Open Market Handsets (OMH)  
  
*(Companion document to CDG169 PRI Workbook)*

CDG Document

Version

CDMA Development Group

575 Anton Boulevard, Suite 560

Costa Mesa, California 92626

PHONE +1 888 800-CDMA

+1 714 545-5211

FAX +1 714 545-4601

<http://www.cdg.org>

[cdg@cdg.org](mailto:cdg@cdg.org)

Notice

Each CDG member acknowledges that CDG does not review the disclosures or contributions of any CDG member nor does CDG verify the status of the ownership of any of the intellectual property rights associated with any such disclosures or contributions. Accordingly, each CDG member should consider all disclosures and contributions as being made solely on an as-is basis. If any CDG member makes any use of any disclosure or contribution, then such use is at such CDG member’s sole risk. Each CDG member agrees that CDG shall not be liable to any person or entity (including any CDG member) arising out of any use of any disclosure or contribution including any liability arising out of infringement of intellectual property rights.

<page left blank intentionally>

Contents

[1. Introduction 1](#_Toc255489577)

[1.1 Purpose and Scope 1](#_Toc255489578)

[1.2 Outline 1](#_Toc255489579)

[2. Handset and R-UIM Identifiers 3](#_Toc255489580)

[2.1 EFIMSI\_M  [6F22] 3](#_Toc255489581)

[2.2 EFIMSI\_T [6F23] 4](#_Toc255489582)

[2.3 EFUSGIND [6F42] 5](#_Toc255489583)

[2.4 EFMDN [6F44] 5](#_Toc255489584)

[2.5 EFRUIMID [6F31] 6](#_Toc255489585)

[2.6 EFRevision [6F39] 6](#_Toc255489586)

[3. Analog Service Information 7](#_Toc255489587)

[3.1 EFAH [6F39] 7](#_Toc255489588)

[3.2 EFAOP 7](#_Toc255489589)

[3.3 EFACP 8](#_Toc255489589)

[4. CDMA Service Information 11](#_Toc255489591)

[4.1 EFCDMAHOME  [6F28] 11](#_Toc255489592)

[4.2 EFACCOLC  [6F2C] 11](#_Toc255489593)

[4.3 EFTERM [6F2D] 12](#_Toc255489594)

[4.4 EFSSCI [6F2E] 12](#_Toc255489595)

[4.5 EFPRL [6F30] 13](#_Toc255489596)

[4.6 EFMAXPRL [6F45] 13](#_Toc255489597)

[4.7 EFSP [6F37] 14](#_Toc255489598)

[4.8 EFECC [6F47] 14](#_Toc255489599)

[4.9 EFSSFC [6F3F] 15](#_Toc255489600)

[5. OTASP/OTAPA 17](#_Toc255489601)

[5.1 EFOTAPASPC [6F34] 17](#_Toc255489602)

[5.2 EFNAMLOCK [6F35] 18](#_Toc255489603)

[5.3 EFOTA [6F36] 19](#_Toc255489604)

[5.4 EFSPC [6F33] 19](#_Toc255489605)

[5.5 EFSPCS  [6F46] 20](#_Toc255489606)

[6. Carrier Customization 21](#_Toc255489607)

[6.1 EFSPN [6F41] 21](#_Toc255489608)

[6.2 EFAppLabels [6F92] 22](#_Toc255489609)

[7. Root Certificates 25](#_Toc255489610)

[7.1 EFRC [6F91] 25](#_Toc255489611)

[8. SMS – Basic 27](#_Toc255489612)

[8.1 EFSMSCAP [6F76] 27](#_Toc255489613)

[9. SMS – Broadcast 29](#_Toc255489614)

[9.1 EFBCSMScfg [6F5B] 29](#_Toc255489615)

[9.2 EFBCSMSTable [6F5D] 29](#_Toc255489616)

[9.3 EFBCSMSP [6F5E] 31](#_Toc255489617)

[10. 3GPD – Basic 33](#_Toc255489618)

[10.1 EFME3GPDOPC [6F48] 33](#_Toc255489619)

[10.2 EF3GPDOPM [6F49] 33](#_Toc255489620)

[10.3 EFTCPConfig [6F79] 34](#_Toc255489621)

[10.4 EFDGC [6F7A] 34](#_Toc255489622)

[11. 3GPD – Simple IP 37](#_Toc255489623)

[11.1 EFSIPCAP [6F4A] 37](#_Toc255489624)

[11.2 EFSIPSP [6F4E] 38](#_Toc255489625)

[11.3 EFSIPUPP [6F4C] 38](#_Toc255489626)

[11.4 EFSIPUPPExt [6F7D] 39](#_Toc255489627)

[11.5 EFSIPPAPSS [6F50] 41](#_Toc255489628)

[11.6 EFSIPCHAPSS [Hidden] 42](#_Toc255489629)

[12. 3GPD – Mobile IP 43](#_Toc255489630)

[12.1 EFMIPCAP [6F4B] 43](#_Toc255489631)

[12.2 EFMIPSP [6F4F] 44](#_Toc255489632)

[12.3 EFMIPUPP [6F4D] 44](#_Toc255489633)

[12.4 EFMIPUPPExt [6F80] 47](#_Toc255489634)

[12.5 EFMIPSS [Hidden] 49](#_Toc255489635)

[12.6 EFMIPFlags [6F78] 50](#_Toc255489636)

[13. 3GPD – IPv6 53](#_Toc255489637)

[13.1 EFIPV6CAP [6F77] 53](#_Toc255489638)

[14. HRPD 57](#_Toc255489639)

[14.1 EFHRPDCAP [6F56] 57](#_Toc255489640)

[14.2 EFHRPDUPP [6F57] 57](#_Toc255489641)

[14.3 EFHRPDSS [HIDDEN] 58](#_Toc255489642)

[15. WAP Browser 59](#_Toc255489643)

[15.1 EFWAPBrowserCP [6F7B] 59](#_Toc255489644)

[15.2 EFWAPBrowserBM  [6F7C] 61](#_Toc255489645)

[16. MMS 63](#_Toc255489646)

[16.1 EFMMSICP [6F67] 63](#_Toc255489647)

[16.2 EFMMSConfig [6F7E] 66](#_Toc255489648)

[17. Java Catalog 69](#_Toc255489649)

[17.1 EFJDL [6F7F] 69](#_Toc255489650)

[18. BREW Catalog 71](#_Toc255489651)

[18.1 EFBREWDownload [6F81] 71](#_Toc255489652)

[18.2 EFBREWTSID [6F82] 74](#_Toc255489653)

[18.3 EFBREWSID [6F83] 75](#_Toc255489654)

[18.4 EFBREWAEP [6F89] 75](#_Toc255489655)

[19. Location Based Services 77](#_Toc255489656)

[19.1 EFLBSXTRAConfig [6F84] 77](#_Toc255489657)

[19.2 EFLBSXSURL [6F85] 78](#_Toc255489658)

[19.3 EFLBSV2Config [6F86] 79](#_Toc255489659)

[19.4 EFLBSV2PDEADDR [6F87] 80](#_Toc255489660)

[19.5 EFLBSV2MPCADDR [6F88] 81](#_Toc255489661)

[20. Terminology 83](#_Toc255489662)

[21. References 87](#_Toc255489663)

Revision History

| Date | Version | Description |
| --- | --- | --- |
| March 2010 | 3.0 | * This CDG169 PRI Guidelines document was created as a companion document to the CDG169 PRI Workbook. The two documents should always be used together. Originally this information was in the CDG169 PRI Workbook. Having a separate companion document allows for more complete guidelines, examples, etc. to assist operators in completing the PRI Workbook. |

# Introduction

## Purpose and Scope

This document provides guidelines and recommendations to operators for provisioning parameters in R-UIM cards. It also provides a detailed description of each of the parameters listed in [CDG169 Part 1] and meaningful information regarding these parameters and their significance.

This document is targeted toward operators who need to:

* understand what a particular parameter is used for,
* know the typical values (or range of values),
* understand the reason behind the choice of typical values, and
* learn the tradeoffs, if any, in setting these parameters to values other than those recommended.

## Outline

A standard template is used for each parameter description, as follows:

Definition: Brief explanation of the parameter

Allowed Range: The permitted range and unit of each parameter

Typical Value: The single value the parameter needs to be set to, which is most commonly used by operators

**Notes:**

* A brief description of the tradeoffs involved in the setting of this parameter, providing an explanation of the effects of setting it “too high” and “too low,” beyond the normal operating range
* Any other remarks on the parameter setting (e.g., common mistakes, other useful information)

<page left blank intentionally>

# Handset and R-UIM Identifiers

## EFIMSI\_M [6F22]

Definition: This EF stores the five components of IMSI\_M. An IMSI\_M is always a class 0 IMSI.

Size (bytes): 10 (fixed)

### IMSI\_M\_CLASS

Definition: This parameter identifies the class assignment of the International Mobile Station Identity (IMSI). An IMSI that is 15 digits in length is called a class 0 IMSI [the National Mobile Station Identity (NMSI) is 12 digits in length]; an IMSI that is less than 15 digits in length is called a class 1 IMSI.

