Cellular Networking Perspectives

David Crowe [Editor] • Phone 1-403-289-6609 • Fax 403-289-6658 Vol. 7, No. 5 May, 1998

In This Issue...

Next issue: June 2, 1998

Has GSM Been Cloned?

Reports of the demise of GSM have been greatly exaggerated. While a SIM card *was* cloned, the process required physical access to the card. Not only was the cloning process time consuming and complex, most people who have stolen a SIM card will simply go out and use it. GSM, like all wireless technologies, has larger fraud problems to worry about - most notably subscription fraud and establishing a global signaling network for real-time validation of calls from international roamers.

Last year's wireless encryption scare (see the April and May 1997 issues) was the cracking of the TIA CMEA algorithm. This was also over-rated in significance, as it affected only the protection of user-dialed digits (e.g. credit card numbers) and could not be done unless the unencrypted digits for a number of transmissions were known.

Perhaps people expect perfection from technology, but no technology that interacts with people will ever be totally secure. Even if voice encryption on wireless phones was perfect, people would still talk loudly on their phones in public places. The level of security of consumer electronics has to be viewed in the context of the purpose of the device, and weighed against the cost of each degree of higher security. The original analog cellular phones certainly had inadequate protection from fraud and eavesdropping, but this does not mean that new generations need to be completely uncrackable.

We Now Accept MasterCard

We are now able to accept payment by MasterCard, as well as by American Express, Visa, Cheques, Bank Drafts etc. Please choose the form of payment that is most convenient for you.

The Editor in *Cellular & Mobile International*

A feature article on the termination of the AMPS system in Australia will be published in the July/August issue of *Cellular & Mobile International* (an Intertec publication).

Get 'em While They're Cool

We have just received a large batch of *Cellular Networking Perspectives* 'golf' shirts. These attractive shirts are made out of environmentally friendly recycled cotton material with either Green (XL) or Burgundy (L) collars. Even the buttons are made of the nuts of the Tagua Palm, which creates sustainable jobs in South American rain forests.

There are several ways that you can win or earn a shirt. All of our premium subscribers (those who have more than a 10 copy license) will receive one, as will any subscriber who upgrades their subscription, and those who lead us to a new subscriber. Our shirts will be the first prize for our monthly quiz and for the quiz for our upcoming second issue of trading cards. If desperate, you can

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http://www.cnp-wireless.com/.
Subscriptions: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. Payment by cheque, American Express, MasterCard or Visa.
Delivery: Email or 1st class mail. **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. **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.

also purchase one for US$30 (CDN$40).

Crypto Quiz(es)

Readers of *Cellular Networking Perspectives* have a one-week head start on a new cryptology quiz kindly contributed by Les Owens of Iridium (and formerly chair of the TIA AHAG - *Ad Hoc* Authentication Group). Information on the quiz and prizes is available at:

www.cnp-wireless.com/quiz.html

Also, don't forget that our trading cards each have a number in square brackets on the front. When lined up in order, they form a clue to the location of a quiz which, if answered correctly, deserves a really good prize.

New Projects: ESN Expansion and Calling Party Pays (CPP)

TIA subcommittee TR–45.2 has initiated a project for ESN expansion, due to the decision by TIA TR-45 to expand from a 32 bit ESN to 56 bits, to accommodate more than 250 different manufacturer codes (see the January 1998 issue). This expansion will not be necessary for about 5 years if the current rate of allocation of manufacturer codes continues to average 2 per month. However, standardization often takes 1-2 years, followed by a 1-2 year development cycle for design and implementation. Consequently, it is not too early to start investigating the modifications that will be required to the TIA/EIA–41 intersystem operations standard and the TIA/EIA–124 call detail/billing record standard. Modifications will obviously also be required to all radio interfaces and to the IS-634 "A" interface that can be used to connect an MSC to Base Stations.

The second new project is for Calling Party Pays, which will require modifications to interfaces throughout the telecommunications network. Within wireless systems, CPP will likely require modest changes to intersystem operations (e.g. TIA/EIA-41) to support notification to incoming callers and possible redirection to an alternate billing system. CPP will also require modifications to call detail and billing record formats (probably also minor).

