Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-403-289-6609 • Fax 403-289-6658 Vol. 6, No. 12 December, 1997

In This Issue...

CALEA Gets a Standard p. 1

The telecom industry's blueprint for US law enforcement surveillance requirements will be published as an interim standard (J–STD–025), and possibly as a full ANSI standard.

The Ninety-Nine Names of IS–41 p. 1

It is time to review the latest names given to the almost published ANSI version of TIA IS–41 (and the winner is; ANSI TIA / EIA-41 Rev. D!)

Advanced CDMA Network Features: PN–3619 p. 2

What are TMSI and NDSS? And, how do CDMA roamers benefit from them? Only PN–3619 knows for sure.

TR–45.2 Standards Update p. 5

Much has changed since our last report on the status of the TIA TR–45.2 subcommittee's network standards. Many important new capabilities (including data and over-the-air activation) and US government mandates (CALEA, number portability and Enhanced 9–1–1) either have a new standard, or soon will.

New US Mailing Address
3401 W. Airport Freeway,
Suite 106-306
Irving, TX 75062, USA

Next issue: January 5, 1998

CALEA Gets a Standard

Last month we reported on the trials and tribulations of the telecommunications industry's attempts to develop a standard to meet the requirements of the US CALEA legislation. This month we can report that at least one standard will soon be available, and possibly two.

On November 21, 1997 the TIA subcommittee TR–45.2 and ATIS committee T1 agreed to publish the agreed LAES (Lawfully Authorized Electronic Surveillance) document as joint TIA/ATIS standard J–STD-025. This had been balloted by the TIA as PN–4116, and received virtually unanimous support from the wireless industry. No votes were accepted from law enforcement (as they are not members of TIA or ATIS).

TIA TR–45.2 and ATIS T1 also agreed to request that the same document, balloted as SP–3580–A,be considered as an ANSI standard. Publication of this version is problematic, as almost 200 negative ballots were received from law enforcement (which *is* entitled to vote on an ANSI standard). Will ANSI treat all these votes as a single law enforcement vote, as they all stated supported for the one set of law enforcement comments submitted by the FBI, and contained no distinct technical comments?

Mail Strike in Canada

Due to a postal strike in Canada, there may be delays in getting the newsletter to mail subscribers. We will be providing fax or email as alternatives to our Canadian postal subscribers. We appreciate your patience!

The Ninety-Nine Names of IS–41

The names of the first ANSI version of the IS–41 intersystem operations standard keep changing. While still a TIA interim standard, IS–41 went through four revision levels:

IS–41 Rev. 0 - Intersystem Handoff.

IS–41 Rev. A - Added automatic roaming (call delivery etc.).

IS–41 Rev. B - Enhanced roaming and handoff.

IS–41 Rev. C - Added a large number of new features, including SMS.

Now the first ANSI standard is being prepared for publication, what will it be called? Initially it was referred to as IS–41–D, but this is not appropriate as it will no longer be an Interim Standard. For a while, the name TIA/EIA–689 was reserved. However, the TIA TR–45.2 subcommittee worried that this could be confusing and requested that the name TIA/EIA–41 be reserved, if available. As it was (available) it was (reserved).

The next question was, which revision number or letter should be used to identify the first ANSI version of TIA/-EIA–41? Traditionally the first revision of a standard is called Rev. 0 and the second Rev. A, but this could cause

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/. **Language Editions:** English - Español.

confusion because TIA/EIA/IS–41–0 and TIA/EIA/IS–41–A are still in use, which could cause confusion with ANSI standards TIA/EIA–41–0 and TIA/EIA-41–A (note that the omission of the "IS–" is the only distinguishing mark for an ANSI standard name). To prevent this confusion it was decided, at a recent TIA TR–45.2 meeting, to call the first ANSI standard TIA/EIA-41-D and the second (due to be published in 1998) TIA/EIA-41–E.

This is not 99 names, but then the first ANSI version of IS–41 has not been published yet, so there is plenty of time for more name changes!

Advanced CDMA Network Features: PN–3619

TMSI (Temporary Mobile Station Identity) and NDSS (Network Directed System Selection) are two new CDMA roaming features specified in the nearly complete standard PN–3619. Perhaps this standard was motivated by competition with TDMA proponents and their DCCH roaming features (see the October and November, 1997 issues). PN–3619, was, at press time, almost ready for publication as a TIA interim standard although it is in reality an addendum to ANSI TIA/EIA-41.

