Cellular
Networking
Perspectives

David Crowe [Editor] • Phone 1-403-289-6609 • Fax 403-289-6658 Vol. 7, No. 1 January, 1998

In This Issue...

WIN Phase II: Charging Ahead p. 1

The ink is not yet dry on the Wireless Intelligent Network Phase I, and the CTIA has already submitted the requirements for Phase II, largely related to new charging capabilities.

Erratum: Network TMSI p. 2

TIA TR-45 Cryptographic Development Policy Approved p. 2

Future TIA wireless standards should be more secure following the adoption of a new development policy that includes outside input.

ESN Update p. 3

An update on the new TIA responsibility for allocating ESN manufacturer codes, and the latest plans for an expanded (56 bit) EESN.

New Working Group in TIA TR-45.1 p. 3

TR-45.1 WG IV has been created to develop a standard portable phone to vehicle interface.

International Applications of TIA Wireless Standards p. 3

Although TIA wireless standards are in use around the world, seamless international roaming is not yet possible. Here's why.

TIA TR-45.1 Analog Air Interface Standards Report p. 6

Next issue: February 2, 1998

WIN Phase II: Charging Ahead

The CTIA approved a System Requirements Document for the Wireless Intelligent Network, Phase II on November 4, 1997. This document was submitted to TIA committee TR-45 on December 3, 1997 to initiate standardization. Most standardization will take place within the TR-45.2 subcommittee which maintains the TIA/EIA–41 standard for intersystem operations and the TIA/EIA–124 standard for exchange of call detail and billing records. It is unlikely that the BS-MSC “A” interface or radio interfaces will be modified.

WIN Phase II concentrates on enhanced network charging capabilities, in contrast to Phase I which focused on three enhanced feature drivers (Voice Controlled Services, Calling Name Presentation and Incoming Call Screening). Like Phase I, the intention of Phase II is not to create specific new services, but to create “service drivers” that can allow carriers to differentiate their services from other carriers while still maintaining interoperability with other carriers, and therefore seamless roaming to their customers. The Phase II charging service drivers are:

- Freephone

  The entire cost of a mobile originated call, including airtime, is charged to the owner of the destination number. Since WIN Phase II will use standard freephone numbers (1–800 and 1–888 rather than the #800 currently used for this service by some carriers) a database of 1–800/1–888 numbers that accept airtime charges will have to be maintained.

- Premium Rate

  Charges vary based on the identity of the caller or destination, time and date, network congestion or the type of radio access (e.g. data, priority access).

- Customized Account

  The mobile subscriber can enter a sub-account identifier (e.g. a particular client or project) for each call, or the network may determine the sub-account based on the calling number identity, dialed digits or other information. Bills can then be sorted by sub-account number, possibly with summary totals.

- Feature Use

  Use of a feature is charged, possibly varying based on the method of invoking the feature (e.g. by feature code or spoken command) or other information.

- Split Charging

  Charges for a call are shared by two or more parties, not necessarily evenly.

- Third-Party

  A mobile subscriber can specify a third party to pay for the call (e.g. a residential line or another mobile).

- Charge Card

  Call charges can be assigned to a credit card, debit card or prepaid card.

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cr. NW, Calgary AB, T2N 3W1, Canada. Phone: 1-800-633-5514 (+1-403-274-4749). Fax: +1-403-289-6658. **Subscriptions**: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. Payment by cheque, American Express or Visa. **Delivery:** Email, fax or 1st class mail. Additional charges apply for international fax delivery. **Copies:** Each subscriber may make up to 10 copies of each issue. Rates are available for more copies. **Discounts:** Educational and small business discount: 25% off any order (no fax delivery). **Back Issues:** Available individually for $35, or in bulk at reduced rates. **Email:** cnpsales@cnp-wireless.com. **Web:** http://www.cnp-wireless.com/.

- Calling Party Pays (CPP)

  The calling party pays all charges. Note that the CTIA is expected to publish a separate requirements document exclusively for CPP in early 1998 (see November 1997 issue of *Cellular Networking Perspectives*).

