

3GPP2 C.S0066-0

Version 2.0

Date: 25 July 2008



**3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"**

Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Revision History

<u>Revision</u>	<u>Description</u>	<u>Date</u>
C.S0066-0 v1.0	Initial publication	27 August 2004
C.S0066-0 v2.0		25 July 2008

CONTENTS

1
2
3
4
5
6
7
8
9

1 INTRODUCTION..... 1-1

2 Changes required for Enhanced Protocol Capability Messaging..... 2-1

3 3.3 Programming Procedure..... 2-1

4 3.3.1 *OTASP Data Message* Processing..... 2-1

5 3.5.1.17 Extended Protocol Capability Response Message 2-2

6 4.3 Programming Data Download 2-8

7 4.3.1 OTA Data Message Processing 2-8

8 4.5.1.7 Protocol Capability Request Message..... 2-8

9

REFERENCES

The following standards are referenced in this text. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

1. TIA/EIA-95-B, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Cellular System*, March 1999.
2. TIA/EIA/IS-683, *Over-the-Air Service Provisioning of Mobile Stations in Wideband Spread Spectrum Systems*, February 1997.
3. 3GPP2 C.S0016-0, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, December 1999.
4. 3GPP2 C.S0016-A, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, December 2001.
5. 3GPP2 C.S0016-B, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*, October 2002.
6. Reserved.
7. 3GPP2 C.S0005-D, *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems – Release D*, March 2004.
8. 3GPP2 C.S0006-D, *Analog Signaling Standard for cdma2000 Spread Spectrum Systems – Release D*, March 2004.
9. 3GPP2 C.S0024-A, *cdma2000 High Rate Packet Data Air Interface Specification*, March 2004.
10. 3GPP2 S.R0048-A, *3G Mobile Equipment Identifier (MEID) Stage_1*, May 2004.
11. 3GPP2 C.S0057-0, *Band Class Specification for cdma2000 Spread Spectrum Systems*, February 2004.
12. 3GPP2 C.S0023-C, *Removable User Identity Module for Spread Spectrum Systems, June 2006.*

1 INTRODUCTION

This Standard was prepared by Technical Specification Group C of the Third Generation Partnership Project 2 (3GPP2). This Standard presents recommendations for supporting a mobile station equipped with a Mobile Equipment Identifier (MEID) [10] in the OTASP Systems defined in [2], [3], [4] and [5].

The OTASP feature allows a potential wireless service subscriber to activate (i.e., become authorized for) new wireless service, and allows an existing wireless subscriber to make changes in existing services without the intervention of a third party.

For the initial provisioning, the Electronic Serial Number (ESN) is used to identify the mobile station. ESN is a 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment. Due to the ESN exhaustion, the MEID was introduced in the cdma2000^{®1} systems as the alternative to ESN for new mobile stations complying with [7].

During the migration period from ESN to MEID, Pseudo-ESN is used by the MEID-equipped mobile stations. Pseudo-ESN is a 32-bit number derived from MEID and used in place of ESN. For the provisioning, however, Pseudo-ESN may not be used to uniquely identify a particular mobile station since Pseudo-ESN is not unique.

In order to solve this problem, the following new capability is introduced in this Standard.

- Enhanced Protocol Capability Messaging - This provides the means for the base station to ascertain the detailed capabilities of the mobile station, such as supported band classes, operating modes, MEID, SF EUIMID and LF EUIMID.

This Standard uses the same structure and section numbering as [2], [3], [4] and [5], except for all the references. Sections of this Standard that remain unchanged relative to [2], [3], [4] and [5] are represented using ellipses contained within brackets ([...]). Modified sections are either reproduced in their entirety or use the [...] notation to represent unchanged portions. Within modified sections, change bars indicate the specific paragraphs, figures, or table cells that have changed. Within modified paragraphs and table cells, strike-throughs indicate deleted text and underlines indicate new text.

¹ cdma2000[®] is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000[®] is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

C.S0066-0 v2.0

1

2 No text.

2 CHANGES REQUIRED FOR ENHANCED PROTOCOL CAPABILITY MESSAGING

[...]