The Network TMSI feature of PN–3619 provides greater user anonymity, while NDSS guides a mobile, faced with possibly 8 different cellular and PCS systems to choose from, to the best system (e.g. from a cost or service viewpoint).

Table 1: Mobile Identifiers

Identifier	Purpose & format
IMSI	15 digit identifier of mobile, HLR and home country
MIN	10 digit mobile and HLR identifier
MSID	IMSI or MIN
Local tmsi	Serving system temporary identification of mobile
Network TMSI	Local TMSI plus system identification

TMSI: Temporary Mobile Station Identity

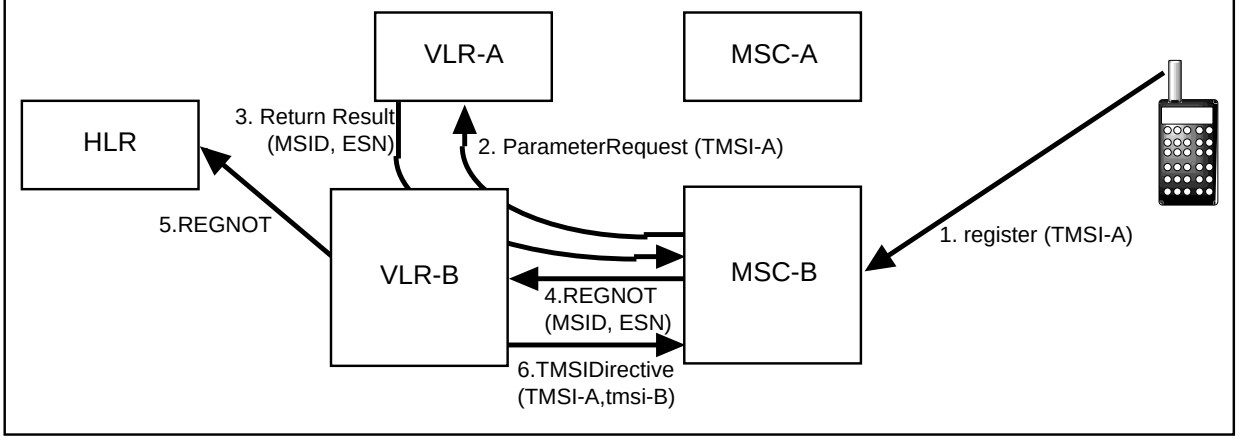
Cellular phones traditionally identified themselves to base stations, and base stations communicated with a specific mobile, by including the MIN (10 digit Mobile Identification Number) in signaling messages. Since 1995, however, the TIA committee TR–45, following the lead of the GSM community, has been committed to a long term transition to the 15 digit IMSI identifier, mainly to facilitate international roaming. The differences between MIN and IMSI are summarized in Table 1 and described in detail in our April 1996 issue.

TMSI is yet another concept borrowed from GSM. It is simply a number assigned to identify a specific mobile while it is roaming in a system. This hides the true identity of the mobile most of the time. Obviously the identity has to be revealed in the transaction that assigns a TMSI to a mobile. The use of TMSI will also reduce control channel bandwidth requirements *if* it is significantly smaller than the MIN or IMSI. This is true of some standards (e.g. IS–136) but not of IS–95 CDMA.

One might expect that the TMSI is exposed every time a mobile registers in a new system, with a separate pool of TMSI numbers. However, PN–3619 has a method to avoid this exposure, although at the expense of some complexity. Figure 1 shows how a mobile can register in one system, with a TMSI assigned by another, and have the appropriate identifying information exchanged via the TIA/EIA-41 network.

1. The mobile registers using the TMSI assigned by the previous serving system (TMSI-A from MSC-A). Because the mobile has recognized that it has moved to a

Figure 1: Transferring TMSI Between Systems



different system, it must transmit the full "Network" TMSI, including the E.212 (IMSI) identification of the assigning system.