- Prepaid Calling

  Wireless services are paid for in advance, with the network decrementing credits as calls proceed, until the prepaid amount is exhausted or more payments are received.

- Advice of Charging

  Special charging information can be provided automatically by a tone or announcement (indicating that a higher charge applies, but not specifying what the charge is), or precise charging information can be provided upon request by the caller via a display or spoken words.

- Location-based

  Charges vary based on the mobile location. One application is to allow free calling in a mobile subscriber's home cell to mimic combined cordless/cellular operation.

Implementation of WIN Phase II will require modifications to TIA/EIA-41 (intersystem operations to carry charge profile information around the network), TIA/EIA-124 (to record charge information) and possibly TIA/EIA-93 (to allow the flow of charge-related signaling information from other telecommunications networks.

WIN Phase I is not yet complete, with the document still in V&V (Verification and Validation). Balloting is expected to begin shortly after V&V ends in April 1998. Phase II is scheduled for publication in August 1999.

Erratum: Network TMSI

In the December 1997 article *Advanced CDMA Features: PN-3619* it was stated that the CDMA version of TMSI did not support increased paging efficiency, as it was not significantly smaller than a MIN identifier. In fact, IS-95 Rev. A CDMA can support a TMSI of 16, 24 or 32 bits. The smaller TMSI values are significantly smaller than the standard MIN identifier (34 bits).

Also, another benefit of network TMSI that has not previously been reported, is a possible reduction in Border Cell problems (see the May, June and July 1996 issues for more details on these problems). When an unsolicited page response containing MIN or IMSI is received by a system, the receiving system has to guess which neighboring system may have initiated the page. With a mobile using a network TMSI, the identity of the paging system is transmitted. This allows for more efficient and reliable identification of the system to which the unsolicited page response should be transmitted to arrange for redirection of the incoming call.

TIA TR-45 Cryptographic Development Policy Approved

Following the cracking of the TIA CMEA encryption algorithm in 1997 (see April, May 1997 issues), the TIA TR-45 AHAG (*ad hoc* Authentication Group) has been planning to strengthen not only the algorithms used, but also the process used to develop them.

TIA standards committee TR-45 recently endorsed an AHAG proposal that will allow public contributions for the development of new security designs. Following an internal review, the chosen algorithms and procedures will be made public, with time allowed for external review. It is hoped that this process will provide a greater assurance that the security of phones and networks will be at the desired level.

The AHAG is also developing Enhanced Subscriber Authentication (ESA) and Privacy (ESP) algorithms and procedures, that will follow the new method, allowing outside input and review for the first time.

ESA will have to meet several requirements:

- interoperability with phones and base stations that do not support the new algorithms,
- minimal impact on TIA/EIA-41 intersystem operations,
- minimal increase in network traffic,
- US exportability and
- all requirements met by the current CAVE algorithm.

ESP (Enhanced Subscriber Privacy) is intended to increase the privacy of wireless phone calls, through stronger encryption. It will have to meet the following requirements;

- Eavesdropping on one call should take at least 10,000 hours using commercially available equipment costing less than $10,000 up to the year 2007,
- Applicable to all subscribers on digital channels (with new phones, presumably),
- Ability to enhance the algorithm if the security is ever compromised,
- Minimal impact on existing network elements and network traffic,
- Cryptographic decoupling of the ESP and ESA keys, to ensure that compromise of ESP will not result in ESA being compromised,
- US exportability and
- all requirements met by the current voice privacy algorithm.

The development of these new algorithms will take quite some time, and it will be even longer before equipment supporting these algorithms will be in commercial service. Luckily, the cracking of CMEA will have little impact in the interim, as a large effort is required to obtain information, such as credit card numbers, that can be obtained much more easily in other ways (e.g. by patrolling payphones with binoculars or trolling through trash cans looking for credit card receipts). The current authentication algorithm is not believed to be compromised, and the voice encryption algorithm has (luckily) never been advertised as being very strong.

