MEID Standards Update

(version 1.1 – February 2004)

TIA Committee TR-45

Authors:
David Crowe
(David.Crowe@cnp-wireless.com)
Ravindra Patwardhan
(ravindra@qualcomm.com)
TIA ESN/UIM/MEID ad hoc

TIA Website: http://www.tiaonline.org

Equipment vs. Subscription Identifiers

- An equipment identifier is a globally unique number for a physical piece of equipment. Equipment identifiers are ‘burned’ into a device, and should be resistant to modification.
- A subscription identifier is a globally unique number that can be associated with (usually) a single device for the purpose of wireless communication. Examples are MIN and IMSI. The device associated with the subscription identifier may change (e.g. when a UIM is inserted into another phone).

Equipment Identifier Examples

- MAC Address is a 48 bit identifier for Ethernet and WiFi devices.
- ESN (Electronic Serial Number) is a 32 bit number invented for AMPS. Sometimes what is transmitted is not a true ESN (tESN), but a pseudo-ESN (pESN) or UIMID.
- UIMID is a 32 bit number that identifies a UIM for use on TIA-41 networks. The UIMID may replace the ESN in air interface and TIA–41 messages.
- Pseudo-ESN (pESN) is a 32 bit hash of the MEID that will replace the true ESN for MEID-equipped terminals.
- IMEI is a 56 bit (14 decimal digit) identifier for GSM and W-CDMA terminals.
- MEID is an IMEI using hexadecimal digits (except for devices that also support GSM or W-CDMA modes).

ESN Issues

Many lessons were learned over 20 years of experience with ESN. Characteristics that will not be repeated with MEID are:

- ESN was tied to a single subscription, because of the need to match an MSID with a single ESN for HLR validation and assist in early fraud control efforts.
- ESN was used as an input to authentication.
- ESN was used to derive the Public Long Code Mask (PLCM) for CDMA phones.
- Only 256 distinct manufacturer assignment blocks existed.
- ESN codes were initially assigned by a national authority (FCC), rather than a global authority.

ESN Substitutes

It will sometimes be necessary to use UIMID or pESN as a substitute for a true ESN (tESN) on radio interfaces and in the TIA–41 networks:

- UIMID is stored on a UIM and used to maintain the static MSID/ ‘ESN’ association required by TIA-41 validation and CAVE authentication. Each UIMID should be unique, not matching any other assigned UIMID or tESN.
- Pseudo ESN (pESN) is derived from the MEID using the SHA-1 algorithm to reduce 56 bits to 24. pESN codes are not unique, but will not match any UIMID or tESN because they have a unique manufacturer code of 0x80 (decimal 128)
- An ESN type can be distinguished as tESN, UIMID or pESN based on the first 8 or 14 bits (‘manufacturer’ code).

Pseudo-ESN (pESN)

Pseudo-ESN is used in places where ESN is used

- RN_HASH_KEY. Used to randomize the start of transmission in CDMA systems.
- IMSI_M & IMSI_T (if not configured, last 4 digits derived from ESN).
- CAVE Authentication input.
- ESN based PLCM. This will only be used by legacy base stations (P_REV < 11) as there will be other ways to generate PLCM for Release C and beyond.
- Pseudo-random Number Generator for CDMA timer-based registration.
- Replaces the ESN in CDMA status response/extended status response message.
- LAC header on CDMA r-csch.

Purposes of MEID

- Allow special handling for stolen or malfunctioning devices.
- Migration from 32 bit ESN, which may be exhausted by 1Q05.
- Accommodate future subscriber growth through a larger identifier (56 bits, 14 hexadecimal digits).
- Identification of CDMA terminals conforming to TIA-2000 Release D or later and TDMA terminals conforming to TIA-943.
- Compatibility with 3GPP terminals for multi-technology devices (GSM, CDMA, W-CDMA, TIA-136/943).
- Separation from 3GPP terminals for terminals without GSM or W–CDMA operational modes through the use of hexadecimal digits.
- Stage I Requirements are defined in 3GPP2 S.R0048-A . This includes a detailed report from an April, 2002 Joint Experts Meeting (JEM).

MEID Format

MEID (14 Hexadecimal Digits, 56 bits)

Manufacturer Code								Serial Number						C D
RR		XXXXXX												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Definitions of MEID Fields

Manufacturer Code.

