Cellular Networking Perspectives

Editor: David Crowe • Email: David.Crowe@cnp-wireless.com Vol. 10, No. 9 September, 2001

In This Issue...

Data Snapshot

For a summary of major cellular and PCS data technologies, consult:

www.cnp-wireless.com/data.html

Please send us any comments, corrections or additions to this information that you have.

Next Issue: October 1st, 2001

CALEA Rolls Over

Telecom industry adherence to the US government CALEA legislation for electronic surveillance is not dead. Perhaps somnolent (half-asleep) would be a better description. On good days it is quite active, but most of the time it is resting, waiting for the sun to warm again.

FCC order DA 01-1902 (Docket 97-213) was released on August 15, 2001. It provides an extension to the CALEA deadline to over 700 mostly small US telecom carriers (not just wireless).

The industry standardization effort on CALEA has been on hold since a US Appeals court ruling on August 15, 2000 overturned much of the original FCC order on CALEA. However, an August 29, 2001 meeting initiated a joint TIA TR-45/ATIS T1 ad hoc group, which agreed to initiate a project to produce "a revision of [J-STD-025-A] to refine the packet data surveillance solution". This project is being initiated even though a request for clarification of requirements to the FCC has not yet been answered.

The ad hoc group was recently elevated from TR-45.2 to TR-45, as its focus on packet data requires cooperation of other subcommittees, particularly TR-45.6, which is responsible for wireless packet data standards.

There has been some discussion of the consideration of international requirements for lawfully authorized electronic surveillance in the ad hoc group. TR-45 has long had Canadian carriers as members, and its subcommittees now work closely with 3GPP2, which has members from Japan, Korea and China. For many countries, however, electronic surveillance is a sensitive area, and they may be uncomfortable with the open process used for the development of standards for CALEA. However, the lure of cheaper wiretapping equipment from economies of scale is also great. To this end, some of the more European-focused work in 3GPP will be considered.

TIA Spins Standards Off

On August 20, 2001 the TIA announced that it intended to spin its large standards development organization off as an autonomous entity, leaving the TIA as a US-based trade association with lobbying and trade-promotion activities as its focus. Active standards committees currently within the TIA – and their study topics – are:

TR-8	Private Radio (including public safety communications)
TR-14	Microwave Communications
TR-30	Fax, Modems and TTY
TR-34	Satellite
TR-41	User premises terminals
TR-42	User premises cabling
TR-45	AMPS, N-AMPS, D-AMPS, CDMA cellular and PCS
TR-46	GSM
FO-2	Optical Communications Systems (test and specification)
FO-6	Fiber Optics

Editor: David Crowe.
Accounts: Evelyn Goreham.
Marketing: Muneerah Vasanji.
Distribution: Debbie Brandelli.
Production: Doug Scofield.

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Crescent NW, Calgary AB, T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** www.cnp-wireless.com.
Subscriptions: CDN$350 in Canada (incl. GST), US$350 in the USA and US$400 elsewhere. Payment by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery***:* Email or 1st class mail.
Back Issues: Single issues are $40 in the US and Canada and $45 elsewhere, or in bulk at reduced rates.
Discounts: Educational and small businesses: 25% off any order. **Copies***:* Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

This change will allow companies from outside the United States to hold full membership in TIA standards development. Standards produced by its committees are already in use worldwide, and this move may bring greater acceptance.

The other major US-based telecommunications organization is ATIS (Alliance for Telecommunications Industry Solutions). There is considerable overlap between the standards development activities of TIA and ATIS. For example, TR-46 and ATIS T1P1 both work on the adaptation of GSM to North American requirements. It is reasonable to speculate that this is the first step towards a merger of these two bodies.