ESN Update

The TIA ESN Ad Hoc Group has released Version 1.2 of the ESN Assignment Guidelines and Procedures. It describes three different ESN formats, distinguished by the high order bits (24–31) of the current 32 bit ESN (see Table 1). The document also includes a list of currently assigned manufacturer codes and the forms necessary to apply for them. It is available from:

Engineering Committee TR-45
ESN Administrator
c/o TIA
2500 Wilson Blvd., Suite 300
Arlington, VA 22201, USA
Phone: 1-703-907-7700
Fax: 1-703-907-7727

The current 32 bit ESN will accomodate only 251 distinct manufacturer codes, each with over 16 million serial numbers. Adoption of the 14 bit format would add a further 128 manufacturer codes, although with only 262,000 serial numbers each. Finally, the 56 bit expanded ESN format would provide an additional 65,536 manufacturer codes, each with over 16 million serial numbers.

Since the wireless industry has used less than half of the first format manufacturer codes, it is expected that it will be some time before either or both of the expansion steps are required. However, because the 56 bit ESN would have an enormous impact on all wireless systems (data entry, signaling, databases, recording, billing and others), work on the expanded ESN format must proceed. New and modified standards should support EESN to ensure that the industry is prepared when the time comes.

New Working Group in TIA TR-45.1

TIA subcommittee TR-45.1, responsible for analog radio interface standards has created a new working group (TR–45.1 WG IV) to develop a standard interface from a portable wireless phone to a vehicle, providing external power, antenna, speaker and microphone.

The main focus of TR–45.1 is still on EIA/TIA–553 Rev. A and IS-91 Rev. A. These standards have been delayed due to a major effort to convert EIA/TIA–553–A from simply an analog cellular standard to the “core” standard for all air interfaces that have an analog compatibility mode, including NAMPS (IS-91), TDMA digital (IS-136) and CDMA digital (IS-95). This involves the creation of a new Protocol Capability Indicator (PCI) parameter that will help ensure that the wireless phone and base station only use compatible signaling. This will allow new capabilities to be introduced by various radio interfaces without interfering with the operation of mobiles and base stations that do not support them.

A complete list of TR-45.1 analog standards and projects is provided on Page 6 of this issue.

International Applications of TIA Wireless Standards

TIA wireless standards for cellular and PCS systems have proven so popular that they have been implemented around the world (see the August 1996 issue). However, because they were conceived in a single country environment (by AT&T for the US market only) and not in a multi-country environment (as GSM was), there are a number of challenges to be overcome before seamless international roaming becomes a reality.

There are several categories of international hurdles for TIA wireless standards:

- <u>Identifiers</u>
    - MIN Ambiguity
    - Transition to IMSI
    - SID Coordination
    - ESN Coordination
- <u>SS7 Signaling</u>
    - ANSI versus ITU protocols
    - Point Code Routing
    - Global Title Routing
- <u>Dialing Plans</u>
    - International TLDNs
    - Other IS-41 parameters

Identifiers

Identifiers are essential to telecommunications systems, and TIA wireless standards are no exception. Every subscription has to be identified by a MIN or IMSI, every mobile by an ESN and every system by a SID (System Identification Number). Each of these identifiers has international implications.

MIN Ambiguity

The MIN was created as a 10 digit number to allow the phone number of the mobile to be used as the mobile’s identifying number. Many people still think that the mobile’s MIN and directory number (MDN) are the same. However, this connection has to be broken to allow new capabilities such as International Roaming and Number Portability to work. While the long term solution is IMSI, in the short and medium term it is necessary to ensure that all MIN blocks throughout the world are unique.

Table 1: ESN Formats

			Manufacturer's	Code (MFR)	Serial	Number
	ESN length	Value in bits 24-31	Bit range	Number	Bit range	per MFR
1. Traditional	32 bits	2-254 except 128, 250	24-31	251	0-23	16,777,216
2. Long manufacturer code	32 bits	0 or 1	18-24	128	0-17	262,144
3. Expanded (EESN)	56 bits	128	32-47	65534	0-23	16,777,216

For North American Numbering Plan systems (e.g. the US and Canada), choosing a MIN is easy, the 10 digit dialable directory number is usually used. For international systems there is little guidance. Most numbers that are chosen may conflict with US or Canadian telephone numbers now or in the future, and those telephone numbers may be used as MINs by wireless systems.