Of greater significance, CPP will require a method of exchanging wireless billing information (e.g. CIBER, IS–124) with wireline companies. Today, there is no billing record format used by both wireline and wireless carriers. A significant hurdle is the use of 3 digit RAO codes to identify wireline switches on billing records. There are not enough of these codes to identify wireless carriers, and no way to map the RAO to the 5 digit SID that is used for comparable purposes in wireless billing.

Other challenges for CPP, although outside the bounds of TR–45.2 standardization, are possible modifications to ISUP signaling to identify whether the calling line can accept CPP charges and, according to billing consultant John Willse of CRAG, acceptance into the wireline settlement "pot" to retrieve the wireless portion of CPP charges.

Enhanced Wireless 9-1-1, Part I

Enhanced Wireless 9–1–1 (E911) is one of three major US government mandates facing the wireless industry. Like the others (electronic surveillance and local number portability), the mandate may be imposed on wireless carriers in other countries, and TIA standards may be applicable solutions.

FCC Rules

E911 rules were imposed by the FCC in June 1996 (FCC Docket No. 94-102) and modified in December 1997. The requirements are to be implemented according to three major deadlines:

A. Basic 911

By October 1, 1997 wireless carriers were required to deliver all 9-1-1 calls from all mobiles, whether valid (e.g. subscribed) or not. Deaf people or others using a TTY to make phone calls should also be able to make wireless 9–1–1 calls (although this requirement was delayed until October 1, 1998 for digital systems).

B. Enhanced 911, Phase I

By April 1, 1998 wireless carriers were required to provide both the mobile's callback number (e.g. MDN, the Mobile Directory Number) and approximate location (cellsite or sector identity), if requested by a PSAP.

The wireless industry response to this requirement was the publication of Joint TIA TR–45/ATIS T1P1 interim standard J-STD-034.

C. Enhanced 911, Phase II

By October 1, 2001 wireless carriers are required to provide, upon request from a PSAP, the latitude and longitude of the calling mobile within 125 meters (400 feet) approximately 67% of the time.

The wireless industry is currently developing a standard to meet these requirements in a joint TIA TR–45/ATIS T1P1 *ad hoc* group under the leadership of Jeff Crollick of SCC.

Future Capabilities

Two additional capabilities are being lobbied for by a group known as the *Ad Hoc Alliance for Public Access to 911* - the ability for mobiles to make 9–1–1 calls on the strongest compatible signal and providing capabilities such as callback to all mobiles. The FCC will monitor progress on these issues annually through reports from an organization known as WEIAD (Wireless E911 Implementation Ad Hoc Group). This group consists of wireless trade associations (CTIA, PCIA), manufacturers, carriers and the *Ad Hoc Alliance*. A similar group (the "TTY Forum") is working to resolve TTY issues.

History

A considerable amount of work was done before the FCC rule-making. Two wireless industry Joint Experts Meetings (JEMs) were sponsored by the TIA in August 1994 and by PCIA in October

1994. The two JEMs reached similar conclusions, which went far beyond the requirements being imposed by the FCC.

In February 1996, the CTIA signed a consensus agreement with NENA (National Emergency Number Association), APCO (Associated Public-Safety Communications Officials) as well as NASNA (National Association of State Nine One One Administrators). This agreement bears a striking resemblance to the subsequent FCC rule-making.

Basic 9-1-1

The FCC imposed three requirements for Basic 9-1-1, of which all have proved unexpectedly controversial.

Valid Mobiles

There is no disagreement that valid mobiles should always be able to make 9–1–1 calls. However, the *Ad Hoc Alliance* has suggested that current mobile origination procedures are inadequate. Analog cellular mobiles, for example, can be programmed to access only the "A" or "B" system, and would be unable to make a 9–1–1 call (or any call) if programmed for "A only" when only a "B" signal is present. This problem can easily be resolved by programming mobiles for "A preferred" or "B preferred", which allows them to access the alternate frequency band, if the preferred band is not available. However, the *Ad Hoc Alliance* is not satisfied with this solution, believing that the strongest signal should always be used. They are concerned that the preferred band may not offer a signal strong enough to support a call (although strong enough to allow the mobile to lock on to the control channel). One problem with this proposal is that mobiles would lock onto the non-preferred system about half the time, which may not be able to obtain the information required for callback and other advanced services. Also, this solution would only work with new phones.