IMEI - The GSM Mobile Equipment Identifier

The International Mobile Equipment Identifier (IMEI) is a unique number assigned to every GSM phone. It is similar in concept to the ESN (described in our August, 2001 issue) used for identification by AMPS, D-AMPS (ANSI-136) and cdma2000 mobiles. IMEI and ESN differ from subscription identifiers (IMSI and MIN) that can be moved by a subscriber from phone to phone and that are used to control billing and other subscription-oriented services.

IMEI versus ESN

IMEI is a pure equipment identifier, largely due to the physical split between a phone (Mobile Equipment - ME) and the SIM (Subscriber Identity Module or 'Smart Card') that is a characteristic of GSM or the similar UIM (User Identity Module) used by UMTS. The ESN, on the other hand, is currently used for validation and authentication, which means it has to be recorded along with other subscription data. This use of the ESN has made the implementation of Smart Cards – in standards that use it – much more challenging.

Role in GSM

Because the IMEI identifies phone hardware, it plays no role in the validation or authentication of GSM (and UMTS) phones. In fact, for some time, this separation made it difficult to track stolen phones that were being used with a legitimate SIM card. Since only the SIM identity (IMSI) was required for operations, a stolen phone could be used virtually with impunity.

Emergency Calling

There is one tiny place where the IMEI plays a role in GSM/UMTS call processing – for an emergency call placed in a phone without a SIM/UIM installed, which means the phone will have no IMSI or TMSI available to identify itself. This normally precludes a mobile from being able to make a call, but emergency calls are an exception. In this case, the IMEI is transmitted instead of IMSI or TMSI. It is still not used for validation, but could be used to track the use of a GSM phone being used to make prank or malicious emergency calls.

EIR - Equipment Identity Register

The EIR (Equipment Identity Register) was always defined in GSM standards, but not originally implemented. Unlike the HLR (Home Location Register), which contains a list of subscribers indexed by IMSI, the EIR contains lists of mobile phones indexed by IMEI. Consequently, when a phone is known to be stolen or malfunctioning, consulting the EIR can block it from obtaining service.

The EIR may contain three lists:

- White List. All valid IMEI ranges.
- Grey List. Individual IMEI codes that are being tracked, but still allowed to obtain service.
- Black List. IMEIs of mobiles that are barred from obtaining service (e.g. stolen or incorrectly functioning).

Mobiles are denied service if they have an IMEI that is in the Black list or *not* within any range in the White list.

An IMEI can be checked by an MSC or VLR sending a 3GPP 29.002 MAP_CHECK_IMEI message to the EIR.

Structure of the IMEI

The IMEI structure (see Figure 1) is defined in 3GPP TS 23.003 (Numbering, addressing and identification). The TAC and FAC fields are similar in function to the Manufacturer's Code field of the ESN. The SNR field corresponds to the Serial Number field of the ESN, and is uniquely assigned by a manufacturer to a single mobile. The SV field is transmitted along with the IMEI, but it is not strictly considered part of it.

The IMEI is transmitted as 16 decimal digits, encoded using BCD and stored two to an octet. Consequently, the IMEI is transmitted as 8 octets.

Obtaining the IMEI

On most GSM phones, the IMEI can be obtained with the key sequence "*#06#". However, the manufacturer's phone manual should be checked to be sure.

A single check digit, calculated from the remainder of the IMEI (see 23.003 for details) is also shown on the phone display. This is used to reduce manual data entry errors (e.g. when entering the IMEI of a stolen phone into a database).

A base station can obtain the IMEI (without the check digit) by transmitting a 3GPP 24.008 IDENTITY REQUEST message to the mobile.

An MSC can either obtain the IMEI from the mobile via the base station, or from the VLR using a 3GPP 29.002 MAP_OBTAIN_IMEI message (assuming that another MSC has already cached it there).

How Many are There?

