Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 1 January, 1996

*In This Issue...*



*Look forward to your next issue on: February 1, 1996*

## IFAST - USLOW? AMPS Technology Gets a New Friend

A joint committee on cellular roaming, known as the JCCR, was set up by Mexican, US and Canadian carriers, as well as related associations and equipment and service vendors early in 1995. The group was so successful in achieving its original goals of resolving Mexican international roaming problems, that it will live on, although under a different name.

To refresh your memory, the problem with Mexican phones roaming is their use of MINs starting with 52 (their country code) while the North American Numbering Plan Authority has recently assigned a 520 area code. Consequently, a registration by a cellular phone with a 52XXXXXXXX MIN is ambiguous. The resolution that was chosen, was for Mexican carriers to reprogram all their MINs to start with 05. This was reported in the September, 1995 issue of *Cellular Networking Perspectives.*

IFAST, the International Forum on AMPS Standards Technology was created at the last JCCR meeting in Tampa, on December 6th, 1995. It will be:

> "An open international forum, with voluntary participation of wireless service providers, equipment vendors, intersystem vendors and associations that provide intersystem operations implementing the AMPS family of standards (e.g. IS-41, EIA/TIA-553, IS-91, IS-95 and IS-136)."

Initially this group will look at facilitating the international use of AMPS in five areas:

- Mobile Station Identification, using MIN or IMSI.
- SS7 signaling networks (e.g. interoperability between ANSI and ITU SS7).
- Dialing (e.g. a standard international emergency number).
- Fraud (validation and authentication).
- Call detail record transfers using IS-124.

Each of these areas contains special challenges related to international use. The technical focus of IFAST should help achieve efficient resolution to these problems. The first challenge of the group will be to expand its membership beyond the US, Canada and Mexico.

IFAST is expected to meet quarterly, with its first meeting following the CTIA Wireless'96 show in March in Dallas. The first co-chairs (subject to approval by their associations) are Ed Hall of the CTIA and Enrique Corral Mijares of AMCEL (an association of Mexican non-wireline cellular carriers).

For the record, some of the acronyms that were rejected included "Global Organization for Roaming Enhancements" and "Forum for International AMPS Technology". Others do not bear repeating.❑

*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, money order or American Express Card. Issues are faxed or mailed 1st class. 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.

## TR45 and TR46 Reorganization

TIA committees TR45 and TR46 have been reorganized over the past few months. While the role of TR45 now encompasses the definition of cellular and PCS standards in the 'AMPS' family, regardless of frequency, the future of TR46 is muddier.

The mandate of TR45 has been changed to remove references to the 800 MHz and 1800 MHz frequency range, and is only restricted to developing standards related to the 'AMPS' family. This includes analog, NAMPS, TDMA (IS-54 and IS-136) and CDMA (IS-95) cellular standards. All of these original cellular standards have been, or are being, adapted to the 1800 MHz PCS frequency band. While subcommittees TR-45.1, TR-45.3 and TR-45.5 will study, respectively, the analog, TDMA and CDMA air interfaces, TR-45.2 continues to study network standards and TR-45.4 studies the BS/MSC "A" interface for systems based on cellular or PCS cellsites, or even a combination of both.

The future of TR46 now appears to be linked with the ATIS T1P1 committee. TR46 (and T1P1) will continue to study standards related to the GSM PCS-1900, Omnipoint, PACS and other air interfaces.

Some standardization efforts are air interface independent. In these cases, TR45 will have prime responsibility, in cooperation with TR46. This covers the Enhanced 9-1-1 and Lawfully Authorized Intercept standardization efforts, both of which are being investigated by ad-hoc groups with cellular and PCS membership.❑

***HAPPY NEW YEAR!***

In 1996, we would like to hear from YOU! We welcome your views on the content and format of this newsletter. We invite you to offer suggestions for future topics, submissions, and corrections.

Call us at 1-800-633-5514 or email at 102371.3324@compuserve.com.❑

## Harry Young on Number Portability: A Gathering Storm for Cellular

Many years ago, storms caused great damage to property and life because there was little warning of their impending arrival. Cellular carriers face an approaching storm called number portability, but at least there is some warning of this storm.

