded to handle the new MEID HardwareIDType, as described in Section 7.2.2.2 .

7.3.2.3 Other Applications

Applications would typically be expected to honor the R-UIM usage indicator bit, and therefore use the UIMID as the “ESN” value. In this case no change from existing behavior would be required for this scenario.

If the application used the device ESN, then use of the MEID instead as per Section 7.2.2.3 is recommended, although note that “subscription mobility” (moving the R-UIM to a different ME) may be compromised in this case regardless of MEID issues.

7.3.3 Lost/Stolen Phone

A subscriber whose phone has been lost or stolen typically contacts Customer Service from an alternate number. Assuming the subscriber’s identity is verified satisfactorily, the HLR subscription may be call-barred to prevent charges to the subscriber’s account.

R-UIM devices present a particular challenge for the stolen phone case, as the thief can replace the legitimate subscriber’s R-UIM with their own (e.g. if the device had more functionality than the thief’s). Prior to the introduction of MEID, there was no way for the network to track the device independently of the R-UIM (assuming the usage indicator was set to replace the ESN with the EUIMID).

---

[35] The 3GPP2 specification for EV-DO was originally not clear on this point. To rectify this C.S0024-B v3.0 states that, “The unique ID [HardwareID Value] is never assigned to the terminal using an identifier stored in a Removable User Identity Module.”

X.S0008 and C.S0072 address this issue by allowing the device MEID to be retrieved, and checked against a record held in a new network element, the Equipment Identity Register (EIR). The new CheckMEID operation is defined for this purpose, as shown in Figure 7-11. Note that in order for the MEID to be listed as stolen in the EIR, the network must have previous knowledge of which MEID was in use for the stolen IMSI (see Section 7.2.3):

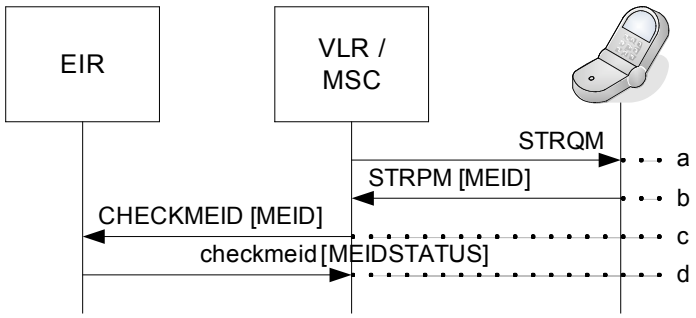

Figure 7-11 - CheckMEID Operation

Steps are as follows:

a-b) The VLR/MSC does not have the current MEID, and so retrieves it via *Status Request/Response Message*.

c) The VLR sends the CheckMEID message to the EIR containing the MEID.

d) The EIR returns the MEID Status (e.g. Normal, Block, Track).

Ultimately, the success of EIR deployment to identify stolen phones depends on the extent to which EIRs of different operators are interconnected – from GSM experience, the “SIM/R-UIM lock” which restricts a device to a particular operator can often be defeated by the thief. At the time of writing, no CDMA operators were known to have deployed or be actively pursuing deployment of an EIR.

7.3.4 Over the Air Service Provisioning

OTASP provisioning for the “UIMID in MEID” scenario is the same as the existing “UIMID in ESN” flow (assuming the MSC does not autonomously include the MEID in the initial smdpp to the OTAF). The unique UIMID would not trigger the OTAF to request the MEID from the handset. The unique UIMID can be used to index a database to retrieve card-specific information (e.g. A-key, SPC).

7.3.5 Roaming

7.3.5.1 Outbound Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. The “UIMID in MEID” configuration is susceptible to this issue.
- **No C.S0072 support in visited network**. Since the UIMID is unique, there is no risk of PLCM collision even if C.S0072 is not supported.
- **No X.S0008 support in visited network**. X.S0008 support is of limited use in this scenario, as the subscriber may move their R-UIM between MEs without advising the operator. X.S0008 support would be beneficial to address stolen phone scenarios while roaming.
- **MEID presence in CIBER.** The two identifiers (UIMID and MEID) potentially available for inclusion in the CIBER record are not hash-related. Use of the UIMID is recommended in this case (see Section 6.)
- **No MEID in A12 authentication**. Some operators may not send HardwareID in A12 at all. Others may support ESN as HardwareID, but not MEID.
- **MEID in UDR.** In 1x mode the MEID may be included in the UDR instead of the UIMID, or vice versa, which may differ from the home operator’s own network practice. In EVDO mode the MEID may be included but the UIMID cannot be included unless it is calculated from the MEID.