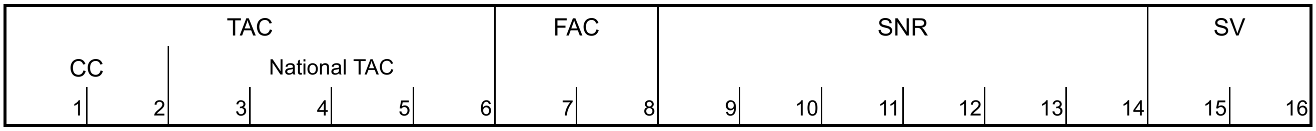
The IMEI is transmitted as a 16 decimal digit number. However, the SV (Software Version Number) is not part of the IMEI. Furthermore, each country normally uses only one CC (country code), meaning that each country can assign a trillion unique codes. The actual number assigned will be less than this, because there is some inefficiency of assignment (e.g. a TAC will probably not be fully utilized).

Assigning the IMEI

Unlike the ESN, which is assigned globally to manufacturers, IMEI codes can be assigned independently by each country (the country of the manufacturer, not of the carrier where the phone is subscribed). The only time when international coordination might be needed is when a

Figure 1: Structure of the IMEI

IMEI (16 Decimal Digits)



Definitions of IMEI Fields

TAC - Type Approval Code.

CC - E.164 Country Code of Manufacturer (e.g. 01 for USA, 44 for UK).

National TAC - Type Approval Code assigned by national authority.

FAC - Final Assembly Code. Assigned by manufacturer to identify a model.

SNR - Serial Number. Assigned by manufacturer to identify an individual phone.

SV - Software Version Number. Assigned by manufacturer. Digit 15 is set to 0 and Digit 16 is set to Filler (1111 Binary) if the SV is not available.

country runs out of IMEI codes or when a country with a 3-digit E.164 country code wants to assign ranges of IMEI codes to manufacturers, because only 2 digits are assigned for this purpose.

Expanding the IMEI

The IMEI has enough space to assign unique identifiers to wireless devices for many years, so expansion is not required because of a concern that the IMEI resource will be exhausted. However, there has been some discussion in 3GPP2 about expanding the IMEI to incorporate an ESN within it, allowing a smoother transition. Since it is stored as decimal digits in BCD format, there are 6 unused values in every digit. If the IMEI was expanded to hexadecimal digits (0..9,A..F representing the values 0 through 15), the SNR field could be expanded from 1 million values to almost 17 million, exactly enough space to store the 24 bit serial number as used within the ESN. A mapping could be established from the TAC+FAC to the Manufacturer's Code, allowing one identifier to contain all the information required to produce a valid ESN, when operating in systems that only support this mobile identifier.

Standards

Various aspects of IMEI are defined by the following 3GPP technical specifications (to convert to ETSI GSM standard numbers, consult our June, 2001 issue):

- TS 22.016 (International Mobile Station Equipment Identities (IMEI)) defines the usage of IMEI.
- TS 23.003 (Numbering, addressing and identification) defines the structure of the IMEI (see Figure 1).
- TS 24.008 (Mobile radio interface layer 3 specification; Core Network Protocols - Stage 3) defines the format of IMEI sent across the radio interface.
- TS 29.002 (Mobile Application Part (MAP) specification) describes the format of IMEI transmitted through the GSM signaling network.

3GPP specifications are available (at no charge) from:

www.3gpp.org/ftp/Specs

Conclusions

The IMEI is a very rational mobile equipment identifier. If an identifier is to disappear in the future, it is most likely to be the ESN. The IMEI was developed for a technology that had a clean split between the phone hardware (ME) and the subscription information (including IMSI) stored in the physically removable SIM. Consequently, there was no temptation to use it for subscription-related functions.

The adoption of IMEI by all 3G standards (i.e. those produced by both 3GPP and 3GPP2) would be one more step towards global mobile interoperability. Other similar steps in this direction are the adoption of IMSI and the use of AKA security algorithms. Even though 3GPP and 3GPP2 standards will be very different on the radio interfaces, these steps should improve interworking, making it much easier than it currently is between second generation GSM and ANSI-41 based standards. This will allow users of dual-technology phones easier roaming at a lower cost and with a greater level of functionality.

