Moving Forward on MEID and Expanded UIMID (E-UIMID)

February, 2008

Contacts
Bill Dahnke, David Crowe
meid@cdg.org

Revision A

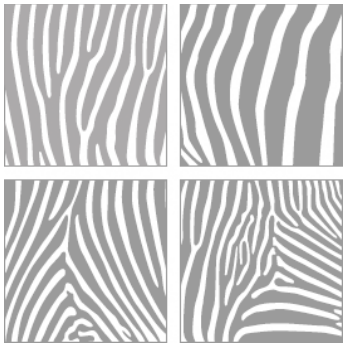
Moving Forward on MEID and EUIMID

- Mobile devices and R-UIMs (Removable User Identity Modules) must be identified by a unique code for a variety of reasons.
- The original 32 bit identifiers known as ESN and UIMID are almost entirely depleted. Full depletion is expected in 2008.
- Replacement identifiers are standardized and available –
  - MEID: Mobile Equipment Identity
  - EUIMID: Expanded UIM Identity
- This presentation describes the current situation for ESN and UIMID, the format and purpose of MEID and EUIMID, and information to assist the migration.

Presentation Outline

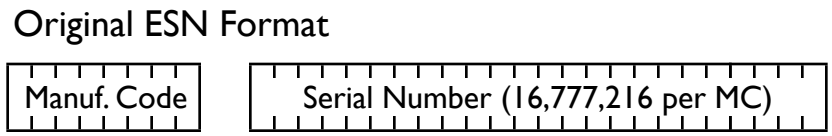
- Yesterday (the way things were)
  - ESN (Electronic Serial Number)
  - UIM and UIMID in cdma2000®
  - The Time to Act is Now!
- Today (the way things should be)
  - MEID (Mobile Equipment ID)
  - ESN Collisions
  - Expanded UIMID (EUIMID)
  - Protocol Impacts
  - Migration
- Tomorrow (optional extras)
  - Equipment Identity Register (EIR)
- Standards Summary
  - What has changed
  - What might still change

ESN – Electronic Serial Number

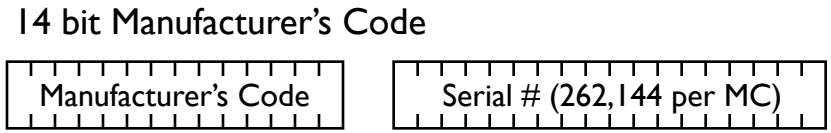


- A 32-bit number used to *uniquely* identify cellular phones since the days of analog (AMPS) in the early 1980s. Now almost all have been allocated…

ESN History and Format



- A 32 bit identifier for a cellular phone.
- Identifies the phone, not the subscription.
- Intended to uniquely identify all phones.
- Originally allocated with an 8 bit manufacturer code (MC). 16,777,216 serial numbers were assigned with each MC.
- Used first by AMPS analog in 1983 and then TDMA and CDMA digital systems.
- Available in EVDO as the Hardware ID parameter.



- Assignments are now with a 14 bit MC, making assignments smaller and thus more efficient.

Uses of ESN

- ANSI-41 validation needs ESN and IMSI matching record at HLR.
- An input to CAVE authentication.
- Uniquely identifies mobiles when a valid IMSI is not available (e.g. during OTASP).
- Used alone to generate PLCM (Public Long Code Mask), a numeric code that distinguishes mobiles on the reverse traffic channel.
- May also be used to identify the manufacturer of a phone, for inventory control, tracking stolen phones and…

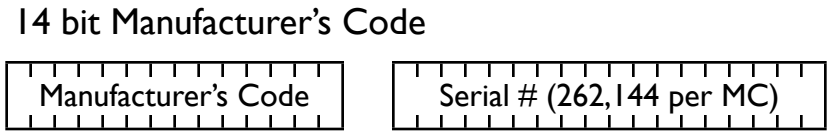
Assignment & Resource Depletion

- ESN assignment is managed by TIA (Telecommunications Industry Association based near Washington, DC)
- Stringent conservation has been followed in last few years, using only 14 bit MC assignment and requiring more justification for assignments.
- Codes allocated to analog (AMPS) or TDMA that may have been programmed in phones are being re-used as UIMIDs.
- Last few blocks of never assigned ('virgin') codes are being used as hardware ESNs or UIMIDs.
- Virgin code exhaust expected by April, 2008.
- Previously allocated but never used sub-blocks can be re-used for either ESNs or UIMIDs. The number of such reclamations is impossible to determine ahead of time.

