Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email: David.Crowe@cnp-wireless.com Vol. 10, No. 8 August, 2001

In This Issue...

Glossary

For any terms you are unfamiliar with, please consult:

www.cnp-wireless.com/glossary.html

Next Issue: September 4th, 2001

Mobile Identifiers – ESN and IMEI

Wireless services generally require separate identifiers for subscriptions and equipment identities. Systems based on TIA/EIA-41 networks usually use the MIN (Mobile Identification Number) as a subscription identifier and ESN (Electronic Serial Number) as an equipment identifier, although IMSI (International Mobile Subscription Identity) is also allowed by TDMA and CDMA standards. GSM networks use IMSI as a subscription identity and IMEI (International Mobile Equipment Identity) as an equipment identifier.

ESN is tightly coupled to the subscription identity and is used for validation and authentication. IMEI is completely separate from the subscription identity, and is largely used to track stolen phones, or other mobile equipment that should not be given service (e.g. malfunctioning units).

We discuss the ESN in this issue and the IMEI in the September, 2001 issue.

Electronic Serial Numbers (ESN)

The ESN is the equipment identity used by TIA/EIA-41 systems, including:

- EIA/TIA-553 and IS-91 AMPS/ N-AMPS analog
- IS-54 through TIA/EIA-136 TDMA (D-AMPS)
- IS-95 through IS-2000 CDMA

The ESN is a 32-bit number, usually represented as 8 hexadecimal (base 16) digits or as two separate decimal numbers, the first representing the first 8 bits (Manufacturer Code) and the second representing the remaining 24 bits.

Uses for the ESN

The ESN identifies a wireless phone as well as identifying the manufacturer, via the MC portion. This is useful for many purposes, including stock control and tracking malfunctioning or stolen mobiles.

The ESN goes beyond its role as a hardware identifier. In TIA/EIA-41 networks it also performs important roles, along with the MSID, in validation and authentication.

Validation

TIA/EIA-41 positive validation consists of checking that the MSID (MIN or IMSI) and ESN presented by a mobile to a wireless system matches a pair of values stored at an HLR. Neither an MSID or ESN is valid alone. They are only valid when presented as a matched pair. Early negative validation systems merely checked an ESN, by itself, against a blacklist.

Validation makes it necessary to update the ESN recorded at the HLR every time a subscriber purchases a new mobile phone or receives a loaner while a phone is being repaired.

Editor: David Crowe.
Accounts: Evelyn Goreham.
Marketing: Muneerah Vasanji.
Distribution: Debbie Brandelli.
Production: Doug Scofield.

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.

Authentication

Authentication is a method of requiring that mobiles not only present a valid MSID/ESN pair, but be able to prove that they hold a pre-programmed secret key. Currently, authentication systems rely on CAVE, which performs authentication through a challenge-response algorithm. The mobile is provided with a challenge (a random number), which it uses as input to the CAVE algorithm, along with a derivative of the secret key (Shared Secret Data) and various combinations of MIN, ESN and Dialed Digits (depending on the operation being authenticated). Authentication is completed by the network performing the same algorithm, with the same data and verifying that its result is the same as the response from the mobile.

3G authentication based on AKA will not use ESN as an input for any security purposes. Authentication will probably be mandatory in 3G systems (with exceptions for emergency calls, etc.) and there will therefore be little value in validation, meaning that 3G systems will not require the ESN for either of these purposes.

ESN Hardening

The US FCC has always insisted that ESNs be very difficult to change, even rendering the phone inoperable if the chip(s) containing the ESN are modified. However, hardening a value within a software controlled device, such as a wireless phone, is impossible because software modifications can always be made to substitute a non-hardened value when using a phone for fraudulent purposes. It does, however, provide a barrier to cloning fraud, albeit incomplete.