2. MSC-B, recognizing that a foreign TMSI has been received, initiates a new PN–3619 transaction, ParameterRequest INVOKE, including the Network TMSI (TMSI-A). This transaction is sent to MSC-B's VLR, and then across to the old serving system VLR (VLR-A), which originally assigned TMSI-A.
3. VLR-A retrieves the MSID (MIN, IMSI or both) and ESN from its roamer database and returns that information in the ParameterRequest RETURN RESULT back to VLR–B, which records the assignment in its roamer database. VLR–B also forwards the message to MSC-B.
4. MSC-B can now launch a RegistrationNotification INVOKE (or AuthenticationRequest INVOKE) to VLR-B, including the mandatory MSID and ESN.
5. VLR-B forwards the RegistrationNotification INVOKE to the HLR, and responds with validation and profile information (note: the RETURN RESULT is not shown for clarity).
6. VLR-B will now likely decide to assign a new TMSI to the registering mobile, to avoid the additional bandwidth of transmitting a full Network TMSI on every access. It launches a TMSIDirective INVOKE, containing both the current TMSI (TMSI-A) and the new TMSI, identified as tmsi-B (shown in lower case letters to indicate that only the local 32 bit TMSI code is transmitted).

Why Provide Anonymity?

The benefit of the network based TMSI is limited to anonymity, as only a local TMSI would ever be smaller than a regular identifier. Today, knowing someone's MSID (almost always the MIN) provides their phone number, and could be useful in tracking people and, perhaps more importantly, in cloning their phone. However, in the future, this (mis)use of the MSID will decline.

First of all, number portability will break the connection between a MIN and a directory number, so that for all ported subscribers, knowing the MIN will not provide their directory number. Also, when the transition to IMSI occurs, the IMSI identifier will be independent of the directory number in many systems (IS–95 Revision A being one exception).

For people who do not want to actually identify a mobile, but just want to clone it, authentication will prevent the use of a stolen MIN/ESN combination over the air by requiring knowledge of the A–Key and SSD, which are never transmitted (unless encrypted) over the radio interface.

NDSS: Network Directed System Selection

PCS has introduced a new problem for mobile phones. Faced with a choice of possibly 8 different wireless systems (2 cellular and 6 PCS), and possibly more for phones that have ESMR or Satellite modes - what is a poor old phone supposed to do to pick the best system?

Why Picking the Right System is Important

It is important to pick the right system to ensure that a mobile subscriber is able to obtain service on the chosen system, that as many advanced services as possible are provided (such as call waiting or calling number identification) and a good roaming rate is obtained.

Cellular phones have a much easier job, generally assuming that their home system band (A or B) is always preferable. Another simple algorithm would be to choose the system with the strongest compatible signal, but it might not even have a roaming arrangement with the home system, consequently preventing the mobile from obtaining any service.

Picking a system when a PCS-capable phone is at home is not a problem. If a signal from the mobile's home system can be detected it should be used. System selection when roaming is the challenge.

Who Picks? The Mobile or the System?

There are two logical choices for picking the right serving system. The mobile could have a database of systems, each marked with a priority. While this makes the picking algorithm simpler, managing the database is not. The IS–136 TDMA strategy is to update the mobile's internal database through the use of short messages. Consequently, mobiles either use their internal database or, if their database does not cover their current location, they use the strongest signal method to access one system and hope that this stimulates a database update to redirect them to a better system, if necessary.

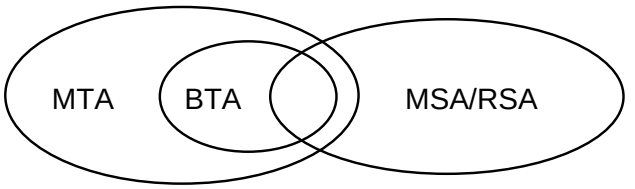
The other choice, apparently preferred by CDMA proponents, and specified in PN–3619, is to let the mobile access the system using the strongest local signal and redirect it to the preferred system. This method is known as NDSS; Network Directed System Selection.

There are two challenges with NDSS: getting competitors to cooperate (the business problem), and implementing the required database and algorithms at the HLR (the technical problem).

The Business Problem

The business problem with NDSS is whether competing systems will cooperate. Superficially, it is strange for a business to cooperate in removing itself from a revenue stream. Either the rejected serving system will want to be compensated for its efforts (which would result in charges for roaming mobiles that might not produce any revenue) or there will have to be mutual agreements between competitors to redirect each other's roaming mobiles, which relies on a great deal of trust between competitors and assumes a reasonable balance between the traffic given away and received.

