Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 Vol. 3, No. 12 December, 1994

In This Issue ...

☆✷Merry Christmas✷☆

This is our last issue before Christmas. We hope you have a Happy Holiday and a marvellous New Year. Publication of the first 1995 issue will be delayed until January 6th.

Comments Welcome

We welcome comments on the contents and format of this newsletter, suggestions for future topics, letters, submissions and corrections.

Phone us: 1-800-633-5514

The Emperor's New PIN

The latest anti-fraud technique being employed by carriers requires subscribers to enter a Personal Identification Number (PIN) at the start of every call. RCR reported NYNEX, for example, as claiming that "even if the thieves are able to capture a PIN number off the air, they won't be able to pair it with the proper ESN-MIN number to program a cloned phone." Well, Virginia, life just ain't that simple.

This technique does not rely on the system protecting cloners capturing the PIN as it is transmitted. Indeed, that is not possible with current phones. It relies on the difficulty of associating the PIN, transmitted on whichever voice channel is assigned to the call, with the MIN and ESN that are transmitted on the control channel. Because of this, the PIN technique will inconvenience cloners, but only for a short while. Anyone with a basic knowledge of the EIA/TIA-553 analog air interface standard, a cellular phone, a PC, easily available software (about $100), a special cable (about $25) and some "C" programming skill can overcome this technique. The reason that it is so easy to overcome is the same reason the legitimate cellular phone has no trouble finding the correct voice channel and transmitting the PIN digits. Following similar logic to the legitimate phone, the forger will have no trouble finding the same voice channel and receiving and storing the digits. Another way around the system is for cloners to emulate roamers, for which no PIN will be recorded in the local switch. This will work until IS-41 Revision C is generally available, which supports the PIN concept.

It is quite possible that, as the PIN technique is implemented, subscribers and carriers will see a large drop in cloning traffic for a short time ... followed by a resurgence. Trouble is brewing for carriers when they try to defend continued use of PINs when their subscribers start seeing large clone-attack bills again.

If a PIN is not the answer, what is the counterweight to counterfeiting? In one word; *Digital*. In the short term digital is just a much more complex and inaccessible technology for cloners to monitor than analog. In the long term digital will provide authentication, which is virtually immune to cloning (if used correctly). Digital phones also provide voice encryption which is important for preventing fraud, because it may make stolen service unusable, even if the authentication barrier can be overcome. Analog and NAMPS phones with authentication (TIA IS-91) will also be important, but only in the long term, because the current cellular network does not generally support authentication even for home subscribers, let alone for roamers. Also, analog phones do not support voice encryption, making them less secure even when authentication is fully available.◊

The TIA International Roaming JEM

The TIA held a Joint Experts Meeting (JEM) on International Roaming from November 7th to the 10th in Arlington, Virginia. The major goal was to determine the encoding of mobile identification for both existing MIN based terminals and future terminals with an extended mobile identification number. This issue was not resolved and the previously low profile problem of SS7 Global Title Translation (GTT)

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 or 1-403-289-6609. Fax: 403-289-6658. **Subscriptions**: CDN$250 in Canada (incl. GST), US$250 in the USA and US$300 elsewhere. Payment by cheque or money order. Issues are faxed or sent by 1st class mail. **Copies:** Each subscriber may make up to 10 copies of each issue. Rates are available for more copies. **Discounts:** Educational and small business rates: CDN$150 (incl. GST), US$150 and US$200, by mail only. **Back Issues:** Phone for price list and table of contents.

was recognized as a major issue.

The report of this Joint Experts Meeting was presented and approved at a TIA TR-45 committee meeting on November 29th.

Existing Terminals

Existing terminals today have a 10 digit Mobile Identification Number (MIN) that is usually programmed with the cellular subscriber's directory number (see following article). This creates ambiguity when cellular phones are programmed for countries outside the North American 10 digit dialing plan. In Mexico, for example, cellular phones are programmed with their landline country code (52) followed by their 8 digit national number. Confusion with North American mobiles may occur when area codes 52X are allocated. The first such area code, 520, will be allocated to Arizona in 1995. Luckily, no Mexican national numbers start with 0, so there is, as yet, no conflict. Allocation of the remaining 52X area codes is temporarily on hold.

