Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email: David.Crowe@cnp-wireless.com Vol. 10, No. 7 July, 2001

In This Issue...

Next Issue: August 1st, 2001

FCC NPRM on Cellular Fundamentals (Part 22)

A US FCC Notice of Proposed Rulemaking (NPRM) released on May 17, 2001 may result in modifications to Part 22 of the commission's rules, based on changes in technology since the early 1980's when they were first developed. Part 22 governs many important aspects of cellular phones and, to a lesser extent, PCS and ESMR phones produced for use in the United States.

ESN Changes

Part 22 currently requires that a mobile phone's Electronic Serial Number be unique, unalterable and untransferrable. Attempts to change it are supposed to render the phone inoperable. Unfortunately, with software-controlled devices, it is easy to transmit a substitute for the stored ESN, even if it is successfully hardened, making the goal of the FCC impossible to achieve. Even though these Part 22 requirements appear to have little benefit, they do make it difficult to implement new capabilities – notably, the use of a Smart Card in TDMA or CDMA phones. The requirements also bar ESN manufacturer code conservation via re-use of under-utilized codes because of a small risk of duplicate ESN codes occurring (but no risk of any operational problems). The existing Part 22 requirements have definitely slowed TIA TR-45 standardization and conservation efforts.

The FCC is considering removal of the hardened ESN requirements, which would allow the wireless industry to move forward with use of Smart Cards and ESN number conservation.

SID Changes

SID (System Identification) codes are the equivalent of a call sign for a cellular system. These 15-bit numbers were initially assigned by the FCC to uniquely identify all US cellular licenses. Later, they were assigned to PCS licenses, as well. Many changes have been made to the original assignments, often due to consolidation of SID codes to match large local calling areas. Some SID codes are used for billing or accounting purposes. These codes, known as BIDs (Billing Identifiers) are assigned by Cibernet. Some of these are outside the 15-bit range of transmittable codes (i.e. above 32,767).

The FCC is now considering handing over responsibility for SID code assignment to Cibernet Corp., a CTIA subsidiary. Unfortunately, the NPRM does not recognize the extensive international use of SID codes. Individual codes are assigned by national authorities based on blocks defined in TIA/EIA/TSB29, but additional blocks are assigned by IFAST (www.ifast.org).

Analog Service

When cellular service was first approved by the FCC, it required adherence to detailed technical requirements (OET 53) that later evolved into the analog cellular standards EIA/TIA/IS-3 and then TIA/EIA-553. The FCC is considering removal

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.

of the requirement that cellular carriers continue to support analog. This could have a considerable impact on US consumers who are still using analog cellular phones (42 million in 1999, down from 44 million in 1998), along with rural areas that still have only analog coverage. Analog cellular is still useful for extending roaming service areas for digital customers to places where analog is available, but not their flavor of digital. There are also a number of businesses relying on analog for universal coverage (e.g. GM OnStar system and emergency-only phones) or data services (e.g. Aeris and Cellemetry).

Book Review: *Wireless Telecommunications with ANSI-41*

Ben Levitan, TSI Connections

If you read the Second Edition of Snyder and Gallagher's book, *Wireless Telecommunications with ANSI-41*, it is possible to justifiably claim "Expertise in ANSI-41 Revision E" on your resumé, even though publication of the standard is still several months away.

Their easy to follow book is again an excellent and comprehensive resource on the IS-41/ANSI-41 standards and the technologies it supports. Even if you have the first edition, you'll find value in reading this sequel as one-quarter of it (about 140 pages) covers new material developed by TIA standards sub-committee TR-45.2 since the release of IS-41 Rev C and TIA/EIA-41-D.

The book's release is well timed, as the technical content of IS-41 Rev E is frozen. All that is left for the standards committees to do is a detailed review, consisting mostly of minor editing and technical corrections which will not affect what Snyder and Gallagher have written.

This edition stays with the logical outline and flow of the first, punctuated with their easy to follow illustrations throughout. The new book is slightly bigger in format (without affecting the amount of text per page) making it easier to read.

While everything is well covered, Gallagher and Snyder go heavy on Over-the-Air Activation and Provisioning (OTA), an important feature that's not on everybody's radar today (a full 39 pages), and they go light on Local Number Portability and 911 (only 10 pages, but sufficient to understand it) which are topics of urgent interest to carriers today.