7.3.5.2 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network’s ability to serve roamers from other markets. Operators who themselves use R-UIMs may be more cognizant of the potential CIBER ramifications of including the MEID rather than the UIMID.

7.4 R-UIM Operator – Short-Form EUIMID

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. The operator has chosen to deploy Short-Form EUIMID. Following the argument in Section 5.2 , the assumption here is that Bit 2 of the Usage Indicator is set to 1, i.e. the SF_EUIMID overrides the device MEID if present. The EUIMID-equipped R-UIMs may be inserted into devices that are equipped with either an ESN, or an MEID. MEID equipped devices are assumed to be C.S0023-C/C.S0065 capable (see Section 5.2), unless otherwise noted.

Note that in the case where an ESN-equipped handset includes the necessary software to support MEID, it might be thought that the handset would use the SF_EUIMID and report MEID availability. However C.S0023-C specifically prohibits an ESN-equipped ME from interpreting the SF_EUIMID Usage Indicator bit. Such a device will operate as a pure ESN device and SF_EUIMID will not be used.

In general, insertion of a SF_EUIMID card into an ESN-equipped device is shown to create potential for PLCM collisions, regardless of the network support for C.S0072.

7.4.1 Basic Operation

7.4.1.1 Registration – No X.S0008 support

This scenario is equivalent to that shown in Section 7.2.1.1 , except that pUIMID is sent in the ESN parameter instead of pESN. HLR validation is performed on the basis of the MIN/IMSI – pUIMID combination.

7.4.1.2 Registration – X.S0008 supported

In this scenario, the SF_EUIMID can be included in the registration message, as shown in Figure 7-12. This is only possible if the handset has an MEID (even though the MEID itself is not sent to the network), since C.S0023 prohibits use of the SF_EUIMID for MEID protocol fields if the mobile is not provisioned with an MEID_ME.

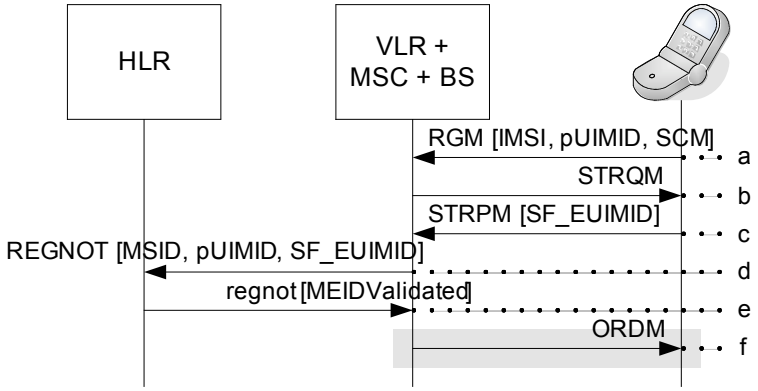

Figure 7-12 - SF_EUIMID Registration with X.S0008 support

Steps are as follows (for MEID-equipped ME):

a) MS sends a *Registration Message*, including its IMSI, pUIMID and Station Class Mark set to indicate MEID support. The MS cannot include its MEID or the SF_EUIMID in this message.

b) Based on the SCM, the MSC recognizes that the mobile has a MEID, and that the MSC does not know this value. It solicits the MEID (or MEID_ME if both BS and ME support this) via the *Status Request Message* (new Information Record in C.S0072 for MEID and new Information Record in CDMA2000 Release E for MEID_ME).

c) The MS responds with a *Status Response Message*. Based on the value of the Usage Indicator and the Information Record requested, the SF_EUIMID may be returned instead of the MEID.

d) The MSC sends a RegistrationNotification to the HLR, including the MSID, pUIMID (required for backwards compatibility) and the MEID or SF_EUIMID.

