Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-403-289-6609 • Fax 403-289-6658 Vol. 7, No. 3 March, 1998

In This Issue...

Next issue: April 2, 1998

Wireless '98

It would be impossible to summarize all the products shown at Wireless'98 within our normal 6 page confines. We were looking for new network infrastructure product categories. Two of the most interesting and dynamic were in the provision of equipment to meet the US FCC's Phase II location mandate (locating cellular/PCS phones within 125 meters, 67% of the time) and for provisioning Authentication A-Keys into mobile phones. There were glimmers of new products available for Calling Party Pays (from AGCS, although little technical information was available) and J–STD–025 CALEA (from ADC NewNet).

Phase II Location

Several companies exhibited technology that they claimed will meet the US FCC Phase II E9–1–1 location mandate or, failing that, technology that soon will. Some of the exhibitors were:

- TruePosition
  The early market leader, with a Time Difference of Arrival (TDOA) system.
- KSI
  Developers of an Angle of Arrival (AOA) solution, which they claim requires 2 measurement sites versus the 3 required by TOA/TDOA systems.
- Cell-Loc
  A Time of Arrival (TOA) technology with enhancements to minimize the impact of multipath,
- Corsair
  Adapting their RF Fingerprinting technology to mobile location,
- US Wireless
  Developing a system based on multipath analysis that they claim can determine location from a single site (rather than triangulation required by most other systems), Since Wireless'98 they have announced that they will be teaming with CTS, the "other" manufacturer of RF Fingerprinting technology.

A–Key Entry

One of the challenges of authentication is entering a unique "A–Key" into every authentication-capable mobile phone. Most phones are pre-provisioned with an A–Key value by the manufacturer which can be obtained through an EDI transaction using the ESN as a key. However, subsequent activations of the phone require a manual A–Key entry or an equivalent automated method. Also, a large number of authentication capable phones were never programmed with an A-Key when activated, because authentication was not available on the network at that time. Three distinctly different A-Key programming systems were being promoted at Wireless'98. Seldom is one problem solved in three so different ways!

- EDS
  EDS has teamed up with ASI to provide a system that programs many different phone models by using a robotic pointer-finger. A

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 or 1st class mail. **Copies:** Each subscriber may make up to 10 copies of each issue. Rates are available for more copies. **Back Issues:** Available individually for $35 in the US and Canada and $40 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Email:** cnpsales@cnp-wireless.com **Web:** http://www.cnp-wireless.com/

different robot program is required for each model, based on the X, Y and Z coordinates of each key, relative to the holder, and based on the key sequence used to enter an A-Key. Security is based on the difficulty of interpreting the thousands of low level robot commands that are transmitted on the controlling datalink.

- Synacom
  Synacom provides a programming device with multiple different cables that can be used by dealers to program phones via the electronic interface provided on the bottom of most phones. Security is provided by transmitting the A-Key over an encrypted phone line from the carrier.
- GTE
  GTE has teamed up with ORA to provide a cable with a plastic pod containing a small circuit board. When plugged into a phone it receives power and then initiates software that programs the A–Key. Unlike the EDS and Synacom solutions this could not only be used by dealers, but also mailed directly to consumers.

Another approach to activation is over-the-air activation (OTA), which is applicable to CDMA and TDMA capable cellular and PCS phones.

Cloudy Skies for CALEA

The "When" and "What" for a standard to support the US CALEA law for Lawfully Authorized Electronic Surveillance are still in doubt. The telecommunications industry is still lobbying hard for the joint TIA/ATIS interim standard J–STD–025 to be considered compliant with CALEA, and for legislated delays in implementation until the year 2000. Meanwhile, the US Department of Justice (representing law enforcement interests) is expected to challenge J–STD–025 in front of the FCC in mid-March and still insists that telecommunications carriers must adhere to the original 1998 deadline.