- RR - Regional Code. A0-FF are assigned by the Global Hexadecimal MEID Administrator (GHA). Other codes are reserved for use as IMEIs. RR=99 is reserved for MEIDs that can also be used as IMEIs.
- XXXXXX - 6 hexadecimal digit code assigned by the regional administrator to a manufacturer for a line of phones.

Serial Number - Assigned by manufacturer to identify an individual device.

CD - Checksum Digit. Not transmitted.

Comparison with IMEI

- MEID and IMEI are the same size (14 four-bit digits).
- MEID allows the use of hexadecimal digits (note: first digit must be “A” to “F” to distinguish MEID from IMEI).
- IMEI must be used by phones with GSM/UMTS capabilities (i.e. all 3GPP/3GPP2 multimode phones).
- The meanings of some digits within the MEID and IMEI differ slightly.
- 3GPP does not support regular transmission of the IMEI, so tracking stolen phones is difficult.
- MEID provides more unique codes (>27 x 1015 codes) than IMEI because of the use of hex digits and because digits are less constrained (e.g. the first two digits of IMEI are the country code of the manufacturer).

Administration & Standardization

Support for the MEID requires a number of administrative and standardization activities:

- Defining the requirements for the MEID.
- Defining and implementing the process for assigning MEID codes to manufacturers.
- Modifying radio interface and network protocols to support MEID.
- Back office administration modifications as determined by carriers.
- (Optional) Supporting an Equipment Identity Register to validate MEIDs.

These activities are well under way.

Administration

3GPP2 completed MEID Administrative Procedures in S.R0088 and Assignment Guidelines in S.R0089 at the end of 2003.

- A Global Hexadecimal Administrator (GHA) will assign MEID code prefixes.
- The TIA will act as the GHA, which already acts as the ESN administrator.
- Phones that also operate in GSM or UMTS modes will need to acquire an IMEI instead or use a decimal MEID assigned by the GHA from RR=99.
- IMEIs will continue to be assigned by the GDA.

MEID Support in Standards

Support for MEID in standards is still being defined. A Stage 1 description has been revised as 3GPP2 S.R0048-A. Protocol changes being examined are:

- Transmission of MEID from ME over TIA-2000 Release D air interface upon request (Status Request message).
- Transmission of MEID instead of ESN in CDMA LAC Addressing (based on PREF_MSID_TYPE, EXT_PREF_MSID_TYPE).
- An overhead flag (MEID_REQD) may be added to include MEID in Origination, Page Response and Registration.
- Addition of MEID to IOS (BSC/MSC interface).
- Adding and updating TIA-41 messages to include MEID.
- Using MEID as a database index for OTA instead of ESN.

Standards Timeline

Interface	Standard	Pub’n
Assignment Guidelines	S.R0089-0	01/2004
Law Enforcement	J-STD-025-C	11/2004
MSC-VLR-EIR-HLR	TIA-928/X.P0008	07/2004
MSC-PSAP (E911)	J-STD-036-B	tbd
MSC-BS	IOS/A.S0001	1Q’04
Packet Data	TIA-835/X.S0011	tbd
Radio (CDMA)	TIA-2000-D/C.P0005-D	1Q’04
Radio (TDMA)	TIA-943	11/2003

EIR – Equipment Identity Register

Standards for MEID will support an EIR as a carrier option. It maintains three different lists of MEIDs, and can be queried using the new TIA–41 CHECKMEID message:

- Normal (‘White’) list – A list of assigned MEID code ranges (not a list of individual MEID codes).
- Block (‘Black’) list – A list of MEIDs that should be denied service (e.g. because they represent stolen phones or those with service-impacting hardware issues).
- Track (‘Grey’) list – A list of MEIDs to be tracked (but not denied service). This includes lost phones and those with minor hardware issues.

EIR’s need to be globally linked or centralized to maximize their ability to track mobile equipment.

