Mobile Equipment Identifier:Future of CDMA Mobile Identification

Transition to 56 bit Mobile Equipment Identifier from 32 bit Electronic Serial Number

Prem Kumar, Syscom Corporation Ltd.

Abstract**-**During the invent of Code Division Multiple Access (CDMA) mobile phones, no one could ever imagine a day would arise,when more than a billion mobile phones would be manufactured and used worldwide over a short span of time. Each mobilephone is required to have a unique serial number burned into its chips in order to prevent fraud. Without a unique number, the phone can't be sold. So initially in order to identify phones on a network, engineers developed a 32-bit code called the Electronic Serial Number (ESN). This code was used for billing and to make sure the right call went to the right phone. But 32 bits only allowed 4 billion unique numbers; engineers probably didn't forecasted ESN to be a long-term solution.IfESNs ran out and there was no standard to replace them, manufacturers would literally have to shut down production of CDMA phones. Certainly a technology was required which could provide a long term solution to the current problem and bring about a change before ESNs were exhausted. Thuscamethe role of Mobile Equipment Identifier (MEID).This paper aims to present the need, role, future, issues and challenges CDMA phones face due to 32 bit ESN and how 56 bit MEID is going to rectify it.

Index Terms**-**CD, CDMA, ESN, GHA, GSM, IME , MEID, RUIMs, SIM, SMS, TDMA.

I. Introduction

CDMA wireless subscribers around the world are using a smart card in the back of their R-UIM-enabled CDMA handsets. These CDMA smart cards, called Removable User Identity Modules (R-UIMs) are used to hold and protect all of the subscriber’s data necessary to receive wireless services. Subscribers remove R-UIMs from one phone and insert them into another without loss of subscription data or phone book. This portability makes it easy for users to change phones while keeping the same operator. Sowe have a concept of identification in the name of ESN and MEID. A mobile Equipment Identifier (MEID) is a globally unique number identifying a physical piece of CDMA mobile station equipment. It is basically an ID unique for each CDMA mobile phone in the world.

Need for MEID

A. CDMA Management

General question may arise in the minds of the readers that why MEID is required when already we have ESN for identification in CDMA handsets.Answer is migration from 32 bit ESN, which is on the verge of exhaustion to 56 bit MEID so as to accommodate future subscriber growth through a larger identifier.

However, as technology advanced from analog to Time Division Multiple Access (TDMA) or CDMA and then CDMA2000, the networks continued to use ESNs to identify phones. It made sense to use them in order to maintain compatibility with older networks, since many carriers upgraded their systems piece by piece. We still have dual- or tri-mode phones today. Once they upgraded to digital networks, carriers also started using ESNs to secure phone calls and eventually prevent fraud.

Unfortunately, the rapid growth of TDMA and CDMA have nearly exhausted the supply of ESNs. In addition, early on in cell phone history, large blocks of serial numbers were distributed to manufacturers rather liberally, speeding the depletion of a limited supply.

B. GSM Management

The fact that it only took 20 years to use 4 billion serial numbers is even more amazing when you consider that Global System for Mobile communications(GSM) phones don't use ESNs. Since GSM was launched as an all-digital system with no need for backward compatibility, they use a different numbering system called International Mobile Station Equipment Identity(IMEI). Probably since GSM came along later, and could learn from the mistakes of ESN, IMEI is almost twice as long, providing a significantly higher limit of unique codes.

So before the ESNs get exhausted, manufacturers and carriers will need to be ready for ESN's successor, Mobile Equipment Identifier (MEID).

Technical Break-up

As depicted in Figure1, Mobile Station Equipment Identifier is a 56-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.

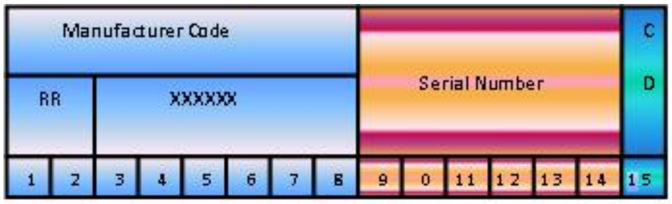

Figure1: MEID (14 Hexadecimal Digits, 56 bits)

RR- Regional Code.A0-FF are assigned by the global hexadecimal MEID administrator (GHA).Other codes are reserved for use as IMEI'S.RR=99 IS reserved for MEID's that can also be used as IMEI's

XXXXXX-6 hexadecimal digit code assigned by the administrator to a manufacturer for a line of phones.