The solution agreed to by participants at the JEM was to perform HLR "double-dipping" when mobiles register with an ambiguous MIN (i.e. sequential queries to HLR's that both "own" the same MIN prefix). It was not felt that this would put an undue burden on cellular systems and networks because:

a. Conflicts may occur with the area code digits (first 3), but not if more than 3 digits are examined.

b. Even when conflicts occur, the local system can probably guess where the mobile came from most times.

Consequently, if the MIN to HLR translation tables are designed intelligently, the fraction of registrations when double-dipping will be required will be small.

New Terminals

JEM participants were not able to reach consensus on whether future mobile identifications should be based on the E.164 landline numbering plan or the E.212 mobile numbering plan. This is a critical issue, because the IS-136 TDMA air interface standard, which recommends E.212-based mobile identification, has already been published. Proponents of E.212 praise its compatibility with GSM while proponents of E.164 praise its compatibility with the way things are done now. E.212 also is ranked low by some because there is no method of allocation of these numbers in North America. Others see this is a benefit, because it could give the cellular industry more flexibility and independence from the North American Numbering Plan Administration.

SS7 Global Title Troubles

Global Title Translation (GTT) refers to the ability of an SS7 network router (Signaling Transfer Point or STP) to direct messages to the appropriate destination based on a portion of a phone number or other identifier (e.g. calling card number), rather than on the physical SS7 addresses (point codes). Unfortunately, several troubles with the application of GTT to international roaming were identified. All of them potentially affect every SS7 STP in the world!:

1. A GTT for an E.164 Directory Number GTT is required. This translation type does not exist.

2. The E.214 GTT for E.212 mobile identification numbers does not work well in North America, and would require the tight coordination of numbering within the approximately 20 E.212 countries.

3. Using E.212 numbers directly as a global title would require the standardization and implementation of yet another GTT type.

Summary

The TIA committee TR45, which inherited the problem due to lack of consensus at the JEM, agreed at its November 29th meeting to postpone a decision until its next meeting, in February, 1995. Until this time, the TR45 subcommittees, particularly TR45.3 (TDMA) and TR-45.5 (CDMA) were requested not to make any final decisions on the mobile identification numbering plan. This presumably means that the already published IS-136 and soon to be published IS-95-A should be modified so that either mobile identification numbering plan could be used.◊

Why MINs are Phone Numbers and Why They Shouldn't Be

Everyone knows that a cellular phone's MIN is its phone number. What few know is that it doesn't have to be that way, and that some problems of the cellular industry are caused because today it usually is that way.

First it is important to distinguish between the terms Directory Number (DN) and MIN (Mobile Identification Number). The directory number is the phone number that can be used to dial a cellular phone from anywhere in the world while the MIN is designed for use across the radio interface to identify a cellular phone, and by the network to identify the home system that the phone belongs to. Figure 1 illustrates where the MIN is used, where the directory number is used, and the gateways between the world of directory numbers and the arena of MINs.

Directory Numbers

Directory numbers are phone numbers that can be dialed from any phone to access any other phone in the world, conforming to the ITU-T E.164 standard. When dialing internationally, the full directory number must be used including the Country Code, some regional digits (the area code in North America) and the local number. Directory numbers have several uses for reaching cellular phones:

1. To make a call *to* a cellular phone.

2. To allow an originating MSC to request a routing number from the HLR (which will perform the Directory Number to MIN translation) to allow use #1 to work even when the cellular phone is roaming.

3. To enable the SS7 data network to route the IS-41 LocationRequest message to the correct HLR (to support use #2 above).

MIN

The MIN is used only within the cellular network (the oval area in Figure 1). Within its domain, the MIN is used for several purposes:

1. To identify the mobile sending a message across the air interface to a base station (e.g. registration, origi-

nation or page response).

2. To direct a radio interface message to a specific mobile (e.g. page).
3. To route IS-41 messages (e.g. using SS7 global title translation) to the HLR (Home Location Register) of a cellular phone when its presence is detected by an MSC (e.g. by autonomous registration).
4. To make a roamer port call from outside the cellular network when the location of the mobile is known by the caller.