TIA TR-45.3 TDMA Digital Air Interface Standards

Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email David.Crowe@cnp-wireless.com

Last published March, 2001

Note:
1. IS- Interim Standard, TSB- Telecommunications Systems Bulletin, PN- Project Number, SP- ANSI Standards Proposal.
2. Bold Type indicates a modification since the previous publication of this information.
3. Published TIA standards can be obtained from TIA at www.tiaonline.org/standards/search_n_order.cfm.

First Generation (IS-54)

Standard	Description	Status
TIA/EIA-627	ANSI version of TDMA Dual-Mode Air Interface Standard	Published 06/96
TIA/EIA-627-1	Addendum to TDMA dual-mode air interface standard	Published 04/98 Rescinded 06/00
TIA/EIA-628	TDMA mobile station minimum performance standards	Published 06/96 Rescinded 06/00
TIA/EIA-629	TDMA base station minimum performance standards	Published 06/96 Rescinded 06/00
TIA/EIA-635	TDMA full-rate voice coder (3:1)	Published 06/96 Rescinded 06/00
IS-54-B	Original TDMA Dual-Mode Air Interface Standard (replaced by TIA/EIA-627)	Published 01/92 Rescinded 09/96
IS-55	TDMA mobile station minimum performance standards (replaced by TIA/EIA-628)	Published Rescinded 09/96
IS-56	TDMA base station minimum performance standards (replaced by TIA/EIA-629)	Published Rescinded 09/96
TSB-46	Verification of Authentication for IS-54-B Mobiles	Published 03/93 Rescinded 10/00
TSB-47	IS-54 Implementation Issues	Published 05/94 Rescinded 10/00
TSB-50	User Interface for Authentication Key Entry	Published 03/93

Second Generation (IS-136 Revision 0 - Digital Control Channel)

Standard	Description	Status
IS-130	Data services radio link protocol (RLP)	Published 04/95
IS-135	Asynchronous data and fax services	Published 04/95 Rescinded 04/00
IS-137	TDMA/analog mobile minimum performance standards	Published 12/94
IS-138	TDMA/analog base station minimum performance standards	Published 12/94
IS-136.1	Digital Control Channel (DCCH)	Published 12/94
IS-136.1/2-1	Addenda to IS-136 Rev. 0	Published 12/94
IS-136.2	FSK control channel, analog voice channel, TDMA traffic channel	Published 12/94

Third Generation - IS-136 Revision A (ACELP Voice Coder)

Standard	Description	Status
IS-130-A	Data Services Radio Link Protocol (RLP)	Published 09/97 Rescinded 04/00
IS-137-A	Mobile minimum performance standards for IS-136-A	Published 07/96 Rescinded 04/00
IS-138-A	Base station minimum performance standards for IS-136-A	Published 07/96 Rescinded 04/00
IS-641-A	Enhanced full-rate (ACELP) voice coder, Revision A	Published 05/96
IS-684	Isochronous radio link protocol for data (for STU-III). Replaced by TIA/EIA-136-320	Published 07/96 Rescinded 04/00
IS-686	Enhanced full rate voice coder performance standards	Published 12/96 Rescinded 04/00
IS-727	Discontinuous transmission (DTX) with ACELP (IS-641) voice coder, including generation of comfort noise	Published 07/98
IS-136.1-A	Enhanced digital control channel (9-1-1, OTA, Calling Name ID, One-button Callback, Private Networks (enhanced), PACA)	Published 10/96 Rescinded
IS-136.1-A-1/2	IS-136 Rev. A corrections (two addenda)	Published 11/96, 12/97
IS-136.2-A	FSK control channel, analog voice channel, TDMA traffic channel	Published 10/96 Rescinded
TSB-73	IS-136 Rev. 0/Rev. A compatibility issues	Published 07/96
TSB-77	Interoperable Implementation Issues in IS-641 (ACELP voice coder)	Published 07/97
TSB-105	Audit order clarification	Published 03/99
TSB-108	Determining when R-DATA is encrypted	Published 03/99