Allowed Range: 0, 1

Typical Value: 0

### IMSI\_M\_S

Definition: This parameter identifies a 10-digit (34-bit) number derived from the IMSI. When an IMSI has 15 digits, IMSI\_S is equal to the least significant 10 digits of the IMSI. When an IMSI has fewer than 15 digits, zeros are added to the most significant side of MSIN to obtain a 15-digit padded IMSI; IMSI\_S is equal to the last 10 digits of the padded IMSI.

Allowed Range: Ten decimal digits

Typical Value: Operator specific

### IMSI\_M\_11\_12

Definition: This parameter comprises the 11th and 12th digits from the right of the IMSI address.

Allowed Range: Two decimal digits

Typical Value: Operator specific

Note: This is also known as Mobile Network Code (MNC) and is assigned by the International Telecommunication Union (ITU) to the operator.

### IMSI\_M\_MCC

Definition: This parameter identifies the Mobile Country Code (MCC).

Allowed Range: Three decimal digits

Typical Value: The MCC is assigned by the ITU.

## ***EFIMSI\_T [6F23]***

Definition: IMSI\_T is an IMSI that is not associated with the Mobile Identification Number (MIN) assigned to the mobile station.

Size (bytes): 10 (fixed)

### IMSI\_T\_CLASS

Definition: This parameter identifies the Class assignment of the IMSI.

Allowed Range:

* 0
* 1

Typical Value: 0

Note: An IMSI\_T can be a class 0 or class 1 IMSI.

### IMSI\_T\_S

Definition: This parameter identifies the last 10 digits of the IMSI. These are the same 10 digits as the directory number.

Allowed Range: Ten decimal digits

Typical Value: Operator specific

### IMSI\_T\_11\_12

Definition: This parameter comprises the 11th and 12th digits from the right of the IMSI address.

Allowed Range: Two decimal digits

Typical Value: This is assigned by the ITU.

### IMSI\_T\_MCC

Definition: This parameter identifies the Country Code.

Allowed Range: Three decimal digits

Typical Value: This is assigned by the ITU.

## ***EFUSGIND [6F42]***

Definition: This EF contains the Removable UIM\_ID/SF\_EUIMID Usage Indicator.

Size (bytes): 1 (fixed)

### Handset Authentication Indicator

Definition: This parameter indicates whether to use ESN\_ME or UIM\_ID for Cellular Algorithms for Validation and Encryption (CAVE) authentication and MS identification.

Allowed Range:

* ESN\_ME
* UIM\_ID

Typical Value: Always use UIM\_ID for OMH.

Note: For OMH devices, this should always be set to UIM\_ID and not ESN.

### Handset Identification Indicator

Definition: This parameter indicates whether to use MEID or SF\_EUIMID to identify the mobile station (MS).

Allowed Range:

* MEID
* SF\_EUIMID

Typical Value: Always use SF\_EUIMID for OMH.

## EFMDN [6F44]

Definition: This parameter indicates the dialable number associated with the mobile station through a service subscription. A Mobile Directory Number (MDN) is not necessarily the same as the mobile station identification on the air interface, i.e., MIN, IMSI\_M, or IMSI\_T. An MDN consists of up to 15 digits. The mobile station should have memory to store at least one MDN.

Size (bytes): 11 (fixed)

### Mobile Directory Number

Definition: This parameter indicates the MDN.

Allowed Range: 15 decimal digits programmable

Typical Value: Operator specific

### Mobile Directory Number Type

Definition: This parameter indicates the MDN Type.

Allowed Range:

* National
* International
* Unknown

Typical Value: Operator specific

### Mobile Directory Number Plan

Definition: This parameter indicates the MDN Plan.

Allowed Range:

* Telephony
* Private
* Unknown

Typical Value: Operator specific

## EFRUIMID [6F31]

Definition: This EF contains the R-UIM Identifier.

Size (bytes): 8 (fixed)

### R-UIM Identifier

Definition: This parameter contains the R-UIM Identifier.

Allowed Range: 32-bit number

Typical Value: This is not to be provisioned by the operator; the value depends on the particular R-UIM card vendor.

## EFRevision [6F39]

Definition: This EF contains the revision number of the R-UIM.

Size (bytes): 1 (fixed)

### R-UIM Revision

Definition: This parameter contains the revision number of the R-UIM.

Allowed Range: 0−255

Typical Value: 00000100 (R-UIM complying with [[CS0023-D](#CS0023D)])

Note: This allows the mobile equipment (ME) to communicate with different versions of the R-UIM (i.e., R-UIM with different set of capabilities).

# Analog Service Information

## ***EFAH [6F39]***

These EFs pertain to Analog. Since none of the operators are using AMPS, they do not need to be provisioned.

Definition: This EF indicates the Analog Home SID.

Size (bytes): 2 (fixed)

### Analog Home SID

Definition: This parameter indicates the Cellular Service Provider analog home system ID for the given NAM. This is automatically filled from the CDMA Home SID.

Allowed Range: 5 decimal digits from 0−65535

Typical Value: Operator specific

## ***EFAOP***

Definition: This EF indicates the Analog Operational Parameters, namely, Extended Address bit (Exp), the Local Use Mark (LCM), and the Group ID (GID) field.

Size (bytes): 1 (fixed)

### Extended Address

Definition: This parameter specifies whether the Extended Address bit is enabled.

Allowed Range:

* True
* False

Typical Value: False

### Local Use Mark

Definition: This parameter specifies whether the Local Use Mark bit is enabled.

Allowed Range:

* True
* False

Typical Value: False

### Group ID

Definition: This parameter indicates whether the Group ID bit is enabled or not.

Allowed Range: 0−15

Typical Value: Operator Specific

## EFACP

Definition: This EF indicates the Analog Mode Channel Preferences, as determined by the service3 provider in accordance with the terms of the subscription. The items addressed are the Analog Initial Paging Channel, the Analog First Dedicated Control Channel for System A, the Analog First Dedicated Control Channel for System B, and the Number of Dedicated Control Channels to scan.

Size (bytes): 7 (fixed) [[CS0023-D](#CS0023D)]

### Analog Initial Paging Channel

Definition: This parameter indicates the Analog Initial Paging Channel.

Allowed Range: 5 decimal digits from 0−65535

Typical Value: Operator specific

### Analog First Dedicated Control System A

Definition: This parameter indicates the Analog First Dedicated Control Channel System A.

Allowed Range: 5 decimal digits from 0−65535

Typical Value: Operator specific

### Analog First Dedicated Control System B

Definition: This parameter indicates the Analog First Dedicated Control Channel System B.

Allowed Range: 5 decimal digits from 0−65535

Typical Value: Operator specific

### Analog Number of DCC

Definition: This parameter identifies the Analog Number of the Dedicated Control Channel to scan.

Allowed Range: 0−255

Typical Value: Operator specific

<page left blank intentionally>

# CDMA Service Information

## EFCDMAHOME [6F28]

Definition: This EF indicates the CDMA Home System Identification (SID) and Network Identification (NID) when the mobile station is operating in CDMA mode.

Size (bytes): 5 x # of records

### Home SID and NID

Definition: This parameter indicates the Home SIDs and NIDs for the given NAM.

Allowed Range: Multiple pairs of up to 5 decimal digits, ranging from 0−32767; with corresponding Band Class.

Typical Value: 4–6 pairs

**Note:** The first SID cannot be 0. SIDs must be all even or all odd.

### Band Class

Definition: This parameter indicates the band class supported.

Allowed Range: This is a 1 byte field that represents the corresponding Band Class.

Typical Value: Operator Specific

## EFACCOLC [6F2C]

Definition: This EF indicates the 4-bit Access Overload Class indicator (ACCOLCp), which is used to identify which overload class controls access attempts by the mobile station and is used to identify redirected overload classes in global service redirection.

The mobile station shall store the 4-bit access overload class (ACCOLCp). Mobile stations that are not for test or emergency use should be assigned to overload classes ACCOLC 0 through ACCOLC 9. For mobile stations that are classified as overload classes ACCOLC 0 through ACCOLC 9, the mobile station’s 4-bit access overload class indicator (ACCOLCp) shall be automatically derived from the last digit of the associated decimal representation of the IMSI\_M by a decimal to binary conversion, as specified in [[CS0005-A](#CS0005A)].

Size (bytes): 1 (fixed)

### Access Overload Class

Definition: This parameter indicates the Access Overload Class (ACCOLCp).

Allowed Range: 4-bit access overload class indicator.

Typical Value: The value is derived from the last digit of the associated decimal representation of the IMSI\_M.

## EFTERM [6F2D]

Definition: This EF indicates the Call Termination Mode Preferences.

Size (bytes): 1 (fixed)

### Home SID Term Reg

Definition: This parameter indicates the CDMA mobile-terminated home SID registration.

Allowed Range:

* True
* False

Typical Value: True

### Foreign SID Term Reg

Definition: This parameter indicates the CDMA mobile-terminated foreign SID registration.

Allowed Range:

* True
* False

Typical Value: True

### Home NID Term Reg

Definition: This parameter indicates the CDMA mobile-terminated home NID registration.