CDMA PLCM Generation

For Release C and beyond, BS decides which PLCM type to be used (signals in ECAM, UHDM):

- BS assigned PLCM
  - PLCM collision not an issue
  - BS uses LAT/LONG based or proprietary scheme to avoid collisions
- MEID based PLCM
  - No signaling overhead (need not include PLCM bits in signaling message)
  - Probability of PLCM collision less than pseudo-ESN based PLCM, but not zero

PLCM Generation (cont’d)

IMSI based PLCM

- Use IMSI_S (34 bits) in PLCM
- No signaling overhead
- No collision when used in home network
  - » IMSI_T case: IMSI_S unique in a given MCC & MNC
  - » IMSI_M case: IMSI_S unique in given MCC and operator

ESN based PLCM

- For backwards compatibility (P_REV < 11)

CDMA PLCM Format

BS assigned and MEID based PLCM

- Currently unused value used for bits 41-40. Ensures no PLCM collisions with legacy PLCM generation procedures.
- Bit 39 distinguishes *BS assigned* from *MEID based* PLCM
- Ensures no PLCM collision between 2 generation options.

IMSI based PLCM

- Currently unused value used for bits 36-35. Ensures no PLCM collisions with legacy PLCM generation procedures.
- Bit 34 distinguishes *IMSI_M (MIN)* from *IMSI_T based* based PLCM.
- Ensures no collision between 2 PLCM generation options.

CDMA PLCM Formats

BS Assigned PLCM

4x		3x										2x										1x										0x									
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0
1	0	1	39 bits assigned by BS																																						

MEID based PLCM

4x		3x										2x										1x										0x									
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0
1	0	0	39 bits from MEID hash																																						

IMSI_M (MIN) based PLCM

4x		3x										2x										1x										0x									
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	1	IMSI O S (34 bits)																																	

IMSI_T (True IMSI) based PLCM

4x		3x										2x										1x										0x									
1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	0	IMSI O S (34 bits)																																	

New CDMA LAC Addressing

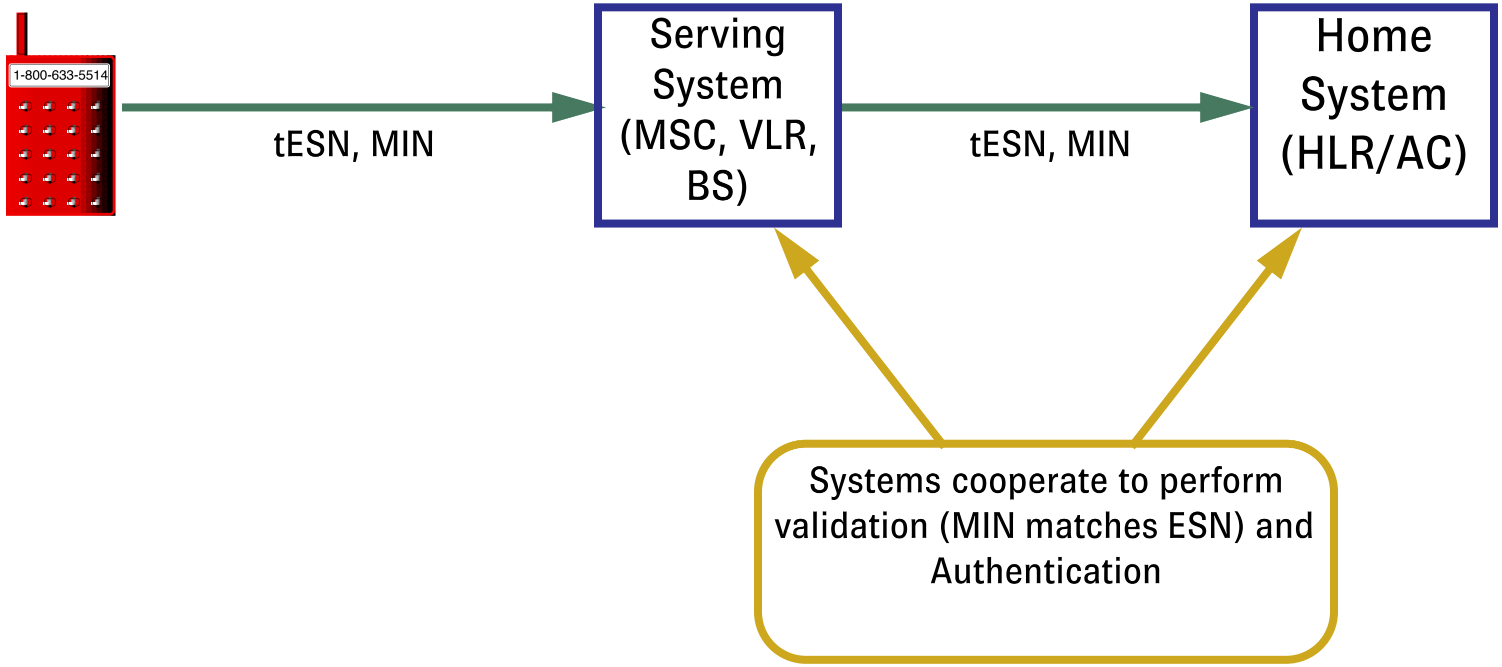
(P_REV_IN_USE ≥ 11)