Fourth Generation - TIA/EIA-136 Revision 0

Standard	Description	Status
TIA/EIA-136	SMS enhancements, double/triple rate channels (symmetrical/asymmetrical), EPE and charge rate indicator.	Published 03/99
TIA/EIA-136-010	Optional mobile station facilities	
TIA/EIA-136-020	SOC, BSMC and carrier specific HLPI assignments	
TIA/EIA-136-100	Introduction to channels	
TIA/EIA-136-110	RF channel assignments	
TIA/EIA-136-12x	Digital control channel (DCCH) layer 1 (136-121), 2 (136-122) and 3 (136-123)	
TIA/EIA-136-13x	Digital traffic channel (DTC) layer 1 (136-131), 2 (136-132) and 3 (136-133)	
TIA/EIA-136-140	Analog (FSK) control channel	
TIA/EIA-136-150	Analog voice channel	
TIA/EIA-136-2x0	Minimum performance requirements for ACELP voice coder (136-210), VSELP voice coder (136-220), mobile station (136-270) and base station (136-280)	
TIA/EIA-136-410	**ACELP voice coder**	
TIA/EIA-136-420	VSELP voice coder	

TIA/EIA-136-510	Authentication and encryption of signaling information, user data and voice	
TIA/EIA-136-7x0	SMS: Introduction to teleservices (700), text/numeric messaging (710), Over-the-Air Activation (OATS; 720) and Over-the-Air Programming for intelligent roaming (OPTS; 730)	
TIA/EIA-136-910	Informative information	

Fifth Generation - TIA/EIA-136 Revision A

Standard	Description	Status
TIA/EIA-136-A	Revised parts include 136-010, 020, 100, 121,131,133,140,150,270, 280, 510, 700, 710, 720 and 910. New parts are listed separately	Published 12/99
TIA/EIA-136-310-1	Radio link protocol 1 (for data services)	
TIA/EIA-136-310-A	**Addendum to RLP**	**Ballot**
TIA/EIA-136-350-1	Data services control	
TIA/EIA-136-350-A	**Data services control addendum**	**Ballot**
TIA/EIA-136-410-1	**ACELP voice coder, addendum 1**	**Ballot 07/01**
TIA/EIA-136-430	US1 voice coder (GSM compatible)	
TIA/EIA-136-511	List of messages subject to encryption	
TIA/EIA-136-620-1	TSAR: teleservice allowing segmentation and reassembly	
TIA/EIA-136-630	BATS: broadcast short message	
TIA/EIA-136-730-1	OPTS: over-the-air programming teleservice to support intelligent roaming	
TIA/EIA-136-750	GUTS: general UDP transport service	

Sixth Generation - TIA/EIA-136 Revision B - UWC-136 - ITU-R 3G Specification

Standard	Description	Status
TIA/EIA-136-B	Revision B. Only new parts are listed	Published 03/00
TIA/EIA-136-230	US1 (GSM) voice coder minimum performance requirements	
TIA/EIA-136-270-1	**MS minimum performance standards (Addendum)**	
TIA/EIA-136-290	RF minimum performance for 200 kHz and 1.6MHz bearers (136HS)	
TIA/EIA-136-330	Packet data service - overview	
TIA/EIA-136-331	Packet data service - physical layter	
TIA/EIA-136-332	Packet data service - medium access control (MAC)	
TIA/EIA-136-333	Packet data service - logical link control. Based on GSM 04.64.	
TIA/EIA-136-334	Packet data service - subnetwork dependent convergence protocol. Based on GSM 04.65.	
TIA/EIA-136-335	Packet data service - radio resource management	
TIA/EIA-136-336	Packet data service - mobility management	
TIA/EIA-136-337	Packet data service - tunneling of signaling messages. Subset of GSM 09.18	
TIA/EIA-136-34X	Outdoor high-speed packet data service: Overview (340), Physical layer (341) and MAC (342)	
TIA/EIA-136-36X	Indoor high-speed packet data service: Overview (360), Physical layer (361) and MAC (362)	
TIA/EIA-136-511	Messages subject to encryption	
TIA/EIA-136-610	R-DATA/SMDPP Transport	
TIA/EIA-136-760	Charge-rate indication teleservice (CIT)	
TIA/EIA-136-900	Introduction to Annexes and Appendixes	