e) Text extracted from X.S0008: “Based on the existence of a provisioned MEID value for this subscription, and the presence of the MEID parameter in the REGNOT, the HLR includes an MEID comparison in the validation of the subscription. The HLR then registers the indicated MS and returns a regnot to the Serving VLR. The regnot includes the MEIDValidated parameter to inform the Serving VLR/MSC that the MEID associated with the system access has been validated.” In this case, the value included in the MEID parameter may be the SF_EUIMID. In this case, even if the subscriber transfers the R-UIM to another (MEID-equipped) device, this value will remain constant, and can therefore be reasonably expected to be stored in

the HLR. If the MEID_ME is transferred to the HLR this will change for a given subscription if a R-UIM card is moved to a different ME.

f) Optionally, the BS sends a *Registration Accepted Order* to the MS

7.4.1.3 Authentication

Authentication is performed on the basis of the pUIMID. The SF_EUIMID, if included, will not be used for authentication calculations.

A-key checksum calculations should use the pUIMID as an input for verification although other implementations may be possible in devices predating S.S0053-0 v2.0 (May, 2009).

7.4.1.4 Call Origination/Termination

If the SF_EUIMID-equipped R-UIM is inserted in an MEID-equipped ME, PLCM assignment will be as per Section 7.2.1.4 (i.e. network recognizes SCM and provides BS-assigned PLCM). pUIMID and SF_EUIMID replace pESN and MEID respectively from the earlier scenario.

If however the card is inserted in an ESN-equipped ME, this device will not understand the new PLCM types or set the SCM bit flag. The pUIMID-based PLCM will be used, and there is a risk of PLCM collision.

7.4.1.5 Call Detail Record Production

The two identifiers available (pUIMID and SF_EUIMID) for inclusion in the CDR are hash-related, but since both are associated with the R-UIM, there is no opportunity to capture information about specific hardware usage.

It is recommended that operators include the pUIMID since it is more compatible with existing billing systems until it can be verified that all roaming partners will accept a 56-bit identifier for billing. Note that an operator serving a roamer cannot determine whether the 56-bit identifier is SF_EUMID (and therefore associated with the subscription) or an MEID (and therefore not associated with the subscription, but with the phone hardware).

Note that some billing record formats, notably CIBER, do not support the inclusion of two hardware identifiers.

7.4.1.6 Mobile Terminated SMS

ESN-addressed messages over the paging channel would in this configuration use the pUIMID derived from the SF_EUIMID. Regardless of whether the card was inserted in an ESN- or MEID-equipped device, messages could be received by other mobiles in addition to the intended recipient due to pUIMID duplication.

7.4.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM. If the R-UIM is inserted in an ESN-equipped device, BS-assigned PLCM is not possible, regardless of the status of C.S0072 support in the network.

7.4.1.8 Handset Compatibility Issues

If the R-UIM is inserted in a device affected by the issue described in Section 5.4 , the device may indicate “Service Required”, or otherwise refuse to operate.

If the R-UIM is inserted into an MEID-equipped device without C.S0023-C support, it will return the handset shell (ME) MEID rather than the desired SF_EUIMID.

7.4.2 Data Services

7.4.2.1 CDMA2000® Packet Data

Data originations when an ESN-equipped device is used are subject to the same potential for PLCM collision as for voice.

NAI assignment using UIMID@realm will no longer be unique – an upgrade to another value that is unique, such as SF_EUIMID@realm is necessary.

For 1x packet data SF_EUIMID or pUIMID or both may be included in the airlink record and subsequent PDSN UDR.

7.4.2.2 1xEV-DO Packet Data

HardwareID handling (if implemented) should be upgraded to accept the MEID format as described in Section 7.2.2.2 . This parameter will be the MEID or ESN not the UIMID or EUIMID.

If an MEID-equipped handset is used, then the handset MEID will be present in the airlink record and subsequent PDSN UDR (unless the associated pESN is calculated from the MEID by the PCF/PDSN).

7.4.2.3 Other Applications

Applications should use the EUIMID in preference to the pUIMID as a unique identifier. The exact access method for the application to obtain the EUIMID is beyond the scope of this document.