Standards organizations, while waiting to see whether J–STD–025 needs to be modified, are working on the so-called FBI "Punch List" that contains capabilities that the industry refused to put in J–STD–025. TIA subcommittee TR–45.2 (jointly with ATIS T1P1) has initiated an Enhanced Surveillance Services *ad hoc* group (ESS), chaired by Peter Musgrove of AT&T Wireless. Any standard that they produce will be edited by Mike Hammer of Booz, Allen, Hamilton (consultants to the FBI). The "punch list" items can be summarized as:

- Access to all conference call parties (including the identity of all parties and access to conversations occurring when the intercept subject is not connected),
- Transmission of a message whenever a party is added, deleted or placed on hold in a multi-party call,
- Access to user controlled signaling (e.g. DTMF tones that could be used to access long distance, banking, voice mail and other services outside the control of the wireless system),
- Network signaling that cannot be derived from examination of call content or current call data messages (e.g. air interface messages such as Power Up/Power Down registrations),
- Precise time-correlation of call data messages and call content (e.g. voice),
- Regular reports of all active surveillances,
- Reports on feature status (e.g. type of call forwarding activated, including the forward-to number),
- Continuity check, to verify that call content can be delivered on all available call content channels,
- A standardized interface at all layers as J–STD–025 only defines the upper (application) protocol layer.

Cellular Networking Perspectives Around the World

Cellular Networking Perspectives is read in twenty different countries around the world:

- Australia
- Brazil
- Canada
- England
- Finland
- France
- Germany
- Indonesia
- Ireland
- Israel
- Japan
- Korea
- Mexico
- New Zealand
- Peru
- Russia
- Scotland
- Thailand
- USA
- Venezuela

IS–136 Reorganization

TDMA digital cellular with an AMPS compatibility mode has evolved from the IS–54 standard, that provided TDMA digital voice, but used the existing FSK ("analog") control channel through the IS–136 standard that included a new control channel (DCCH: Digital Control Channel), PCS operations (in Revision A) and a new voice coder (ACELP: IS–641). All along, in the shadow of the major standards (IS–54 and IS–136), were several other standards, such as IS–130/IS–135 for data and IS–137/IS–138 for minimum performance standards. Now the standard is undergoing another documentation metamorphosis into a much larger single, full ANSI standard, with multiple parts. While this is not a technical change, it is important to understand why some older standards numbers are

being retired and why the format of the IS–136 name has changed.

The new name for the TDMA digital standard is TIA/EIA–136, and each part will have a separate identifier. For example, TIA/EIA–136–150 will define the analog voice channel. Some standards will continue to live alone before being absorbed, such as TIA/EIA/-IS–641 (ACELP voice coder), if they are not near the 5 year expiry period for a TIA interim standard. A complete list of TDMA digital standards is provided in a table on pages 5 and 6 of this issue.

TIA/EIA–41 Revision E

The standard for roaming between AMPS, CDMA and TDMA (D-AMPS) systems has long been TIA/EIA/IS–41, now known as full ANSI standard TIA/EIA–41.

The first ANSI version of IS–41 was TIA/EIA–41 Revision D, which was published in December 1997. This document was basically IS–41 Revision C, with minor enhancements. Revision E, which is still officially scheduled for publication in 1998, will have to incorporate a large number of other capabilities that have been standardized since IS–41–C and TIA/EIA–41–D were finalized. A list of capabilities that *probably* will be included in Revision E follows. Note that some may be excluded due to scheduling constraints:

TSB–76: PCS Operation

Operating phones in a different frequency band (e.g. the PCS 1800-2200 MHz band) has little impact on network protocols, unless those phones have the capability to roam into the existing cellular (800 MHz band) or into a different mode (i.e. analog). Since there are many carrier and consumer motivations for inter-band capabilities, TSB–76 was written to allow inter-band handoff. Since this TSB was written against IS–41–C and not TIA/EIA–41–D some additional editing will be required before it can be incorporated into TIA/EIA–41–E.

TIA/EIA/IS–76 is described in the January and February 1997 issues of *Cellular Networking Perspectives*.

IS–725: Over-the-Air Activation

IS–725 defines network operations for over-the-air activation of cellular and PCS phones. This complex transaction is initiated by the phone, when it is first purchased, or when a modification to some parameters inside the phone is required (e.g. an area code change might require MIN reprogramming). This standard supports both TDMA and CDMA phones, although the methods used by each are quite different, and the majority of the document is divided into two quite distinct sections.