Invalid Mobiles

The FCC reaffirmed its belief that uninitialized and other invalid mobiles should be able to call 9–1–1 in its second order (December 1997), although they did not require that these mobiles receive advanced capabilities such as callback. Even this level of service still allows nuisance 9–1–1 calls from mobiles without a valid subscription or (in the case of GSM phones) without an identity at all. Also, it enables people to avoid paying the 9–1–1 fees that may be imposed on cellular bills to subsidize the emergency services infrastructure.

The *Ad Hoc Alliance* believes that invalid mobiles should be able to receive callback and accurate location identification. It is difficult to provide callback to invalid mobiles because they do not have an MDN assigned. Callback would have to be via a temporary number, which requires a definition of how long the number needs to be retained for, to determine how large a pool of numbers would be required. Even then, callback would be limited to the system from which the call originated. Furthermore, uninitialized mobiles may not have a unique mobile identifier (e.g. MIN or IMSI), which might cause callbacks to reach the wrong mobile. This is a problem for mobiles with a factory default identifier (i.e. never programmed) and those with a lapsed subscription with the identifier assigned to another (valid) mobile.

TTY and Digital Phones

TTY refers to a method of transmitting characters over a phone line, that is based on 1960's teletype technology (transmitting at 45.45 baud). While old and slow, it meets the need of the deaf and other disabled groups, and has become a cost effective and widely used standard in North America. Europe, by contrast uses a variety of different standards.

TTY works by generating tones, like most modems, and thus is compatible with analog cellular phones. Groups of tones represent letters from a restricted character set. Digital cellular phones, however, may not transmit the tones through their voice coders or may have an elevated error rate. It is for this reason that the FCC gave an extension for digital systems only. It is expected that digital carriers and manufacturers will request permission from the FCC to offer TTY support for only a limited number of digital models.

Enhanced 9-1-1, Phase I

E9–1–1 Phase I capabilities are defined in joint TIA TR-45/ATIS T1 interim standard J–STD–034. These include:

- Callback
- Cell/Sector Identification
- E9–1–1 Call Routing
- Reconnect
- 3-way 9–1–1 Calls

The first two features are mandated by the FCC. The first three primarily require modifications to signaling from the MSC to the Emergency Services network, while the latter two require modifications to inter-system operations (e.g. TIA/EIA-41).

Callback

It is sometimes necessary for PSAP (Public Safety Answering Point) call takers to call back to a phone that previously made a 9–1–1 call. This may be required if the caller hangs up before enough information was obtained, if attempts to locate the emergency fail or, in rare cases, for investigations following an emergency that may have involved a crime.

Callback is facilitated by transmitting the MDN during call setup. Callbacks will be routed through the home system of the mobile, and may be subject to call diversion at that point (e.g. call forward immediate). Public Safety organizations have accepted this limitation.

Other callback methods were investigated by TIA subcommittee TR–45.2. A pool of temporary callback numbers, for example, requires significant MSC call processing changes, and re-use of callback numbers could result in calls terminating at the wrong mobile. The roamer access port was rejected because it is a more complex method of termination (requiring overdial) and it does not allow callback to mobiles that leave the system from which they originated the

9-1-1 call.

The use of the MDN requires that the serving MSC obtain this identifier, something that was not available for roamers prior to the implementation of IS–41 Rev. C and TIA/EIA-41 Rev. D. Carriers can no longer assume that the MDN is the same as the MIN, due to the implementation of local number portability. This creates a problem for carriers that are not covered by the number portability mandate. They will still need to upgrade to IS-41 Rev. C to support E9–1–1 calls from roamers (and other directory number based services, such as 1+ long distance dialing and operator services).

Callback can be supported both for calls made with an MF interface to the PSTN or with ISUP. A callback scenario is illustrated in Figure 1.

Cell/Sector Identification

The FCC Phase I mandate requires that the approximate location of a calling mobile be made available to the PSAP, defined as the cellsite or sector from which the 9–1–1 call was placed. The identification is in the form of a unique phone number. This forms the second digit field transmitted to the PSTN for an E9–1–1 call.

E9–1–1 Call Routing

Wireless systems are often connected to an emergency services Selective Router by direct trunks – but this is not always possible. In this case, a slight modification to the Cell/Sector identifying digits can allow them to serve two purposes.