Number portability has several aspects, but the most prominent form is service provider portability which allows a customer to keep their telephone number even when changing service providers. A number of regulatory agencies are examining local competition and there is a general feeling that having number portability will promote local loop competition.

One of the questions being asked by regulators is exactly who should be included in the number portability universe. Should every customer, wireline or wireless, have the opportunity to retain their own telephone number when changing service providers? Or, should the obligation be restricted to just wireline carriers?

At first glance it would appear that cellular carriers would not be affected by the implementation of number portability if they are not included in the list of carriers that must provide that capability. However, the fact is that cellular will be affected regardless of whether their customers have the right to number portability or not.

### Wireless Number Portability

If cellular carriers must provide number portability, one of the changes that would be required is in the registration process used to track roamers. Currently, a six-digit translation is used for this process, in which the NPA-NXX of the Mobile Identification Number (MIN) is used to identify the Home Location Register (HLR). With number portability, the use of six digits would no longer be possible since the association between the MIN and the HLR is broken. One solution is to use ten-digit Global Title Translation (GTT) in the signaling message in order to identify the proper HLR. This, of course, requires additional processing time and larger tables in the Signal Transfer Points (STPs) in the signaling network and probably additional facilities as well, to handle the increased traffic loads.

An alternative is to use a system that does not require a relationship between the MIN and the MSC. One possibility is the use of the Home Network Identifier (HNI) portion of the International Mobile Subscriber Identity (IMSI) number. IMSIs are non-dialable, fifteen-digit numbers that are widely used in Europe today for systems using the Global System for Mobile (GSM) protocol, of which only one exists in North America today (the APC Washington, DC area PCS system). Eventually, North American systems will include IMSIs in their wireless units and the first six digits of the IMSI, which identify the country and the network carrier, could be used for identifying the Home MSC. However, it will be years before all of the terminals in North America will be equipped with IMSIs, so this is definitely not a short-term alternative.

There is no industry consensus regarding what type of number portability solution will be implemented. Several candidates exist and it is conceivable that different states or areas may select different alternatives. To a landline carrier operating within the confines of a specific state, this is a manageable arrangement.. To a wireless carrier that operates in several states, using a single switch, it becomes an insurmountable problem that likely can be solved only by adding more switches. While that has definite economical consequences for wireless carriers serving that region, what about a wireless carrier that is located across the country but has subscribers that roam in different regions? If different solutions are implemented in multiple states, the HLR must cope with the protocols of all of the number portability solutions in order to support roaming in all of those states or regions.

Given the issues outlined above, the number portability storm has the potential to cause damage if cellular carriers must provide number portability to their customers.

## Landline Portability will Affect Wireless

Even if wireless carriers are not required to provide number portability, problems will be caused by number portability in landline carriers.

The majority of cellular traffic is mobile-to-land. If only landline carriers have to provide number portability, cellular carriers still have to be able to route traffic so it will complete to the intended destination. This means that cellular carriers must either be able to determine routing themselves, or they will have to pay someone else to do it for them.

Regardless of the ultimate number portability solution that is adopted, each is predicated on using a query to a database to determine the carrier. Moreover, the proposed solutions are based on using Intelligent Network (IN) or Advanced Intelligent Network (AIN) triggers in the switch to launch the query. Cellular switches are not based on either IN or AIN. Cellular is developing its own intelligent network protocol, the Wireless Intelligent Network (WIN), but it will not be entirely compatible with either IN or AIN-based switches.

Without the capability of launching a query themselves, the cellular carriers will have to rely on the Local Exchange Carrier (LEC), or some other entity, to perform the query for them. This may be a suitable alternative if there is no charge for this query and some cellular carriers believe that the LECs should have the obligation to route the traffic just as before, if cellular is not included in the number portability universe. It is possible that regulators would agree with this point of view, but there is a cost involved for performing that query and the LECs do not have a history of providing service at no charge.

