



MEID IOS Issue

CDG Technical Bulletin 070301IRT v1.0
1 March 2007

To: All CDMA2000 Operators, BS and MSC Vendors

From: CDMA Development Group

-- URGENT --

Introduction

The Mobile Station Equipment Identifier (MEID) is a new 56-bit identifier intended to address the impending exhaustion of the 32-bit Electronic Serial Number (ESN) resource. MEID-equipped terminals are now being sold to subscribers from multiple operators and the use of MEID-equipped terminals is increasing rapidly as handset OEMs migrate from ESN to MEID. The latest TIA TR-45 ESN Administrator's report (January 2007) indicates that ESN codes are projected to be exhausted by roughly Q4 '07.

An interoperability issue on the 'A' interface has been discovered between certain BS and MSC implementations, which results in MEID-equipped terminals not receiving service. If present, this issue could have two effects:

- 1. The operator's own subscribers will not receive service when MEID-equipped terminals are deployed.**
- 2. In-bound roamers using MEID-equipped devices will not receive service. *Several large roaming operators have deployed MEID-equipped devices; these devices are roaming today.***

The purpose of this document is to describe the issue in detail, so that operators and vendors can determine whether their own systems may be affected. Please ensure that the appropriate people/departments in your organizations review this CDG Technical Bulletin. After reviewing it, if you have additional questions, please contact roaming@cdg.org.

Actions

For Operators:

1. Operators are strongly recommended to obtain MEID-equipped devices for testing. Even if the operator's own subscribers do not currently have MEID mobiles, they may already be used by in-bound roaming partners' subscribers.
2. Operators should determine if the 'A' interface(s) in their networks have the problem which is described below, under "Detailed Issue Description." If the problem is present, operators should work with their infrastructure vendors to address it. The problem can typically be addressed by a software patch or upgrade on the BSC or MSC (or both). Note that the use of IOS v5 (the version designed to handle the MEID) will not by itself resolve the issue.

For BS and MSC Vendors:

1. Determine if this problem exists in the field or in new software loads. If it exists, steps should be taken to address the problem. Note that the use of IOS v5 (the version designed to handle the MEID) will not automatically resolve the issue.

Detailed Issue Description

In the failure case, the following behavior is observed:
(Numbering aligns with that in the following section)

1. Per C.S0072, MEID-equipped mobiles transmit a '1' in bit 4 of the Station Class Mark (SCM), which is now designated the "MEID support indicator." Prior to this, the bit function was "IS-54 Power Class" and was always set to 0 for CDMA MSs.
2. Following TIA-EIA-136-140, the BS/BSC combines bits 4, 1 & 0 of the SCM to form the IOS "RF Power Capability" field. Note: This is not a CDMA2000[®] standard, but infrastructure vendors may have shared software between their TDMA and CDMA products, or otherwise decided to use this method for deriving the RF Power Capability value.
3. The RF Power Capability field is included in the Classmark Information Type 2 Information Element, which is a mandatory part of various IOS messages on the A1 interface.
4. When the MSB (i.e., SCM bit 4) is set to 1, the resulting value for the RF Power Capability field is one of the "unused" values as defined in the IOS standard (even in the latest IOS version (v5), which is otherwise updated to handle MEID).
5. Following IOS Message Sending Guidelines, the receiving MSC initiates failure handling, and **the MS does not receive service.**

Standards Excerpts and Additional Information

(Numbering aligns with that in the previous section)

1. Station Class Mark Setting in C.S0072:

Table 2.1.2-1. Station Class Mark

Function	Bit(s)	Setting	
Extended SCM Indicator	7	Band Classes 1,4	1XXXXXXX
		Other bands	0XXXXXXX
Dual Mode	6	CDMA Only	X0XXXXXX
		Dual Mode	X1XXXXXX
Slotted Class	5	Non-Slotted	XX0XXXXX
		Slotted	XX1XXXXX
MEID Support Indicator	4	MEID not configured	XXX0XXXX
		MEID configured	XXX1XXXX
25 MHz Bandwidth	3	Always 1	XXXX1XXX
Transmission	2	Continuous	XXXXX0XX
		Discontinuous	XXXXX1XX
Power Class for Band Class 0 Analog Operation	1 – 0	Class I	XXXXXX00
		Class II	XXXXXX01
		Class III	XXXXXX10
		Reserved	XXXXXX11

Bit 4 Setting in C.S0005-0 v3 (Table 2.3.3-1):

IS-54 Power Class	4	Always 0	XXX0XXXX
-------------------	---	----------	----------

2. Station Class Mark Setting in TIA-EIA-136-140 §2.3:

Table 1 Station Class Marks (Bits 4-0)

Power Class	SCMp	Transmission	SCMp	Bandwidth	SCMp
Class I	0XX00	Continuous	XX0XX	20 MHz	X0XXX
Class II	0XX01	Discontinuous	XX1XX	25 MHz	X1XXX
Class III	0XX10				
Class IV	0XX11				
Class V	1XX00				
Class VI	1XX01				
Class VII	1XX10				
Class VIII	1XX11				

3. Classmark Information Type 2 IE is Mandatory in CM Service Request, Paging Response and Handoff Request, Optional Required in Location Updating Request and Handoff Required, and Optional Conditional in ADDS Transfer.

Excerpt of IE structure and notes from A.S0014-C v2 - IOS 5.0.1:

4.2.12 Classmark Information Type 2

7	6	5	4	3	2	1	0	Octet
A1 Element Identifier								1
Length								2
MOB_P_REV			Reserved	See List of Entries	RF Power Capability			3
Reserved								4
NAR_ AN_ CAP	IS-95	Slotted	Reserved		DTX	Mobile Term	ANSI/ EIA/ TIA-553	5
Reserved								6
Reserved						Mobile Term	PSI	7
SCM Length								8
Station Class Mark								9
...								...

“See List of Entries”:

This field is an escape mechanism that allows octets 3 through 6 to be ignored by the receiver. When set to ‘1’, the receiver shall ignore the contents of octets 3 through 6 and shall instead use the contents of octets 7 through the end of the element to derive the valid class mark information. When this field is set to ‘0’, the receiver shall process the contents of octets 3 through 6 and ignore any additional data that may be present after these octets. A BS shall be required to populate both portions of this element, i.e., octets 3-6 and 7 through the end-of-element, to provide backward compatibility...”

In the observed failure case, “See List of Entries” was set to 1.

4. RF Power Capability values (A.S0014-C v2 - IOS 5.0.1):

Table 4.2.12-1 Classmark Information Type 2 - RF Power Capability

Binary Values	Meaning	ANSI/EIA/TIA-553	TIA/EIA/IS-2000
000	Class 1, vehicle and portable	4 W	1.25 W
001	Class 2, portable	1.6 W	0.5 W
010	Class 3, handheld	0.6 W	0.2 W
011	Class 4, handheld	Unused	
100	Class 5, handheld		
101	Class 6, handheld		
110	Class 7, handheld		
111	Class 8, handheld		

5. Excerpt from IOS Message Sending Guidelines A.S0014-C v2 (IOS 5.0.1) §1.8:

“For supporting backward compatibility on the A1 interface[...] no IE shall be sent which [...] have values other than expected [...] If an IE is sent in a manner that violates the above principle [...] then failure handling may be invoked by the receiving node.”

Author: Daniel Salek – QUALCOMM Engineering Services Group
dsalek@qualcomm.com