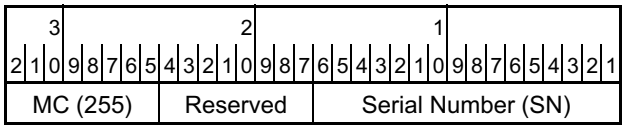
Evolution of the ESN

The ESN was originally specified as containing an 8 bit MC (Manufacturer Code), 8 reserved bits and a 16 bit SN (Serial Number). Manufacturers eventually started to use the 8 reserved bits, expanding the SN to 24 bits. As of June 1, 2001, the MC has been expanded to 14 bits for some future assignments, reducing the SN to 18 bits for this ESN format. There have been proposals to expand the ESN to 56 bits, but these have not been commercially implemented, largely due to the assumptions by most supporting systems that ESNs are always 32 bits long.

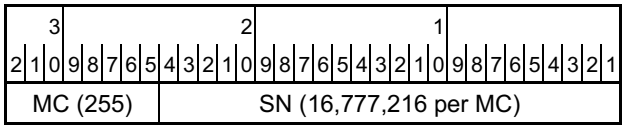
The evolution of the ESN is illustrated in Figure 1.

Figure 1: Evolution of the ESN

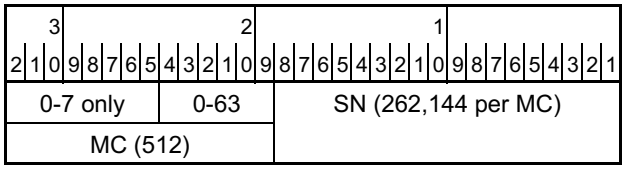
Original ESN Format



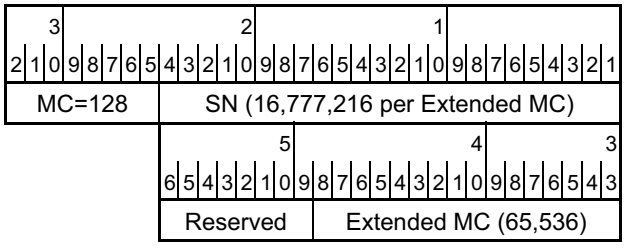
Current Format



14 bit Manufacturer Code Format



Expanded (56 bit) Format



Example of ESN Representations (assuming 8 bit MC and 32 bit format)

Binary:	10101010101010101010101010101010
Hexadecimal:	AA AA AA AA
Decimal:	70,11184810

Table 1: Available ESN Manufacturer Code (MC) Blocks (as of August 1, 2001)

First 8 bits of ESN	Usage	# of MCs	MCs Available
0-7	14 bit MCs	512	512
8-127, 129-249, 251-254	8 bit MCs	245	76
128, 250, 255	Reserved	0	0
Total available		757	588

ESN in User Identity Modules (UIM)

UIMs (also known as 'Smart Cards' or SIM – Subscriber Identity Modules) are a characteristic of GSM systems. Both CDMA and TDMA standards have recently been modified to support a UIM. However, moving the MSID to the UIM causes problems because TIA/EIA-41 validation and authentication rely on the MSID and ESN being a matched pair. If the MSID is on the UIM, this association will be broken every time it is moved to another mobile phone.

A simple solution is to also move the ESN to the UIM, maintaining the close association with the MSID. However, this violates the US FCC Part 22 requirements, and it makes it difficult to track mobile equipment (ME).

A compromise is to maintain the ESN in the ME, but to have an identically structured UIM Identifier for use in validation and authentication. The true ESN would be available only through new messaging in air interface standards that support it.

Saving the ESN

The original ESN manufacturer code was only 8 bits long, meaning that, at most, 256 different blocks could be assigned. Each block of ESN codes is therefore extremely large (enough for almost 17 million phones), much larger than required by most manufacturers, including those who went bankrupt, ceased operations, went out of the wireless phone business or were swallowed by another company before building that many mobiles.

All available ESN codes from 254 down to 83 had been assigned by July, 2001. At current assignment rates, this would result in ESN resource exhaustion occurring in 2004 or 2005. The use of the ESN address space for UIM and disposable phones could result in exhaust in 2003.