User Identity Modules (UIM) in cdma2000®

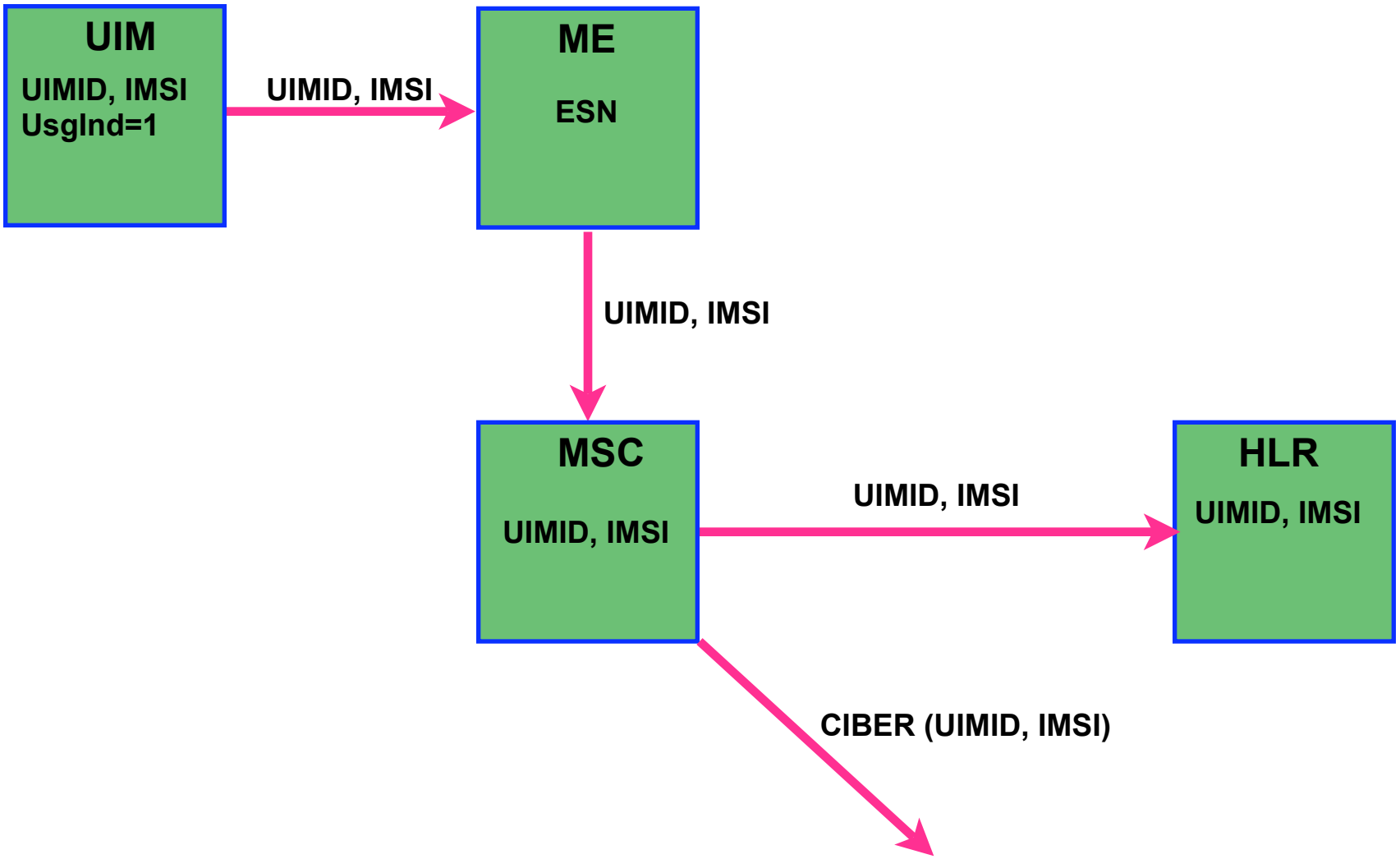
- User identity modules or ‘smart cards’ have been used in cdma2000® systems for several years. They contain a UIMID that replaces the ESN in some situations…

UIMID Concept



- ANSI-41 requires that the IMSI and ESN transmitted by a phone match at the HLR.
- Problem:
  - Moving a UIM (containing IMSI) from one phone (with a particular ESN) to another (with a different ESN) would result in ANSI-41 validation and authentication failures.
- Solution:
  - Storing a unique ESN-like (32 bit) identifier in the UIM allows ANSI-41 validation and authentication to work without modifications.
  - Bit 1 of the 'UsgInd' field in the R-UIM allows the UIMID to override the ESN when set to '1' (which we believe all systems do).
- UIMID is only allocated with a 14 bit Manufacturer's Code but from the same pool of numbers as the ESN.

Today's Network with R-UIM



Current Status

- There are currently more requests for new UIMID blocks than codes are available.
- Requests are only being partially fulfilled.
- TIA continues to add more blocks of old analog and TDMA codes to the UIMID pool.
- The final exhaustion of this numbering resource can only be a matter of months.
- UIMIDs are assigned by TIA (uimadmin@tiaonline.org) or by regional authorities such as CCSA and ARIB.

Rapid UIMID Depletion

	June 30, 2007	September 30, 2007	December 31, 2007
Total 14 bit Manufacturer Codes	1,091	1,471	1,571
Assigned 14 bit Manufacturer Codes	1,023	1,210	1,328
Pending Requests	311	247	346
Expected Requests	250	250	250
Surplus Codes (Deficit)	(493)	(236)	(353)

The Time to Act is Now!

- **Existing resources are close to fully depleted. Now is the time to implement new identifiers…**

Time to Act…

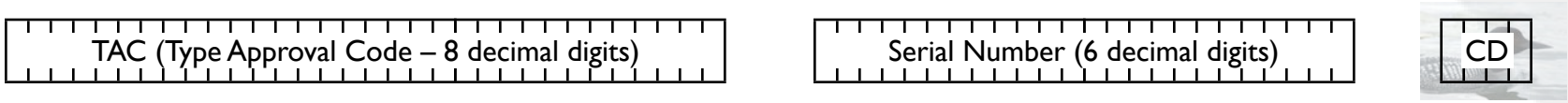
- Existing hardware identifiers, ESN and UIMID, are almost completely depleted.
- A replacement mobile device hardware identifier is available – MEID (Mobile Equipment Identifier).
- A replacement UIM identifier is available – EUIMID (Expanded UIMID).
- Networks need to be upgraded to support these new identifiers.
- New devices, such as phones and removable UIMs must be capable of supporting these new identifiers.
- Carriers must provision phones, UIMs, back office systems and network databases with the new identifiers.
- 2008 is the year to act!

Mobile Equipment Identifier (MEID)

- The MEID is the replacement identifier for cellular phones, relying on the Pseudo-ESN (pESN) for backwards compatibility…

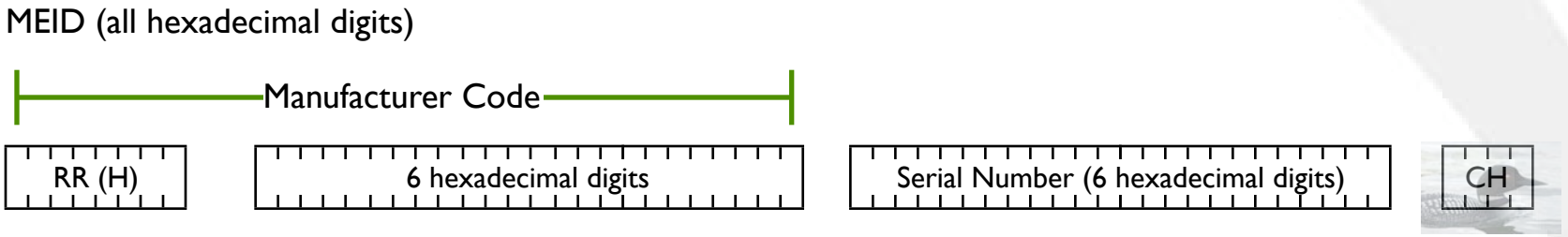
IMEI: The Basis for the MEID

IMEI (all decimal digits encoded in BCD, 4 bits per digit)