It would seem reasonable that the phone number assigned to identify each cellsite or sector was one that belonged to the wireless carrier. However, this would make the digits useless for routing. If the digits are instead assigned from numbers belonging to the emergency services network (or the LEC that provides it with telecommunications services) then they can not only uniquely identify the cellsite or sector, but also route the call to the correct PSAP.

These digits are known as the ESRD (Emergency Services Routing Digits) and can combine both routing and cell/sector identification functions.

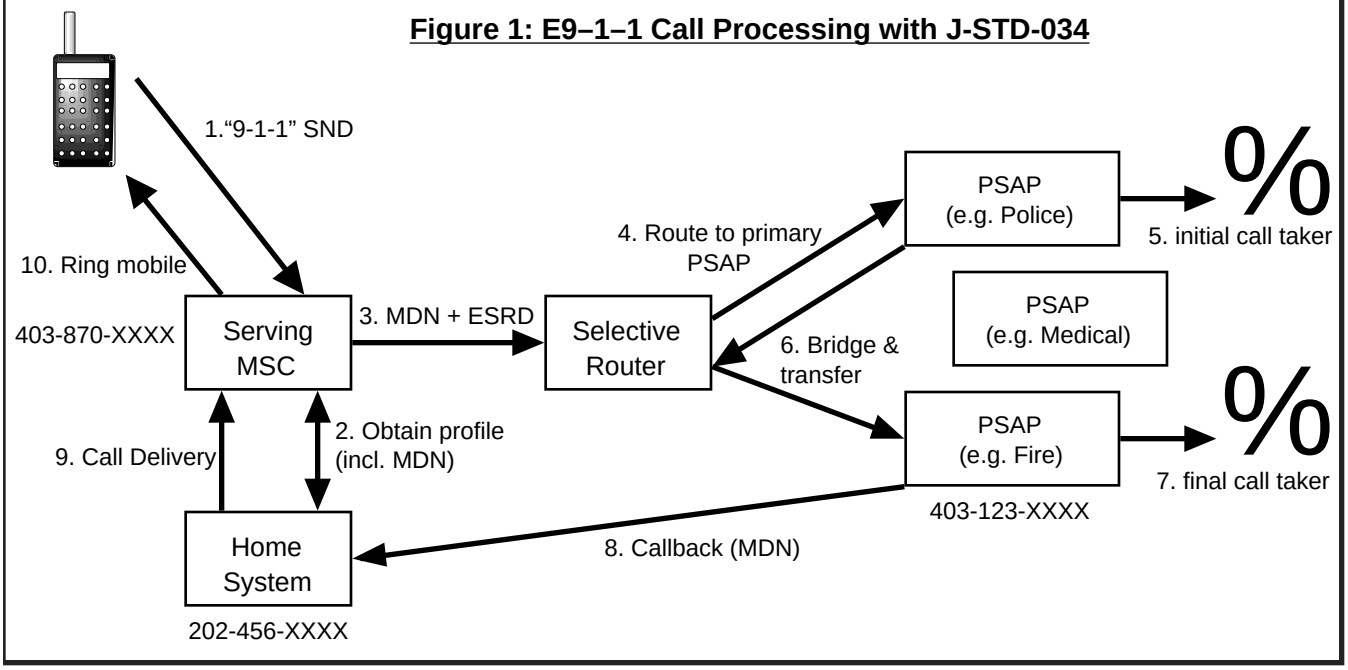
E9–1–1 Routing Scenario

Figure 1 illustrates the J–STD–034 process for callback, cell/sector identification and for E9–1–1 call routing:

1. A mobile initiates an emergency call by transmitting both the dialed digits (“911”) and its 10 digit Mobile Identification Number (MIN).
2. The MSC usually will already have the profile for the mobile (which includes the MDN) but, if not, queries the Home System HLR (using a TIA/EIA–41 Registration-Notification message). If this query fails (e.g. because the mobile is not a valid subscriber) the call will still proceed, but callback will not be possible.
3. The MSC transmits both the MDN and ESRD to a selective router.
4. The selective router routes to the primary PSAP based on the ESRD, time of day, etc.
5. If the first call taker determines that another PSAP should handle the call…
6. …they command the selective router to bridge to the alternate PSAP and then transfer the call.
7. The emergency is then handled.
8. If a callback is necessary, the MDN is dialed as a regular phone call to the 9–1–1 caller’s home system.
9. The home system routes the call to the current serving system (not necessarily the one from which the 9–1–1 call was made).
10. The call is connected to the mobile that originally reported the emergency.