3.3 Programming Procedure

3.3.1 OTASP Data Message Processing

The mobile station shall discard all *OTASP Data Messages* received, if the programming procedure is not initiated as described in 3.2 or when the mobile station is in any state, substate or task other than the *CDMA Conversation Substate* or the analog *Conversation Task*. If the mobile station is in the *Mobile Station Control on the Traffic Channel State*, the mobile station shall send the *Mobile Station Reject Order* with ORDQ equal to '00000010'.

While in the *CDMA Conversation Substate* or the analog *Conversation Task*, the mobile station shall process *OTASP Data Messages* as follows:

[...]

7. *Protocol Capability Request Message: If the Protocol Capability Request Message contains the OTASP_P_REV field and the mobile station is able to parse it, then the mobile station shall send the Extended Protocol Capability Response Message within 750 ms after receiving the message; otherwise, the mobile station shall send a Protocol Capability Response Message within 750 ms after receiving the message. The mobile station shall send a Protocol Capability Response Message or an Extended Protocol Capability Response Message within 750 ms after receiving the message. If the Protocol Capability Request Message contains the OTASP_P_REV field and the mobile station is able to parse it, then the mobile station shall send the Extended Protocol Capability Response Message; otherwise, the mobile station shall send the Protocol Capability Response Message.*

[...]

1 3.5.1.17 Extended Protocol Capability Response Message

2 The *Extended Protocol Capability Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00010000')	8
OTASP_MOB_P_REV	8
MOB_FIRM_REV	16
MOB_MODEL	8
NUM_FEATURES	8

NUM_FEATURES occurrences of the following features:

FEATURE_ID	8
FEATURE_P_REV	8

NUM_CAP_RECORDS	8
-----------------	---

NUM_CAP_RECORDS occurrences of the following records:

CAP_RECORD_TYPE	8
CAP_RECORD_LEN	8
Type-specific field	8 × RECORD_LEN

3

4 OTASP_MSG_TYPE - *OTASP Data Message* type.

5 The mobile station shall set this field to '00010000'.

6 OTASP_MOB_P_REV - OTASP Mobile Protocol Revision.

7 The mobile station shall set this field to the value shown in the
8 following table.

1

OTASP MOB_P_REV (Binary)	Associated Standard
00000000	[2]
00000001	[3]
00000010	[4]
00000011	[5]
00000100	Reserved ²
All other values are reserved.	

2

3

MOB_FIRM_REV - Mobile station firmware revision number.

4

The mobile station shall set this field to the value of the MOB_FIRM_REV_p permanent mobile station indicator (see F.2.1 of [1, 7]).

5

6

7

MOB_MODEL - Mobile station manufacturer's model number.

8

The mobile station shall set this field to the value of the MOB_MODEL_p permanent mobile station indicator (see F.2.1 of [1, 7]).

9

10

NUM_FEATURES - Number of Features.

11

The mobile station shall set this field to the number of features supported by the mobile station using the OTASP protocol.

12

13

FEATURE_ID - Feature Identifier.

14

The mobile station shall set this field according to Table 3.5.1.7-1 to indicate the feature supported by the mobile station.

15

16

FEATURE_P_REV - Feature protocol version.

17

The mobile station shall set this field according to Table 3.5.1.7-1 to indicate the protocol version of the feature supported by the mobile station.

18

19

NUM_CAP_RECORDS- Number of Capability Records.

20

The mobile station shall set this field to the number of Capability Records contained in the Extended Protocol Capability Response Message.

21

22

23

24

The mobile station shall include all the records requested in the corresponding *Protocol Capability Request Message*. The mobile station shall include the following fields for each capability record to be included:

25

² This value is reserved for designating the next revision of [5].