Allowed Range:

* True
* False

Typical Value: True

## EFSSCI [6F2E]

Definition: This EF indicates the Suggested Slot Cycle Index.

Size (bytes): 1 (fixed)

### Slot Cycle Index

Definition: This parameter indicates the duration and frequency that the phone checks the paging channel.

Allowed Range: 2 decimal digits, range 0−7

Typical Value: 2

## EFPRL [6F30]

Definition: This EF stores the Preferred Roaming List.

Size (bytes): MAX\_PRL\_LIST\_SIZE.

**Note:** See Section , .

### PR\_LIST

Definition: This parameter indicates the Preferred Roaming List. See [[CS0016-C](#CS0016C)]. This may contain IS-683A PRL for 1x only devices or Concatenated PRL (cPRL) with IS-683A PRL and IS-683C PRL for EV-DO devices. See the appendix in [[CDG167](#CDG167)] for more information on cPRL.

Allowed Range: This is the actual PRL.

Typical Value: Operator specific.

## EFMAXPRL [6F45]

Definition: This EF indicates the maximum size for EFPRL and EFEPRL.

Size (bytes): 2 (fixed)

### Maximum PRL Size for EFPRL

Definition: This EF indicates the maximum PRL size for EFPRL. The mobile station shall set this field to the maximum size, in octets, that the mobile station can support for the preferred roaming list (PR\_LISTs-p).

Allowed Range: 0−65535

Typical Value: 6−7k (For both 1X and EVDO systems)

Note: Operator to specify based upon entries in PRL.

### Maximum PRL Size for EFEPRL (not used in OMH context)

## EFSP [6F37]

Definition: This EF identifies Service Preferences.

Size (bytes): 1 (fixed)

### System A/B Preference

Definition: This EF indicates the System A/B Preference.

Allowed Range:

* No preference
* A preferred
* B preferred
* A only
* B only

Typical Value: No preference

### Analog/CDMA Preference

Definition: This EF indicates the Analog/CDMA Preference.

Allowed Range:

* No preference
* Analog preferred
* CDMA preferred
* Analog only
* CDMA only

Typical Value: CDMA Preferred

## EFECC [6F47]

Definition: This EF identifies Emergency Call Codes.

Size (bytes): 3n (n <=5)

### **Emergency Call Codes**

Definition: This EF identifies Emergency Call Codes and contains up to five emergency call codes. Each digit is encoded in BCD format. The emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of fewer than 6 digits is chosen, then the unused nibbles shall be set to “F.”

Allowed Range: 0−5 emergency call codes wherein each emergency call code is a maximum of 6 digits

Typical Value: Operator specific

## EFSSFC [6F3F]

Definition: This EF identifies the Supplementary Services Feature Code Table. It stores the numeric feature code to be used by the ME when a supplementary service is invoked in CDMA or analog mode via an implementation-dependent user interface (such as a menu) that automatically inserts a feature code into the dialed digit string. Because feature codes are service-provider specific, this EF is required to enable the ME to perform the mapping to the feature code.

When a supplementary service is invoked in CDMA or analog mode, the mobile station shall determine the feature code by reading the Supplementary Service Feature Code Table entry for the selected supplementary service, and pre-pending with an asterisk.

Size (bytes): Variable

Note: A feature code of up to four digits shall be encoded via BCD into the two bytes of the feature code table entry as follows:

* Represent these four digits as D1D2D3D4.
* If a feature code (FC) of fewer than four digits is used, the digits shall be right justified and the unused digits shall be set to “F.”

The following feature codes are available, each with a maximum size of 4 decimal digits:

* CD Activate – Feature Code: Call Delivery
* CD De-Activate – Feature Code: Call Delivery
* CFB Register New Forward-to Number – Feature Code: Call Forwarding – Busy
* CFB Register to Voice Mail – Feature Code: Call Forwarding – Busy
* CFB De-Register – Feature Code: Call Forwarding – Busy
* CFB Activate – Feature Code: Call Forwarding – Busy
* CFB De-Activate – Feature Code: Call Forwarding – Busy
* CFD Register New Forward-to Number –Feature Code: Call Forwarding – Default
* CFD Register to Voice Mail – Feature Code: Call Forwarding – Default
* CFD De-Register – Feature Code: Call Forwarding – Default
* CFD Activate –Feature Code: Call Forwarding – Default
* CFD De-Activate – Feature Code: Call Forwarding – Default
* CFNA Register New Forward-to Number – Feature Code: Call Forwarding – No Answer
* CFNA Register to Voice Mail – Feature Code: Call Forwarding – No Answer
* CFNA De-Register – Feature Code: Call Forwarding – No Answer
* CFNA Activate – Feature Code: Call Forwarding – No Answer
* CFNA De-Activate – Feature Code: Call Forwarding – No Answer
* CFU Register New Forward-to Number – Feature Code: Call Forwarding – Unconditional
* CFU Register to Voice Mail – Feature Code: Call Forwarding – Unconditional
* CFU De-Register – Feature Code: Call Forwarding – Unconditional
* CFU Activate – Feature Code: Call Forwarding – Unconditional
* CFU De-Activate – Feature Code: Call Forwarding – Unconditional
* CW Activate – Feature Code: Call Waiting
* CW De-Activate – Feature Code: Call Waiting
* CW Cancel (Temporarily) – Feature Code: Cancel Call Waiting
* CNIR Activate (per-call blocking) – Feature Code: Calling Number ID Restriction
* CNIR De-Activate (per-call allowed) – Feature Code: Calling Number ID Restriction
* CC Invoke – Feature Code: Conference Calling
* CC Invoke Drop Last Party – Feature Code: Conference Calling
* DND Activate – Feature Code: Do Not Disturb
* DND De-Activate – Feature Code: Do Not Disturb
* MWN Activate Alert Pip Tone – Feature Code: Message Waiting Notification
* MWN De-Activate Alert Pip Tone – Feature Code: Message Waiting Notification
* MWN Activate Pip Tone – Feature Code: Message Waiting Notification
* MWN De-Activate Pip Tone – Feature Code: Message Waiting Notification
* MWN Cancel (Temporarily) – Feature Code: Cancel Message Waiting Notification
* PACA Invoke – Feature Code: Priority Access and Channel Assignment
* VMR Invoke – Feature Code: Voice Message Retrieval
* CNAP Activate – Feature Code: Calling Name Presentation
* CNAP De-Activate – Feature Code: Calling Name Presentation
* CNAR Activate – Feature Code: Calling Name Restriction
* CNAR De-Activate – Feature Code: Calling Name Restriction
* AC Activate – Feature Code: Automatic Callback
* AC De-Activate – Feature Code: Automatic Callback
* AR Activate – Feature Code: Automatic Recall
* AR De-Activate – Feature Code: Automatic Recall
* USCF Register New Directory Number – Feature Code: User Selectable Call Forwarding
* RUAC Activate – Feature Code: Rejection of Undesired Annoying Calls
* RUAC De-Activate – Feature Code: Rejection of Undesired Annoying Calls
* AOC Invoke – Feature Code: Advice of Charge
* COT Invoke – Feature Code: Invoke Call Trace

For a complete list of features, see [[CS0023-D](#CS0023D)].

# OTASP/OTAPA

## EFOTAPASPC [6F34]

Definition: This EF identifies OTAPA/SPC\_Enable Settings. It contains user-entered control information that either prevents or (else) permits network manipulation of the Service Programming Code (SPC), and either prevents or (else) permits OTAPA to be performed on the NAM.

Size (bytes): 1 (fixed)

### OTAPA\_Enable

Definition: This sets forth user-entered control information that either prevents or (else) permits Over-the-Air Parameter Administration (OTAPA) to be performed on the NAM.

Allowed Range:

* True
* False

Typical Value: True

**Note:** For OTAPA\_Enable, a value of “0” for the NAM indicates that the user consents to the performance of OTAPA for the NAM by the service provider. A value of “1” indicates that the user does not permit OTAPA to be performed on the NAM.

### SPC\_Change\_Enable

Definition: This EF sets forth user-entered control information that either prevents or (else) permits network manipulation of the SPC.

Allowed Range:

* True
* False

Typical Value: True

**Note:** For SPC\_Change Enable, a value of “0” for the R-UIM indicates that the user consents to allow the service provider to change the value of the SPC. A value of “1” indicates that the user denies permission for the service provider to change the value of the SPC.

## EFNAMLOCK [6F35]

Definition: This EF identifies NAM\_LOCK Settings.

Size (bytes): 1 (fixed)

### Current NAM Lock State

Definition: This indicates whether NAM is locked by the Subscriber Parameter Administration Security Mechanism (SPASM).

Allowed Range:

* Locked
* Unlocked

Typical Value: Locked

**Note:** A value of “1” indicates that the NAM is locked by the SPASM protection mechanism. A value of “0” indicates that the NAM is unlocked.

### Permanent NAM Lock Setting

Definition: This indicates whether or not the SPASM protection mechanism must be satisfied for network-initiated OTA.