International systems can best avoid ambiguity by applying to the IFAST (International Forum on AMPS Standards Development) for an International Roaming MIN (IRM). IFAST can be contacted c/o:

Ms. Lori Messing
(lmessing@ctia.org)
CTIA
1250 Connecticut Ave. NW
Washington, DC, 20036

The IRM is a 4 digit prefix, starting with 0 or 1, that identifies a block of one million MINs. Some of the IRM codes that were allocated by IFAST in 1997 include 0128 to Piltel in the Philippines, 0188 and 0189 to Mobikom in Malaysia, 0732 to Comcel in Colombia, 0886 and 0887 to the Iridium Satellite system, 0972 and 0973 to Pele-Phone of Israel, 1119 to Telefonica del Peru and 1311 to ReadyCom in the US.

Allocation of an IRM cannot prevent MIN conflicts, but it will minimize the chance of this occurring. An IRM cannot conflict with MIN blocks based on North American directory numbers, E.164 international directory numbers or E.212 IMSI based MINs because none of these formats can produce a number starting with the digits 0 or 1. The IFAST can ensure that all allocations of IRM codes are unique, but cannot ensure that the block of MINs is not being used by a company somewhere that has not informed IFAST.

A list of known MIN blocks using various non-NANP formats (including the IRM) is published in TIA TSB-29.

Transition to IMSI

Coordination of MIN allocation is not a long term solution, because it requires a single international authority to allocate resources to each carrier. The IMSI resource, on the other hand, allows each country to allocate identifiers within the block defined by a Mobile Country Code (MCC). The international authority (ITU in this case) only needs to be involved in the event of misuse or exhaustion of national codes or when political changes require the allocation or deallocation of a country code.

The IMSI is an identifier of up to 15 digits, usually composed of a 3 digit MCC, 3 digit MNC (Mobile Network Code) and a 9 digit mobile identifier (MSIN). Allocation of one MCC allows a nation to provide one billion identifiers to each of 1,000 different carriers. For a few countries, most notably the USA, multiple MCC codes are required because of the number of wireless licenses granted (about 3,500 in the US).

The transition to IMSI has proceeded to the point where it is available in both TIA digital standards (IS-95 Rev. A CDMA and IS-136 Rev. A TDMA) as well as the IS-124 call detail/billing record exchange standard and the IS-634 BS-MSC “A” interface standard (when TSB–80 is used to enhance Revision 0). Modifications to TIA/EIA–41 to support IMSI in intersystem operations were approved for publication following the completion of project PN–3892 in December 1997. The one major group of standards remaining to be updated are the analog air interfaces, EIA/TIA-553 and IS–91. Support for IMSI is expected in Revision B of both of these standards.

SID Coordination

Every system supporting TIA wireless standards broadcasts a SID to identify itself. This value is used to indicate when a mobile is at home, and can be used to distinguish preferred from non-preferred systems while roaming (by some mobiles). The SID is also used in call detail records and the TIA/EIA-41 intersystem operations standard to identify home and serving systems.

Most countries have been allocated a range of SID codes in TIA document TSB-29 Revision B. Unfortunately, a number of countries have been unaware of the existence of this document, and have allocated SID’s from the range assigned to another country. Several of these conflicts have been documented in TSB-29 and several resolved with the assistance of TIA subcommittee TR–45.2 and the IFAST.

New SID blocks were traditionally allocated by TIA TR-45.2, but recently IFAST has indicated that it intends to act as the allocation authority in future. Once a SID block is allocated to a country, that country’s national telecommunications authority is responsible for assigning individual SID codes.

One exception to the rule that SID blocks are assigned to countries is CIBERNET, which has been assigned a large number of SID codes for use as billing identifiers. This includes the 16 bit SID codes above 32767 which cannot be used on the radio interface, but can be on the network and in call detail/billing record exchange to identify subsets of a system for accounting purposes.

One problem with the TSB-29 allocation of SID blocks is that they were allocated to all countries without waiting for requests. Consequently, many SID blocks will never be used (e.g. those assigned to GSM countries) and the number of spare SIDs is quite low.