ESN preservation can be accomplished by administrative measures, expansion of the resource or more efficient usage.

Administrative Measures

Ever since September of 1997, when the US FCC granted the TIA the role of assigning ESN manufacturer codes, there has been an awareness of the need for conservation. The current ESN administrator closely examines applications. A few have been refused, but in most cases, these applicants will just reapply with better justification. Administrative controls are imperfect, but do slow down the rate of assignment, by making applicants more frugal in their requests.

Expansion of the ESN

The first approach at making the ESN resource last longer was to expand it to 56 bits. Unfortunately, this would cause enormous costs, as most wireless systems for subscriber database management, billing, traffic analysis, performance monitoring as well as real-time call processing rely on the knowledge that an ESN is a 32 bit number. This approach would therefore entail significant upgrade costs.

The Expanded ESN would be implemented by taking the reserved 8 bit MC of 128 as an indicator that the Extended MC exists (as 16 bits within a 24 bit extension). Unfortunately, this means that systems that only support 32 bit MC will be unable to determine the manufacturer, and may see many apparently duplicate ESNs.

After several years of study, and largely because of the expensive compatibility problems, this approach was shelved, although there is a possibility it will be implemented in 3G systems.

ESN MC Reuse

The only current proposal, that would result in expansion of the ESN resource, is reuse of manufacturer codes assigned in the early 1980's. This would require modifications to FCC regulations (which are, fortuitously, currently under review, as described in our July, 2001 issue), and possibly, regulations in other countries.

There is actually little reason for ESN codes to be unique. Positive validation has long taken over from negative validation, which did require uniqueness. CDMA standards do allow paging by ESN (e.g. for handling phones that have not yet been fully programmed), but these capabilities are not often used.

Code uniqueness is only necessary to make it unlikely that two mobiles with the same ESN are present in the same cell. With a 32 bit identifier, this will be the case with most methods of assigning ESN codes.

If ESN codes are re-used, the ESN resource effectively becomes infinite in size, and the ESN conservation problem is solved.

More Efficient Assignments

One solution recently implemented for conserving ESN MC's is to expand it from 8 to 14 bits. This increases the number of blocks available to small manufacturers (with each block holding approximately 1/4 million unique codes).

The current ESN assignment guidelines only allow the 14-bit format to be used when the first 8 bits (old MC) are 0 through 7 (see Table 1). This does expand these 8 codes to 512, which has tripled the size of the resource. However, if 0 through 63 had been reserved, the ESN MC space would have been expanded even more – from 256 to 4,288 codes.

There is one minor problem with this solution: Neither the hexadecimal nor decimal formats for ESN display (e.g. on packaging) make it easy to determine the manufacturer code.

ESN Administration

ESN manufacturer codes are currently administered by John Willse, on behalf of the TIA. ESN assignment guidelines, application forms and information on current assignments can be obtained at:

www.tiaonline.org/standards/esn

Current assignment fees are US$1,000 for an 8 bit and US$200 for a 14 bit MC.

The serial number portion of the ESN is administered by the manufacturer.