Allowed Range:

* On
* Off

Typical Value: On

**Note:** A value of “1” indicates that the SPASM protection mechanism must be satisfied for network-initiated OTA. A value of “0” indicates that SPASM protection is not required.

### Current OTA Mode

Definition: This indicates whether the current OTA session is network- or user-initiated.

Allowed Range:

* Network-initiated
* User-initiated

Typical Value: User-initiated

**Note:** A value of “0” indicates user-initiated, and a value of “1” indicates network-initiated.

## EFOTA [6F36]

Definition: This EF identifies OTASP/OTAPA features. The EF stores a listing of the following OTASP/OTAPA features supported by the R-UIM, along with protocol revision codes, each with an allowed range of 0–255:

* DATA\_P\_REV ID – OTA Feature: NAM Download
* DATA\_P\_REV – OTA Feature: NAM Download
* A\_KEY\_P\_REV ID – OTA Feature: Key Exchange
* A\_KEY\_P\_REV – OTA Feature: Key Exchange
* SSPR\_P\_REV – OTA Feature: System Selection for Preferred Roaming
* SPL\_P\_REV ID – OTA Feature: Service Programming Lock
* SPL\_P\_REV – OTA Feature: Service Programming Lock
* OTAPA\_P\_REV ID – OTA Feature: OTAPA
* OTAPA\_P\_REV – OTA Feature: OTAPA
* PUZL\_P\_REV ID – OTA Feature: Preferred User Zone List
* PUZL\_P\_REV – OTA Feature: Preferred User Zone List
* 3GPD\_P\_REV ID – OTA Feature: 3GPD
* 3GPD\_P\_REV – OTA Feature: 3GPD
* SECURE\_MODE\_P\_REV ID – OTA Feature: Secure MODE
* SECURE\_MODE\_P\_REV – OTA Feature: Secure MODE

Size (bytes): 2N+1 (where N is the number of OTASP/OTAPA features supported)

## **EFSPC [6F33]**

Definition: This EF includes the Service Programming Code (SPC).

Size (bytes): 3 (fixed)

### **Service Programming Code**

Definition: This parameter cites the security code that provides access to service programming for individual service provider networks.

Allowed Range: 6 decimal digits from 0−9, random

Typical Value: Operator specific

Note: The SPC is a simple means to protect the contents of the R-UIM from being programmed without authorization.

## EFSPCS [6F46]

Definition: This EF identifies the Security Programming Code Status. This identifies whether the EFSPC(Service Programming Code) is set to default and internally updated in the card to reflect the current state of SPC after an OTASP commit if the SPC was changed.

Size (bytes): 1 (fixed)

### **SPC Status**

Definition: This parameter identifies the Security Programming Code Status.

Allowed Range:

* OFF: SPC has the default value
* ON: SPC is set to other value

Typical Value: ON

# Carrier Customization

## EFSPN [6F41]

Definition: This EF identifies the CDMA Home Service Provider Name (SPN). The operator should allocate n17 in EF\_CST and provision the following parameters, if CDMA Home service provider name is to be displayed when the MS is in the Home Service area.

Size (bytes): 35 (fixed)

### SPN Display Condition

Definition: This indicates whether or not a Service Provider Name should be displayed when the MS is registered in the home service area.

Allowed Range:

* OFF: display is not required
* ON: display is required

Typical Value: ON

### SPN Character Encoding

Definition: This contains encoding for the SPN string.

Allowed Range:

* 7-bit ASCII
* IA5
* UNICODE

Typical Value: 7-bit ASCII

### SPN Language Indicator

Definition: This contains the Language Indicator for the SPN string.

Allowed Range:

* English
* French
* Spanish
* Japanese
* Korean
* Chinese
* Hebrew

Typical Value: English

### SPN String

Definition: This contains the actual Service Provider Name string.

Allowed Range: 32-byte string

Typical Value: The value needs to be specified by the Operator.

## EFAppLabels [6F92]

Definition: Application Labels are used for carrier customization. They are used by devices to display operator-branded services. The text label the operator desires to provision in this EF is the text associated with the icon or menu item used to launch the application, such as BREW, MMS, Browser, etc.

These labels are optional and need only be provisioned if an operator desires to override the handset vendor-defined labels.

Note: In the absence of the application labels provisioned by an operator, the device will display the default values.

Size (bytes): 4+N\*32 (where N is the number of application labels)

* Typical EF Size (bytes): 132 bytes (assumes 4 application labels)
* Maximum EF Size (bytes): 516 byes (assumes 16 application labels)

### App Label Character Encoding

Definition: This parameter specifies the encoding for Application Labels.

Allowed Range:

* Octet (unspecified)
* 7-bit ASCII
* IA5
* UNICODE unspecified

Typical Value: 7-bit ASCII

### Language of App Labels

Definition: This parameter specifies the Language in which application labels are provisioned.

Allowed Range:

* English
* French
* Spanish
* Japanese
* Korean
* Chinese
* Hebrew

Typical Value: 7-bit ASCII

### MMS App Label

Definition: This parameter specifies the text label for the MMS application icon or menu item.

Allowed Range: 32-byte string

Typical Value: Operator specific

### WAP Browser App Label

Definition: This parameter specifies the text label for the WAP Browser application or menu item.

Allowed Range: 32-byte string

Typical Value: Operator specific

### BREW App Label

Definition: This parameter specifies the text label for the BREW application downloader icon or menu item.

Allowed Range: 32-byte string

Typical Value: Operator specific

### Java App Label

Definition: This parameter specifies the text label for the Java application downloader icon or menu item.

Allowed Range: 32-byte string

Typical Value: Operator specific

<page left blank intentionally>

# Root Certificates

## EFRC [6F91]

Definition: The root certificates are used for operator-signed applications. If the same root certificate is used for all operator-signed applications, then the application bit mask is set to “Unspecified.” If not, the application bit for each application shall be set accordingly.

The operator should allocate n16 in EF\_CST and provision the following parameters, if root certificates are to be used on its network.

Note: Root certificates are not mandatory for operators to use. Only in cases where the operator’s applications are signed using root certificates they would need to be provisioned.

Size (bytes): Typical EF size (bytes): 1500 bytes (assumes one 1.5kB certificate)

### Certificate Type

Definition: This parameter identifies the type of certificate.

Allowed Range:

* DER Encoded Binary X.509
* Base64 Encoded X.509
* PKCS #7
* PKCS #12

Typical Value: This is the actual certificate type used by the operator.

### Certificate Information

Definition: This is the actual certificate used by the operator encoded according to the type specified in Section 7.1.1

Allowed Range: N/A

Typical Value: N/A

### Associated Applications

Definition: This parameter identifies which applications are associated with this certificate. One, multiple, or all applications may be associated with a certificate.

Allowed Range: 1 or more of the following:

* Unspecified (i.e., all)
* WAP Browser
* BREW
* Java
* LBS
* Terminal

Typical Value: This parameter identifies the applications selected by an operator to use with the actual certificate defined in Section 7.1.2.

# SMS – Basic

## EFSMSCAP [6F76]

Definition: The operator should allocate n4 in EF\_CST and provision the following parameters, if SMS service is supported on its network.

Size (bytes): 4 (fixed)

### SMS Retry Period

Definition: This is the overall time period (in seconds) during which the Mobile Originated (MO) SMS retries can be performed. A value of “0” implies that MO SMS retry is disabled.

Allowed Range: 0−255 seconds

Typical Value: 30−60 seconds

Note: The SMS retry period needs to be larger than the SMS retry interval period.

### SMS Retry Interval

Definition: This is the time interval (in seconds) that the device shall wait before the next retry attempt can be made after an MO SMS failure.

Allowed Range: 0–255 seconds

Typical Value: 3−5 seconds

Note: The SMS retry interval needs to be smaller than SMS retry period. Setting this to a value smaller than 5 seconds could lead to multiple SMS originations being sent before a delayed acknowledgment to the previous SMS attempt is received.

### SMS Send on Access Flag

Definition: This flag indicates whether the operator wants to allow messages to be sent over Access Channel.

Allowed Range:

* True
* False

Typical Value: True

### SMS Send on Traffic Flag

Definition: This flag indicates whether the operator wants to allow messages to be sent over Traffic Channel.

Allowed Range:

* True
* False

Typical Value: True

### SMS Send Standard EMS Flag

Definition: This parameter specifies whether to allow Long SMS (LMS) messages to be sent as standard Enhanced Messaging Service (EMS) messages.

Allowed Range:

* True
* False

Typical Value: False (unless operator’s network supports EMS)

### SMS Preferred Service Option

Definition: This is the preferred service option to be used by the device when it sets up SMS traffic channel for sending SMS.

Allowed Range:

* Device Default
* Service Option 6
* Service Option 14

Typical Value: Service Option 6

Note: This is what the device uses for origination, but the traffic channel assignment sent by the BS will override the service option if different from that used by the device.

# SMS – Broadcast

## EFBCSMScfg [6F5B]

Definition: Broadcast SMS messages are messages sent by the Base Station (BS) to the Mobile Stations. They can be sent on the Paging Channel, Forward Common Control Channel, or the Broadcast Control Channel. These messages can also be sent to individual mobile stations on the Forward Traffic Channel.