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

- CAP_RECORD_TYPE - Capability Record Type.
The mobile station shall set this field to the record type value shown in Table 3.5.1.17.1-1 corresponding to the type of this information record.
- CAP_RECORD_LEN - Capability Record Length.
The mobile station shall set this field to the number of octets included in the type-specific fields of this information record. If the mobile station doesn't support a requested CAP_RECORD_TYPE or supports a requested CAP_RECORD_TYPE, but doesn't have a value, the mobile station shall include the CAP_RECORD_TYPE with the CAP_RECORD_LEN field set to '00000000'.
- Type-specific field - Type-specific field.
The mobile station shall set these fields to the information as specified in 3.5.1.17.1 for the specific type of records.

3.5.1.17.1 Capability Information Record

Table 3.5.1.17.1-1 lists the information record type values that can be used in the *Extended Protocol Capability Response Message*. The following sections describe the contents of each of the record types in detail.

Table 3.5.1.17.1-1 Capability Information Record Types

Capability Information Record	Record Type (binary)
Operating Mode Information	'00000000'
CDMA Band Class Information	'00000001'
MEID	'00000010'
<u>ICCID</u>	<u>'00000011'</u>
<u>EXT UIM ID</u>	<u>'00000100'</u>
<u>MEID ME</u>	<u>'00000101'</u>
All other values are reserved.	

3.5.1.17.1.1 Operating Mode Information

This capability information record is used to return operating mode information supported by the mobile station.

Type-Specific Field	Length (bits)
OP_MODE_INFO	8 × CAP_RECORD_LEN

OP_MODE_INFO – Operating mode information.

This field indicates which operating modes are supported by the mobile station in the band class for which information is requested.

This field currently consists of the following subfields which are included in the information record in the order shown in Table 3.5.1.17.1.1-1.

Table 3.5.1.17.1.1-1. OP_MODE

Subfield	Length (bits)	Subfield Description	Standards
OP_MODE0	1	Analog mode	[8]
OP_MODE1	1	CDMA mode	[7]
OP_MODE2	1	HRPD mode	[9]
RESERVED	5	–	–

The mobile station shall set each subfield to '1', if the corresponding operating mode is supported by the mobile station; otherwise, the mobile station shall set the subfield to '0'.

RESERVED – Reserved bits.

The mobile station shall set each bit in this field to '0'.

When more operating modes are defined, the reserved bits will be used for the new corresponding subfields. Sufficient octets will also be added to this field to accommodate the corresponding new subfields. All the undefined bits in an additional octet will be reserved bits.

If all bits are set to '0' in an octet and all succeeding octets, the mobile station shall omit the octet and the succeeding octets.

3.5.1.17.1.2 CDMA Band Class Information

This capability information record is used to return band class information about the mobile station.

Type-Specific Field	Length (bits)
BAND_CLASS_INFO	8 × CAP_RECORD_LEN

1
 2 BAND_CLASS_INFO – Band class information.
 3 This field indicates which band classes are supported by the
 4 mobile station.
 5 The mobile station shall set the Nth significant bit of this field to
 6 ‘1’ if the Nth band class defined in [11] is supported by the mobile
 7 station; otherwise, the mobile station shall set the Nth most
 8 significant bit of this field to ‘0’.
 9 The mobile station shall add reserved bits as needed in order to
 10 make the length of the entire information record equal to an
 11 integer number of octets. The mobile station shall set these bits
 12 to ‘0’.

13
 14 **3.5.1.17.1.3 MEID**

15 This capability information record is used to return the mobile station MEID or R-UIM’s
 16 SF EUIMID based on the SF EUIMID Usage Indicator as defined in [12].

17 ~~This capability information record is used to return the mobile station MEID.~~

Type-Specific Field	Length (bits)
MEID	56

18
 19
 20 MEID – Mobile Equipment Identifier.
 21 ~~The mobile station shall set this field to its Mobile Equipment~~
 22 ~~Identifier.~~The mobile station shall set this field according to Table
 23 3.5.1.17.1.3-1.