TIA/EIA-136-905	Normative information	
TIA/EIA-136-932	Packet data services - Stage 2 description	
TIA/EIA-136-933	Packet data services - Description of MAC layer	
TIA/EIA-136-940	Capacity and performance characteristics of UWC-136 (TIA/EIA-136-B)	
IS-839	**R-UIM Overview, Operation, and File Structure Support in TIA/EIA-136, Rev B**	**Published 11/00**
IS-842	GSM Hosted SMS Teleservice (GHOST)	Ballot 07/00

Seventh Generation - TIA/EIA-136 Revision C

Standard	Description	Status
TIA/EIA-136-C	Revised parts include 000-C, 005-B, 010-C, 020-C, 100-B, 110-B, 123-C, 131-C, 133-C, 210-A, 270-C, 280-C, 290-A, 350-B, 610-A, 620-A, 700-C	In press
TIA/EIA-136-030	R-UIM (Smart Card) overview and operation	
TIA/EIA-136-033	R-UIM/ME file structure	
TIA/EIA-136-033-1	**R-UIM/ME file structure addendum 1**	**Ballot 08/01**
TIA/EIA-136-034	R-UIM/ME interface procedures	
TIA/EIA-136-036	Personalization of mobile equipment (ME)	
TIA/EIA-136-037	R-UIM/ME application toolkit	
TIA/EIA-136-240	AMR (Adaptive Multi-Rate Vocoder) minimum performance	
TIA/EIA-136-250	VAD (Voice Activity Detection) minimum performance	
TIA/EIA-136-270-C	**MS minimum performance standards**	**Ballot**
TIA/EIA-136-350-C	**Data services control addendum**	**Ballot**
TIA/EIA-136-351	EGPRS-136 - AT commands	
TIA/EIA-136-370	EGPRS-136 - Overview	
TIA/EIA-136-376	EGPRS-136 - Mobility management	
TIA/EIA-136-377	EGPRS-136 - Gs interface specifications	
TIA/EIA-136-440	AMR adaptive multirate codec (also used in GSM and UMTS)	
TIA/EIA-136-440-AD1	**Revision to AMR adaptive multirate codec**	**In press**
TIA/EIA-136-670	Broadcast teleservices over GSM SMS (TOGS)	
TIA/EIA-136-740	SAMPS - System assisted MS positioning through satellite (i.e. GPS)	
TIA/EIA-136-972	EGPRS-136 - Stage 2 descriptions	
IS-823	Modification to ACELP voice coder to transmit 45.45 and 50 bps TTY/TDD tones	Published 05/00
IS-823-A	**Modification to ACELP voice coder to transmit 45.45 and 50 bps TTY/TDD tones**	**Ballot 08/01**
IS-840	**Minimum performance for TTY/TDD detector and regenerator**	**Published 05/00**
IS-840-A	**Minimum performance for TTY/TDD detector and regenerator**	**Ballot 08/01**
IS-869	**Analog SAMPS support in TIA/EIA-136-C**	**Development**

Eighth Generation - TIA/EIA-136 Revision D

Standard	Description	Status
TIA/EIA-136-D	**GHOST, multilingual SMS, handoff improvements, tandem free operations, analog SAMPS and R-UIM**	**Development**
TSB-xxx	**UIM elementary file alignment issues**	**Development**