Finally, the fundamental nature of the existing interconnections that have been so painstakingly negotiated over the past decade could be changed even if the cellular carriers do not have to provide number portability. In a number of locations, it is cheaper to use Type 2B connections, which are high-usage trunks serving the NXX codes provided in a specific end office. A number of carriers have a network architecture that employs large numbers of Type 2B connections which can carry both originating and terminating traffic. If the LEC decides to equip only tandem offices with the ability to perform a query, the cellular carrier may be faced with the choice of either changing to a more expensive Type 2A connection or equipping their own switch to perform the query for traffic that now terminates on a Type 2B connection. It is possible that similar problems could occur with cellular carriers that currently use Type 1 connections.

The storm is gathering but at least the industry has been warned and is taking action. A number of cellular carriers are involved in the various state regulatory proceedings that are in progress. In addition, the wireless industry is increasing its involvement in the Industry Numbering Committee (INC), an industry numbering group that is attempting to sort out the many issues associated with the number portability concept.

Only time will tell how damaging this storm will be to cellular.

## About the author

Harry Young is a well known consultant in the wireless industry, currently working as *Consultant to the Firm* for MTA-EMCI. If Harry has one area of particular expertise, it is interconnection; the methods used by wireless carriers to connect to local and long distance landline carriers. He is also respected for his Bellcore sponsored *Wireless Interconnection* seminar and his book, *Wireless Basics*.❑



# Fraud and Countermeasures, Part IV: Implementation of Authentication

In our most recent issue we discussed a number of technical issues related to cellular authentication. But, the implementation of authentication is just as difficult as understanding the technology. The aim of an implementation strategy must be to eventually ensure that 100% of mobiles authenticate. Achieving that will not be easy, but even partial success will have significant benefits.

## Authenticating Roamers

We have criticized some cloning countermeasures, such as RF and voice fingerprinting, as having weak support for roaming. Authentication, however, has been integrated into IS-41 intersystem operations since the publication of TIA TSB-51 in 1993. This document should be seen as an addendum to IS-41 Revision B. Authentication is also supported, with some compatible enhancements, in IS-41 Revision C, currently in press. Support for authentication for roaming is critical to achieve the full benefits of authentication.

There are several IS-41 transactions that allow authentication while a mobile is roaming outside its home market:

### *AuthenticationRequest*

This is the prime authentication transaction, and must be completed prior to sending a RegistrationNotification. Sent from a serving MSC to the Authentication Center (AC), via the HLR, this message can either request a one-time authentication or can retrieve the Shared Secret Data (SSD) for autonomous authentication by the visited system.

### *AuthenticationDirective*

This message allows an AC to update the authentication status of a mobile, most likely by performing an SSD Update operation. This is a very powerful capability, as it gives the network the ability to manage fraud detected while their customers are roaming. This message has to be used with care, as discussed in last month's issue, to avoid updating a clone and cutting the legitimate subscriber off.

### *AuthenticationStatusReport*

Reports on the status of an Authentication Centre initiated authentication operation.

### *AuthenticationFailureReport*

Reports an unusual authentication related event (such as suspected fraud) to an Authentication Centre.

### *AuthenticationDirective Forward*

Allows an AuthenticationDirective to be forwarded along the handoff chain, to support operations such as SSD-Update even following an inter-system handoff. New in IS-41 Rev. C.

### *RandomVariableRequest*

This message allows neighbouring systems to coordinate their broadcast global challenge RAND values. This is necessary due to a border cell problem that can result in a mobile using a RAND received from one system to access a neighbouring system. This problem must be dealt with to prevent cloners from simulating it as a way to bypass authentication. This message is new in IS-41 Rev. C.

### *CountRequest*

An operation that allows an AC to request the current Call History Counter value from the serving system, assuming that COUNT updates are being handled autonomously by the serving system.

### *BaseStationChallenge*

An operation that allows a serving system to request a response to a base station challenge even if the AC has refused to share SSD (somewhat of an oxymoron). This is beneficial if the AC does not trust the current serving system.

## Authentication Misconceptions

If authentication is so great, why is it not universally implemented? The answer is perhaps to be found in the many misconceptions regarding authentication:

- It is too complicated.

  Yes, it is complicated. Running a business that is losing money is complicated too.