7.4.3 Lost/Stolen Phone

Overriding the ME’s MEID with the SF_EUIMID means that a stolen device cannot be tracked/blocked independently of its R-UIM unless both the terminal and network support protocols that allow explicit transmission of MEID_ME. Without these

updates a thief would be able to replace the legitimate subscriber's R-UIM with their own without the network being aware of the change.

This limitation is essentially equivalent to the situation today with UIMID cards in ESN devices.

7.4.4 Over the Air Service Provisioning

OTASP (when the SF_EUIMID R-UIM is inserted into an MEID ME) is essentially equivalent to the non-R-UIM MEID device scenario shown in Section 7.2.4, with pUIMID and SF_EUIMID replacing pESN and MEID respectively.

When the card is inserted into an ESN device, it may not be possible to retrieve the SF_EUIMID[36]. In fact, the OTASP session may fail, as the ESN-equipped handset may not handle the additional fields in the *Protocol Capability Request Message*[37]. A solution is to store the SF_EUIMID or a unique provisioning identifier in fields that are accessible to ESN mobiles but not filled with data until the time of provisioning, fields such as MDN and IMSI_T.

The new capabilities introduced in C.S0066 v2.0 and C.S0016-C v2.0 allow the retrieval of both the SF_EUIMID and the handset MEID during the OTASP session.

[36] C.S0023-C Section 4.3.2.1 implies the ME is required to process the additional fields in the *Protocol Capability Request Message* (including the request for MEID) not the R-UIM.

[37] C.S0066 (Section 4.3.1) states “The base station shall not send the *Protocol Capability Request Message* with additional fields to the mobile stations which don’t support the additional fields”, yet the presence of the pUIMID means that OTAF may assume the mobile does support these fields.

7.4.5 Roaming

7.4.5.1 Outbound Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. When inserted in a MEID-equipped device, the SF_EUIMID R-UIM is susceptible to this issue.
- **No C.S0072 support in visited network**. In this case the pUIMID will be used to form the PLCM, with the associated risk of collision.
- **No X.S0008 support in visited network**. As per Section 7.2.5.1 , the SF_EUIMID may not be available in ANSI-41 messaging.
- **SF_EUIMID presence in CIBER.** The two identifiers (pUIMID and SF_EUIMID) potentially available for inclusion in the CIBER record are hash-related. There may be a preference for the unique identifier (i.e. SF_EUIMID), although it is likely that roaming partner behavior will vary.
- **No MEID in A12 authentication**. Some operators may not send HardwareID in A12 at all. Others may support ESN as HardwareID, but not MEID.
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pUIMID) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.
- **MEID in UDR.** The SF_EUIMID may be included in a 1X UDR instead of the pUIMID, or vice versa, which may differ from the home operator's own network practice. For EVDO modes, the serving network may not be able to include the MEID or pUIMID in the UDR.

7.4.5.2 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network's ability to serve roamers from other markets.

7.5 R-UIM Operator – Long-Form EUIMID

The scenarios in this section apply to an operator whose subscribers use R-UIM devices. The operator has chosen to deploy Long-Form EUIMID. The full LF_EUIMID can be retrieved remotely from the MS via C.S0016-C v2.0 or C.S0066-0 v2.0 OTASP/OTAPA messaging, via CDMA2000 Release E signaling or through the use of a special CCAT/UTK application (see Section 5.3). The EUIMID-equipped R-UIMs may be inserted into devices that are equipped with either an ESN or an MEID

In general, insertion of a LF_EUIMID card into an ESN-equipped device is shown to create potential for PLCM collisions, regardless of the network support for C.S0072.

7.5.1 Basic Operation

7.5.1.1 Registration – No X.S0008 support

This scenario is equivalent to that shown in Section 7.2.1.1 , except that pUIMID is sent in the ESN parameter instead of pESN. HLR validation is performed on the basis of the MIN/IMSI – pUIMID combination.

7.5.1.2 Registration – X.S0008 supported

When X.S0008 is supported, the registration scenario is equivalent to that shown in Section 7.3.1.2 , except that pUIMID replaces the UIMID. No checking for a hash relationship between the received 32- and 56-bit identifiers should be performed.