The operator should allocate n14 in EF\_CST and provision the following parameters, if Broadcast SMS service is supported on its network.

Size (bytes): 1 (fixed)

### **Broadcast SMS Config**

Definition: This indicates the operator broadcast configuration setting for Broadcast SMS. This information, determined by the operator, defines the filtering criteria that can be used by the ME to receive Broadcast SMS.

Allowed Range:

* Disallow
* Allow table only
* Allow all

Typical Value: Allow All

Note: The choices in the allowed range indicate the following:

* **Disallow**: This setting disables the mobile station’s broadcast SMS capability (i.e., the mobile station will not process broadcast SMS).
* **Allow Table Only**: This setting allows the mobile station to receive only broadcast messages for the service categories that have been programmed in EFBCSMStable.
* **Allow All:** This setting allows the mobile station to receive broadcast messages for all service categories.

## EFBCSMSTable [6F5D]

Definition: This EF contains information in accordance with comprising service category program parameters, which can be used by the ME for Broadcast SMS filtering.

Size (bytes): Variable

### **Service Information: Category**

Definition: This field contains the value of the Service Category for the operation.

* UNKNOWN
* EMERGENCY
* ADMIN
* MAINTENANCE
* General News – Local
* General News – Regional
* Etc.

Typical Value: Operator specific

Note: Note that the list of categories above is only a subset and not the complete list

### **Service Information: Language**

Definition: This parameter specifies the Language used for the message text.

Allowed Range:

* English
* French
* Spanish
* Japanese
* Korean
* Chinese
* Hebrew

Typical Value: English

### Service Information: Max Messages

Definition: This field shall be set to the Maximum Number of Messages that may be stored in the ME for this service category.

Allowed Range: 0–255

Typical Value: 255

### **Service Information: Alert Option**

Definition: This parameter specifies the alert option to be used when the mobile station receives a message for this service category. This field shall be set according to Table 4.5.19-1 of [[CS0015-B](#CS0015B)].

Allowed Range:

* NONE
* MS Default Alert
* VIBRATE\_ONCE
* VIBRATE\_REPEAT
* VISUAL\_ONCE
* VISUAL\_REPEAT
* LOW\_PRIORITY\_ONCE
* LOW\_PRIORITY\_REPEAT
* MEDIUM\_PRIORITY\_ONCE
* MEDIUM\_PRIORITY\_REPEAT
* HIGH\_PRIORITY\_ONCE
* HIGH\_PRIORITY\_REPEAT

Typical Value: Operator specific

### Service Information: Label Encoding

Definition: This parameter defines the encoding scheme used for the label.

Allowed Range:

* 7-bit ASCII
* IA5
* UNICODE

Typical Value: 7-bit ASCII

### Service Information: Label

Definition: This is the actual text specified by the operator for the service.

Allowed Range: Up to 258 bytes of characters

Typical Value: Operator specific

## **EFBCSMSP [6F5E]**

Definition: This EF specifies the parameters used for the Broadcast SMS.

Size (bytes): 2 (record)

### Service Information: Selected Flag

Definition: This parameter indicates whether service is selected or not by the operator.

Allowed Range:

* True
* False

Typical Value: Operator specific

### Service Information: Priority

Definition: This parameter identifies the priority level of service.

Allowed Range:

* Normal
* Urgent
* Emergency

Typical Value: Normal

# 3GPD – Basic

## EFME3GPDOPC [6F48]

Definition: If either service n20 or n38 is allocated (see Section 3.4.18 of [[CS0023-D](#CS0023D)]), this EF shall be present. This parameter specifies the operation modes supported by the ME. The ME sets this field in the form of a bitmap as defined in [[CS0016-B](#CS0016B)].

Size (bytes): 1 (fixed)

### **3GPD Operation Capability**

Definition: This EF stores IP operation capabilities supported by the ME. After the selection of DFCDMA (7F25) during the initialization, the R-UIM shall set the value of this byte to “0.” Mobile equipment that supports Simple IP or Mobile IP shall set each subfield to “1” if it supports the corresponding operating mode.

Allowed Range: One or more of the following:

* SimpleIP Supported
* MobileIP Supported
* MobileIP with SimpleIP Fallback supported

Typical Value: Does not need to be provisioned by the operator

## EF3GPDOPM [6F49]

Definition: If either service n20 or n38 is allocated (see Section 3.4.18 of [[CS0023-D](#CS0023D)]), this EF shall be present.

Size (bytes): 1 (fixed)

### 3GPD Operation Mode

Definition: This EF stores the 3GPD Operation Mode Parameter Block. For further details, refer to 3GPP2 [[CS0016-B](#CS0016B)] and [[CS0023-D](#CS0023D)].

Allowed Range:

* SimpleIP
* MobileIP
* MobileIP with SimpleIP Fallback

Typical Value: Simple IP

## **EFTCPConfig [6F79]**

Definition: This EF contains information about Transmission Control Protocol (TCP) configurations. If service n20 (3GPD-SIP) or n38 (3GPD-MIP) is allocated and service n15 (Messaging and 3GPD Extensions) is allocated, this EF shall be present.

Size (bytes): 2 (fixed)

### TCP Graceful Close of Dormant Connections

Definition: This parameter specifies whether the TCP socket should be closed gracefully, even if the underlying interface is dormant.

Allowed Range:

* True
* False

Typical Value: False

Note: If the value of this flag is TRUE, this means that the TCP socket should be closed gracefully. This in turn means that the network connection will be brought out of dormancy and the TCP FIN will be sent out on the network. If the value of this flag is set to FALSE, the local TCP connection will be closed forcefully without going through the TCP graceful close cycle.

### TCP Keep Alive Idle Timer

Definition: This configuration item is used primarily to deal with dead TCP peers. If there is no TCP message being sent from the peer for the “TCP Keep Alive Idle Timer,” then keep-alive probes will be sent to the peer. With a default value of 120 minutes, the mobile would not send keep-alive probes for at least 120 minutes when there is no TCP activity from the remote end.

Allowed Range: 0–255 minutes

Typical Value: 120 minutes

Note: A value of 0 means that the TCP keep-alive feature is disabled on the ME.

## **EFDGC [6F7A]**

Definition: This EF specifies miscellaneous data configuration items.

Size (bytes): 3 (fixed)

### Data Dormant Timer

Definition: This parameter specifies the number of seconds to wait before going into data dormant mode, which shall be at least 20 seconds.

Allowed Range: 20–255 seconds

Typical Value: 30 seconds

### EPZID Type

Definition:

Allowed Range:

* Packet Zone ID
* Packet Zone ID plus SID
* Packet Zone ID plus SID and NID

Typical Value: Packet Zone ID plus SID and NID

### Hysteresis Activation Time

Definition: This parameter specifies the number of seconds the device should wait before it adds a new Packet Zone ID.

Allowed Range: 0–255 seconds

Typical Value: 30 seconds

<page left blank intentionally>

# 

# 3GPD – Simple IP

## EFSIPCAP [6F4A]

Definition: This parameter specifies the SimpleIP Capability Parameter Block defined in [[CS0016-C](#CS0016C)].

The operator should allocate n20 in EF\_CST and provision the following parameters, if 3GPD Simple IP is supported on its network.

Size (bytes): 4 (fixed)

### Simple IP Max Number of NAIs

Definition: This parameter defines the total number of Network Address Identifiers (NAIs) that an operator intends to use. If an operator needs to specify different NAIs/usernames for the different applications or groups of applications, then multiple profiles are used.

Allowed Range: 0–15

Typical Value: Operator specific

Note: Most operators worldwide use a single NAI/username profile shared by all applications. In cases where an operator requires a separate NAI/password profile for each of the applications (or groups of applications) requiring differing treatment[[1]](#footnote-1) at the network end, multiple profiles may be used.

### SIP Max NAI Length

Definition: This parameter specifies the maximum length of Simple IP NAI. This value specifies the maximum memory allocated in the card for this field.

Allowed Range: 0–255

Typical Value: 255

### SIP Max SS Length

Definition: This parameter specifies the maximum length of the Simple IP password. This value specifies the maximum memory allocated in the card for this field.

Allowed Range: 0–31

Typical Value: 31

### SIP Authentication Algorithms

Definition: This parameter specifies the authentication algorithm used for PDSN authentication.

Allowed Range:

* PAP
* CHAP
* CHAP & PAP

Typical Value: CHAP & PAP both

## EFSIPSP [6F4E]

Definition: This EF stores the SimpleIP Status Parameters Block defined in [[CS0016-B](#CS0016B)]. If service n20 is allocated, this EF shall be present.

Size (bytes): 1 (fixed)

### ACT\_NAI\_ENTRY\_INDEX

Definition: This specifies the active SimpleIP NAI entry index.

Allowed Range: 0–15

Typical Value: 0 (when all applications are using one profile)

## EFSIPUPP [6F4C]

Definition: This parameter specifies the SimpleIP User Profile Parameter Block defined in [[CS0016-C](#CS0016C)].