MS without R-UIM OR R-UIM Usage Indicator ≠ “Use UIMID”	
EXT_PREF_MSID_TYPE	PREF_MSID_TYPE = “ IMSI+ESN” instructs MEID-equipped MS to transmit…
00	IMSI + pESN
01	IMSI + MEID
MS with R-UIM AND R-UIM Usage Indicator = “Use UIMID”	
EXT_PREF_MSID_TYPE	
00	IMSI + UIMID
01	
10	reserved for future use
11	IMSI + UIMID + MEID

Information Flows

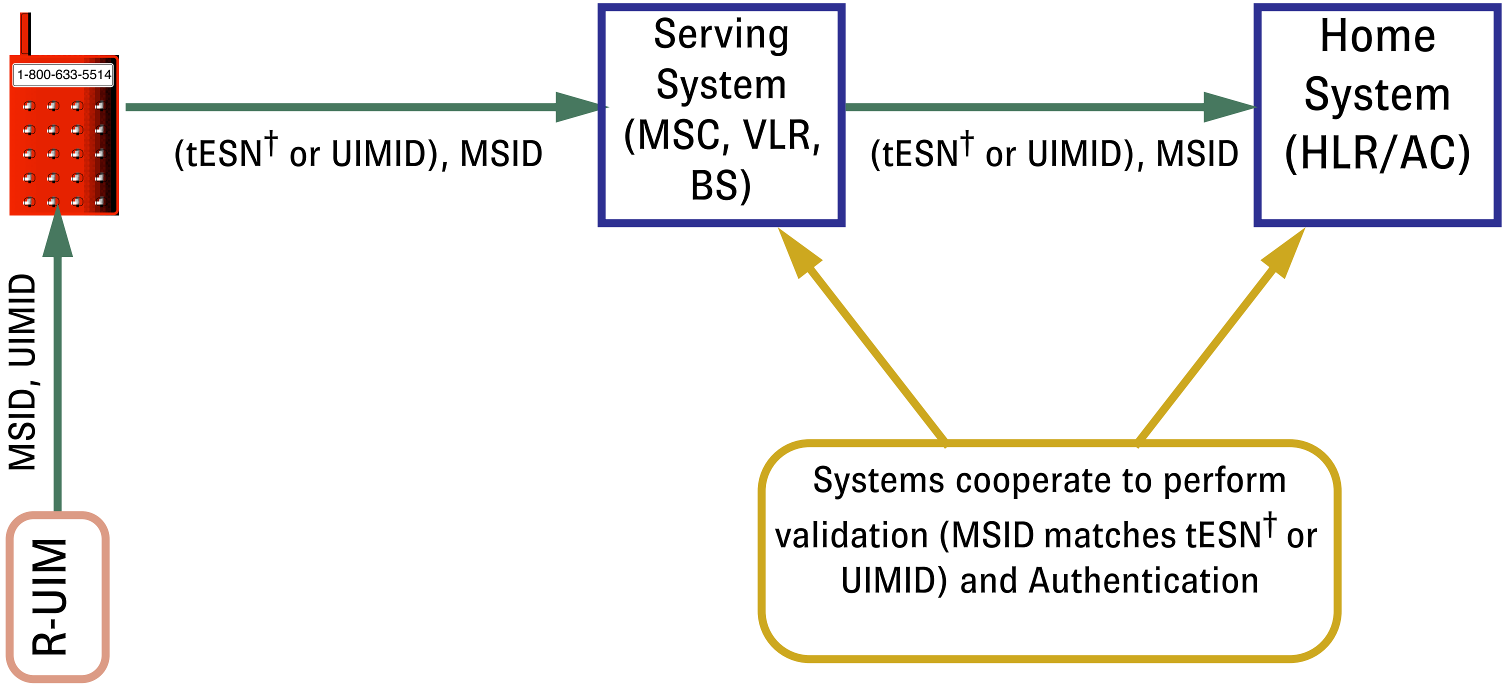
- Basic ESN Usage
- ESN with R-UIM
- MEID in Backwards Compatibility Mode
- MEID with R-UIM in Backwards Compatibility Mode
- MEID Usage
- MEID with R-UIM