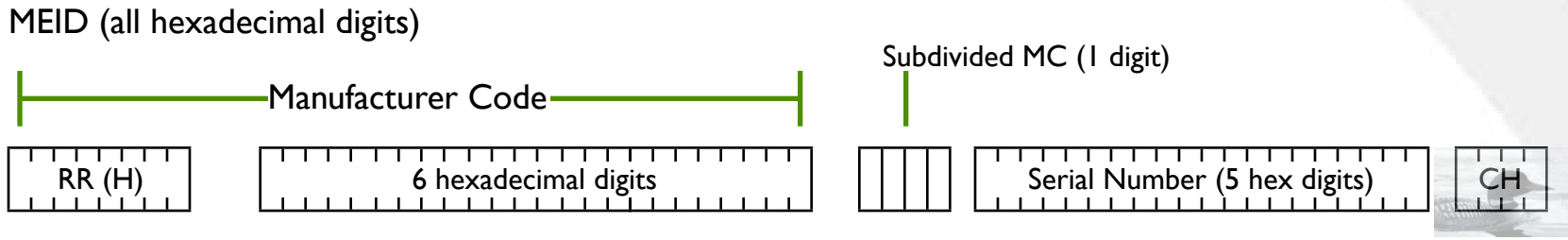
- International Mobile Equipment Identifier (IMEI) has always been used to identify GSM and W-CDMA phones.
- The basis for the MEID concept.
- Consists of 14 BCD (binary coded decimal) digits (56 bits).
- First 8 decimal digits (32 bits) identify a manufacturer (TAC=Type Approval Code).
- The remaining 6 digits (24 bits) are a serial number providing unique identification for 1 million devices.
- The Luhn Check Digit (CD) is used to validate data entry. It is not part of the stored IMEI.
- TAC codes are allocated from 00 00 00 00 upwards.
- Assignments are by GDA (Global Decimal Administrator, currently BABT) or designated regional authorities.

MEID Format



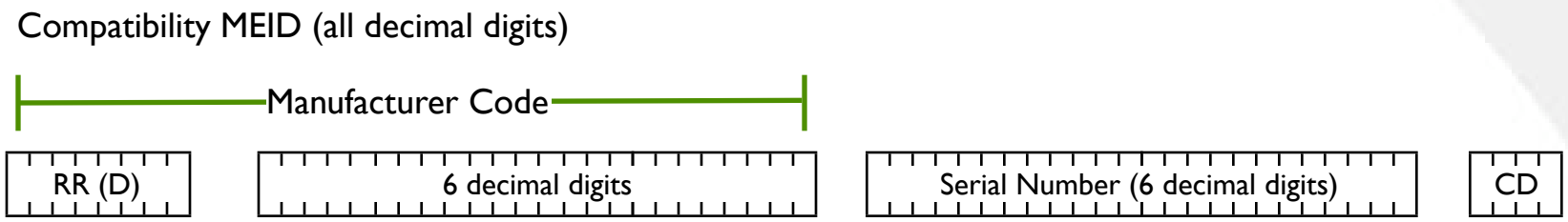
- Same size as IMEI in bits (56) and digits (14).
- All digits from the hexadecimal range (0-9 and A-F representing 10-15).
- RR digits are in the range A0 through FF to provide separation from the IMEI numbering space.
- First digit must be hexadecimal, so some RR codes are unavailable (e.g. 0A).
- Use of hex digits allows one manufacturer code to uniquely identify 16,777,216 devices (2^24) versus one million if decimal digits were used (10^6).
- 3GPP2 and TIA specifications to support MEID are in place for network, IOS and mobile interfaces.
- Assignment is by GHA (Global Hexadecimal Administrator, currently TIA) or by regional authorities (e.g. ARIB).

MEID Subdividing



- The MEID administrator is subdividing blocks for assignment to some applicants, effectively adding a digit to the Manufacturer Code.
- Such blocks provide 1,048,576 serial numbers.
- This makes number assignment more efficient.
- If a billion MEID devices were produced each year, with 50% efficiency (e.g. half of numbers wasted), the resource would last only 13 million years!
- Subdividing must be taken into account when trying to associate an MEID with a manufacturer name (e.g. in test equipment)

GSM/W-CDMA Compatible MEID



- RR is 99 (or lower, if needed)
- There are one million manufacturer codes for each RR prefix, each with one million serial numbers.
- All digits are decimal, as well as the Check Digit (CD) calculated as for the IMEI (see 3GPP TS 23.003).
- This identifier can be used in cdma2000® modes as well as in GSM or W-CDMA modes.
- Suitable for dual-mode phones that can be used in at least one cdma2000®/EVDO mode and at least one GSM/W-CDMA mode. Alternatively, phones may be given both an IMEI and an MEID.
- The display format is to show all 14 BCD digits as decimal.
- Assignment requires coordination between GHA and GDA.