DN/MIN Segregation

Figure 1 illustrates the two interface points between the domain of DN's and MINs:

1. The HLR is the point where a dialed DN is translated to a MIN for a call incoming to a mobile.
2. The Roamer Port is accessed by dialing a DN (often NXX-ROAM) in the system the mobile is believed to be in. It provides second dialtone and then accepts the MIN, before using it to page the mobile.

Advantages When MIN = DN

There are advantages to keeping the MIN and directory number the same:

1. Carriers do not need to enter, and HLR's do not need to store, a separate MIN and directory number for every cellular phone.
2. Subscribers need only know one number.
3. The same phone number can be used to dial a cellular phone using call delivery (DN required) and via the roamer port (MIN required).
4. MINs do not need to be allocated and managed.

Problems When MIN = DN

Life is never simple and there are, as you may have guessed, several problems that occur because the MIN and DN are required to be the same:

1. Services, such as extension phone, that allow several mobiles to share a single directory number do not work well if the mobiles share the same MIN, due to restrictions in the analog and digital air interface standards, and some fraud management systems, that assume that MINs are assigned to one, and only one, phone. Therefore, full implementation of these features requires all but one member of the extension phone group to have a MIN that is not the same as the group's directory number.
2. MINs are only 10 digits long and therefore cannot encode all international directory numbers. Even when international numbers fit in 10 digits, they will match a *potential* North American directory number. On the other hand, if MINs were allocated separately from directory numbers there would be no ambiguity.
3. Directory numbers are allocated by the North American Numbering Plan Administrator. With a shortage of numbers, many constraints are placed on the allocation of MINs. If MINs were allocated separately, 10 billion numbers would be available exclusively to cellular phones.
4. Due to the shortage of directory numbers, services that could be built upon multiple MINs within a single phone are not, in order to conserve directory numbers. An example of this would be having a separate MIN for Voice, Fax, Data and Short Message services in one phone. Separate MIN's would make it easier to identify the terminating service and also to route outgoing calls using SS7 networking Global Title Translation.
5. If a MIN has to be changed, the directory number must also be changed, causing unnecessary inconvenience to the subscriber, who may have to reprint business cards etc. An example is when a MIN is reused and the discontinued phone with the same MIN is still turned on, although not in use. This phone will intercept calls to the legitimate subscriber,