Basic ESN Usage



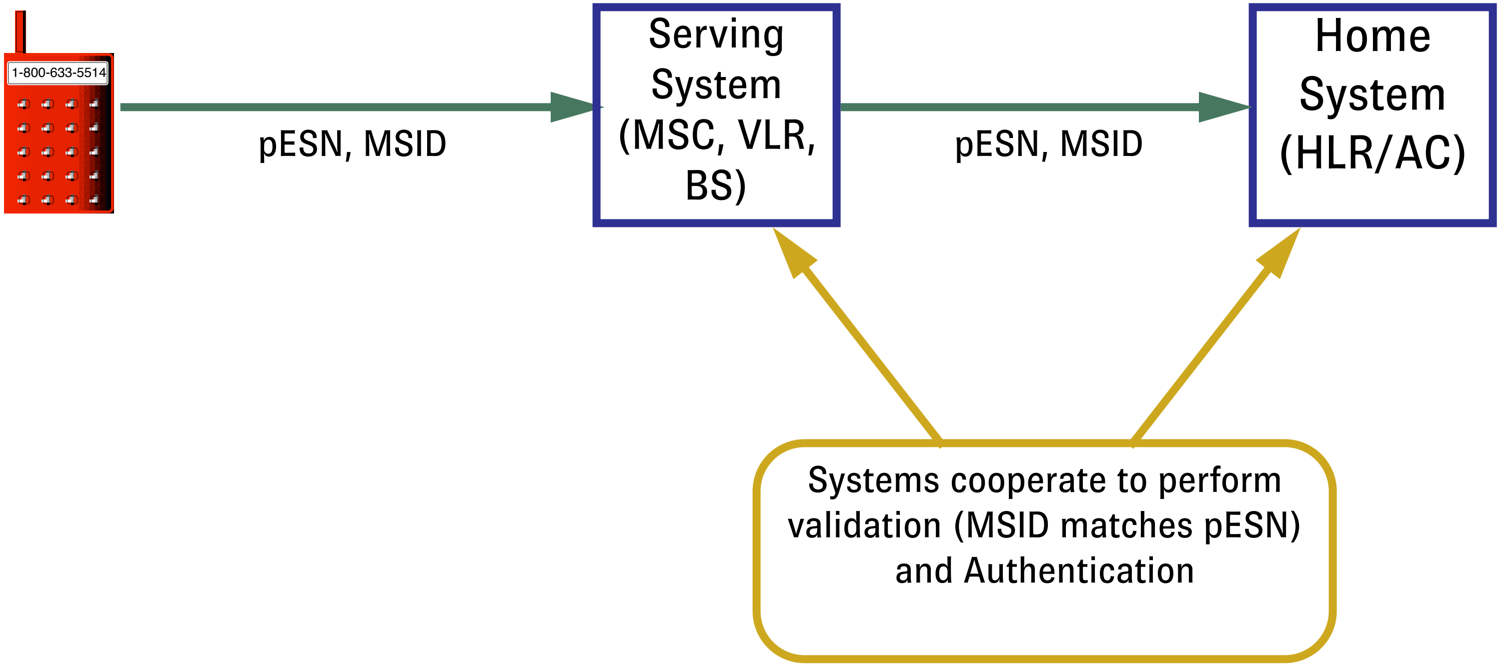
Systems cooperate to perform validation (MIN matches ESN) and Authentication