7.5.1.3 Authentication

Authentication is performed on the basis of the pUIMID.

A-key checksum calculations should use the pUIMID as an input for verification, although other implementations may be possible in devices predating S.S0053-0 v2.0 (May, 2009).

7.5.1.4 Call Origination/Termination

If the LF_EUIMID-equipped R-UIM is inserted in an MEID-equipped ME, PLCM assignment will be as per Section 7.2.1.4 (i.e. network recognizes SCM and provides BS-assigned PLCM). pUIMID replaces pESN from the earlier scenario, but the MEID_ME may still be retrieved via the *Status Request/Response Messages*.

If however the card is inserted in an ESN-equipped ME, this device will not understand the new PLCM types or set the SCM bit flag. The pUIMID-based PLCM will be used, and there is a risk of PLCM collision.

7.5.1.5 Call Detail Record Production

Similar to the registration case in Section 7.5.1.2 , both the MEID and pUIMID may be available in the MSC CDR, a change from current operation where only the UIMID is available and not the handset ESN. Billing system changes would presumably be needed if the operator wished to take advantage of this new information (e.g. for statistical information on handset usage). The unique LF_EUIMID is not available unless protocols such as the Release E Status Request messages are implemented by the ME, RAN and Core Network. The inclusion of two hardware identifiers may not be supported by all CDR formats, and is not supported by the CIBER billing record format. In this case it may be desirable to include the pUIMID instead of the MEID to allow validation of a matched pair of identifiers (the MEID will change if the R-UIM is moved but the pUIMID comes from the card along with the IMSI).

7.5.1.6 Mobile Terminated SMS

ESN-addressed messages over the paging channel would in this configuration use the pUIMID derived from the LF_EUIMID. Regardless of whether the card was inserted in an ESN- or MEID-equipped device, messages could be received by mobiles in addition to the intended recipient due to pUIMID duplication. IMSI-addressed messages significantly reduce this problem.

7.5.1.7 Handoff

Handoff scenarios are as per Section 7.2.1.7 - the handset and network capabilities determine the outcome, not the nature of the R-UIM. If the R-UIM is inserted in an ESN-equipped device, BS-assigned PLCM is not possible, regardless of the status of C.S0072 support in the network.

7.5.1.8 Handset Compatibility Issues

If the R-UIM is inserted in a device affected by the issue described in Section 5.4 , the device may indicate “Service Required”, or otherwise refuse to operate.

7.5.2 Data Services

7.5.2.1 CDMA2000® Packet Data

Data originations when an ESN-equipped device is used are subject to the same potential for PLCM collision as for voice.

NAI assignment using UIMID@realm will no longer be unique – an upgrade to a unique value such as LF_EUIMID@realm is necessary.

Either MEID or pUIMID or both may be included in the airlink record and subsequent PDSN UDR.

7.5.2.2 1xEV-DO Packet Data

HardwareID handling (if implemented) should be upgraded to accept the MEID format as described in Section 7.2.2.2 . Devices source the HardwareID from the device (ESN or MEID), not the R-UIM.

If an MEID-equipped handset is used, then the handset MEID will be present in the airlink record and subsequent PDSN UDR (unless the associated pESN is calculated from the MEID by the PCF/PDSN).

7.5.2.3 Other Applications

Applications should use the EUIMID in preference to the pUIMID as a unique identifier. The exact access method for the application to obtain the EUIMID is beyond the scope of this document.

7.5.3 Lost/Stolen Phone

The stolen phone scenario for LF_EUIMID is equivalent to the “UIMID in MEID” case shown in Section 7.3.3, provided the lost phone is MEID-equipped. If the MEID has been previously recorded, it could be marked as stolen in the EIR, and blocked from further usage within the scope of connectivity to that EIR.

If the device is ESN-equipped, its ESN is not transmitted to the network, and therefore the device cannot be barred from operating using a different R-UIM.

7.5.4 Over the Air Service Provisioning

OTASP using LF_EUIMID can present some challenges, as the LF_EUIMID often cannot be retrieved from the card (only the new capabilities recently added in C.S0066-0 v2.0,C.S0016-C v2.0 and CDMA2000 Release E provide standard methods for this). If there is any card-specific information stored in a database (e.g. A-key and/or SPC) but no IMSI on the R-UIM it is difficult to retrieve data for provisioning accurately. In addition, subsidy protection may present a challenge as it may not be possible to determine that a particular card was sold by a particular operator.