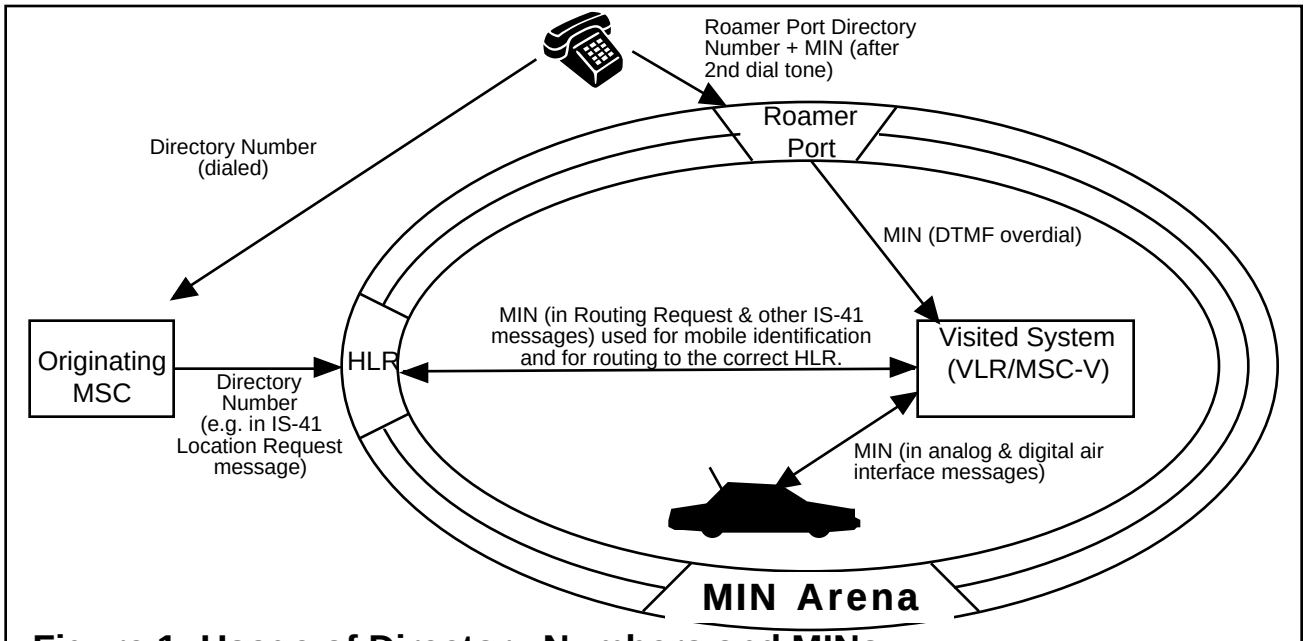

Figure 1: Usage of Directory Numbers and MINs

whose phone number will have to be changed to keep it the same as the MIN.

6. If a directory number has to be changed, the MIN has to be reprogrammed. Changing the directory number is simple for the carrier, but forcing a parallel change to the MIN requires reprogramming all affected cellular phones. This situation occurs when an area code is split or overlayed, and some or all mobiles are moved into the new area code.
7. Preprogrammed, mass distribution, phones are not possible (e.g. shrink-wrapped) as the MIN must be programmed in the phone. If the MIN is the same as the directory number, it is not be possible to ensure that it is a local number to the purchaser. If the Directory Number is separate, it could be allocated after service is established or, if terminating service is not required, not allocated at all.

When a MIN does not match a DN

There are phones in use today which have a different MIN and DN. This can be accomplished in two ways: by wasting a DN or by allocating a non-dialable MIN.

An example of the first method is to configure an extension phone service with a separate MIN and DN for each phone in the group. One, or any, DN could be used to reach a phone with any MIN in the group. Assuming that such services are used by a small fraction of subscribers, the waste of directory numbers will not be significant.

A more exotic alternative, is to take advantage of the 2 billion MINs that cannot be directory numbers. These are all the MIN's starting with the digit 0 or 1. Some of these numbers are already in use for special services (such as shrink wrapped phones). The problem with these numbers at present, is that there is no agency authorized to allocate them to carriers. Currently the CTIA subsidiary, Cibernet, is compiling a list of the blocks that have been allocated. This, however, is a voluntary effort and could easily allow conflicts or inefficient allocation to result.

Summary

There are advantages and disadvantages to both keeping the MIN and Directory Number the same, and in separating them. The trend appears to be slowly toward separation of MIN and DN, but possibly so slowly that the majority of phones will always have the same MIN and DN. Luckily, the transition can be gradual, assuming that the available non-dialable MIN resource is not exhausted wastefully before carriers realize its full value and potential.◊

TR-45.2 Standards Update: IS–52 Dialing Plan Approved for Publication

TIA subcommittee TR-45.2 has approved IS-52, the Cellular Dialing Plan, for publication. This document joins TSB-41, known as the IS-41 Revision B Technical Notes which was approved for publication after two ballots. IS-53 Revision A is still in the ballot process.

The status of each major outstanding TR45.2 project is listed below, in approximate order of completion:

IS-41 Rev. B Technical Notes (TSB–41, SP-2985) •In Press.

Cellular Dialing Plan (IS-52 Rev. A, PN-3166) • In Press. All ballot comments were resolved at the October and November TR45.2 meetings. All negative votes were withdrawn. IS-52 will be sent for ANSI ballot when published.

Subscriber Features (IS-53 Rev. A, PN-2977) • A fraction of ballot comments were reviewed at the November TR45.2 meeting. Due to the large volume of comments, more time has been allocated to review at the December meeting. In the ballot, 9 companies voted to approve without comments, 10 voted to approve with comments, 5 voted against (AT&T, Alcatel, Ericsson, NTI and Qualcomm) and 2 companies voted "No Comment". It is interesting to note that only manufacturers voted against IS-53 Revision A. Perhaps it is true that carriers can never "just say no" to more features. IS–53 Revision A will be sent for ANSI ballot after publication as a TIA interim standard.

IS-41 Revision C (PN-2991) • This revision of IS-41 was scheduled for ballot in October, 1994. That date has been slipped to **ballot starting January, 1995**. The ballot period will likely be 60 days. Following TIA approval of IS-41 Rev. C, this document must be sent for ANSI balloting. When past these two hurdles, IS-41, currently a TIA interim standard, will receive a new number as a full standard.