ESN with R-UIM

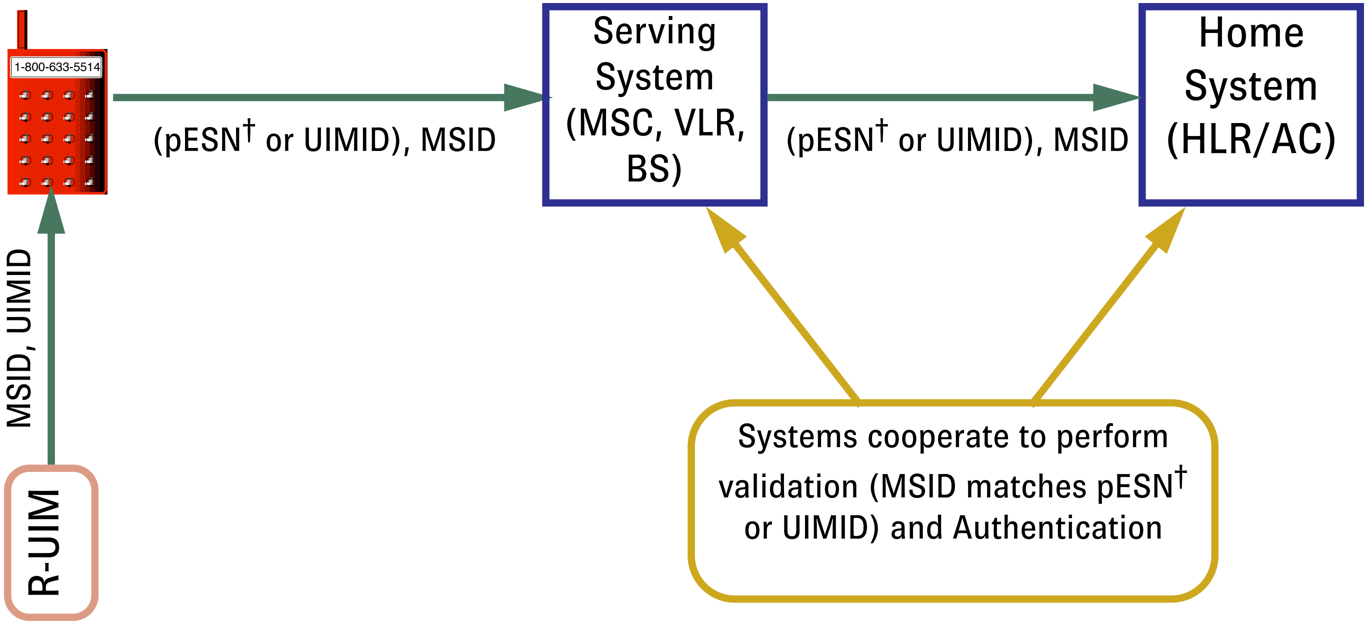

1-800-633-5514
(tESN† or UIMID), MSID
Serving System (MSC, VLR, BS)
(tESN† or UIMID), MSID
Home System (HLR/AC)
MSID, UIMID
R-UIM
Systems cooperate to perform validation (MSID matches tESN† or UIMID) and Authentication

† Using the True ESN instead of the UIMID will cause problems if the UIM is moved between phones while roaming.