- It is no good until all phones can do it.

  Authentication protects your revenue from subscribers that have that capability, and will make cloners attack a diminishing percentage of the subscriber base, making their attacks obvious more quickly and fail more often.

- Customers can't enter 26 digits.

  Carriers used to say that customers cannot be expected to enter a 26 digit A-Key. But, they have stopped saying this since they now expect their customers to enter a 4 digit PIN several times a day.

- Most phones don't do authentication.

  This is true today, but less so every day. Hopefully, the CTIA requirement to include authentication in phones before receiving their "Gold Seal" approval, that comes into effect in February 1996, will convince carriers and manufacturers that authentication is available, is cost-effective and is desirable. See the "Authentication Strategy" sidebar for more details on how carriers can increase the percentage of phones that authenticate.

- Only digital phones can authenticate.

  This is not true, although carriers did take a couple of years to admit that the transition to digital was going to be much slower than expected and start work to include authentication in analog standards. Authentication is available in any analog cellular phones designed according to any revision of TIA IS-91 or to the future ANSI standard EIA/TIA-553 Revision A.

- It won't work. Nothing else has.

  This is the latest, totally false misconception about authentication. Only 18% of respondents to a recent Cellular Integration survey believed that authentication will significantly reduce fraud. This shows a dangerous lack of understanding regarding authentication technology, perhaps based on a faulty analogy with the over-hyped PIN countermeasure to fraud. The bottom line is that authentication does work because it is provably, mathematically highly secure, something that cannot be said about any other cloning countermeasure.

  International experience, primarily with GSM, has proven that authentication will prevent cloning. And this has occurred even though GSM authentication is technically weaker than TIA authentication.

- A-Keys can't be kept secret.

  Yes, but so what? Loss of a few A-Keys will not allow fraud unless the theft also includes the SSD information. Even if A-Keys are stolen along with the current SSD, the SSD can be changed through the cellular network. In the worst, and quite unlikely case, an A-Key may occasionally need modification.

## Carrier Authentication Strategy

An effective strategy for cellular carriers to get authentication into the field should include the following components:

- Lobby the FCC (or equivalent organizations in other countries) to make authentication required in new phones.
- Promote the CTIA gold seal program.
- Educate customers about cloning fraud and authentication.

- Educate customer service about entering A-Keys in mobiles.
- Educate key employees about cloning fraud and authentication (if copies of our series of articles would help, call us at 1-800-633-5514 for reduced prices on bulk orders).
- Calculate your losses due to cloning fraud and use these numbers to justify expenditures on authentication.
- Provide incentives for subscribers to use authenticating phones.
- Give new authenticating phones to heavy usage customers at no charge. Let them know why you are doing this.
- Only sell authenticating phones, and ensure that they conform to TIA TSB-50 for standardized A-Key entry.
- Remove the PIN requirement for customers with authenticating phones once authentication is activated in the network.

## Summary

Countermeasures to cloning are available, but vary widely in their cost, effectiveness and impact on customers. None of the countermeasures are as effective as authentication, but due to the lack of this capability in most cellular phones, several alternative approaches will continue to be used for several years until the entrance of new authenticating phones significantly outnumbers the older non-authenticating phones. Even then, cloners will focus on the diminishing numbers of non-authenticating phones and, at some point in the far distant future, all non-authenticating phones will have to be recalled and either upgraded, if possible, or replaced at no cost before the bleeding finally stops.❒

## The CTIA Total Fraud Management Program

According to Tom McClure, the CTIA Director for Fraud Management, the CTIA is promoting a 5 step program for the management of fraud among its member carriers:

1. Shore up Business Practices

   In the rush to satisfy the needs of the ever growing number of subscribers, some carriers have not had tight enough business practices. Every carrier should ensure that IS-41 validation is operating, that all programs are audited and that their networks and equipment are protected from penetration by hackers.

2. Certification of Mobiles

   Carriers should attempt to ensure that as many mobiles as possible that are installed on their system are capable of authentication and that the hardware is secure from ESN tampering.