Serial Number – Assigned by manufacturer to identify an individual device.

CD - Checksum Digit. Not transmitted.

Each mobile station is assigned either a single unique 32-bit binary serial number (ESN) or a single unique 56-bit binary serial number (MEID) that cannot be changed by the subscriber without rendering the mobile station inoperative.

The mobile station shall be configured with a 56-bit MEID. MEID is used to uniquely identify the mobile station in a wireless system. The mobile station shall store a 32-bit pseudo-ESN value, derived fromMEID[2].

Challenges and Solution

C. Switching Challenges

First, the industry requires a way to let MEID phones work on old networks that use ESN. This is critical for manufacturers that will run out of ESNs before networks are ready to use MEID. The phones will be programmed with an MEID which they will use to generate a temporary ESN called pseudoESN (pESN).

D. PseudoESN

PseudoESN(pESN)is a 32 bit number derived from MEID and is used in place of ESN. The mobile station shall use the following procedure to derive pseudo-ESN from MEID. The upper 8 bits of pseudo-ESN shall be set to 0x80. The lower 24 bits of pseudo-ESN shall be the 24 least significant bits of theSHA-1 digest of the MEID.

For the 56-bit MEID ➔ FF 00 00 01 12 34 56,

Pseudo-ESN calculated is ➔ 80 07 37

The problem is that the pESN will not be unique. There is a chance that more than one phone with the same pseudoESN is on the same network. There would be no way for the network to tell them apart. If this happens the 2 phones would probably get each other's SMS messages, at the least, or cancel out each others' service preventing both phones from working, in a worst case scenario. Engineers are working to minimize these problems before pESNs handsets are rolled out.

E. Solution

To genuinely solve this problem, the industry needs to come up with a way to recognize MEIDs on current networks. This effort is known as "MEID on CDMA2000"[1]. It consists of two parts. The first is getting handset manufacturers to comply with a little trick. In addition to ESNs, every handset has an additional set of codes that tell the network what the phone is capable of. One of those codes has previously gone unused and has always been set to "off". Manufacturers would set this code to "on" for all handsets with an MEID[4].

Base stations would then need to be upgraded to query phones entering a cell for this code, which they never cared about before. If a phone responded with the code "on", then the cell would address all traffic to the phone using MEID, if it was still "off," the cell would continue to use an ESN. This would assure that every phone on a network would have a unique identifier, and thus avoid mixing up transmissions (which the network types call data collisions). MEID-equipped handsets will need to be able to generate a pseudoESN as well as comply with MEID for CDMA2000 inorder to be compatible with CDMA networks for the foreseeable future.

Conclusion

CDMA has proved to be a promising technology for 3G networks. As described in this paper, MEID is the next mandatory change in telecommunications domain.World's leading providers of smart cards are currently offering R-UIM based MEID services to CDMA operators around the globe. This whitepaper would prove to be an eye opener to the new techies, digging versatile subjects in Subscriber Identity Module(SIM) or Mobile domain.This Whitepaper is intended only for knowledge purpose and contains confidential information. Unless stated to the contrary, any opinions or comments are personal to the writer and do not represent the official view of the company / organization.

Acknowledgment

I would like to acknowledge my family and co-workers for supporting and encouraging me throughout the course work.

References

[1] *3GPP2 C.S0072, Mobile Station Equipment Identifier (MEID) Support for cdma2000 Spread Spectrum Systems,Version 1.0.*

[2] *3GPP2 SC.R4002-0, Mobile Equipment Identifier(MEID) GHA (Global Hexadecimal Administrator)Assignment Guidelines and Procedures,Version 5.0.*

[3] *3GPP2 C.S0016-C, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems,Version 1.0.*

[4] *3GPP2 C.S0023-C,Removable User Identity Module for Spread Spectrum Systems, Version 1.0.*

Author

Author Name: Prem Kumar

Qualification /Experience: Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards. I am having more than 7 yrs of experience in this niche technology.

Email Address: prem.get@gmail.com