Validity of Numbers

- Identifiers valid in cdma2000 networks (includes all MEIDs and IMEIs as well as numbers not yet available for allocation):

0	0	0	0	0	0	0	0	0	0	0	0	0	0
to													
F	F	F	F	F	F	F	F	F	F	F	F	F	F

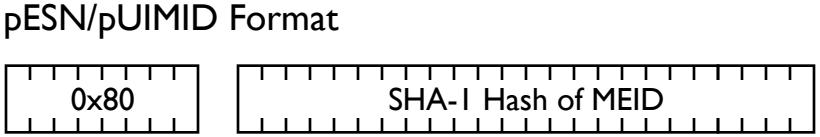
- Identifiers valid in GSM/W-CDMA networks (IMEIs only, including RR=99 codes):

0	0	0	0	0	0	0	0	0	0	0	0	0	0
to													
9	9	9	9	9	9	9	9	9	9	9	9	9	9

Display Formats

- There are three different display formats:
  - Hexadecimal MEID Display Format:
    - » 14 hexadecimal digits (e.g. 'AF 01 23 45 0A BC DE').
    - » A single hexadecimal check digit (e.g. 'C')
    - » Identified by initial digit being hexadecimal ('A'–'F')
  - Decimal MEID Display Format
    - » 18 decimal digits (e.g. '29360 87365 0070 3710', corresponding to above).
    - » A single decimal check digit (e.g. '0' for above example).
    - » Identified by length (18 digits).
  - Decimal IMEI Display Format
    - » 14 decimal digits.
    - » A single decimal check digit.
    - » Identified by length (14 digits) *and* initial digit ('0'–'9').
- All check digit calculations use Luhn formula but hexadecimal digit string requires base 16 arithmetic in formula.
- Decimal display formats are most useful when the numbers may be entered via a DTMF telephone key pad.
- The two MEID formats may be displayed together, but the IMEI only has one format.

Pseudo-ESN (pESN) / pUIMID



- MEID-provisioned MS operating in ESN-based systems must be able to provide a 32 bit ESN-like identifier for air interface and network signaling.
- pESN consists of an 8 bit reserved manufacturer's code (hex 80) and 24 bits from a hashed MEID.
- The hash is constructed using SHA-1 (Secure Hash Algorithm) with the MEID as input.
  - The same pESN will be generated from millions of different MEID codes. The pESN is not unique!
  - Two consecutive MEIDs, when hashed, will almost always produce radically different pESNs.
- The least significant 24 bits of the SHA-1 output are used as the pESN.
- The manufacturer cannot be determined from a pESN.
- pUIMID is similarly derived from EUIMID.

Signaling Considerations

- The pESN will be transmitted for every mobile provisioned with MEID unless it is overridden by the UIMID.
- MEID can be retrieved via a Status Request or OTASP Extended Protocol Capability Request.
- In cdma2000® Release D, MEID can also be included in LAC addressing, but there are no plans to implement this release.
- The mobile indicates to the base station that it is MEID capable by setting bit 4 of the SCM (Station Class Mark) — the 0x80 prefix alone must *not* be used to determine this!
- Use of the 0x80 prefix to determine that a mobile is MEID capable will fail when an EUIMID capable R-UIM is inserted into an ESN-provisioned mobile (because pUIMID also begins with 0x80) *and* when a UIMID R-UIM is placed in an MEID phone.
- ANSI-41 changes in 3GPP2 X.S0008 provide stolen and malfunctioning mobile tracking capabilities and also visibility and validation of the MEID at the HLR, but are not essential.

ESN Collisions

- The pESN and pUIMID concepts result in duplicate identifiers and the possibility of collisions…

Consequences of Collisions and Duplication

- *Duplication* occurs when mobiles with the same pESN (or pUIMID) have records in the same database.
- *Collisions* occur when duplicate pESN mobiles operate in the same or interfering sectors.
- Only a handful of applications and services require uniqueness:
  - PLCM is derived from the ESN. On the reverse channel it must be unique to separate user traffic. Two mobiles operating in the same or adjacent sectors with the same pESN may fail call attempts.
  - Databases indexed by ESN can cause the wrong record to be retrieved or not allow records to be added. This is likeliest in systems provisioning mobiles without an IMSI (e.g. OTASP).
  - ESN-based addressing on the paging channel can lead to messages such as SMS being delivered to multiple mobiles.
  - Some software for fraud detection and stolen mobile tracking may assume that ESN codes are unique.

Probability of Duplication and Collisions

- Databases that use ESN as the index (e.g. for OTASP) will have a 50% chance of at least one duplication when they contain about 4,800 pESN devices.
- It is harder to calculate the probability of PLCM collisions, but calculations for a very large, 60,000 *carrier-sector* network, with each *carrier-sector* having 6 interfering *carrier-sectors*, the number of daily collisions over the entire system will grow from 0 with no pESN mobiles to almost 600 per day with 100% pESN mobiles.
- A '*carrier-sector*' refers to a single carrier in a single sector. Each carrier in a sector operates independently from a collision perspective.
- The problem of collisions will grow as new mobiles with pESN enter the system.
- Collisions will never be more than a tiny fraction of calls, but when they occur they may persist for some time (as long as the two mobiles are in the same vicinity).

Collisions and Duplications Resolved

- Solutions can be implemented in software.
- The PLCM problem is resolved by:
  - Implementing BS-assigned PLCM, as defined in 3GPP2 C.S0072 perhaps supplemented by PLCM derived from MEID or IMSI.
  - A mobile can handoff from an ESN-based PLCM to another type (or vice-versa).
- The OTA problem is resolved by:
  - OTASP signaling, defined in C.S0016 or C.S0066. The OTAF will obtain MEID from the mobile during to determine which record in the database applies to the mobile.
  - The implementation in the MS relies on C.S0072 being implemented but *not* BSC, BTS or MSC support.
  - EUIMID visibility for EUMID-based R-UIM in an ESN mobile is being addressed by 3GPP2.
- ESN-addressed messages on the paging channel:
  - Avoid problem by using IMSI or TMSI addressing or another channel.