ESN Coordination

Every mobile should have a unique ESN. This is arranged by assigning manufacturer codes, which allows manufacturers of mobiles to autonomously assign a large block of unique ESN’s.

This assignment was performed by the US FCC prior to September 1997, which may have led some manufacturers to believe that mobiles not destined for export to the US could be allocated any ESN codes. Now that the TIA is the allocation authority (see related article on Page 3) it may be clearer that all ESN codes should be allocated from a block assigned to the manufacturer.

The impact of non-unique ESN codes is not as significant as non-unique MIN’s or IMSI's. While two mobiles with the same ESN (but different MIN's) can operate in the same cell, two mobiles with the same MIN or IMSI but different ESN codes would be unable to coexist. The major impact of non-unique ESN's is on fraud management software that may check for multiple mobiles using the same ESN or may maintain a negative list of ESN codes that should be denied service.

SS7 Signaling

Communication between wireless network elements generally uses SS7 signaling. Although some systems still use X.25 signaling locally, the backbone inter-carrier networks (e.g. NACN, Illuminet and GTE) rely exclusively on SS7 signaling. SS7 networks are national in scope, which raises some international roaming issues.

ANSI versus ITU Protocols

SS7 signaling exists at two different levels: national and international. National signaling is between network elements in the same national SS7 network or to international gateways. International signaling is between international gateways. International gateways have to be able to provide routing and protocol conversion services which affect the MTP and SCCP layers of the SS7 protocol, but not the higher layers such as TCAP, ISUP or the application (e.g. TIA/EIA–41 MAP).

Two of the commonest forms of SS7 signaling are ANSI (used by the US and Canada) and ITU (international signaling). Each country may define its own national SS7 variant.

Point Code Routing

The simplest and most efficient routing in SS7 is based on the concept of Point Codes (PC) and Subsystem Numbers. A Point Code is a unique address assigned to an SS7 network element, and a Subsystem Number is a sub-address within a network element. This type of routing is used for most IS-41 and TIA/EIA-41 signaling today.

The biggest problems with point code routing is that it is national in scope, it is not possible to specify a point code in another national SS7 network. This requires the use of the more complex and somewhat less efficient global title routing (see next section). The national scope also invalidates a TIA/EIA-41 parameter which is found in many messages: PC_SSN (as the name suggests, a combination of the Point Code and Subsystem Number). If a TIA/EIA-41 message is sent across a national SS7 boundary, the PC_SSN parameter becomes meaningless. Yet, international gateways cannot reach into the TIA/EIA–41 application layer and modify this parameter. Consequently, an alternative is required. One is to use the address carried in the SS7 MTP/SCCP layers instead, and a second is to use the IS-41 Rev. C parameters MSCIdentificationNumber or SenderIdentificationNumber. A third method is indirect, using the MSCID parameter (SID + switch number) to consult a table that contains the desired SS7 address.

A second problem with the PC_SSN parameter is that it assumes a 24 bit Point Code format, yet many countries use a 14 bit format in their national networks. Consequently, there could be interoperability problems between systems within the same national SS7 network, where the Point Code address is valid. A modification to TIA/EIA–41 to support formats of less than 24 bits has been accepted for inclusion in TIA/EIA–41 Revision E, although this revision has not yet been published.

Global Title Routing

SS7 is a unique protocol in having an extensible addressing capability. New types of addresses can be added to the protocol, allowing routing of messages to be performed based on an identifier such as a credit card number or telephone number – although there is usually a small delay while the necessary modifications to standards, STP routing nodes and other network elements are made.

Global title addressing has so far been avoided in international routing by extending the ANSI SS7 network to other countries. Rumor has it that Hong Kong, according to the SS7 network, is connected to the middle of Kansas (right next to the Emerald City, presumably). This is not an ideal solution for several reasons. First, the managers of ANSI SS7 resources do not look favorably on them being used in countries outside the North American Number Plan area. Secondly, this could lead to exhaustion of resources if the global wireless network ended up within the ANSI network. And, this solution is more expensive for countries that are forced to run an ANSI SS7 network (for TIA/EIA–41 signaling) in parallel to their national SS7 network (e.g. for ISUP signaling), rather than merging them.