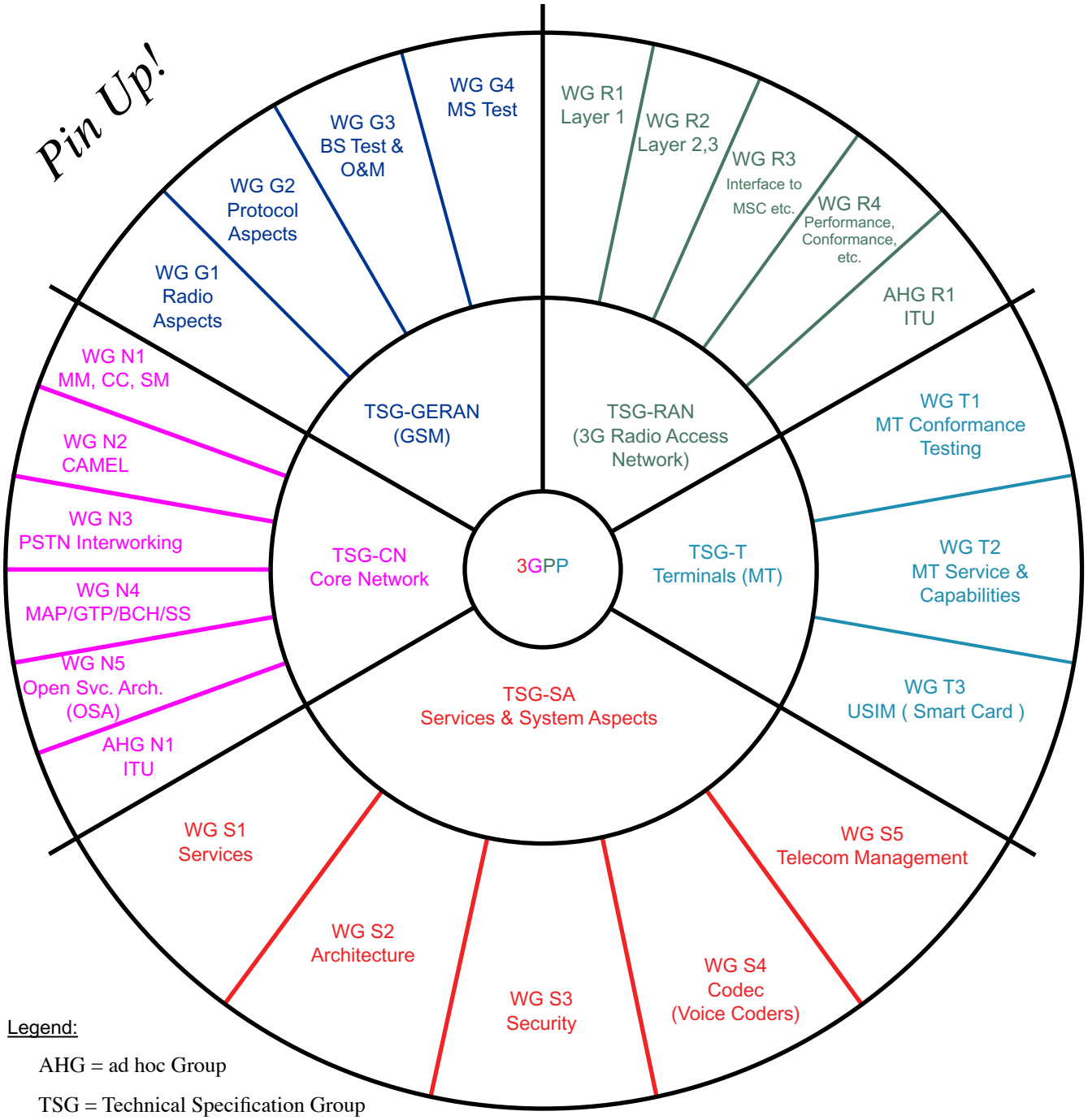
Conclusions

The ESN still plays a critical role in cellular and PCS systems based on TIA standards. As authentication takes over from validation as a method of fraud prevention, and as authentication moves away from reliance on the ESN, the importance of the ESN will diminish. The ESN will only retain its role as a simple hardware identifier, like the IMEI, which we will discuss next month.

Structure of 3GPP Standards Groups for GSM, GPRS, EDGE, UTRA

Cellular Networking Perspectives

Editor: David.Crowe@cnp-wireless.com *Initial Publication*



Legend:

AHG = ad hoc Group

TSG = Technical Specification Group

WG = Working Group

Other acronyms: www.cnp-wireless.com/glossary.html

TIA TR-45.2 Wireless Network 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.