24
 25 **Table 3.5.1.17.1.3-1. MEID Field Setting**

<u>SF EUIMID Usage Indicator</u>	<u>MEID</u>
<u>0</u>	<u>MEID</u>
<u>1</u>	<u>SF EUIMID</u>

26 **3.5.1.17.1.4 ICCID**

27 This capability information record is used to return the ICCID in the R-UIM.

<u>Type-Specific Field</u>	<u>Length (bits)</u>
<u>ICCID</u>	<u>80</u>

ICCID – Integrated Circuit Card Identifier.

The mobile station shall set this field to the Integrated Circuit Card Identifier (LF EUIMID) stored in the R-UIM.

3.5.1.17.1.5 EXT UIM ID

This capability information record is used to return the EXT UIM ID in the R-UIM based on the SF EUIMID-based EUIMID service as defined in [12].

<u>Type-Specific Field</u>	<u>Length (bits)</u>
<u>EXT UIM ID</u>	<u>8 × CAP RECORD LEN</u>

EXT UIM ID – Mobile station Extended User Identity Module identifier.

The mobile station shall set this field according to Table 3.5.1.17.1.5-1.

Table 3.5.1.17.1.5-1. EXT UIM ID Field Setting

<u>SF EUIMID-based EUIMID</u>	<u>EXT UIM ID</u>	<u>Length (bits)</u>
<u>0</u>	<u>LF EUIMID</u>	<u>80</u>
<u>1</u>	<u>SF EUIMID</u>	<u>56</u>

3.5.1.17.1.6 MEID ME

This capability information record is used to return the mobile station MEID.

<u>Type-Specific Field</u>	<u>Length (bits)</u>
<u>MEID ME</u>	<u>56</u>

MEID ME – Mobile Equipment Identifier of ME.

The mobile station shall set this field to its Mobile Equipment Identifier.

[...]

4.3 Programming Data Download

4.3.1 OTA Data Message Processing

[...]

7. *Protocol Capability Request Message*: The base station should wait for a *Protocol Capability Response Message* or an *Extended Protocol Capability Response Message*. The base station shall not send the *Protocol Capability Request Message* with additional fields to the mobile stations which don't support the additional fields defined in Section 4.5.1.7³.

Note:

The base station may use the first 8 bits of the received value in the ESN field to determine if the value in the ESN field is a true ESN/UIMID (with prefix other than 0x80) or a pseudo-ESN/pseudo-UIMID (with prefix 0x80). The first 8 bits only indicates the MEID capability of the mobile station if it is known that the mobile station is non-RUIM capable.

[...]

4.5.1.7 Protocol Capability Request Message

The *Protocol Capability Request Message* has the following variable -length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00000110')	8
OTASP_P_REV	0 or 8
NUM_CAP_RECORDS	0 or 8
One or more occurrences of the following record:	
CAP_RECORD_TYPE	0 or 8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to '00000110'.

OTASP_P_REV - OTASP protocol revision.

If the ~~mobile-base~~ station does not request new capability information records as defined in Table 3.5.1.17.1-1 is not MEID-capable (See footnote 3), the base station shall omit this field; otherwise, the base station shall set this field to the value shown in the following table.

³ ~~The base station may use the first 8 bits of the received value in the ESN field to determine if the mobile station is MEID capable (i.e. MEID capable mobile stations will have '10000000' to indicate a pseudo ESN).~~

1

OTASP_P_REV (Binary)	Associated Standard
00000000	[2]
00000001	[3]
00000010	[4]
00000011	[5]
All other values are reserved.	

2

3 NUM_CAP_RECORDS-

Number of Capability Records.

4

If ~~OTASP P REV field is not included~~~~the mobile station is not MEID-~~~~capable (See footnote 3)~~, the base station shall omit this field; otherwise, the base station shall set this field to the number of Capability Records requested.

5

6

7

8 CAP_RECORD_TYPE -

Capability Record Type.

9

If ~~OTASP P REV field is not included~~~~the mobile station is not MEID-~~~~capable (See footnote 3)~~, the base station shall omit this field; otherwise, the base station shall set this field to the record type value shown in Table 3.5.1.17.1-1 corresponding to the information record requested.

10

11

12

13

14

15