An upcoming enhancement to over-the-air activation for both technologies will be to support network initiated parameter administration (OTAPA: Over-the-Air Parameter Administration), which would allow the network to initiate modifications to internal mobile data. This would be applicable in situations when the carrier recognizes the need to change a parameter such as the MIN or authentication parameters. Modifications to IS–725 will be made in the form of an addendum to support OTAPA operations for CDMA (PN–4173). This capability for TDMA systems is already supported by IS–725.

In addition, IS–725 Addendum 1 will also contain any necessary corrections to IS–725.

IS–730: Advanced TDMA Features

The Digital Control Channel (DCCH) is the pride and joy of IS–136 TDMA digital. Although it is no more “digital” than the so-called “analog” control channel, it does have about 10 times the capacity, allows multiple control channels in one cell (further increasing its effective capacity) and is a more structured protocol than the FSK control channel used in EIA/TIA–553 and IS–91 analog, and also in IS–54 TDMA digital cellular. TIA/EIA/IS–730 defines network operations to support some advanced features that are supported only on the DCCH, including user groups, hierarchical cell structures (using PSID/RSID) and sleep mode for extended battery life. Network operations for these capabilities will also be included in TIA/EIA–41–E.

TIA/EIA/IS–730 is described in detail in the October and November 1997 issues of *Cellular Networking Perspectives*.

IS–735: Advanced CDMA Features

CDMA proponents are also looking for new tricks for their favored system. TIA/EIA/IS–735 contains inter-system modifications to support additional capabilities, also taking advantage of their greater control channel flexibility. The most significant of these features is the TMSI: Temporary Mobile Station Identity, that can both reduce the paging load and reduce the exposure of the sensitive MIN, IMSI and ESN identifiers, further reducing the possibility of cloning fraud.

IS–737: Circuit Data

It is ironic that there are currently more challenges to transmitting data over digital cellular phones than over analog. However, as the world turns from faxes, BBS’s and computer-to-computer connections to the Internet, and as direct digital connections replace analog modems, the tide may well turn. To allow wireless phones to make and receive data calls while roaming, IS–737 provides a number of new and modified transactions, that will be incorporated in TIA/EIA–41 Revision E.

The fundamental problem with data is that wireline transmissions have generally been modem oriented, and digital cellular cannot reliably transmit modem tones (due to the voice coder). It obviously does not make long term sense to take digital information, translate it to modem tones and then digitize the modem tones as if they were analog signals. One solution is to provide special purpose modem pools at the MSC site, and another (being heavily promoted by Qualcomm, among others) is to provide

direct digital connections to the internet from the wireless system, so that modems can be avoided entirely.

If the modem pool approach is used, a further problem is that the modem cannot be moved from the Anchor MSC following an inter-MSC handoff. Consequently, true digital information has to be transmitted on the DS0 channels between MSC's. This capability is provided by IS–728 which, unlike IS–737, may remain a separate standard.

IS–751: IMSI

The International Mobile Station Identity is the identifier used for GSM mobiles and will eventually replace the current MIN identifier that is still prevalent in AMPS, D-AMPS and CDMA. The impact of a new mobile identifier on inter-system operations is tremendous, as the MIN is currently a mandatory parameter in most intersystem messages. In fact, according to the TIA/EIA–41 compatibility rules a mandatory parameter may not be made optional, yet this is precisely what IS–751 is forced to do. The introduction of this standard will have to be handled carefully to avoid messages being sent containing IMSI (and not MIN) to network elements that have not been upgraded to support this.

The need for IMSI is still not widely appreciated, yet international carriers will soon run out of IFAST-allocated International Roaming MIN codes, and will have nowhere to turn except IMSI.

J–STD–034: Enhanced 9–1–1

The US FCC order for enhanced 9–1–1 is best known for its demand that wireless systems be able to locate mobiles within 125 meters 67% of the time. However, the first phase of the order is to provide both the cell/sector location of the call (i.e. approximate location) and the mobile identity (MDN: Mobile Directory Number). The MDN will allow callback to someone who has made a 9–1–1 call and then disconnected. Another feature that is included (although not mandated by the FCC) is Reconnect, the ability to automatically re-page a mobile that disconnected abnormally during a 9–1–1 call.