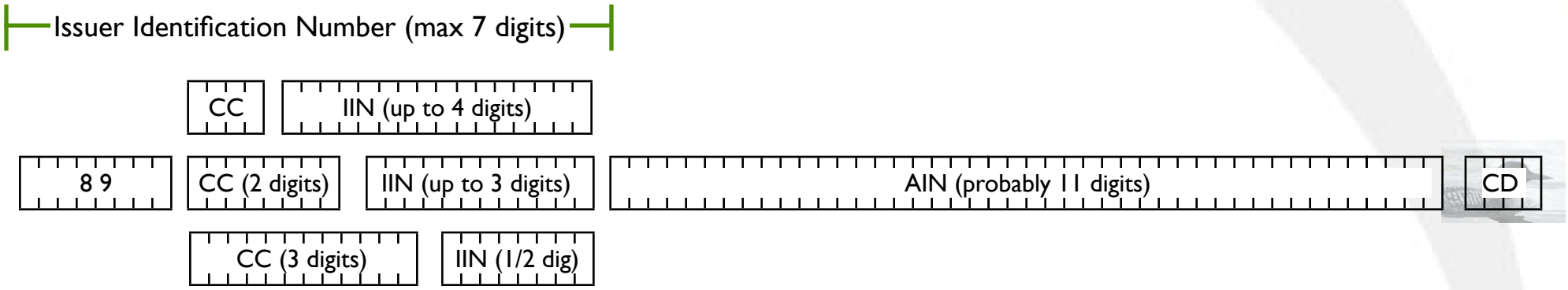
Expanded UIMID (EUIMID)

- EUIMID will replace the ESN-like UIMID. It can be based either on MEID or ICCID…

EUIMID: A Tale of Two Codes

- EUIMID replaces the 32 bit UIMID
- Two formats exist:
  - LF_EUIMID: Long Form (LF) based on ICCID
  - SF_EUIMID: Short Form (SF) based on MEID
- The two formats are compatible and roaming problems should *not* occur between systems that have chosen different formats.
- A pseudo-UIMID (pUIMID) can be produced by feeding either form into the SHA-1 hash algorithm.
- The pUIMID replaces the ESN or pESN in signaling.
- pUIMID has the same format as pESN (0x80 prefix followed by 24 bit hash).
- pUIMIDs and pESNs share the same numbering space and cannot be distinguished.
- pUIMID has the same collision problems as pESN.
- The R-UIM manufacturer cannot be determined from the pUIMID.

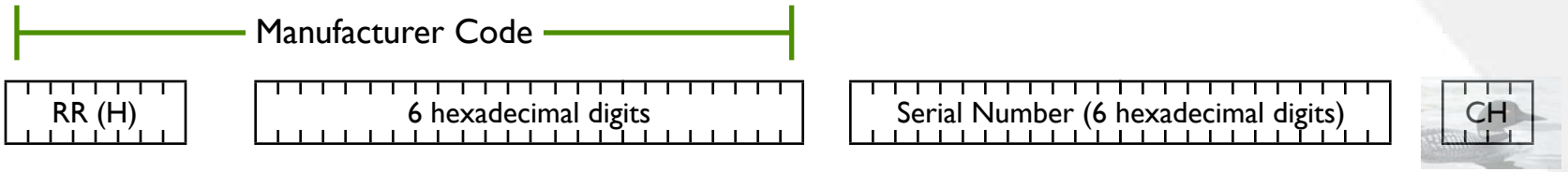
Long Form EUIMID (LF_EUIMID) - ICCID



- Already in all R-UIMs and all other smart card types (e.g. SIM).
- Standards may be modified to allow transmission of the full ICCID in the future.
- Access to the full ICCID may be useful for OTASP on 'blank' UIMs (i.e. with no IMSI).
- Administered nationally.

ICCID – International Telecommunication Charge Card ID
8 9 – Major Industry Identifier (MII) for Telecommunications
AIN – Individual Account Identification Number
CC – ITU-T E.164 Country Code; 1–3 digits (e.g.'1'=North America; 86=China, 880=Bangladesh)
CD – Check Digit (Decimal)
IIN – Issuer Identifier Number

Short Form EUIMID (SF_EUIMID) – MEID



- SF_EUIMID is based on the MEID format.
- It is recommended that UIMs be provisioned to provide not only a pUIMID but also the SF_EUIMID to override the phone's MEID. This will, however, not allow EIR capabilities.
- Standards are being modified to allow retrieval of the short form EUIMID via OTASP signaling without overriding the phone's MEID. This will enable EIR operation and provisioning that requires knowledge of both the ME and R-UIM.
- SF_EUIMID numbering requests are administered by the Global Hexadecimal Administrator, currently the TIA, or by designated regional authorities.

EUIMID Format Comparison

	SF_EUIMID (MEID)	LF_EUIMID (ICCID)
Already in UIMs?	NO	YES
Accessible to network?	If configured to override hardware MEID	May be included in future standards.
Supported by mobiles?	Requires support of n8 service from C.S0023-C	YES
Large number of issuer codes?	YES (>2 million)	YES (if IIN assigned to carrier)
Compatible with EIR?	Not currently if configured to override hardware MEID	YES
Known Users	India	China

Transmitted Identifiers Before Transition

All Mobiles Equipped with ESN

R-UIM	'ESN' transmitted	MEID available?	Notes
None	ESN	No	ESN resource almost depleted
UIMID UsgInd(b1) = '1'	UIMID		Both ESN and UIMID resources are nearly fully depleted.
UIMID UsgInd(b1) = '0'	ESN		As far as known this configuration is never used.

See spreadsheet "R-UIM, ME and Base Station Combinations" for more details.

Transmitted Identifiers After Transition

All Mobiles Equipped with MEID

R-UIM	"ESN" Transmitted	MEID?	EUIMID?
None	pESN	via Status Request	not applicable
LF_EUIMID (UsgInd b1='1')	pUIMID	via Status Request	unavailable
SF_EUIMID (UsgInd b1='1', b2='0')	pUIMID	via Status Request	unavailable
SF_EUIMID (UsgInd b1='1', b2='1')	pUIMID	not available	via Status Request

UsgInd bit 1 (b1) means that the R-UIM's 32-bit identifier (pUIMID) overrides the mobile's (pESN). Bit 2 (b2) means that the SF_EUIMID overrides the mobile's MEID.

See spreadsheet "R-UIM, ME and Base Station Combinations" for more details.

Transmitted Identifiers During Transition

MEID Support?						
BS	MS	UIM Identifier	"ESN" Transmitted	SCM bit 4	MEID?	Notes
n/a	No	EUIMID (UsgInd bit 1 = '1')	pUIMID	'0'	unavailable	Most subject to collisions because BS-assigned PLCM is not possible. No unique identifier for provisioning.
No	Yes	UIMID (UsgInd bit 1 = '1')	UIMID	'1'	unavailable	No duplication or collision problems (because of unique UIMID)
Yes					available	

See spreadsheet "R-UIM, ME and Base Station Combinations" for more details.