International Applications (TSB–29 Rev. B, PN-3173) • TR–45.2 is studying several problems with international use of AMPS cellular. A TIA Joint Expert's Meeting (JEM) was held the week of November 7, 1994 to try to resolve the most urgent problem; ambiguity of international mobile identification. The meeting was not successful in meeting this goal (see article on the JEM, above).

Online Call Record Transfer (IS-124 Rev. A, PN-3293) • TR–45.2 is considering revisions to the "DMH" standard for the online transfer of call records for billing, fraud and other purposes. This activity is a low priority and will be **completed in 1995**.

Subscriber Features (IS-53 Rev. B, PN-3362) • A list of features (45 so far) is being accumulated for development in Revision B of this standard. Activity beyond this will not proceed until IS-53 Rev. A is approved for publication.

IS-41 Rev. D • Consideration is being given to items for inclusion in IS–41 Revision D. These will likely include:

- IMSI (International Mobile Station Identification).
- Capabilities made possible by the TDMA and CDMA Digital Control Channels.
- Broadcast Short Message Service.
- Enhanced 9-1-1 service.
- Intelligent Networking.
- TDMA and CDMA circuit switched data.
- Support for features from IS-53 Rev. B.

Intercept by law enforcement agencies is being considered, but due to legal and network security constraints will likely not require any inter-system operations.

Work on these new capabilities will proceed following publication of IS-41 Rev. C.◊

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

Obsolete Interim Standards and TSBs

IS/TSB	Title	Published
IS-41-0	Cellular Radiotelecommunications Inter-System Operations	02/88
IS-41-A	Cellular Radiotelecommunications Inter-System Operations	01/91
IS-52-0	**Cellular Subscriber Dialing Plan and Service Codes**	**11/89**
TSB-27	IS-41 Application Notes (never published, date is when released to WG I)	07/89
TSB-56-0	**Application Level Testing for IS-41 Rev. A, IS-53 Rev. 0**	**03/93**

Published Interim Standards

IS	Title	WG	Published
IS-41-B	Cellular Radiotelecommunications Inter-System Operations	I	12/91
IS-52-A	**Uniform Dialing Procedures for use in Cellular Radiotelephone Systems**	**VII**	***in press***
IS-53-0	Cellular Features Description	V	09/91
IS-93-0	Ai and Di Interfaces Standard (PSTN/MSC)	VII	10/93
IS-124-0	Cellular Inter-System Non-Signaling Data Communications	IV	09/93

Published Telecommunications Systems Bulletins (TSBs)

TSB	Title	WG	Published
TSB-29-A	International Implementation of Cellular Systems Compliant with TIA-553	VI	09/92
TSB-41	**Technical Notes for IS-41 Revision B**	**I**	***in press***
TSB-51	Inter-System Authentication, Signaling Message Encryption and Voice Privacy	I	02/93
TSB-55	**IS-41 Rev. A/B Forward Compatibility**	**I**	**05/94**
TSB-56-A	Application Level Testing for IS-41 Rev. B, IS-53 Rev. 0 and TSB-51	II	06/94
TSB-64	Wideband Spread Spectrum Intersystem Operations	I	02/94
TSB-65	Mobile Border System Problems	I	04/94

Projects in Ballot Process (SP = Standards Proposal Number)

SP	Title	Editor	WG	IS/TSB
2977	**Cellular Features Description (Rev. A)**	**Terry Watts**	**V**	**IS-53-A**

Active TR45.2 Projects (PN = TIA Project Number)

PN	Title	Editor	WG	IS/TSB
2991	Cellular Radio Telecommunications Intersystem Operations	Terry Watts	I	IS-41-C
3173	International Implementation of Cellular Radiotelephone Systems Compliant with ANSI/EIA/TIA-553	Steve Jones	VI	TSB-29-B
3293	Cellular Inter-System Non-Signaling Data Communications	Kirk Carlson	IV	IS-124-A
3295	Ai and Di Interfaces Standard		VII	IS-93-A
3362	Cellular Features Description (Rev. B)	Terry Watts	V	IS-53-B
	Cellular Radio Telecommunications Intersystem Operation	**Terry Watts**	**I**	**IS-41-D**