Figure 2: Overlap Between BTA, MTA, MSA and RSA License Areas



Glossary

BTA - Basic Trading Area
MSA - Metropolitan Statistical Area
MTA - Metropolitan Trading Area
RSA - Rural Statistical Area

The Technical Problem

PCS system selection is more complex not only because there are more systems to choose from in each local area than in cellular, but because of overlapping license areas. Figure 2 is a Venn diagram for the overlaps between the MSA/RSA, BTA and MTA license areas in the US (most other countries use simpler licensing systems):

- 2 cellular licenses are available per MSA or RSA. MSA's and RSA's do not overlap.
- 2 US PCS licenses (A and B) are assigned to each of 51 MTA's. Boundaries of MTA's and MSA's are not coordinated.
- 4 US PCS licenses (C, D, E and F) are assigned to each of 492 BTA's. Several BTA's are contained with an MTA.

The varying degrees of overlap between license areas make it difficult for NDSS to determine which other bands to search in for a better system. For example, a mobile that registers in an MTA could be in any one of the BTA's contained within the MTA (an average of about 10) or one of an even larger number of MSA's or RSA's that are within the MTA or that partially overlap the MTA. Table 2 illustrates the difficulty of determining what the alternate systems are based on knowing only the system that the mobile has accessed in.

The most serious effect of this problem is that it could make it virtually impossible to determine alternate, non-MTA, candidate systems for a mobile that registers in an MTA. The smallest problem would occur in redirection of mobiles between systems occupying the same license area.

Any HLR implementing NDSS will have to have a sophisticated geographical information system (GIS) to convert the registered location into a prioritized list of alternates.

How NDSS Works

Figure 3 illustrates how NDSS might work when, sometime long in the future, a mobile is faced with 8 different systems to choose from.

1. The mobile registers on any one of the local systems (based on internal mobile algorithms, which could include signal strength and some knowledge of the local environment).
2. The MSC attempts to register the mobile, transmitting a REGNOT (RegistrationNotification INVOKE) to the HLR identified by the mobile's MIN or IMSI. This message will contain the identity of the serving system (e.g. MSCID) and the current control channel mode (e.g. analog or CDMA).
3. The HLR consults a geographical information system (GIS) using the identity of the serving system as a key.
4. The GIS database query returns the preferred system identity (whether analog or CDMA).
5. The regnot (RegistrationNotification RETURN RESULT) contains the identity of the preferred system (in this example the E block system, although it is not clear how a BTA could be chosen when a mobile registers in an MTA). The message also indicates whether or not the mobile should return to the original system (PCS B-block in this case) if access on the preferred system fails.
6. The initial serving system redirects the mobile.
7. Assuming that the mobile can lock onto the preferred system, it will then register.
8. The new serving system transmits a REGNOT to the HLR (which hopefully is smart enough to avoid re-initiating the NDSS process!).

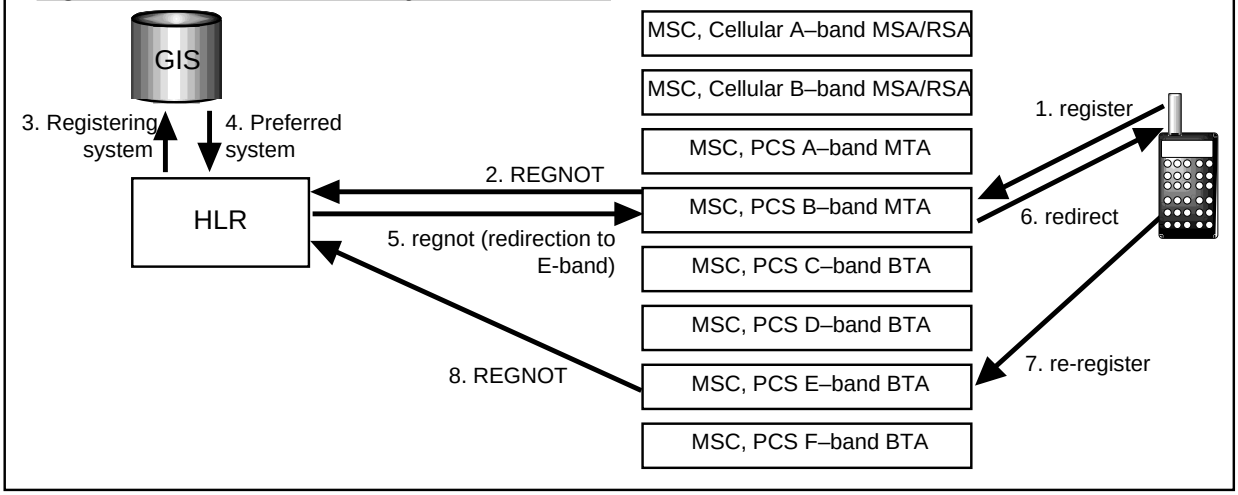
Table 2: Overlap between MSA/RSA, BTA and MTA-based systems