Protocol Changes

- Protocol changes were kept to a minimum when designing standards, but they are important to understand…

Air Interface

- 3GPP2 C.S0072 (TIA-1082) provides basic MEID support:
  - pESN is transmitted instead of ESN (unless overridden by UIMID/ pUIMID) in the LAC addressing
  - Bit 4 of the SCM (Station Class Mark), formerly reserved for TDMA, is recycled to indicate MEID support in the mobile when set to '1'. In this case an upgraded BS may:
    - » Query MS for MEID via Status Request message.
    - » Use new Channel Assignment and Handoff messages supporting BS-Assigned PLCM or PLCM derived from MEID, IMSI_T or IMSI_M.
- cdma2000® Release D provides layer 2 MEID support, but there are no current plans for its implementation.
- Should C.S0072 be modified to allow transmission of EUIMID?

OTASP - Over-the-Air Service Provisioning

- 3GPP2 C.S0066 allows the OTASP server to query the mobile for its MEID to distinguish between mobiles with the same pESN.
- There is no message to query the EUIMID unless UsgInd bit 2 is set in which case the SF_EUIMID overrides the MEID.
- This means that for the EUIMID+ESN combination there is no unique identifier for provisioning :(
- C.S0016 is being updated to allow transmission of EUIMID. C.S0066 may follow :)
- MEID transmission is transparent to intermediate legacy network elements because the "Extended Protocol Capability Response Message" carries the MEID query inside an ANSI-41 SMSDeliveryPointToPoint message.
- Transparency means that MSCs and BSs do *not* need to be updated to support MEID on the air interface to allow OTASP support for MEID to operate :)
- C.S0016 restricts access to band class information in non-MEID mobiles :(This problem is being fixed :)

Network

- The ANSI-41 network protocol is already compatible with pESN or pUIMID.
- Optionally, new and modified messages specified in 3GPP2 X.S0008 can add capabilities to ANSI-41:
  - Communication of MEID to EIR
  - Communication of MEID to VLR and HLR
  - Validation of MEID at HLR and VLR (note that this may not be compatible with R-UIM subscribers unless they are restricted to use of a single phone)
- It is recommended that CIBER records are populated with pESN or pUIMID, not MEID or SF_EUIMID, to allow continued validation of the billing records.

UIM Modifications

- Modifications are defined in 3GPP2 C.S0023-C.
- pUIMID must be provisioned into the UIMID file based on a SHA-1 hash from the chosen EUIMID format.
- When Usage Indicator (UsgInd) bit 1 is set, the pUIMID will override the phone's ESN in signaling. This behavior is no change from the treatment of UIMID.
- No new UIM Elementary Files (EFs) are needed to support LF_EUIMID (ICCID).
- Modifications required to support SF_EUIMID in R-UIMs:
  - New service n8 and an EF (Elementary File) have been defined to allow storage of SF_EUIMID (MEID-like).
  - When newly defined Usage Indicator (UsgInd) bit 2 is set the SF_EUIMID will override the mobile's MEID in signaling.
  - New service n9 provides storage for MEID in card, allowing detection of card movement. This service is optional.
- Clarifications to C.S0023-C are underway to ensure no ambiguity in the format of ICCID, calculation of pUIMID etc.