Superseded Interim Standards

Standard	Description	Status
J-STD-025	**CALEA surveillance support (joint with ATIS T1) - interim standard**	**Published 12/97 Rescinded 05/01**
J-STD-025-1	**Addendum to J-STD-025**	**Published 07/00 Rescinded 05/01**
J-STD-025-2	**Addendum to J-STD-025-A**	**Published 07/00 Rescinded 05/01**
IS-41-C	Cellular Radio Telecommunications Intersystem Operations	Published 02/96
IS-52-A	Uniform Dialing Procedures for use in Cellular Radiotelephone Systems	Published 03/95
IS-53-A	Cellular Features Description	Published 04/95
IS-725	IS-41 support for Over-the-air Service Provisioning (OTASP)	Published 09/97
IS-756	Wireless Number Portability (WNP), Phase I (database query)	Published 04/98
TSB-29-A	International Implementation of Cellular Systems Compliant with TIA-553	Rescinded
TSB-29-B	International Implementation of Wireless Systems	Rescinded
TSB-29-B.1	TSB-29-B addendum including IFAST#6 updates (11/97)	Rescinded
TSB-29-B.2	TSB-29-B addendum, including IFAST #7 updates (02/98)	Rescinded
TSB-29-C	International Implementations of Wireless Systems	Published 09/99
TSB-29-C-1	Addendum to International Implementations of Wireless Systems	Published 12/99
TSB-41	Technical Notes for IS-41 Revision B	Published 11/94
TSB-51	Inter-System Authentication, Signaling Message Encryption and Voice Privacy	Published 05/93
TSB-55	IS-41 Rev. A/B Forward Compatibility ("Tech Notes")	Published 05/94
TSB-64	Wideband Spread Spectrum Intersystem Operations	Published 02/94

ANSI Standards and Annexes

ANSI Std.	Description	Status
TIA/EIA-41-D	Intersystem Operations	Published 12/97
TIA/EIA-93-A	Ai and Di Interfaces Standard (including 9-1-1 Phase I cell/sector location)	Published 11/98
TIA/EIA-93-B	**Ai and Di Interfaces Standard (including JIP and 9-1-1 Phase II location). Formerly PN-4206**	**In press**
TIA/EIA-124-B	Cellular Inter-System Non-Signaling Data Communications	Published 07/99
TIA/EIA-124-C	Support for WIN and CIBERNET NSDP-B-and-S protocol	Published 08/00
TIA/EIA-660	Cellular Dialing Plan (formerly IS-52)	Published 07/96

TIA/EIA-664	Cellular Feature Descriptions (formerly IS-53)	Published 06/96
TIA/EIA-664-A	Cellular features Stage I description (formerly PN-3362)	In press