Size (bytes): Variable [(N\*(X+2))+2], where N is the number of Simple IP profiles and N is the maximum NAI length.

### NUM\_NAI

Definition: This parameter specifies the number of applications having different simple IP profiles.

Allowed Range: 0–15

Typical Value: Operator specific

Note: In order to enable Mobile IP to Simple IP fallback, NAI Entry Indexes used in SIP and MIP User Profiles must be the same.

### Profile Information: NAI Entry Index

Definition: This parameter provides the index to the NAI profile.

Allowed Range: 0–15

Typical Value: Operator specific

Note: In order to enable Mobile IP to Simple IP fallback, NAI Entry Indexes used in SIP and MIP User Profiles must be the same.

### Profile Information: NAI

Definition: This parameter specifies the Network Address Identifier.

Allowed Range: Up to 255 ASCII characters

Typical Value: Operator specific

Note: The NAI should be chosen and managed using procedures that minimize the likelihood of compromise.

### Profile Information: Authentication Algorithm

Definition: This parameter specifies the authentication algorithm used by the operator for PDSN authentication.

Allowed Range:

* None
* CHAP
* PAP
* CHAP with PAP fallback

Typical Value: CHAP & PAP

Note: Always CHAP & PAP for OMH.

## EFSIPUPPExt [6F7D]

**Definition:** This EF contains the additional parameters for Simple IP User Profiles in order to fully support the feature of multiple profiles. NUM\_NAI is the same as NUM\_NAI in SIPUPP as per Section 11.3 of this document. Each index in SIPUPP ext maps to the same index in SIPUPP.

Size (bytes): Variable

* Typical EF Size (bytes): 7 bytes (assumes the common usage of one profile for all applications)
* Maximum EF Size (bytes): 98 bytes (assumes a wildly unlikely usage of 15 different profiles)

### NUM\_NAI

Definition: This parameter specifies the total number of NAIs used for various applications.

Allowed Range: 0–15

Typical Value: Operator specific

### Profile Information: NAI Entry Index

Definition: This parameter indicates the index for the particular application using the simple IP profile.

Allowed Range: 0–15

Typical Value: Operator specific

Note: In order to enable Mobile IP to Simple IP fallback, NAI Entry Indexes used in SIP and MIP User Profiles must be the same.

### Profile Information: Applications

Definition: This parameter specifies which applications are associated with this profile. One, multiple, or all applications may be associated with a profile. The applications shall use the profile with the “unspecified” bit set in the Applications bit mask if they are not present in any other profile.

Allowed Range:

* Unspecified
* MMS
* WAP Browser
* BREW
* Java
* LBS
* Terminal

Typical Value: Unspecified

### Profile Information: Priority

Definition: Application priority. This parameter specifies the priority the device may use when launching a particular application.

Allowed Range:

Value Priority

0 Highest priority category

1 Second highest priority category (lower than 0; higher than 2+)

2 Third highest priority category (lower than 0 or 1; higher than 3+)

255 Lowest priority

Typical Value: Operator specific

### Profile Information: Data Rate Mode

Definition: This parameter specifies whether the data rate mode for a particular profile is low speed, medium speed or high speed

Allowed Range:

* Low
* Medium
* High

Typical Value: High

### Profile Information: Data Bearer

Definition: This parameter specifies the data bearer to be used for a particular profile.

Allowed Range:

* Hybrid 1xEV-DO/1x
* 1x Only
* 1xEV-DO Only

Typical Value: Hybrid 1xEV-DO/1x

## EFSIPPAPSS [6F50]

Definition: This is the Simple IP PAP password.

Size (bytes): Variable

### **Profile Information: PAP SS**

Definition: This parameter specifies the simple IP PAP Shared Secret the operator uses for PDSN authentication.

Allowed Range: Up to 31 bytes of binary data.

Typical Value: Operator specific

Note: The password of choice should be a unique NAI and password for each subscription. A randomized password should also be selected, preferably of size 16 bytes.

## EFSIPCHAPSS [Hidden]

Definition: This EF specifies the Simple IP CHAP shared secret.

Size (bytes): Operator/R-UIM vendor specific

### **Profile Information: CHAP SS**

Definition: This parameter specifies the Simple IP CHAP SS value used by an operator for PDSN authentication.

Allowed Range: 31 bytes of binary data.

Typical Value: Operator specific

# 3GPD – Mobile IP

## EFMIPCAP [6F4B]

Definition: This parameter specifies the MobileIP Capability Parameter Block defined in [[CS0016-C](#CS0016C)].

The operator should allocate n38 in EF\_CST and provision the following parameters, if 3GPD Mobile IP service is supported on its network.

Size (bytes): 5 (fixed)

### MIP Max Number of NAIs

Definition: This parameter specifies the maximum number of NAIs used by an operator.

Allowed Range: 0–15

Typical Value: 1

### MIP Max NAI Length

Definition: This parameter specifies the maximum length of the Mobile IP NAI. This value specifies the maximum memory allocated in the card for this field.

Allowed Range: 0–255

Typical Value: 255

### MIP Max MN-AAA SS Length

Definition: This parameter specifies the maximum length, in units of octet, of the shared secret data (MN-AAA) supported by the R-UIM. If the SS length is greater than 16 bytes, it needs to be ensured that the card vendor supports this SS length. This value specifies the maximum memory allocated in the card for this field.

Allowed Range: 0–31

Typical Value: 31

### MIP MN-AAA Authentication Algorithm

Definition: This parameter specifies the authentication algorithm (MN-AAA) used by the mobile station to authenticate itself to the PDSN/Foreign Agent (FA).

Allowed Range: MD5

Typical Value: MD5

### MIP Max MN-HA SS Length

Definition: Specifies the maximum length, in units of octet, of the shared secret data (MN-HA) supported by the R-UIM. This value specifies the maximum memory allocated in the card for this field.

Allowed Range: 0–31

Typical Value: 31

### MIP MN-HA Authentication Algorithm

Definition: This parameter specifies the authentication algorithm (MN-HA) used by the mobile station to authenticate itself to the Home Agent.

Allowed Range: MD5

Typical Value: MD5

## EFMIPSP [6F4F]

Definition: This EF specifies the MobileIP Status Parameters Block defined in [[CS0016-B](#CS0016B)]. If service n38 is allocated, this EF shall be present.

Size (bytes): Variable

* Typical Size (bytes): 1 (assuming 1 MIP profile)
* Maximum Size (bytes): 8 (assuming 15 MIP profiles)

### Active NAI Entry Index

Definition: This parameter specifies the Active MobileIP NAI entry index.

Allowed Range: 0–15

Typical Value: 0

## **EFMIPUPP [6F4D]**

Definition: This parameter specifies the Mobile IP User Profiles Profile Parameter Block defined in [[CS0016-B](#CS0016B)].

Size (bytes): Variable

### MIP Registration Max Re-tries

Definition: This parameter specifies the maximum number of retries for Mobile IP Registration.

Allowed Range: 0–3

Typical Value: 3

Note: The maximum time until a new Registration Request is sent should not be greater than the requested Lifetime of the Registration Request.

### MIP Registration First Retry Timeout

Definition: This parameter specifies the amount of time elapsed between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply.

Allowed Range: 1–8, in units of 250ms

Typical Value: 8

Note: 1–8 should be provisioned on R-UIM as 0–7, and the device will derive a timeout value by adding 1000ms to this timeout value per [[RFC 2002](#RFC2002)].

### MIP Re-Registration Threshold

Definition: This specifies the time before the lifetime expiration when the mobile attempts re-registration. It is the pre-lifetime expiration re-registration timer.

Allowed Range: 0–63 minutes

Typical Value: 63

Note: Registration lifetime is the number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

### Profile Information: NAI Entry Index

Definition: This parameter specifies the number of profiles used for mobile IP.

Allowed Range: 0–15

Typical Value: The value depends on the number of profiles an operator uses for its applications.

Note: In order to enable Mobile IP to Simple IP fallback, NAI Entry Indexes used in SIP and MIP User Profiles must be the same.

### Profile Information: NAI

Definition: This parameter specifies the actual Network Address Identifier assigned by the operator.

Allowed Range: Up to 255 ASCII characters

Typical Value: Operator specific

### Profile Information: T\_BIT (Reverse Tunneling flag)

Definition: A reverse tunnel is a tunnel that starts at the mobile node’s care-of address and terminates at the home agent. This parameter specifies whether reverse tunneling is required or not. Reverse tunneling support is added directly into the Registration Request (RRQ) by using one of the "rsvd" bits naming it as T bit. If a foreign or home agent that does not support reverse tunnels receives a request with the “T” bit set, the Registration Request fails.

Allowed Range:

* True
* False

Typical Value: True

### Profile Information: Home Address

Definition: This parameter specifies the IP address that is assigned for an extended period of time to a mobile node. It remains unchanged, regardless of where the node is attached to the Internet.