To be continued…

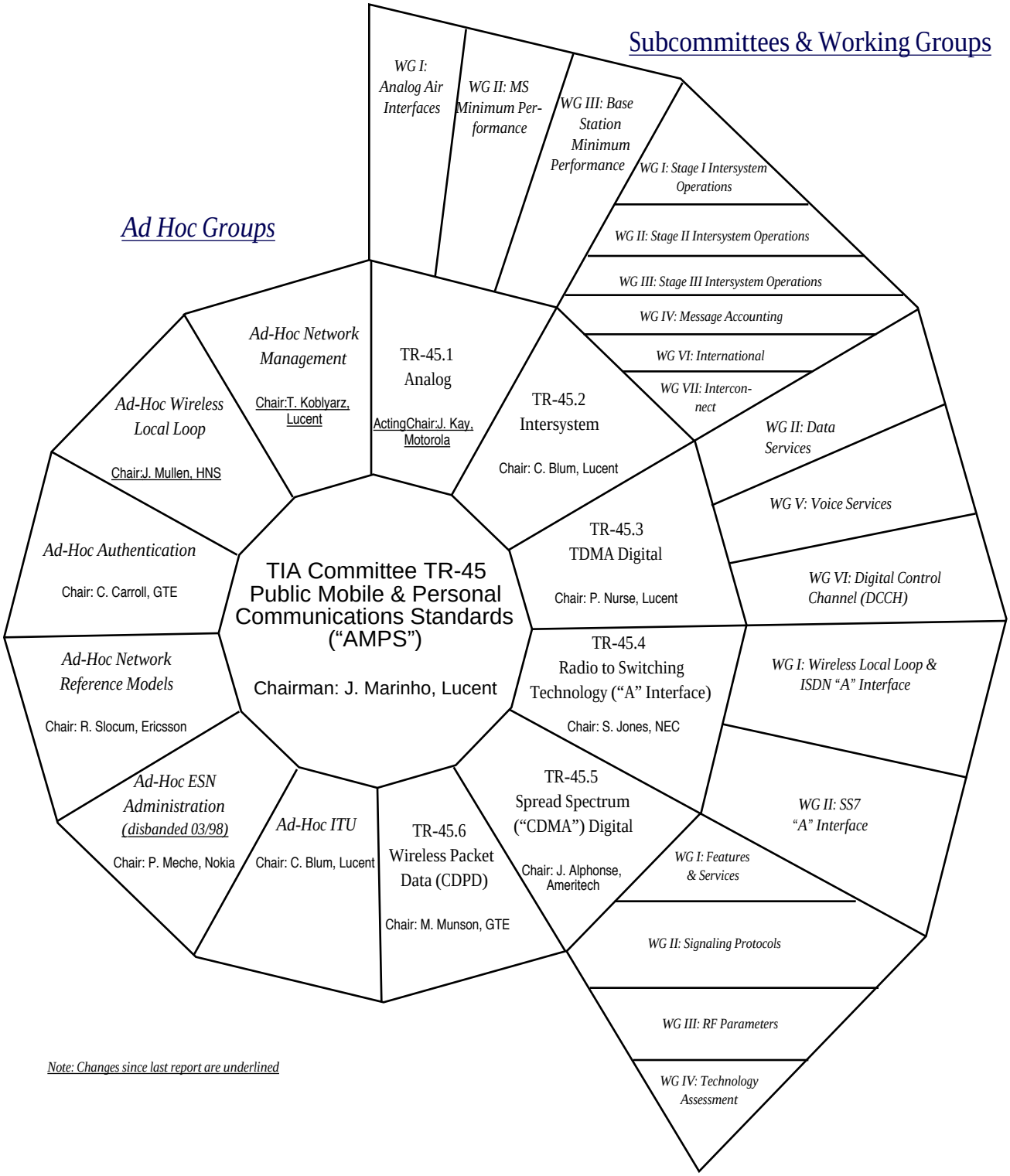
Figure 1: E9–1–1 Call Processing with J-STD-034