	Overlaps with…		
Register in…	**MSA/RSA**	**BTA**	**MTA**
MSA/RSA	1	*multiple*	*multiple*
BTA	*multiple*	3	2
MTA	*multiple*	*multiple (≈40)*	1

Conclusions

PN–3619 provides two new features for roaming CDMA mobiles, TMSI and NDSS. TMSI is an enhancement to anonymity, although perhaps only useful in the short term. NDSS attempts to help roamers lock onto the best serving system, although it raises significant business and technical problems.

Figure 3: Network Directed System Selection



TR–45.2 Standards Update

The surge of government mandates is still washing over TR–45.2, while the earlier wave of new capabilities (data etc.) has still not completely swept past.

Documents within each category are listed alphabetically.

Recently Published

International Applications (TSB–29 Rev. B) • Useful information for developing AMPS-based systems outside North America, including tables of MIN and SID blocks. *Published in July, 1997.*

Online Call Record Transfer (IS–124 Rev. A) • Near real-time transmission of call detail and billing records. This version provides billing grade data. But, can it compete with the venerable CIBER format? *Published September, 1997.*

In Press

Enhanced Wireless Emergency Services, E9-1-1 (J–STD–034; PN–3581) • A standard to support the FCC-mandated Phase I for enhanced wireless 9-1-1. It applies to both IS–41 and GSM based wireless networks. Cell/sector location and mobile identification will both be transmitted to the emergency services system using near-standard PSTN interconnect signaling. *A joint TIA interim standard/ATIS trial use standard is in press as J–STD–034.*

Intersystem Operations (ANSI/TIA/EIA-41-D, SP–3588) • The "IS–41 Rev. C" ANSI ballot review was completed at the September, 1996 TR–45.2 meeting, yet it has still not been published. It will be called Rev. D, instead of Rev. 0, to avoid confusion between TIA/EIA/IS–41-0 (about 100 pages) and TIA/EIA-41-0 (about 2,000 pages). *In ANSI pre-publication review.*

Intersystem Link Protocol (ISLP; PN–3660) • This new inter-MSC rate adaption protocol is required to support the transmission of data from digital phones following an intersystem handoff. *In press.*

Law Enforcement Intercept, LAES (J–STD–025; PN–3580) • Squeezed between the cost concerns of the industry, the constraints of the US CALEA law and the demands of law enforcement, a new standard for intercept has been developed. It will apply to both wireless and wireline networks. See the June, July, August, September and November 1997 issues, as well as a related article on page 1 of this issue. *A joint TIA interim standard/ATIS trial use standard is in press as J–STD–025. The document is also being considered for possible ANSI publication.*

Over-The-Air Service Provisioning (IS–725, PN–3769) • OTASP will provide the ability to program, or reprogram, a digital (TDMA or CDMA) mobiles over the radio interface. *In press as IS–725.* An erratum is under development.

TDMA Digital Control Channel, DCCH (IS–730, PN–3579) • Definition of network support for the IS–136 Rev. A features "User Group" and "Non-public mode service" as well as the System Operator (SOC) and Base Station Manufacturer (BSMC) codes. See October and November 1997 issues for more details. *In press as IS–730.*

Ballot

Advanced CDMA Capabilities (PN–3619) • This standard to support advanced features based on IS–95 Rev. A capabilities includes TMSI (Temporary Mobile Station Identity) and NDSS (Network Directed System Selection). *It may be approved for publication in December 1997.* See related article, this issue.

Digital Data Services (PN–3770) • Transmitting data from CDMA and TDMA digital phones is more complex because voice coders are incompatible

with analog modem tones. *Ballot comments have been reviewed, and a pre-publication version is being developed.*

International Mobile Station Identity (IMSI; PN–3892) • Support for the E.212 IMSI mobile identifier will resolve international roaming problems caused by the current 10 digit MIN identifier. Initially, these modifications were going to be published as part of ANSI TIA/EIA-41 Revision E, but as this standard has been delayed by the onslaught of separate extension to Revision D, it has been decided to publish (yet another) extension to the not-yet-published ANSI TIA/EIA-41 Rev. D.