3. Install Detection Equipment

   Carriers should put systems into place to detect fraud using analysis of IS-41 validation transactions and call detail records to look for suspicious calling patterns. A number of products exist with this capability (see Table 2 in the November, 1995 issue for a list).

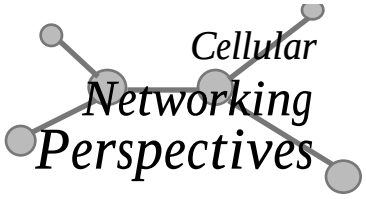
4. Prevention

   Going beyond simply detecting cloning fraud, and reacting to it after a number of fraudulent calls have been accepted, carriers should attempt to prevent cloning fraud through methods such as enhanced call pattern analysis or RF fingerprinting. These methods attempt to identify and prevent fraudulent calls as they are placed.

5. Authentication

   The CTIA is convinced that authentication is the ultimate solution to cloning fraud. Authentication should allow fraudulent calls to be identified more accurately and cost effectively than any other method. They are promoting authentication through education, the activities of their Fraud Task Force and through cooperative industry meetings. These activities and their Gold Seal program, that will soon only be awarded to authentication capable phones, are attempting to increase the availability of authentication capabilities in phones and in the network. ❒

# TIA TR-45
# Analog Air Interface
# Standards Report




Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 02/95*

## Analog Air Interface Standards - First Generation

| Standard | Description (not the official title) | Comment |
|---|---|---|
| IS-3 | Original Analog Air Interface Standard | now EIA/TIA-553 |
| EIA/TIA-553 Rev. 0 | Current Analog Air Interface Standard | Published 09/89 |
| TSB-39 | Message Type Assignment for Extended Protocol | Published 03/93 |

## Analog Air Interface Standards - Second Generation

| Standard | Description (not the official title) | Comment |
|---|---|---|
| **EIA/TIA-553 Rev. A** | **Reaffirmation of EIA/TIA-553 (basically IS-91 Rev. 0)** | **Development** |
| **TSB-70 Rev. A** | **Cross Reference for FSK Control Channel** | **Development** |
| IS-88 | Narrowband (3:1) analog air interface ("NAMPS") | Published 02/93 |
| IS-89 | IS-88 base station performance standards | Published 02/93 |
| IS-90 | IS-88 mobile performance standards | Published 02/93 |
| IS-91 Rev. 0 | Analog air interface (including "NAMPS" and Authentication) | Published 09/94 |
| IS-94 | In-building analog air interface ("FreedomLink") | Published 05/94 |

## Analog Air Interface Standards - Third Generation

| Standard | Description (not the official title) | Comment |
|---|---|---|
| **IS-91 Rev. A** | **Revised version of IS-91 (including IS-94, cordless capability and sleep mode)** | **In Press** |
| **IS-19-C** | **Mobile minimum performance standards** | **Ballot** |
| IS-20-A | Base Station minimum performance standards | ANSI ballot |
| **TSB-70** | **Cross Reference for FSK Control Channel** | **In Press** |
| **PN-3496** | **Wireline interface for cordless/cellular combination phones** | **Ballot** |

## Analog Air Interface Standards - Fourth Generation

| Standard | Description (not the official title) | Comment |
|---|---|---|
| **IS-91 Rev. B** | **Revised version of IS-91 (including IMSI, PCS band support, voice privacy, over-the-air-activation, priority access, 9-1-1 and voice-paging)** | **Development** |

## Authentication Appendices

| Description | Comment | Status |
|---|---|---|
| Message Encryption and Voice Privacy ("Appendix A") | *A US Department of State export license may be required to export these authentication documents. Contact the TIA at 1-703-907-7700 for details of their Technology Transfer Control Plan.* | Published 10/94 |
| Interface specification for common cryptographic algorithms | | Published 12/94 |
| Common Cryptographic Algorithms | | Published 04/95 |

Note: 1. IS- Interim Standard, TSB- Telecommunications Systems Bulletins, PN- Project Number, SP- ANSI Standards Proposal, J-STD- TIA/ATIS Joint Technical Committee standard.

2. **Bold Type** indicates modification since previous publication.