J–STD–034 has two relatively minor impacts on TIA/EIA–41. To allow 9–1–1 calls to be dialed as a 3-way call following an inter-system handoff, several inter-system handoff messages were modified. These same messages were also modified to support Reconnect following an inter-system handoff.

PN–3661: WIN

The Wireless Intelligent Network (WIN) standard is nearing completion of the V&V phase, and may be sent out for ballot as soon as April 1998. If so, this standard, that attempts to optimize communication between traditional wireless network elements (MSC, HLR) and peripheral devices (IP, SCP, SN), will need to be incorporated into TIA/EIA–41–E.

PN–3980: Number Portability

The first phase of Local Number Portability that must be supported by most US wireless carriers (and, eventually, carriers in other countries) is the ability to route a call to a local ported wireline number. This requires that MSC's have a method to query the local Number Portability Database. PN–3980 provides the NumberPortabilityRequest message for this purpose, which will need to be incorporated into TIA/EIA–41–E.

PN–4081: Authentication Enhancements

A theoretical, network-based, attack on authentication was discovered by Nortel, and is being fixed by an enhancement to TIA/EIA–41 that obviously must be included in Revision E. Because the attack is based on network behavior, the resolution does not require air interface modifications (and therefore does not require modified mobiles or base stations). This, along with various corrections, clarifications and simplifications to existing authentication procedures will be included in PN–4081, which may be published as a standalone standard before being incorporated in TIA/EIA–41–E.

PN–4103: Calling Name

Calling Name Presentation and Restriction features (CNAP/CNAR) were originally intended for inclusion in the WIN standard (PN–3661). However, due to a desire for rapid implementation, it has been segregated from WIN and is currently being balloted, for publication as an interim standard.

PN–xxxx: Internationalization

Beyond IMSI (IS–751), a new project has been started to further internationalize TIA/EIA–41, including defining the SS7 global titles that may be used for international transmission of messages. This new project may be incorporated in TIA/EIA–41–E, if ready in time.

Other Enhancements

It is likely that all, or at least most, of the above standards will not only be published as standalone TSB's or Interim Standards (IS–), but also incorporated into TIA/EIA–41–E. In addition, various other enhancements and corrections to the standard may be included before publication. The list of additions is getting so long that a new project has been started simply to track changes, whether they be large or small.

Given that TIA/EIA–41–D was over 1,500 pages, the task of merging in many hundred more pages is immense, especially considering that several of these standards modified the same areas of TIA/EIA–41, which makes the job of merging even more complex. If this was not enough, there is some reorganization planned for TIA/EIA–41 and a conversion from Microsoft Word to Adobe FrameMaker. Consequently, it is unlikely that TIA/EIA–41–E will be completed on schedule in 1998.

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

Last published September, 1997

TDMA Digital Air Interface Standards – First Generation

IS/TSB	ANSI	Description	Status
IS–54-B	TIA/EIA–627	Original TDMA Dual-Mode Air Interface Standard	ANSI pub. 09/96
IS–55/56	TIA/EIA–628/629	TDMA mobile/base station minimum performance standards	ANSI pub. 09/96
IS–85	TIA/EIA–635	TDMA full-rate voice coder (3:1)	ANSI pub. 09/96
TSB–46		Verification of Authentication for IS-54-B Mobiles	Published 03/93
TSB–47		IS–54 Implementation Issues	Published 05/94
TSB–50		User Interface for Authentication Key Entry	Published 03/93