CALEA (lawfully authorized electronic surveillance), the other looming US government mandate affecting wireless, gets a mention as well. This is a good inclusion, even though the protocol is not part of ANSI-41. It is still of interest to carriers, making the book complete. The four pages on this topic, however, are merely an overview. They do not go into the technical solution developed for CALEA, nor do they describe where it fits into the wireless network.

Technical books like this are often bulky, due to extensive appendixes and lists of references. Not so with *Wireless Telecommunications Networking with ANSI-41,* which offers 502 solid pages of well written, technical explanations out of the 610 pages between the bindings. The book builds nicely from basic overviews of wireless telecommunication (a brief chapter) to basics of signaling and wireless functionalities before (at page 100) diving into a logical tutorial of ANSI-41.

Snyder and Gallagher walk you through Basic Handoff, Roaming, Authentication, Call Processing and Short Message Service (SMS) very clearly (adding 2 to 10 pages of new text, beyond their first edition, to each chapter). Of course, they then take the extensive diversion into OTA, but this section is well written and worth reading, especially their concise explanation of the Diffie-Hellman Key Agreement algorithm.

What makes the book complete are the last few chapters covering all the important but peripheral issues of wireless networking, including Roaming Agree ments, SS7, Preferred Roaming Lists and System Operator Codes. Some of these critical topics are rarely covered elsewhere [ed: except within the pages of *Cellular Networking Perspectives*], but without them, your knowledge of ANSI-41 is less than useful. This ties real implementations to the theories. One complaint that I have, however, is that E911 and LNP are relegated to this section.

Another complaint is that the changes between the editions are not "diff-marked". Standards committees have a fine tradition of marking the paragraphs of newly added text with underlines, ~~strikethroughs~~ and change bars, so readers will know the difference between the old and the new text. Snyder and Gallagher's book, sadly, has none of this.

All levels of people who work in the wireless industry with ANSI-41 will find this book invaluable, and I highly recommend it. It is still the only book available exclusively focusing on ANSI-41.

Wireless Telecommunications Networking with ANSI-41, Second Edition, McGraw-Hill, ISBN 0-07-135231-7 sells for $75 (at Amazon.com – see www.amazon.com/exec/obidos/ASIN/0071352317/102-1284304-2449722)

The older edition is still on sale there ($55.20 for Hardcover or downloadable Adobe Acrobat format).

Roamer Agreement Tables Part II: Better Alternatives?

The problems of roamer agreement tables were described in our June, 2001 issue. These tables provide information about business arrangements between two carriers, as well as routing information that is critical for communicating MAP (e.g. TIA/EIA-41) signaling messages between the Serving System (MSC/VLR) and the Home System (HLR, AC and MC) to support roaming.

IS-847 is a partial solution to this problem. However, extensive use of this standard could inject a potentially enormous signaling load into the TIA/EIA-41 network, and it can only detect problems. It cannot fix them or prevent them from occurring.

Is there a better way? One possibility is to allow routing be based on the information obtainable from a Mobile Station (MS) when it registers - the MSID (MIN or IMSI) - without knowing the actual network address of the HLR or MC. Another possibility is to centralize the management of roamer agreement information.

Global Title Routing

SS7 Global Title routing allows routing using a telephony address – for example, a phone number (ITU-T E.164), Calling Card Number or IMSI (ITU-T E.212). An STP (Signaling Transfer Point) or International Gateway will examine the global title, then it will map the address onto a point code, which will either be a destination or another routing point.

When a mobile registers, for example, only the MSID (MIN or ESN) is provided to the serving system. The Serving MSC could use this as a global title to route to the HLR, without needing to have its point code provisioned in its roamer agreement table. However, the use of global titles would not eliminate the need to store other information related to business needs and ANSI-41 protocol levels. This makes the benefit of global title quite small.

Perhaps a large problem is that use of global title would require a worldwide standardization effort, because global titles are defined nationally, and most countries have not defined – let alone implemented – the full range of global titles required for TIA/EIA-41 wireless. Furthermore, due to the lack of international global title standards, international signaling gateways will have to be programmed to map from global titles used in one country to those used in another.

Domain Name Servers

The internet makes extensive use of domain name servers for routing when it is not desirable to use an IP address.

In some ways, the domain name (e.g. cnp-wireless.com) is comparable to a global title, just as the SS7 point code is like an IP address. However, an important difference is that the domain name server (DNS) is queried by the originator of a message, which therefore obtains IP addresses that it can use for routing. This allows caching of addresses by the originator, which significantly improves the efficiency of this system.

In a wireless context, the MSID could be used in a DNS query, obtaining IP addresses for all network elements serving that block.