An alternative to retrieving pre-programmed card-specific information is to generate it during the OTASP session (after which it can be associated with the programmed IMSI). IS-725-A and IS-683 contain procedures for securely creating the A-key in the AC and MS during the OTASP session. Similarly, the SPC could be initially set to a default value, and then changed to a random value using existing OTASP procedures. A PIN issued at the point of sale (as well as the default Preferred Roaming List in the card) can help ensure that the prospective subscriber ultimately obtains service from the correct operator.

Another approach is to provision the LF_EUIMID in fields that are accessible to all mobiles supporting R-UIM, and not required to be filled with valid information prior to provisioning, such as the MDN and IMSI_T fields.

7.5.5 Roaming

The bullet points below relate to the potential issues outlined in Section 7.2.5.1 above.

- **No support for MEID devices**. When inserted in a MEID-equipped device, the LF_EUIMID R-UIM is susceptible to this issue.
- **No C.S0072 support in visited network**. In this case the pUIMID will be used to form the PLCM, with the associated risk of collision.
- **No X.S0008 support in visited network**. X.S0008 support is of limited use in this scenario, as the subscriber may move their R-UIM between MEs without advising the operator. X.S0008 support would be beneficial to address stolen phone scenarios while roaming.
- **MEID presence in CIBER.** The two identifiers (pUIMID and MEID) potentially available for inclusion in the CIBER record are not hash-related. Use of the pUIMID is recommended in this case (see Section 6.).
- **Uniqueness Checks.** A network may refuse to allow two subscribers with the same ESN (e.g. duplicate pESN) to be registered in a VLR, HLR or MSC, resulting in one (or more) mobiles being blocked.

7.5.5.1 Inbound Roaming

Assuming an equivalent network capability to that in Section 7.2.5.2 , there should be no difference to the network's ability to serve roamers from other markets.

8. Terminology

0x	Hexadecimal (base 16) format indicator
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization and Accounting
AC	Authentication Center
A-key	Authentication Key
AMPS	Advanced Mobile Phone Service
AN	Access Network
ANSI-41	American National Standards Institute 41 – TIA mobility standard (also known as 3GPP2 X.S0004)
AT	Access Terminal
AUTHR	AuthenticationResponse
AUTHREQ	AuthenticationRequest Invoke
authreq	AuthenticationRequest Return Result
BCD	Binary Coded Decimal
BS	Base Station
CAVE	Cellular Authentication and Voice Encryption algorithm
CCAT	CDMA Card Application Toolkit
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CIBER	Cellular Intercarrier Billing Exchange for Roamer
CSC	Customer Service Center

CSIM	CDMA Subscriber Identity Module
DBM	*Data Burst Message*
DRM	Digital Rights Management
EF	Elementary File
EIR	Equipment Identity Register
ESN	Electronic Serial Number. Used in a general sense or to refer to a protocol field. See also ESN_ME.
ESN_ME	The permanent and unchangeable ESN stored in an ME. A protocol field that will never include UIMID.
EUIMID	Expanded (Removable) User Identity Module Identifier
f-csch	Forward common signaling channel
GDA	Global Decimal Administrator (currently GSMA and other administrators authorized by them)
GHA	Global Hexadecimal Administrator (currently TIA and other administrators authorized by them)
GPM	General Page Message
GSM	Global System for Mobile
HLR	Home Location Register
HOCM	*Handoff Complete Message*
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
IOS	Interoperability Specification
IRM	International Roaming MIN
ITU-T	International Telecommunication Union – Standardization Sector
LAC	Link Access Control