Published TIA/EIA Interim Standards

Standard	Description	Status
J-STD-025-A	**CALEA Surveillance Support (joint with ATIS T1) including FCC Report and Order requirements**	**Published 05/00**
J-STD-034	Enhanced Wireless 9-1-1, Phase I: Identify mobile and cell/sector location	Published 12/97
J-STD-036	Enhanced 9-1-1 (E911), Phase II (125 m. location accuracy)	Published 08/00
J-STD-036-1	Corrected and Enhanced Emergency Services Support for SMS, Inter-system Handoff and SAMPS	In press
TIA/EIA-664-536	Analog Group III Fax for CDMA Wireless Local Loop Systems (Stage I description)	In press
IS-725-A	IS-725 enhanced to include Over-the-air Parameter Administration (OTAPA)	Published 07/99
IS-728	Inter-System Link Protocol (ISLP). Supports data calls after inter-MSC handoff.	Published 04/98
IS-730	TIA/EIA-41 Support for IS-136 DCCH (TDMA digital control channel)	Published 08/97
IS-735	TIA/EIA-41 Support for IS-95-A (advanced CDMA)	Published 02/98
IS-737	TIA/EIA-41 Support for circuit switched data services for CDMA and TDMA terminals	Published 04/98
IS-751	TIA/EIA-41 Support for International Mobile Station Identity (E.212 IMSI)	Published 02/98
IS-756-A	Wireless Number Portability (WNP), Phase II (MDN/MIN separation to allow porting to or from wireless phone numbers)	Published 12/98
IS-764	Calling Name Presentation/Restriction (Stage II, III)	Published 06/98
IS-771	WIN (Wireless Intelligent Network) Phase I: Voice controlled services and call screening	Published 07/99
IS-778	Authentication Enhancements	Published 03/99
IS-786	**Automatic Code Gapping (ACG) Overload Control**	**Published 11/00**
IS-807	Internationalization of TIA/EIA-41	Published 08/99
IS-807-1	Updates global title translation types in IS-807	Published 06/00
IS-808	**User Identification Module (R-UIM) for use in 3G systems**	**Published 12/00**
IS-812	TIA/EIA-41 Message Segmentation (to overcome SS7 network packet size limitations)	Published 08/99
IS-824	Broadcast/Multicast Short Message Service (BTTC)	Published 11/99
IS-826	WIN Phase II: Prepaid calling	Published 09/00
IS-837	Answer Holding (AH)	Published 07/00
IS-838	User Selective Call Forwarding (USCF)	Published 08/00
IS-841	MDN Based Message Centers	Published 09/00
IS-847	**VLR Roamer Database Verification (RDV)**	**Published 03/01**
IS-848	**WIN Phase II: Premium Rate Charging, Wireless Freephone**	**Published 12/00**
IS-875	**Network-based Enhancements for International Dialing, Calling Number ID and Callback**	**Published 05/01**

Current Telcommunications Systems Bulletins

TSB	Description	Status
TSB-56-A	Application Level Testing for IS-41 Rev. B, IS-53 Rev. 0 and TSB-51	Published 06/94
TSB-76	PCS Multi-Band Support	Published 09/96
TSB-114	Broadcast of emergency alert messages to wireless phones (EAS)	Published 12/99
TSB-124	**Support for WIN Prepaid (IS-826)**	**Published 10/00**

Balloting TR-45.2 Projects

Standard	Project	Description	Status
J-STD-025	**PN-4846**	**ANSI version of J-STD-025**	**Published 03/01**
J-STD-025-A	**SP-4465-UG1**	**ANSI version of J-STD-025-A**	**Development**
	PN-4720	**Intersystem support for 3G packet data, Phase I**	**Ballot**

Developing TR-45.2 Projects

Standard	Project	Description	Status
TIA/EIA-41-E	PN-3590	Intersystem Operations	Ballot 08/01
TIA/EIA-124-D	PN-4853	Further enhancements to call detail and billing records	Development
TIA/EIA-660-A	**PN-3544RV1**	**Cellular Dialing Plan**	**Development**
IS-843	PN-4818	WIN Phase III: location based services	Development
IS-847-A	**PN-4785RV1**	**RDV, allowing MDN range verification and query of nodes other than VLR**	**Development**
IS-868	**PN-4925**	**SIM roaming from TIA/EIA-41 (CDMA) to GSM**	**Development**
IS-872	**PN-4934**	**IP core network support for legacy mobiles**	**Development**
IS-873	**PN-4935**	**IP core network support for multimedia terminals**	**Development**
IS-884	**PN-3-0013**	**CDMA IP Requirements and Network Architecture**	**Development**
TSB-29-D	**PN-4609RV4**	**TSB-29 revision with IFAST-assigned IRM codes removed**	**In press**
	PN-4284	**TIA/EIA-41 and TIA/EIA-124 modifications for expanded ESN (Electronic Serial Number)**	**Project cancelled**
	PN-4288	Enhanced Emergency Services (E9-1-1), Phase III: Optional features beyond FCC mandate	Development
	PN-4392/3	Enhanced Security (authentication and encryption) for TIA/EIA-41	Development
	PN-4610	**Optimal routing to roamers.**	**Project cancelled**
	PN-4747	Location service enhancements, including security	Development
	PN-4755	Intersystem support for 3G packet data, including simultaneous voice and data	Development
	PN-4762	Using IP as transport for TIA/EIA-41 messages	Development
	PN-4926	CDMA roaming between GSM and TIA/EIA-41 networks	Development
	PN-4927	Interworking and interoperability (IIF) enhancements to support IS-868	Development