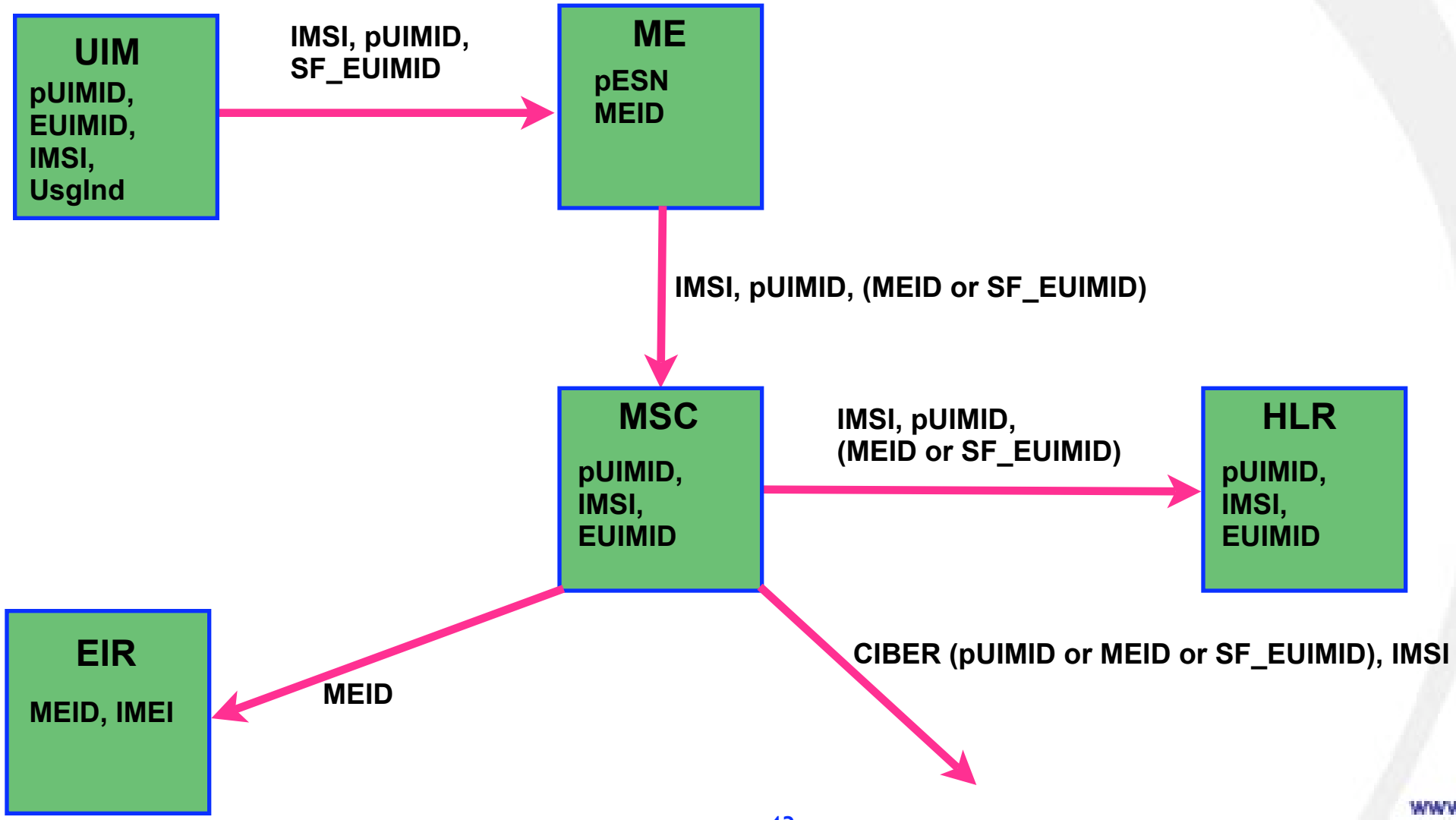
EVDO Operational Mode

- EVDO mobiles usually start in 1X mode where ESN, pESN, UIMID or pUIMID as well as possibly MEID can be exchanged.
- 3GPP2 C.S0024 supports MEID as a Hardware ID Type in queries.
- Hardware ID is used by some operators on the A12 interface for device identification. Systems that assume that the 1X 'ESN' is the same as the EVDO Hardware ID will need to be modified in networks that support R-UIM.
- MEID will always be transmitted in Hardware ID instead of ESN if available. pESN will never be transmitted. Nor will the EUIMID substitute for MEID or UIMID/pUIMID for ESN.
- HardwareIDType on the air interface does not map directly onto Hardware ID Type on the A12 interface. The RAN must understand MEID to pass the identifier through.
- AT should terminate the session when a different R-UIM is inserted.

Migration

- Migration is not complex but requires planning…

Tomorrow's Network with MEID, EUIMID



Mobile Station Migration

- Ensure that MEID and pESN are correctly provisioned.
- Ensure that UIM-capable phones support the desired EUIMID format and settings.
- Ensure that MEID-capable devices support C.S0072, including:
  - Setting SCM bit 4 properly
  - Supporting new PLCM assignment types correctly (i.e. in both new channel assignment and handoff messages)
  - Transmitting MEID in Status Request and OTASP messages
- Ensure that UIM-capable phones can operate either with R-UIM cards containing UIMID or those containing EUIMID/pUIMID.
- See 3GPP2 C.S0073 for a detailed series of tests. Rev. 0 is published and supports MEID. Rev. A will support MEID+EUIMID tests and is in development in 3GPP2.
- * R-UIM carriers should encourage rapid migration to MEID to avoid many EUIMID-equipped R-UIMs operating in ESN phones (a situation in which PLCM collisions etc., cannot be avoided).

Base Station/Air Interface Migration

- 3GPP2 C.S0072 BS-assigned PLCM should be implemented in all base stations.
- Some systems may require IOS 5.0.1 to support BS-assigned PLCM.
- Proper handling of SCM bit 4 should be verified (See CDG Technical Bulletin 070301IRT).
- Avoid “ESN-only” addressing on the paging channel
- Test all major services (such as call types, SMS, packet data access) with all combinations of legacy and new phones and UIM cards.
- Ensure BS does not check received ESN field value against pESN/pUIMID calculated from MEID/SF_EUIMID received.
- Verify the BS algorithms for determining when MEID/SF_EUIMID should be obtained.

Network and Back Office Migration

- Upgrade applications such as OTA that might rely on ESN or UIMID uniqueness.
- Consider implementing 3GPP2 X.S0008 if MEID/SF_EUIMID visibility at the HLR, MEID validation or an EIR would be beneficial.
- Verify the generation, processing and inter-carrier clearing of call detail and billing records for all combinations of UIM and ME identifier types.
- Verify ANSI-41 inter-carrier operations (including registration, call delivery and SMS) with mobiles provisioned with pESN/MEID or pUIMID/EUIMID.
- Verify OTA, call delivery, SMS and other services to a pair of mobiles with different IMSI, but identical pESN or pUIMID in the same, adjacent or different sectors.

Administration

- If LF_EUIMID is chosen, verify that national administration will result in unique assignments.
- For MEID and SF_EUIMID assignments contact the GHA (Global Hexadecimal Administrator), currently the TIA, by email to: meidadmin@tiaonline.org

Recommendations

- Develop a plan to implement MEID.
- If your network uses R-UIM develop a plan to implement EUIMID.
- If your network uses R-UIM, choose SF_EUIMID (overriding MEID) or LF_EUIMID.
- Involve your equipment vendors, software suppliers and companies that provide services.
- Plan for a small field trial using employees or select customers to ensure that all products and services work with MEID/pESN and, if applicable, EUIMID/pUIMID.
- Ensure that testing verifies BS-assigned PLCM usage by pESN/ pUIMID mobiles, ensure that ESN-addressing is not used, and verifies OTASP for new mobiles and, if applicable, new R-UIMs.

Equipment Identity Register (EIR)

- EIRs can use the MEID to track stolen or malfunctioning phones…

The Equipment Identity Register (EIR)

- An MEID from a phone can *optionally* be sent by the network to an EIR using 3GPP2 X.S0008 messaging.
- This works only when *all* following conditions are true:
  - Phone supports MEID (C.S0072).
  - MEID and pESN are provisioned in the phone.
  - MEID is not overridden by SF_EUIMID.
  - MEID is requested from the phone by a base station using Status Request.
- The EIR will report whether the mobile is:
  - Reported stolen,
  - Malfunctioning,
  - Not on a recognized list of MEID values (possibly indicating a modified MEID),
  - Needs to be tracked for some other purpose.
- This can prevent a stolen UIM-capable phone from being used with even a legitimate R-UIM.

Conclusions

- The ESN and UIMID resources are almost fully depleted.
- MEID and EUIMID are standardized and ready for implementation.
- Migration to these new identifiers takes planning.
- Problems that have been discovered have solutions.
- Migration should be completed by mid 2008.