Wireless Number Portability, Phase I (WNP; PN–3980) • Phase I of the Number Portability mandate requires wireless systems to terminate calls to ported wireline subscribers. This requires a new query message, known as NumberPortabilityRequest, based on the IS–41 protocol. *Currently in ballot review, with a re-ballot expected.*

In Development

Authentication Enhancements (PN–4081) • There are some theoretical (at this time) attacks on authentication that do not challenge CAVE, but simply use loopholes in the network to avoid this TIA authentication algorithm. These attacks can be prevented by relatively minor changes to the IS–41 authentication transactions and procedures. Other, less serious, improvements and clarifications to the procedures are also being made.

Broadcast Short Message (PN–4104) • TDMA and CDMA air interfaces provide the ability to transmit a single short message to multiple terminals. This has two flavors; true broadcast that sends a message to all phones in a group of cell-sites (e.g. traffic or weather alerts) and group broadcast or multicast that sends a message only to the phones in a group that subscribe to that service (e.g. stock quotes or sports scores). *Currently in the early stages of development.*

Call Detail/Billing Records (ANSI TIA/EIA–124-B; PN–3816) • Modifications to IS–124 to fully support data services and intelligent peripherals, along with a large number of detailed technical corrections.

Calling Name Presentation/Restriction (CNAP/CNAR; PN–4103) • Due to delays in completing the WIN standard (PN–3661), this one of the three WIN service drivers has been put on a fast track to publication. Calling Name Presentation provides an IS–41 based query (ServiceRequest) to an SCP (possibly the wireline LIDB) that will provide the calling party's name for display on phones with this capability. Calling Name Restriction prevents a wireless subscriber's name from being displayed on another phone. *Currently in V&V, prior to approval for ballot.*

Emergency Services, Phase II (E911–II; PN–3890) • Critical decisions have to be made regarding the network model used to provide more accurate location information to emergency call takers. Will wireless systems merely provide the information, or will it be used to influence routing decisions? Will an SCP be an option? Which interfaces will be standardized? What network elements can provide location information (e.g. mobile, base station or an external device)?

Interconnection (IS–93 Rev. A; PN–3295) • Modifications to this PSTN interconnect standard include emergency services enhancements (taken from J–STD–034), definition of ANI II digits related to wireless calls and various enhancements and corrections from Revision 0. The draft standard is *in V&V until December 1997.*

International Applications (TSB–29–C; PN–4117) • The next publication of TSB-29. *Currently in the early stages of development.*

Intersystem Operations (ANSI TIA/EIA–41 Rev. E; PN–3590) • As with TIA/EIA-664, a big problem with this standard has been organization. It appears that the Stage II portions can be published as separate parts (e.g. the network "ping-pong" flow diagrams), while the Stage III protocol specification will continue to be published as a single monolithic document. This revision will absorb a number of capabilities that already have been published as standalone documents, or soon will be: data services, over-the-air activation, DCCH features, advanced CDMA features, IMSI support etc.

Subscriber Features (ANSI TIA/EIA–664 Rev. B; PN–3362) • This standard, once called TIA/EIA/-IS–53 has been gathering dust, waiting for a decision on how to publish a large modular document, without republishing it in entirety every time a new feature is added. It has been decided that each feature or capability should be a separate part, that can be balloted and published separately.

Wireless Intelligent Network (WIN; PN–3661) • The description of intelligent networking for IS–41 based mobility networks has been completed *and now is in V&V.* It is described in detail in the March, April, June and July 1997 issues.

Pending Projects

IFAST Addenda to TSB–29 (PN–pending) • TSB-29 contains critical information on MIN and SID usage for international systems and, to some extent, for North American systems. To address the concern of the IFAST (International Forum on AMPS Standards Technology) that this information is not published often enough, two projects have been initiated to allow fast-track (i.e. 60-90 days) publication of this information following the November 1997 and February 1998 IFAST meetings. *Project numbers are pending.*

Wireless Number Portability, Phase II (no PN) • No action yet on Phase II portability (allowing wireless subscribers to port).