LBS	Location-Based Services
LF_EUIMID	Long Form EUIMID
MAP	Mobile Application Part
ME	Mobile Equipment (phone 'shell' without R-UIM or CSIM)
MECAM	*MEID Enhanced Channel Assignment Message*
MEID	Mobile Equipment Identifier. Used in a general sense or to refer to a protocol field. Also see MEID_ME.
MEID_ME	The permanent and unchangeable MEID stored in an ME. A protocol field that will never include SF_EUIMID.
MIN	Mobile Identification Number
MS	Mobile Station
MSC	Mobile Switching Center
MT	Mobile Terminated
MUHDM	*MEID Universal Handoff Direction Message*
NAI	Network Access Identifier
ORM	*Origination Message*
OTAF	Over-The-Air Function
OTASP	Over The Air Service Provisioning
PCF	Packet Control Function
PDSN	Packet Data Serving Node
pESN	Pseudo-ESN
PIN	Personal Identification Number
PLCM	Public Long Code Mask
PRL	Preferred Roaming List
PRM	*Page Response Message*

pUIMID	Pseudo-EUIMID
r-csch	Reverse common signaling channel
R-UIM	Removable User Identity Module
SCM	Station Class Mark
SF_EUIMID	Short Form EUIMD
SHA	Secure Hash Algorithm
SMDPP	*ShortMessageDeliveryPointToPoint Invoke*
smdpp	*ShortMessageDeliveryPointToPoint Return Result*
SPC	Service Programming Code
SSD	Shared Secret Data
STRPM	*Status Response Message*
STRQM	*Status Request Message*
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
TMSI	Temporary Mobile Station Identity
TRN	Temporary Reference Number
UDR	Usage Data Record
UHDM	*Universal Handoff Direction Message*
UICC	Universal Integrated Circuit Card
UIM	User Identity Module
UIMID	(Removable) User Identity Module Identifier
UMTS	Universal Mobile Telephone Service
USIM	Universal Subscriber Identity Module
UTK	UIM Tool Kit

1

9. References

[A.S001x]	3GPP2 A.S001*x*-D (TIA-2001.*x*). Interoperability Specification (IOS) for CDMA2000® Access Network Interfaces. v2.0. August, 2009. http://www.3gpp2.org/Public_html/specs/tsga.cfm. • A.S0011. *Overview* • A.S0012. *Transport* • A.S0013. *Features* • A.S0014. *A1, A1p, A2, and A5 Interfaces* • A.S0015. *A3 and A7 Interfaces* • A.S0016. *A8 and A9 Interfaces* • A.S0017. *A10 and A11 Interfaces*
[A.S0008]	3GPP2 A.S0008-C (TIA-878). *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*. v3.0. June, 2010. http://www.3gpp2.org/Public_html/specs/A.S0008-C_v3.0_100621.pdf
[C.S0005]	3GPP2 C.S0005-E (IS-2000). *Upper Layer (Layer 3) Signaling Standard for CDMA2000 Spread Spectrum Systems*. v2.0. June, 2010. http://www.3gpp2.org/Public_html/specs/C.S0005-E_v2.0_cdma2000_1x_L3_Signaling.pdf
[C.S0016]	3GPP2 C.S0016-D (TIA-683). *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*. v1.0. January, 2010. http://www.3gpp2.org/Public_html/specs/C.S0016-D%20v1.0_OTASP.pdf
[C.S0023]	3GPP2 C.S0023-D (TIA-820). *Removable User Identity Module for Spread Spectrum Systems*. v1.0. July, 2009. http://www.3gpp2.org/Public_html/specs/C.S0023-D_v1.0_R-UIM-090720.pdf
[C.S0024]	3GPP2 C.S0024-B (TIA-856-A). *CDMA2000 High Rate Packet Data Air Interface Specification*. v3.0. September, 2009. http://www.3gpp2.org/Public_html/specs/C.S0024-B_v3.0_HRPD.pdf
[C.S0035]	3GPP2 C.S0035-A. *CDMA Card Application Toolkit (CCAT)*. v2.0.