Standards Summary

- A summary of the major standards that have been or will be modified to support MEID or EUIMID…

Key Specifications

Specification	Purpose
A.S0001~6	Base Station/MSC Interface (IOS)
C.S0016	Over-the-Air Service Provisioning (OTASP)
C.S0023-C	R-UIM with SF_EUIMID Support (storage of SF_EUIMID, storage of MEID from mobile, UsgInd bit 2)
C.S0024	EVDO with MEID Support (Hardware ID set to MEID instead of ESN)
C.S0066	OTA Support Modifications for MEID (new *Extended Protocol Capability Response* message containing MEID)
C.S0072-0	Air Interface Modifications for MEID and BS-Assigned PLCM (SCM bit 4 = '1', new PLCM assignment types, transmission of MEID in *Status Request* and *Extended Protocol Capability Response* messages)
C.S0073	Test specification for MEID-equipped mobiles. Revision A also includes EUIMID test cases.
X.S0008-0 v2.0	ANSI-41 Modifications for MEID. Defines the display formats and check digit calculations for MEID and SF_EUIMID as well as the new *CheckMEID* and *StatusRequest* messages. Allows many existing messages to carry MEID.
X.S0033	Modified OTASP network protocol including MEID at ANSI-41 level.
Consult CDG Document 158 ("MEID and EUIMID Migration") for a complete list	
3GPP2 specifications are freely available at: http://www.3gpp2.org/Public_html/specs/index.cfm	

A.S0001–6 (TIA-2001) IOS

- Revision C v2.0 of this specification (IOS 5.0.1) supported:
  - MEID and new PLCM assignment types in systems supporting C.S0072 (TIA-1082).
- Transmission of MEID in Status Request messages was transparent to this specification.
- Transmission of EUIMID in future Status Request messages will also be transparent.

C.S0016 (TIA-683) – OTASP

- Revision C (published 11/2004) provided:
  - Ability to obtain MEID (or SF_EUIMID with UsgInd bit 2=1)
- Future revision may provide:
  - Access to both MEID and EUIMID (accepted August 2007).
  - Resolution of band class/MEID interaction.
- To be resolved:
  - Should transmitted EUIMID be 18 or 20 digits?

C.S0023 (TIA-820) R-UIM Specification

- Revision C (published 06/2006) provides:
  - SF_EUIMID storage
  - Service n8 (SF_EUIMID)
  - Service n9 (storage of MEID)
- New version may provide clarification of:
  - Ordering of ICCID into SHA-1 algorithm to calculate pUIMID.
  - Transmission of 18 or 20 digits for ICCID outside R-UIM.
  - Ordering of digits in SF_EUIMID field.
  - Number of bits in ESN/UIMID (text currently implies they can be 32 or 56 bits, not just 32.

C.S0024 (TIA-856) – EVDO/HRPD

- A high speed data standard within the cdma2000 family.
- Most EVDO or HRPD phones also operate in 1X mode, and thus most impacts from MEID and EUIMID are restricted to that mode.
- It is important to recognize that the EVDO "Hardware ID" parameter is either:
  - ESN, or
  - MEID
- This parameter is never UIMID or EUIMID.
- The only standards change that might be required is a clarification that Hardware ID is never an R-UIM identifier.

C.S0066 (TIA-158) – OTASP for MEID

- This specification was designed to provide MEID support to previously published versions of C.S0016.
- Revision 0 (Published 09/2004) provided:
  - Access to MEID (or SF_EUIMID) during OTASP session.
- A possible future revision may provide:
  - Access to EUIMID as well as MEID during OTASP session.
  - Resolution of band class problem.
- To be resolved:
  - Should transmitted EUIMID be 18 or 20 digits?

C.S0072 (TIA-1082) – MEID in Air Interface

- Revision 0 of this standard (published 08/2005) provided:
  - New PLCM derivation types including BS-assigned at call setup and handoff.
  - Access to MEID (or SF_EUIMID) via Status Request.
- A possible revision of this standard would provide:
  - Access to both MEID and EUIMID via Status Request.

C.S0073 (TIA-1084) – MEID Test Spec'n

- Revision 0 of this specification (published 10/2005) provided:
  - An extensive sequence of test cases for MEID-equipped mobiles.
- Revision A (publication estimated April, 2008) will provide:
  - Test cases for MEID-equipped mobile with R-UIM with either SF_EUIMID or LF_EUIMID.
  - A note indicating that testing R-UIMs equipped with EUIMID in ESN-based mobiles should use C.S0043 and C.S0044, such tests are outside the scope of this specification.

X.S0008 (TIA-928) – MEID in ANSI-41

- Revision 0 of this specification (published 07/2004) provided:
  - Transmission of MEID from MSC to VLR to EIR.
  - Optional inclusion of MEID in most ANSI-41 messages.
- Addendum 1 of Revision 0 (published 11/2005) provided:
  - MEID validation at the HLR (verifying that the MEID being used by a subscriber does not change). This capability is not applicable to all R–UIM subscribers.
- A possible future revision may provide:
  - Visibility of the EUIMID at the VLR and HLR.

X.S0033 (TIA-1074) – OTASP in ANSI-41

- Revision 0 of this standard (published in 11/2005 and revised in 03/2006) provides:
  - Inclusion of MEID in ANSI-41 messages supporting OTASP, providing an alternative to transmitting MEID in the OTASP signaling layer.

Resources

- A glossary. Also see http://cdg.org/MEID

Glossary

Term	Definition	Term	Definition
3GPP2	Third Generation Partnership Project	PLCM	Public Long Code Mask
BABT	British Approvals Board of Telecommunications	R-UIM	Removable UIM
ESN	Electronic Serial Number	SCM	Station Class Mark
EUIMID	Expanded UIMID	TDMA	Time Division Multiple Access
IMEI	International Mobile Equipment Identity	TIA	Telecommunications Industry Association
IMSI	International Mobile Subscription Identity	UIM	User Identification Module
IOS	Inter-Operability Standard ('A' Interface)	UIMID	R-UIM Identifier
MEID	Mobile Equipment Identifier		

Thank You