MEID in Backwards Compatibility Mode

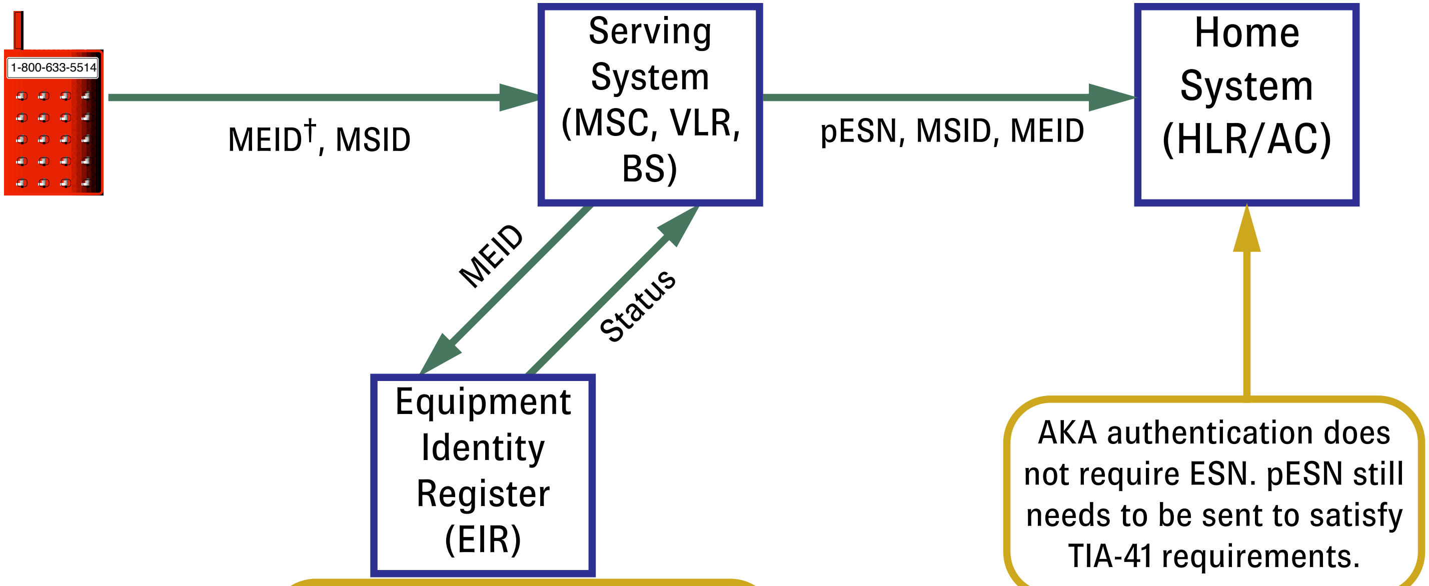

1-800-633-5514
pESN, MSID
Serving System (MSC, VLR, BS)
pESN, MSID
Home System (HLR/AC)
Systems cooperate to perform validation (MSID matches pESN) and Authentication

MEID with R-UIM in Backwards Compatibility Mode


1-800-633-5514
(pESN† or UIMID), MSID
Serving System (MSC, VLR, BS)
(pESN† or UIMID), MSID
Home System (HLR/AC)
MSID, UIMID
R-UIM
Systems cooperate to perform validation (MSID matches pESN† or UIMID) and Authentication

† Using the Pseudo ESN instead of the UIMID will cause problems if the UIM is moved between phones unless the serving system supports IS-808 dynamic rebinding.