However, domain name servers may solve the routing problem better than global titles, but that is still the only problem they solve. Roamer agreement tables would still be required for business and MAP protocol information.

Furthermore, DNS protocols that properly support telephony addresses have not been defined and TIA/EIA-41 systems still use SS7 interfaces, not IP.

Centralized Server

A complete solution to the roamer agreement table problem would be to store this information on central servers that could be queried by network elements such as MSC's when a service request is made by a mobile with no matching entry in the MSC's roamer agreement table.

According to Ken Hammer of TSI Connections, a product like this was marketed, but with little success. Carriers were probably reluctant to have to query a central database every time a roamer requests service.

Using DNS Concepts

Combining DNS concepts with a centralized database may solve the efficiency problem. An MSC (or other MAP network element) could query the database whenever a roamer from a currently unknown system requests service, but once roamer agreement information is obtained, it could cache it for some time, reducing the need for queries. Such a system is shown in Figure 1.

Synchronization

Synchronization is a problem with any distributed database system. Insertion, deletion and updates of records usually require communication to ensure stale data is not present in other network elements.

Deleting records from the cache can occur at any time. For examples: After a given amount of inactivity (i.e. no accesses by mobiles matching the roamer record); when the local table fills up (deleting the longest inactive record first); or when the maximum time specified by the central server has passed.

A more difficult problem is how to coordinate deletion or modification of existing roamer agreement records between the central server and the local cache. If the records are only modified centrally, the serving system will end up with stale data until it removes the record from the cache.

One simple solution would be to insist that all updates occur at the same time (e.g. Sunday, midnight, GMT). The roamer agreement server could then indicate that all records expire at that time. This would, however, cause a spike in traffic at the first busy time after this, as each system starts to fill up its cache.

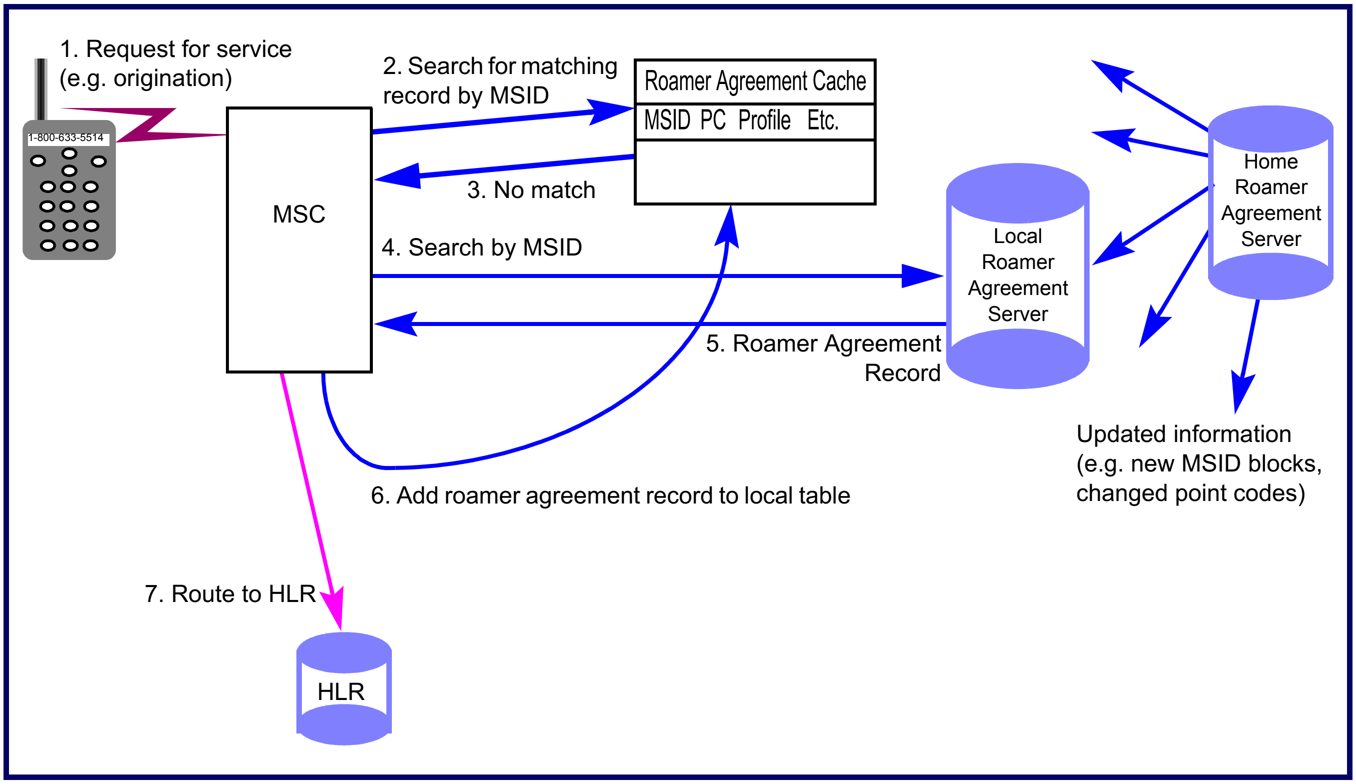
Another solution would be to insist that updates be given at least, say, one week ahead of time. This would allow the central server to ensure that the expiry time of the record in local caches would match, but no cache record could live for longer than this time, even though most cache records would remain unchanged for many update cycles.