	August 2007. http://www.3gpp2.org/Public_html/specs/C.S0035-A_v2.0_070731.pdf
[C.S0065]	3GPP2 C.S0065-B (TIA-1080). *CDMA2000 Application on UICC for Spread Spectrum Systems*. v1.0. January, 2010. http://www.3gpp2.org/Public_html/specs/C.S0065-B_v1.0_cdma2000_Application_for_UICC.pdf
[C.S0066]	3GPP2 C.S0066-0 (TIA-158). *Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems*. v2.0. July, 2008. http://www.3gpp2.org/Public_html/specs/C.S0066-0_v2.0_080729.pdf
[C.S0072]	3GPP2 C.S0072-0 (TIA-1082). *Mobile Station Equipment Identifier (MEID) Support for CDMA2000 Spread Spectrum Systems*. v1.0. July 22, 2005. http://www.3gpp2.org/Public_html/specs/C.S0072-0_v1.0_050727.pdf
[C.S0073]	3GPP2 C.S0073-B. *Signaling Test Specification for Mobile Station Equipment Identifier (MEID) Support for CDMA2000 Spread Spectrum Systems*. v1.0. August, 2009. http://www.3gpp2.org/Public_html/specs/C.S0073-B_V1.0_MEID_Test_Spec.pdf
[CDG Ref Doc 137]	CDG Reference Document #137, Mobile Equipment Identifier Roaming Recommendations. v1.0, December 2006.http://www.cdg.org/members_only/refdocs/137.zip
[Collisions WP]	Pellegrino, Gary; Quick, Frank. *White Paper on Pseudo-ESN Collisions*. TIA TR-45 ESN/UIM Ad Hoc Group. May 26, 2005. http://www.tiaonline.org/standards/resources/esn/documents/Collisions_pESN_wp.pdf
[GSMA TS.06]	GSMA TS.06 (formerly DG.06). IMEI Allocation and Approval Guidelines. December 2010. http://gsmworld.com/documents/TS06_5v1_Approved.pdf
[E.118]	ITU-T Recommendation E.118. *The international telecommunication charge card*. May 2006. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.118-200605-I!!PDF-E&type=items
[MEID Failure Bulletin]	CDG Technical Bulletin 070301IRT. *MEID IOS Issue*. v1.0, March 2007. http://www.cdg.org/members_only/teams/IntRoaming/docs/CDG%20Tech%20Bulletin%20070301IRT%20MEID%20IOS%20Issue%20v1_0.doc

[SC.R4001]	3GPP2 SC.R4001-0. *Global Wireless Equipment Numbering Administration Procedures.* v2.0. December, 2010. http://www.3gpp2.org/public_html/Specs/SC.R4001-0_v2.0_Global Wireless Equipment Numbering Admin Procedures.pdf
[SC.R4002]	3GPP2 SC.R4002-0. *Mobile Equipment Identifier (MEID) GHA (Global Hexadecimal Administrator), Assignment Guidelines and Procedures.* v6.0. July, 2010. http://www.3gpp2.org/public_html/Specs/SC.R4002-0_v6.0_GHA_Assignment_Procedures_for_MEID_and_SF_EUIMID-100723.pdf
[SC.R4003]	3GPP2 SC.R4003. *Expanded R-UIM Numbering Administration Procedures*. v1.0. May, 2007. http://www.3gpp2.org/Public_html/Specs/SC.R4003-0_v1.0_EUIMID_Procedures_070521.pdf
[S.R0048]	3GPP2 S.R0048-A (TIA-928). *3G Mobile Equipment Identifier (MEID), Stage 1*. v4.0. November, 2005. *http://www.3gpp2.org/Public_html/specs/S.R0048-A_v4.0_050630.pdf*
[S.R0111]	3GPP2 S.R0111-0. *Expanded R-UIM Identifier, Stage 1 Requirements*. v2.0. May 2007. http://www.3gpp2.org/public_html/specs/S.R0111-0_v2.0_070521.pdf
[X.S0008]	3GPP2 X.S0008-0 (TIA-928). *MAP Support for the Mobile Equipment Identity (MEID)*. v3.0. January, 2009. http://www.3gpp2.org/Public_html/specs/X.S0008-0_v3.0_090130.pdf
[X.S0011]	3GPP2 X.S0011-xxx-E (TIA-835). *CDMA2000 Wireless IP Network Standard*, v1.0, November, 2009. http://www.3gpp2.org/Public_html/specs/tsgx.cfm
[X.S0033]	3GPP2 X.S0033-0 (TIA-1074). *OTA Support for MEID*. v2.0. March, 2006. http://www.3gpp2.org/Public_html/specs/X.S0033-0_v2.0_060301.pdf

1