TIA TR-45 Cellular/PCS "AMPS" Standards Development

Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 *Last published June, 1997*



Note: Changes since last report are underlined

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 *last published November, 1997*

CDMA Digital Air Interface Standards - First Wave (Cellular)

Standard	Description	Publication
IS-95	CDMA Dual-Mode Air Interface Standard (Authentication Appendix pub. 11/92)	Published 07/93
IS-96	CDMA Option 1: Voice Coder	04/94
IS-97/IS-98	Base Station/Mobile Station minimum performance standards	12/94
IS-126	Service option 2: Loopback	12/94

CDMA Digital Air Interface Standards - Second Wave (Cellular & PCS)

Standard	PN/SP	Description	Publication
IS-95-A		**IS-95 Revised (Authentication Appendix "A" Nov. 1994)**	05/95
IS-96-A		CDMA Voice Coder	12/94
IS-97-A		Base Station minimum performance standards for IS-95-A	07/96
IS-98-A		Mobile minimum performance standards for IS-95-A	07/96
IS-98-A-1	PN-3867	**Errata and additional tests for IS-95 mobile stations**	**09/97**
IS-99		**Data Services (9.6kbps Fax and Circuit Switched Data)**	07/95
IS-125		Voice coder minimum performance standards	05/95
IS-126-A		Mobile station loopback service option	07/96
IS-637		Short message service (rate set 1)	12/95
J-STD-019	SP-3383	Base station minimum performance standards	***In press***
J-STD-008	SP-3384	IS-95 adapted for 1800 MHz frequency band	***In press***
J-STD-018	SP-3385	Mobile minimum performance standards (for J-STD-008)	***In press***
TSB-58		Parameter value assignments	12/95

CDMA Digital Air Interface Standards - Third Wave (Integrated Cellular/PCS)

Standard	PN/SP	Description	Publication
IS-127		Option 3: enhanced variable rate voice coder (EVRC)	01/97
IS-127-1	**PN-4146**	**Addendum to IS-127 (EVRC)**	**Development**
IS-657		**Packet data services (Internet, CDPD)**	07/96
IS-658		Data inter-working function interface (e.g. modem pool)	07/96
IS-683	PN-3569	Over the air activation and service provisioning	02/97
IS-683-A	**PN-3889**	**OTA update: Roaming system selection and programming lock**	**V&V**
IS-683.A		**Authentication/Encryption Annex "A" for IS-683**	**03/96**
IS-707	**PN-3676**	**14.4 kbps data services (including async data, fax, STU-III and packet**	**02/98**
IS-707-A	**PN-4145**	**Revision to IS-707 to be consistent with TIA/EIA-95 capabilities**	**Development**
IS-718	**PN-3648**	**Minimum performance standards for EVRC voice coder**	**Ballot**
IS-733	**PN-3972**	**High rate CDMA voice coder (13 kbps)**	**03/98**
IS-96-B		CDMA Voice Coder (8 kbps)	07/96
IS-736	**PN-3973**	**Minimum performance specification for IS-733**	**Ballot**
TIA/EIA-126-B	**SP-4136**	**ANSI version of IS-126 (MS loopback option)**	**Ballot**
TIA/EIA-95-B	**SP-3693**	**IS-95 for 800 MHz and 1800 MHz frequencies (including J-STD-008)**	**Ballot**
TIA/EIA-96-C	**SP-4138**	**CDMA Voice Coder (8 kbps)**	**Ballot**
TIA/EIA-97-B	**SP-3814**	Minimum performance standards for base stations	Ballot
TIA/EIA-98-B	**SP-3815**	**Minimum performance standards for mobile stations**	**Ballot**
TIA/EIA-98-C	**SP-xxxx**	**Merges TIA/EIA-98-B and J-STD-018**	**Development**
TSB-58-A	**PN-4158**	**Parameter value assignments**	**V&V**
TSB-74		14.4 kbps radio link protocol and inter-band operations	12/95
TSB-79	PN-3823	IS-637 update for 14.4kbps SMS, service negotiation and Year 2000	02/97

Thanks to Sam Broyles, Qualcomm, for providing information for this table