A more sophisticated solution would be to have the roamer agreement server keep track of which systems may have cached information for a roamer agreement. This approach would notify them whenever a change is made. There is no need to actually send updated records, only the key (e.g. MSID) needs to be sent along with a command to delete the record associated with it. Serving Systems could update their cache in the normal fashion. The management burden might be too great for this system. It applies to all records, whether or not they will be updated This solution would also use unnecessary bandwidth to inform Serving Systems of changes that have already been flushed from their cache.

Interworking

It is likely that, if centralized Roamer Agreement Servers were implemented, they would, at first, be standalone. However, it is reasonable to allow some updates to be shared between servers. While business-related information might not be updatable automatically, because this would give one carrier the ability to give its subscribers privileges outside of any contracts that have been signed, routing information (such as a change in point codes serving a block of numbers) might be a candidate for automatic updating. Assuming there are a relatively small number of Roamer Agreement Servers, such updates could

Figure 1: A DNS Model for Roamer Agreement Tables



be broadcast from one server to all others. Slightly more complicated, but still feasible, is addition of new MSID blocks, which could be accomplished by referencing an existing block. This allows all information, except the identity of the number block, to be copied safely from an existing record.

Record Contents

Some of the categories of information that may need to be stored in roamer agreement tables are:

- Network Element Type. An HLR, MC (SMS Message Center) and AC (Authentication Center) may serve the same block of mobiles, but will require separate information to be stored.
- Routing information. Currently, this would most likely be an SS7 point code. In the future, IP addresses and global titles could also be included. The Serving System could use its preferred communications method based on the addresses provided.
- Protocol Capability information. This could indicate what aspects of the TIA/EIA-41 standard are supported, such as the IS-41-C profile, CAVE authentication, international TLDN and so on. While some of this information is available through current messaging, it is only after the first communication with the HLR/AC, and it makes more sense to have it available on a per-system rather than per-MS basis. A richer collection of information could be provided, knowing that it will not waste storage space by being duplicated for every number block from that system.
- Interworking information. ANSI-41 systems can provide a subset of roaming capabilities to dual-technology mobiles homed in a GSM system. Knowing the type of system could optimize the services being provided, avoiding attempts to provide services that cannot be supported by the IIF (Interworking and Interoperability Function). For example, short messages may need to be truncated when crossing a technology boundary, and services like redirection might not be possible.
- Business restrictions. This could include a default profile (if communications with the HLR is not possible) and profile overrides (e.g. international calling may not be allowed, even if the individual MS profile indicates it is allowed in the subscription). A profile validity time may also be useful to provide a maximum time that an MS can access services before being revalidated.
- Security information. This could include information about which security services should be provided (e.g. authentication, voice privacy), and what type of security systems are provided by the network element (e.g. none, CAVE or AKA).
- Carrier information. Carriers should be able to provide information related to services that are only supported within their own network.

Conclusions

It is well past time for making improvements to roamer agreement tables in wireless systems. But, these changes must be made without violating business rules and without introducing unacceptable levels of signaling that just make system performance worse.