TDMA Digital Air Interface Standards – Second Generation

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

TDMA Digital Air Interface Standards – Third Generation

Standard	PN/SP	Description	Status
IS–130-A	**PN–3795**	**Data Services Radio Link Protocol**	**Published 09/97**
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
IS–136.1-A-1		IS–136 Rev. A, first addendum: section 1 corrections (DCCH)	Published 11/96
IS–136.1-A-2		**IS–136 Rev. A, second addendum: section 1 corrections (DCCH)**	**Published 12/97**
IS–136.2-A		FSK control channel, analog voice channel, TDMA traffic channel	Published 10/96
IS–136.2-A-2		**IS–136 Rev. A, second addendum: section 2 corrections**	**Published 12/97**
IS–137-A	PN–3605	Mobile minimum performance standards for IS–136-A	Published 07/96
IS–137-A-1		Revised transmission tests for IS–137-A	Published 08/97
IS–138-A	PN–3606	Base station minimum performance standards for IS–136-A	Published 07/96
IS–641		Enhanced full–rate voice coder (ACELP)	Published 05/96
IS–684		Isochronous radio link protocol for data (for STU-III)	Published 08/96
IS–686		Enhanced full rate voice coder performance standards	Published 12/96
TSB–73		IS–136 Rev. 0/Rev. A compatibility issues	Published 07/96
TSB–77	PN–3731	IS–641 implementation issues	Published 12/96

TDMA Digital Air Interface Standards – Fourth Generation

Standard	PN–/SP-	Description	Status
TIA/EIA–136	**SP–4027**	**Introduction/Document Contents**	**Development**
TIA/EIA–136-010	**SP–4027-010**	**Optional Mobile Station Facilities**	**Development**
TIA/EIA–136-020	**SP–4027-020**	**SOC, BSMC, and Carrier Specific HLPI assignments**	**Development**
TIA/EIA–136-100	**SP–4027-100**	**Introduction to Channels**	**Development**
TIA/EIA–136-110	**SP–4027-110**	**RF Channel Assignments**	**Development**
TIA/EIA–136-121	**SP–4027-121**	**Digital Control Channel Layer 1**	**Development**
TIA/EIA–136-122	**SP–4027-122**	**Digital Control Channel Layer 2**	**Development**
TIA/EIA–136-123	**SP–4027-123**	**Digital Control Channel Layer 3**	**Development**
TIA/EIA–136-131	**SP–4027-131**	**Digital Traffic Channel Layer 1**	**Development**
TIA/EIA–136-132	**SP–4027-132**	**Digital Traffic Channel Layer 2**	**Development**
TIA/EIA–136-133	**SP–4027-133**	**Digital Traffic Channel Layer 3**	**Development**
TIA/EIA–136-140	**SP–4027-140**	**Analog (FSK) Control Channel**	**Development**
TIA/EIA–136-150	**SP–4027-150**	**Analog Voice Channel**	**Development**
TIA/EIA–136-270	**SP–4027-270**	**Mobile Station Minimum Performance Requirements**	**Development**
TIA/EIA–136-280	**SP–4027-280**	**Base Station Minimum Performance Requirements**	**Development**
TIA/EIA–136-300	**SP–4027-300**	**Introduction to Data Services**	**Development**
TIA/EIA–136-310	**SP–4027-310**	**Radio Link Protocol Layer 1**	**Development**
TIA/EIA–136-320	**SP–4027-320**	**Radio Link Protocol Layer 2**	**Development**
TIA/EIA–136-330	**SP–4027-330**	**Packet Data**	**Development**
TIA/EIA–136-350	**SP–4027-350**	**Asynchronous Data/Fax**	**Development**
TIA/EIA–136-420	**SP–4027-420**	**VSELP voice coder**	**Development**
TIA/EIA–136-510	**SP–4027-510**	**Authentication, Encryption of Signaling Information/User Data and Voice Privacy**	**Development**
TIA/EIA–136-700	**SP–4027-700**	**Introduction to Short Message Teleservices**	**Development**
TIA/EIA–136-710	**SP–4027-710**	**Short Message Service (Cellular Messaging Teleservice)**	**Development**
TIA/EIA–136-720	**SP–4027-720**	**Over-the-Air Activation Teleservice (OATS)**	**Development**
TIA/EIA–136-910	**SP–4027-910**	**Informative Information**	**Development**

Note: 1. IS– Interim Standard, TSB– Telecommunications Systems Bulletins, PN– Project Number, SP– ANSI Standards Proposal.
2. **Bold Type** indicates modification since previous publication.
3. Published TIA standards can be obtained from Global Engineering Documents at 1-800-854-7179.

Thanks to Peter Nurse (Lucent) and Al Sacuta (Next Generation) for their assistance compiling the information in this table.