International TIA/EIA-41 signaling can choose from three different global titles:

1. E.164 (international directory numbers)
2. E.212 (IMSI)
3. Q.708 (SANC)

All three global titles can be used for routing any message. However, lookup tables are required when the global title format is not the same as the information that identifies the destination network element. E.164 global titles are best suited for routing messages based on directory number (e.g. from a Gateway MSC to an HLR). E.212 global titles are best suited for routing messages based on IMSI (e.g. from a Serving MSC/VLR to an HLR).

Currently, TIA TR-45.2 is considering the combined use of E.164 and E.212 global titles, which may require assigning numbering resources to network elements to facilitate routing. The use of Q.708 (SANC) was rejected, largely because it is believed that this format is less widely implemented by international gateways.

To be continued…

This article will conclude in the February 1998 issue, with a discussion of the corrupting influence of the North American dialing plan on TIA/EIA-41.

TIA TR-45.1 Analog Air Interface Standards Report

Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658

Last published July, 1997

Analog Air Interface Standards - First Generation

Standard	Description	Status
IS-3 (Rev. A,B,C,D)	Original analog air interface standards (see EIA/TIA-553-0)	Rescinded 09/89
EIA/TIA-553 Rev. 0	Analog air interface	Published 09/89
IS-19-B	Mobile minimum performance standards	Published 06/88
IS-20-A	Base station minimum performance standards	Published 06/88
TSB-35	Cellular mobile receiver dynamic range	Published 04/92
TSB-39	Message type assignment for extended protocol	Published 03/93

Analog Air Interface Standards - Second Generation

Standard	Description	Status
IS-88	Narrowband (3:1) analog air interface ("NAMPS")	Published 02/93
IS-89	IS-88 base station performance standards	Published 02/93
IS-90	IS-88 mobile performance standards	Published 02/93
IS-91 Rev. 0	Analog air interface (including "NAMPS" and authentication)	Published 10/94
IS-94	In-building analog air interface ("CAPS")	Published 05/94
IS-680	Residential ("cordless") base station PSTN interface	Published 05/96
TSB-70	Cross reference for FSK control channel	Published
TSB-83-A (SP-3798)	Additional modem options for IS-680 ("cordless")	Published 04/97

Analog Air Interface Standards - Third Generation

Standard	PN- #	Description	Status
EIA/TIA-553-A	**SP-3598**	**Analog air interface (including authentication, alert/flash with info, abbreviated alert, message waiting indicator, sleep mode & protocol capability indicator (PCI))**	**Second ballot**
EIA/TIA-690	**SP-3495**	**Mobile minimum performance standards (IS-19-C)**	**Second ballot**
EIA/TIA-691	SP-3665	Enhanced analog ANSI version of IS-91-A (w/o IS-680 cordless)	Second ballot
EIA/TIA-712	**PN-3597**	**Base station minimum performance standards (prev. IS-20-A)**	**Published 09/97**
IS-91-A	PN-3476	Revised IS-91 air interface (including IS-94/IS-680/sleep mode)	Second ballot
IS-713	PN-3668	1900 MHz upbanded AMPS (based on IS-91-A)	Pub. est. 4Q'97
TSB-70-A	**PN-3610**	**Updated version of TSB-70 cross reference**	**ballot pending**
TSB-71	PN-3477	IS-94 enhancements and issues	Published 10/95

Analog Air Interface Standards - Fourth Generation

Standard	PN- #	Description	Status
IS-91-B	**SP-3666**	**Revised version of IS-91 (including IMSI, PCS band support,OTA, priority access, 9-1-1, cryptosync & Expanded ESN)**	**Development**
IS-xxx	**PN-xxxx**	**Portable wireless phone to vehicle interface**	**Development**

Note: 1. IS- TIA Interim Standard, PN- TIA Project Number, SP- ANSI Standards Proposal, TIA/EIA- ANSI approved TIA standard, TSB- TIA Telecommunications Systems Bulletin.

2. **Bold Type** indicates modification since the previous publication of this report.

- Thanks to Bob Slocum of Ericsson for his assistance compiling this information.