Status of IS-41 Rev. C & TIA/EIA-41-D (ANSI-41) Implementations

Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email crowed@cnp-wireless.com
Last published April, 2001

Intersystem Operations Capability	Vendor and Radio Technology									
	Alcatel	Ericsson			LG	Lucent			Motorola	
	CDMA	Analog	CDMA	TDMA	CDMA	Analog	CDMA	TDMA	Analog	CDMA
Authentication (CAVE)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
IS-778 Authentication Enhancements			🕒		🕒					
CNAP/CNAR			⚗	✔	✔		⚗	⚗		
CNIP/CNIR	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Data (IS-737)	✔		✔	✔	✔					✔
Inter-MSC handoff: Analog to…		✔		✔		✔		✔	✔	
Inter-MSC handoff: CDMA to…	✔		✔		✔	✔	✔		✔	✔
Inter-MSC handoff: TDMA to…		✔		✔		✔		✔	✔	
International (IS-751 IMSI and IS-807)			✔	✔	⚗		⚗	⚗		
Hyperband handoff (TSB-76)	✔			✔			✔	✔		✔
LNP Phase I (IS-756)	✔	✔	✔	✔		✔	✔	✔	✔	✔
LNP Phase II (IS-756-A)		✔	✔	✔					🕒	🕒
MWN	✔	✔	✔	✔	✔		✔	✔	✔	✔
Origination Triggers	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Over-the-air Activation (IS-725)	✔		✔	⚗	✔		✔	🕒		✔
SMS Origination	✔		✔	✔	✔		⚗	✔		**4Q'00**
SMS Termination	✔		✔	✔	✔		✔	✔	✔	✔
Termination Triggers	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Voice Privacy - basic	✔			✔	✔		✔	✔		✔
Voice Privacy - EPE										
WIN Phase I (IS-771)	🕒	✔	✔	✔	⚗	🕒	🕒	🕒	🕒	🕒
WIN Phase II (Prepaid)	🕒		⚗		🕒				🕒	🕒

Status of IS-41 Rev. C & TIA/EIA-41-D (ANSI-41) Implementations

Cellular ***Networking Perspectives***

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

Last published April, 2001

Intersystem Operations Capability	Vendor and Radio Technology							
	NEC		**Nortel (MSC/BS)**			Telos		
	Analog	CDMA	**Analog**	**CDMA**	**TDMA**	Analog	CDMA	TDMA
Authentication (CAVE)		✔	✔	✔	✔	✔	✔	✔
IS-778 Authentication Enhancements								
CNAP/CNAR			🕒	🕒	🕒			
CNIP/CNIR	✔	✔	✔	✔	✔	✔	✔	✔
Data (IS-737)		✔		🕒	🕒		🕒	
Inter-MSC handoff: Analog to…	✔		✔		✔	✔		
Inter-MSC handoff: CDMA to…	✔	✔	✔	✔		✔	✔	
Inter-MSC handoff: TDMA to…			✔		✔	✔		✔
International (IS-751 IMSI and IS-807)				🕒	🕒		🕒	
Hyperband handoff (TSB-76)				✔	✔			
LNP Phase I (IS-756)			✔	✔	✔	✔	✔	✔
LNP Phase II (IS-756-A)			🧪	🧪	🧪	**3Q'01**	**3Q'01**	**3Q'01**
MWN	✔	✔	✔	✔	✔		✔	✔
Origination Triggers	✔	✔	✔	✔	✔	✔	✔	✔
Over-the-air Activation (IS-725)				✔	✔		✔	✔
SMS Origination		✔		✔	✔		✔	✔
SMS Termination		✔	✔	✔	✔		✔	✔
Termination Triggers	✔	✔	✔	✔	✔	✔	✔	✔
Voice Privacy - basic		✔						
Voice Privacy - EPE					🕒			
WIN Phase I (IS-771)			✔	✔	✔	✔	✔	✔
WIN Phase II (Prepaid)			🕒	🕒	🕒			🕒

Terms & Acronyms

www.cnp-wireless.com/glossary.html.

Symbols

✔	In field trial or commercial service.
XQ'XX	Specifies the quarter during which commercial availability is expected (e.g. 4Q'01).
🧪	In lab trial.
🕒	Under Development
(shading)	Shading indicates a capability that is not technically feasible at present, or for which no standard yet exists.
Bold type	Company names in **bold type** have indicated a change in status since the last report.
Red	Text and figures in red indicate specific changes since the last report (visible only in electronic edition of newsletter).

TIA TR-45.1 Analog Cellular Air Interface Standards

Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email David.Crowe@cnp-wireless.com *Last published January, 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.

Thanks to Bob Slocum (Ericsson) for his assistance compiling the information in this table.