Allowed Range:

Typical Value: Operator specific

### Profile Information: Primary Home Agent

Definition: This parameter specifies the IP address of the mobile node’s primary home agent. A home agent is a router on a mobile node’s home network that tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

Allowed Range:

Typical Value: Operator specific

### Profile Information: Secondary Home Agent

Definition: This parameter specifies the IP address of the mobile node’s secondary home agent in the form of network byte code.

Allowed Range:

Typical Value: Operator specific

### Profile Information: MN-AAA Auth Algorithm

Definition: This parameter specifies the authentication algorithm used to calculate the Mobile IP MN-AAA Authentication Extension.

Allowed Range:

* None
* MD5

Typical Value: MD5

### Profile Information: MN-AAA SPI Indicator

Definition: This parameter specifies the indicator of the Security Parameter Index (SPI) between MN and AAA.

Allowed Range:

* None
* 32-bit number

Typical Value: Operator specific

Note: SPI is an index identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association.

### Profile Information: MN-HA Auth Algorithm

Definition: This parameter specifies the authentication algorithm used to calculate the Mobile IP MN-HA Authentication Extension, as defined in IETF [[RFC 2002](#RFC2002)].

Allowed Range:

* None
* MD5

Typical Value: MD5

### Profile Information: MN-HA SPI

Definition: This parameter is an indicator of SPI between MN and HA.

Allowed Range:

* None
* 32-bit number

Typical Value: Operator specific

## **EFMIPUPPExt [6F80]**

Definition: This EF specifies the additional parameters for MobileIP User Profiles in order to fully support the feature of multiple profiles for MobileIP.

Size (bytes): Variable

* Typical EF Size (bytes): 7 bytes (assumes the common usage of one profile for all applications)
* Maximum EF Size (bytes): 98 bytes (assumes a wildly unlikely usage of 15 different profiles)

### NUM\_NAI

Definition: This parameter specifies the number of MIP profiles.

Allowed Range: 0–15

Typical Value: 1

### Profile Information: NAI Entry Index

Definition: This parameter specifies the number of profiles used for…

Allowed Range: 0–15

Typical Value: 0

Note: In order to enable Mobile IP to Simple IP fallback, NAI Entry Indexes used in SIP and MIP User Profiles must be the same.

### **Profile Information: Applications**

Definition: This parameter indicates which applications are associated with this profile. One, multiple, or all applications may be associated with a profile.

Allowed Range:

* Unspecified
* WAP Browser
* BREW
* Java
* LBS
* Terminal

Typical Value: Unspecified

### **Profile Information: Priority**

Definition: This parameter specifies the application priority associated with a particular profile.

Allowed Range: 0 (highest) to 255 (lowest)

Typical Value: 0

### **Profile Information: Data Rate** Mode

Definition: This parameter specifies the data rate to be used for a particular profile.

Allowed Range:

* Low
* Medium
* High

Typical Value: High

### **Profile Information: Data** Bearer

Definition: This parameter specifies the data bearer to be used for a particular profile.

Allowed Range:

* Hybrid 1xEV-DO/1x
* 1x Only
* 1xEV-DO Only

Typical Value: Hybrid 1xEV-DO/1x

## **EFMIPSS [Hidden]**

Definition: This EF specifies the password for Mobile IP.

Size (bytes): Vendor specific

### Profile Information: MN-AAA Shared Secret

Definition: This parameter specifies the key MN-AAA key used to compute the challenge response to the challenge received in the agent advertisement message. This is included in the authentication extension of the RRQ and must be coordinated and provisioned in both the mobile and the AAA server.

Allowed Range: up to 31 bytes of binary data

Typical Value: Operator specific

### Profile Information: MN-HA Shared Secret

Definition: This parameter specifies the shared key used by the mobile and the message contents to compute an authenticator value, which is included in this MN-HA authentication extension. Upon receiving the RRQ, the HA queries the HAAA to obtain the MN-HA shared key. Using its MN-HA shared key and the message contents, the HA calculates an authenticator value and compares this calculated value to the one provided by the mobile. Upon successful validation, the MIP tunnel is established, and the HA returns a registration reply (RRP) to the mobile indicating that MIP registration has been accepted.

Allowed Range: up to 31 bytes of binary data

Typical Value: Operator specific

## EFMIPFlags [6F78]

Definition: This EF specifies the configuration flags for Mobile IP.

Size (bytes): 1 (fixed)

### MIP 2002bis MN-HA Authentication

Definition: This parameter specifies the MN-HA authentication that will include the SPI in the authenticator calculation.

Allowed Range:

* True
* False

Typical Value: True

### MIP Pre-Rev 6 Handoff Optimization

Definition: This parameter specifies whether Point-to-Point (PPP) re-sync will be performed proactively between the ME and PDSN to maintain correct PPP framing and to avoid not updating PPP framing and PDSN-HA binding when performing an inter-PDSN handoff by a ME during a MIP session, which may result in reconnection to a latent A10/A11 (R-P) connection. The QUALCOMM cdma2000 1X optimized dormant handoff algorithm (QCODH) addresses this by detecting the problematic scenario and proactively initiating a PPP resync between the mobile station and PDSN with zombie PPP state to maintain correct PPP framing.

Allowed Range:

* True
* False

Typical Value: True

Note: When set to True, the mobile will actively renegotiate PPP and reregister MIP when it detects that it might be returning to a previously visited PDSN. This may be enabled or disabled by the carrier to match the capability of their deployed network to address zombie PPP.

### MIP PPP Re-sync During Hand-Down from 1xEV-DO Rev 0 to 1X

Definition: This parameter specifies whether PPP resync on hand-down from High Data Rate (HDR) to 1X for a MIP call will be done or not.

Allowed Range:

* True
* False

Typical Value: False

### MIP Re-Registration – Data Transfer to Extend MIP Address Lifetime

Definition: This parameter specifies the need for MIP Re-Registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime. If this is set, the MIP and PPP sessions for the mobile will be dropped if the link is inactive for the entire duration of a MIP registration. In other words, re-registration will not be performed unless user data (not including Mobile IP registration traffic) is transferred during the registration lifetime.

Allowed Range:

* True
* False

Typical Value: False

Note: When set to False, the idle data sessions will remain connected indefinitely. The mobile will periodically send Registration Requests to the PDSN to refresh the mobile’s MIP registration.

<page left blank intentionally>

# 3GPD – IPv6

## EFIPV6CAP [6F77]

Definition: This EF specifies information about IPv6 capabilities.

The operator should allocate n31 in EF\_CST and provision the following parameters, if IPv6 is supported on its network.

Size (bytes): 21 (fixed)

### IPv6 Initial Neighbor Solicitation Delay Time

Definition: This parameter identifies the time the mobile waits after the Interface ID (IID) has been negotiated during IPv6CP between the ME and the PDSN before sending a Router Solicitation (RS) in an attempt to receive a Router Advertisement (RA).

Allowed Range: 16-bit number, in units of 100ms

Typical Value: 500ms

Note: Neighbor Solicitation is sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address.

### IPv6 Solicitation Interval

Definition: This parameter specifies the amount of time the mobile waits before sending a subsequent Router Solicitation (RS) after a previous one.

Allowed Range: 16-bit number, in units of 100ms

Typical Value: 1000ms

Note: RSs are sent by the mobile to solicit the router, e.g., PDSN/GGSN, for an IPv6 prefix (RA).

### IPv6 Re-Solicitation Interval

Definition: This parameter specifies the amount of time between router solicitations sent while re-soliciting for a new RA. This interval applies only after the mobile has previously received one valid RA and is soliciting for a new one to renew the lifetimes of the current prefix or retrieve a non-deprecated prefix.

Allowed Range: 16-bit number, in units of 100ms

Typical Value: 2000ms

### IPv6 Maximum Solicitation Attempts

Definition: This parameter specifies the number of solicitation attempts to make for initial IPv6 session setup, when a RA is not received in response before giving up IPv6 autoconfiguration.

Allowed Range: 16-bit number

Typical Value: 3

Note: If RA is not received and the ME has already transmitted the maximum solicitation attempts, then the ME fails and tears down the IPv6 session. RAs are sent by the router to advertise IPv6 prefixes, one of which is used by the mobile. They are sent at periodic intervals preset by network administrators, as well as in response to an RS sent by the mobile.

### IPv6 Maximum Re-Solicitation Attempts

Definition: This parameter specifies the number of solicitation attempts to make to re-solicit for a new RA.

Allowed Range: 16-bit number

Typical Value: 3

### IPv6 Pre-RA Expiry Re-Solicitation Time

Definition: This parameter specifies the amount of time before the current RA expires to begin re-solicitations.

Allowed Range: 16-bit number, in units of 100ms

Typical Value: 0

### IPv6 IID

Definition: This parameter specifies the 64-bit IID. It is very likely to be unique on the link or zero, if a good source of uniqueness cannot be found. These are either derived from an IEEE identifier or generated through some other technique.

Allowed Range: 64-bit binary data

Typical Value: Operator specific

Note: The IID is the last 64 bits of the IPv6 addresses that is formed by a combination of prefix and interface ID, represented in the following format:

2002:c023:9c17:314:bceb:acb9:5d51:4045

The IPv6 prefix is represented by the first 64 bits (2002:c023:9c17:314) and can also be represented in the following format:

2002:c023:9c17:314::/64.