TSG-N Projects

Standard	Description	Status
N.0009	**CDMA Packet Data Service, Phase I**	**See PN-4720**
N.0010	**CDMA Packet Data Service, Phase II**	**Development**
N.0011	**WIN Phase III: location based services**	**See IS-843**
N.0013	**Location services authentication, privacy, security and enhancements**	**Development**
N.0019-A	**Enhancements to RDV to validate MC databases and directory number ranges**	**See IS-847-A**
N.0020	**IP based data transfer services**	**See IS-879**
N.0021	**WIN Automatic Call Gapping enhancements**	**See IS-786-A**
N.0022	**WIN prepaid charging enhancements**	**See IS-826-A**

N.0023	IP core network - legacy MS support	See IS-872
N.0024	IP core network - multimedia domain	See IS-873
N.0025	CDMA SIM roaming to GSM	See IS-868
N.0026	IIF enhancements for roaming to and from GSM	See PN-4926
N.0027	IIF enhancements for one-way roaming to GSM	See PN-4927
N.0028	CDMA IP network requirements and architecture model	See IS-884
N.S0003	User Identity Module (UIM)	Published 04/01
N.S0004	WIN Phase II	See IS-848
N.S0005	Intersystem Operations	See TIA/EIA-41-E
N.S0006	PCS Multi-band operations	See TSB76
N.S0007	DCCH (Digital Control Channel for TDMA)	See IS-730
N.S0008	Circuit Mode Services	See IS-735
N.S0009	IMSI support in TIA/EIA-41	See IS-751
N.S0010	Advanced CDMA features	See IS-735
N.S0011	OTASP and OTAPA	See IS-725-A
N.S0012	Calling Name Presentation (CNAP) and Restriction (CNAR)	See IS-764
N.S0013	WIN Phase I	See IS-771
N.S0014	Authentication enhancements	See IS-778
N.S0015	TIA/EIA-41-D miscellaneous enhancements	See TR45.2 internal
N.S0016	TIA/EIA-41-D internationalization	See IS-807
N.S0017	International implementations of systems compliant with TIA/EIA-41	See TSB29-C
N.S0017-A	International implementations of systems compliant with TIA/EIA-41	See TSB29-D
N.S0018	Prepaid charging (WIN Phase II)	See IS-826
N.S0020	Segmentation and reassembly	See IS-812
N.S0021	User selective call forwarding	See IS-838
N.S0022	Answer hold	See IS-837
N.S0023	Automatic code gapping (ACG)	See IS-786
N.S0024	MDN-based Message Centers (MC)	See IS-841
N.S0025	Roamer database verification	See IS-847
N.S0026	Call detail/billing record transfer	See TIA/EIA-124
N.S0027	Enhanced international dialing, calling number identification, callback and calling party category identification	See IS-875
N.S0029	Inter-system operations for roaming and mobility	See TIA/EIA-41-F
N.S0030	Enhanced security services based on AKA	See PN-4393
N.S0032	Mobile Application Part, Revision F	See TIA/EIA-41-F
N.S0033	Addendum 2 for Enhanced Emergency Services Phase II	See J-STD-036-AD2
N.S0034	Emergency services beyond US FCC mandate	See PN-4288
N.S0035	Lawfully authorized electronic surveillance	See J-STD-025-A
N.S0036	Semi-real time call detail and billing record transport	See TIA/EIA-124-C
S.R0006	Features description	See TIA/EIA-664-A