First Generation: Basic Analog

Standard	Description	Status
EIA/TIA-553	Analog air interface	Published 09/89
IS-19-B	Mobile minimum performance standards	Published 06/88
IS-20-A	Base station minimum performance standards (replaced by TIA/EIA-712)	Published 06/88 Rescinded 07/97
IS-3-A,B,C,D	Original analog air interface standards (see EIA/TIA-553-0)	Rescinded 09/89
TSB-16	Assignment of access overload classes	Published 03/85
TSB-35	Cellular mobile receiver dynamic range	Published 04/92
TSB-39	Message type assignment for extended protocol	Published 03/93

Second Generation: NAMPS, In-Building, Residential, Authentication

Standard	Description	Status
TIA/EIA-89	Elevate IS-89 to ANSI standard	Development
TIA/EIA-90	**Elevate IS-90 to ANSI standard**	**Ballot 05/01**
IS-88	Narrowband (3:1) analog air interface ("NAMPS")	Published 02/93 Being rescinded
IS-89	IS-88 base station performance standards	Published 02/93
IS-90	IS-88 mobile performance standards	Published 02/93
IS-91	Analog air interface (including "NAMPS" and authentication)	Published 10/94
IS-94	In-building analog air interface ("CAPS")	Published 05/94 Rescinded 10/00
IS-680	Residential ("cordless") interface between Wireless Residential Extension (WRE) and PSTN	Published 05/96
TSB-70	Cross reference for FSK control channel	Published 12/95 Rescinded 09/99
TSB-83-A	Additional modem options for IS-680 ("cordless")	Published 04/97

Third Generation: Isolation of Core Control Channel Capabilities

Standard	Description	Status
TIA/EIA-553-A	Analog air interface (including authentication, alert/flash with info, abbrev. alert, message waiting indicator and protocol capability indicator (PCI))	Published 11/99
TIA/EIA-690	**Mobile minimum performance standards (previously IS-19-C)**	**Published 11/00**
TIA/EIA-712	Base station minimum performance standards (prev. IS-20-A)	Published 07/97

TSB-16-A	**Assignment of access overload classes**	**Ballot**
TSB-39-A	Message type assignment for extended protocol (analog, TDMA and CDMA standards)	Published 10/94
TSB-70-A	Updated version of TSB-70 cross reference	Published 09/99
TSB-71	IS-94 enhancements and issues	Published 10/95

Fourth Generation: Advanced Capabilities

Standard	Project	Description	Status
TIA/EIA-691	SP-3665	Enhanced analog ANSI version of IS-91-A (w/o Wireless Residential Extension)	Published 11/99
IS-91-A	PN-3476	Revised IS-91 air interface (including IS-94 functionality and sleep mode)	Published 11/99
IS-91-B	SP-3666	Revised version of IS-91 (including IMSI, OTA, priority access, 911, cryptosync and Expanded ESN)	Project cancelled
IS-713	PN-3668	1900 MHz upbanded AMPS (based on IS-91-A)	Published 11/99
IS-788	PN-4205	Portable wireless phone to vehicle interface - Connector	Published 06/99
IS-788-A	**PN-4660**	**IS-788 including IDB (ITS Data Bus)**	**In press**
IS-789	PN-4207	Portable wireless phone to vehicle interface - Electrical Interface	Published 07/99
IS-789-A	PN-4629	Modification to IS-789 to support SAE J2366 ITS Data Bus (IDB)	Published 04/00
IS-790	PN-4208	Portable wireless phone to vehicle interface - Latch	Published 03/00
IS-791	PN-4209	Portable wireless phone to vehicle interface - Test Specifications	Project cancelled
IS-798	PN-4527	Portable wireless phone to vehicle interface: Mounting Envelope	In press
IS-816	PN-4630	IDB message set definition for IS-789	In press
IS-817	**PN-4662**	**Geo-location for analog cellular phones**	**Published 01/01**
IS-817-1	**PN-4862-AD1**	**Geo-location for analog cellular phones, Addendum 1**	**Ballot 05/01**
IS-822	**SP-4560**	**"+" (Plus Code) dialing for international calling from analog cellular phones and Enhanced 911**	**Development**
TSB-119	**PN-4559**	**"Intelligent Retry" for improved access to emergency calling**	**Published 10/00**
TSB-121	**PN-4558**	**Interface between wireless phone and Telephony Device for the Deaf (TDD) - 2.5 mm jack**	**Ballot 01/01**
	PN-4373	Analog Air Interface Support of Expanded ESN (56 bit ESNX)	On hold
	PN-4375	Analog Air Interface Support of International Mobile Station Identity (IMSI)	Project cancelled 03/00