MEID Usage

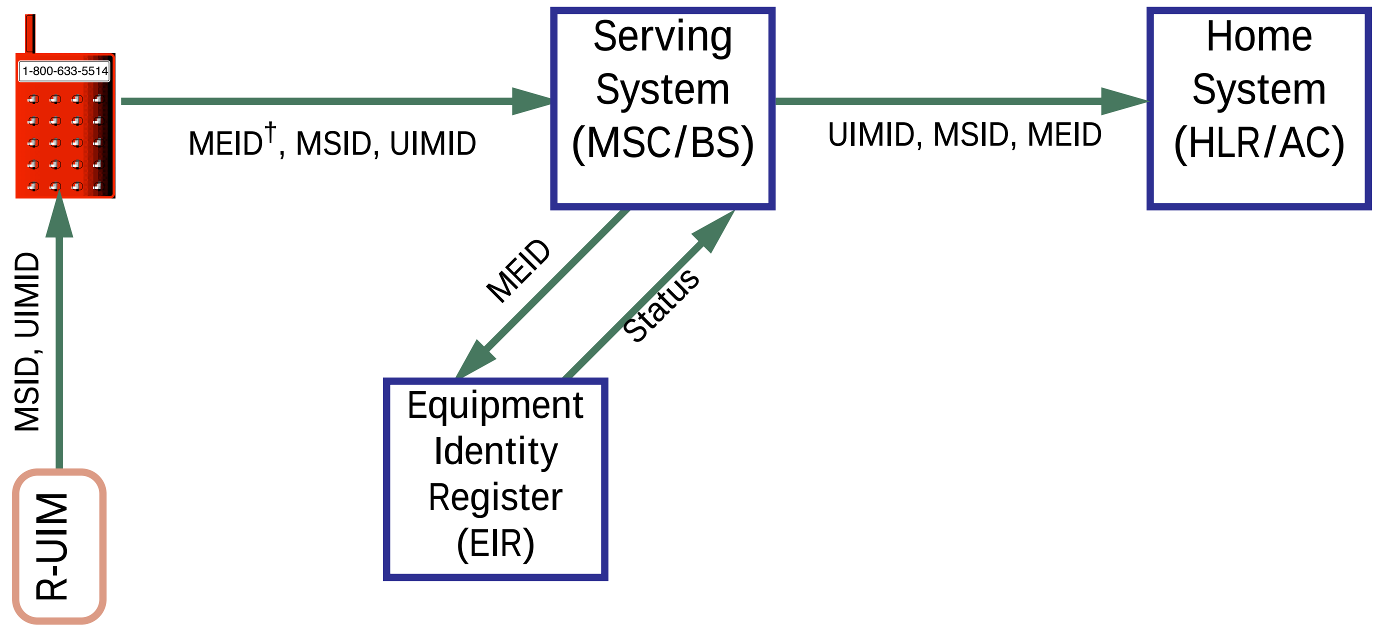


AKA authentication does not require ESN. pESN still needs to be sent to satisfy TIA-41 requirements.

MEID validation is a serving system responsibility. Status may be 'normal', 'block' or 'track'.

† MEID may not need to be sent on every access.

MEID with R-UIM



† MEID may not need to be sent on every access.

When is MEID Transmitted?

	no R-UIM				R-UIM			
ME	no MEID		MEID supported		no MEID		MEID	
Serving	no MEID	MEID	no MEID	MEID	no MEID	MEID	no MEID	MEID
tESN	Must be transmitted		n/a		Transmit UIMID (or tESN)		n/a	
UIMID	n/a						Depends on PREF_MSID_TYPE, EXT_ PREF_MSID_TYPE and Usage Indicator	
pESN	n/a		Depends on PREF_MSID_TYPE and EXT_ PREF_MSID_TYPE		n/a			
MEID								

Note: Coloured shading is for enhanced legibility only.

3GPP Compatibility

ME	3GPP (GSM, W-CDMA)		3GPP2 (cdma2000, TDMA)	
Serving	3GPP2	3GPP	3GPP2	3GPP
tESN	n/a			
UIMID	If requested and available	n/a	If requested and available	n/a
pESN	If requested		If requested	
MEID	n/a			Must be decimal
IMEI	If requested	Transmit	n/a	

Glossary

Term	Definition
3GPP	3G Partnership Project
3GPP2	3G Partnership Project 2
AC	Authentication Center
BS	Base Station
CDMA	Code Division Multiple Access
CDMA	Code Division Multiple Access
EIR	Equipment Identity Register
f-csch	CDMA Forward Common Signaling Channel (BS to ME/MS)
GDA	Global Decimal Administrator (for IMEI)
GHA	Global Hexadecimal Administrator (for MEID)
GSM	Global System for Mobility
HLR	Home Location Register
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscription Identity
IMSI_M	CDMA version of MIN
IMSI_S	10 digit version of IMSI
IMSI_T	CDMA True IMSI
IOS	Inter-Operability Standard (‘A’ Interface)
LAC	Link Access Control
ME	Mobile Equipment (ME + R-UIM = MS)
MEID	Mobile Equipment Identity

Glossary (cont'd)

Term	Definition
MIN	Mobile Identification Number
MSID	Mobile Subscription Identifier (MIN or IMSI)
pESN	Pseudo ESN
PLCM	Private Long Code Mask
P_REV	CDMA Protocol Revision
r-csch	CDMA Reverse Common Signaling Channel (MS/ME to BS)
R-UIM	Removable UIM
TDMA	Time Division Multiple Access
tESN	True ESN (not pESN or UIMID)
TIA	Telecommunications Industry Association
TR-45	TIA Technical Review Committee
UIM	User Identification Module
UIMID	UIM Identifier (ESN-like)
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
W-CDMA	Wideband CDMA

Summary

- MEID is the equipment identifier of the future.
- MEID provides operators with optional capabilities to track stolen or malfunctioning mobiles that are superior to those available with ESN or IMEI.
- It solves many of the problems with ESN, including code exhaustion.
- MEID can be tracked more reliably than GSM or UMTS can track IMEI.
- Implementation and support of MEID by carriers can be phased in as the need arises.
- Support in standards is rapidly being developed.