IIDs can be selected to be random; in which case, a 64-bit IID is generated by the mobile at power-up or can be pre-specified during provisioning of the mobile. Neither of these IIDs are guaranteed to be used, of course, if there is a collision between the two negotiated IIDs during IPv6CP negotiation [[RFC 2472](#RFC2472)]. If there is a collision, both the mobile and PDSN must generate another random IID.

### IPv6 Enabled

Definition: This parameter specifies whether IPv6 is enabled or disabled.

Allowed Range:

* True
* False

Typical Value: False

Note: If the CST indicates via n31 that IPv6 is enabled, then this shall be enabled.

### Failover from IPv6 to IPv4 Enabled

Definition: This parameter specifies whether failover from IPv6 to IPv4 is allowed or not. This feature is not supported.

Allowed Range:

* True
* False

Typical Value: False

### IPv6 PDSN as Proxy DNS Server

Definition: This parameter specifies whether PDSN acts as the proxy IPv6 Domain Name Server (DNS) or not. When enabled, the mobile forwards all DNS requests to the PDSN. The PDSN forwards requests to the appropriate DNS server. This parameter is meaningful only if the primary and secondary DNS server addresses are not available.

Allowed Range:

* True
* False

Typical Value: False

Note: This is only applicable if the parameter IPv6, as specified in Section 13.1.8 of this document, is enabled (set to True).

<page left blank intentionally>

# 

# HRPD

## EFHRPDCAP [6F56]

Definition: This EF specifies the High-Rate Packet Data (HRPD) Access Authentication Capability Parameters as defined in Section 3.5.8.12 of [[CS0016-C](#CS0016C)].

The operator should allocate n5 in EF\_CST and provision the following parameters, if HRPD service is supported on its network.

Size (bytes): 4 (fixed)

### HRPD Maximum NAI Length

Definition**:** This parameter specifies the maximum length for NAI for HRPD access authentication, thus specifying the maximum memory allocated in the card for this field.

Allowed Range: 0−255

Typical Value: 255

### HRPD Maximum SS Length

Definition: This parameter specifies the maximum length of the Shared Secret Data for HRPD access authentication, thus specifying the maximum memory allocated in the card for this field.

Allowed Range: 0−31

Typical Value: 31

### HRPD Authentication Algorithms

Definition: This parameter specifies the authentication algorithm used for HRPD access authentication.

Allowed Range: CHAP

Typical Value: Always CHAP

## EFHRPDUPP [6F57]

Definition: This EF specifies the HRPD Access Authentication User Profile Parameters Block defined in Section 3.5.8.13 of [[CS0016-C](#CS0016C)].

Size (bytes): Variable

### HRPD Profile NAI

Definition: This parameter specifies the Network Access Identifier (NAI), encoded in an ASCII string specified by an operator used for AN-AAA ( A12 ) authentication. The NAI is of the form user@realm.

Allowed Range: up to 255 ASCII characters

Typical Value: Operator specific

Note: The NAI should be chosen and managed using procedures that minimize the likelihood of compromise.

### HRPD Profile Authentication Algorithm

Definition: This parameter specifies the authentication algorithm used for access authentication

Allowed Range: CHAP

Typical Value: CHAP

## EFHRPDSS [HIDDEN]

Definition: This EF specifies the password for HRPD access authentication.

Size (bytes): 31 (fixed)

### **HRPD SS**

Definition: This parameter specifies the password the operator assigns for AN-AAA HRPD access authentication.

Allowed Range: up to 31 bytes of binary data

Typical Value: Operator specific

Note: Even if CHAP is being used in an operator’s network for SIP PPP authentication, a separate CHAP secret key must be provisioned in the mobile device to support A12 authentication (i.e., the device will not use the SIP PPP CHAP secret key for A12 authentication even if the values are the same). The password should be chosen and managed using procedures that minimize the likelihood of compromise (i.e., it should be cryptographically strong). The password choice should be unique and randomized for each subscription, preferably of size 16 bytes.

# WAP Browser

## EFWAPBrowserCP [6F7B]

Definition: This EF identifies WAP Browser connectivity parameters.

The operator should allocate n21 in EF\_CST and provision the following parameters, if WAP service is supported on its network,

Multiple sets of WAP Browser Connectivity Parameters may be configured. If so, multiple instances of the following fields shall be provided.

Size (bytes): Variable

Typical EF Size (bytes): 348 bytes (assumes two Connectivity Parameters TLV objects with 70 bytes of Home URL and 104 bytes for gateway information each)

### Domain Name

Definition: This parameter specifies the WAP Browser Connectivity Parameters: PXADDR-FQDN in WAP.

Allowed Range: Fully qualified domain name

Note: This may be used instead of Address & Address Type (i.e., enables DNS lookup of WAP gateway IP address).

### Address [PXADDR]

Definition: This parameter specifies that PXADDR can store addresses of different kinds, for example an IP address or a SME number.

Note: This parameter is not required when the operator is using domain name (as in Section 15.1.1).

Allowed Range: Digits or characters

### Address Type [PXADDRTYPE]

Definition: The parameter PXADDRTYPE indicates the format and the interpretation of the PXADDR attribute. The PXADDRTYPE can indicate an IP address, a phone number according to the E164 scheme, or a generic alphanumeric address format. This parameter MUST be supported by the WAP client. This parameter is not needed if the operator is using domain name.

Allowed Range:

* IPv4
* IPv6
* E164
* Alpha

Typical Value: IPv4

### Port Number [PORTNBR]

Definition: This parameter contains the value of the port number. The port number must be given as a decimal number and must fit within the range of a 16-bit unsigned integer. The PORTNBR must be unique within its enclosed structure, i.e., within the PXLOGICAL or the PXPHYSICAL characteristic.

If the port number is well known, then the service behind the port is implied and the parameter SERVICE may be omitted. If the port number is not well known, then no service is implied and the service behind the port is defined in parameter SERVICE. If the port number is not well known and the parameter SERVICE is omitted, then the ME must assume a service according to its preferences.

If the parameter SERVICE is present, then the definition in the SERVICE parameter overrides the implicit meaning.

This parameter must be supported by the WAP client.

Allowed Range: 0−65535

Typical Value: Operator Specific

### Service

Definition: The SERVICE parameter specifies which service is available behind this particular port number. This parameter must be supported by the WAP client.

Allowed Range: 0 or more of the following:

* WAP connection-less
* WAP
* WAP secure connection-less
* WAP secure
* WAP WTA secure
* WAP WTA secure connection-less
* OTA-HTTP (push) TO-TCP
* OTA-HTTP secure (push) TO-TCP
* OTA-HTTP (push) PO-TCP
* OTA-HTTP secure (push) PO-TCP

Typical Value: WAP

### Authentication Type [PXAUTH-TYPE]

Definition: The PXAUTH-TYPE indicates the proxy authentication method: HTTP proxy authentication or WTLS methods.

This parameter does not indicate the actual authentication method to use when connecting to the proxy, but links the authentication parameters PXAUTH-ID and PXAUTH-PW to an authentication method. The PXAUTH-TYPE must be unique within its enclosed structure, i.e., within the PXLOGICAL characteristic.

Allowed Range:

* HTTP-BASIC
* HTTP-DIGEST
* WTLS-SS

Typical Value: HTTP-BASIC

### Authentication ID [PXAUTH-ID]

Definition: The PXAUTH-ID indicates the proxy authentication identifier. If it is missing then the Global ID of the device should be used (see Section 6.4 of [[WAP-183](#WAP183)]. The global identifier can be defined, for example, using the ClientIdentity characteristic.

Allowed Range: Binary data

Typical Value: Operator specific

### Authentication Password [PXAUTH-PW]

Definition: The PXAUTH-PW indicates the proxy authentication secret. The usage of the parameter is defined by the PXAUTH-TYPE.

Allowed Range: Binary data

Typical Value: Operator specific

### Home URL

Definition: This parameter specifies the URL of the browser’s home page.

Allowed Range: URL text string

Typical Value: Operator specific

## EFWAPBrowserBM [6F7C]

Definition: This EF specifies the WAP Browser Bookmarks the operator wants to configure.

Multiple bookmarks may be configured. If so, multiple instances of the following fields shall be provided.

Size (bytes): Variable

Typical EF Size (bytes): 500 bytes (assumes five bookmarks with 100 bytes for each TLV object)

### Bookmark URL

Definition: This parameter specifies the URL of the WAP Browser Bookmarks.

Allowed Range: URL text string

Typical Value: Operator specific

### Bookmark Name

Definition: This parameter specifies the descriptive name of the bookmark.

Allowed Range: ASCII string

Typical Value: Operator specific

# MMS

## EFMMSICP [6F67]

Definition: This EF specifies MMS connectivity parameters.

The operator should allocate n40 in EF\_CST and provision the following parameters, if MMS service is supported on its network.

Multiple sets of MMS connectivity parameters may be configured. If so, each set should be provided with all associated fields described below.

Size (bytes): Variable

### Implementation

Definition: This parameter specifies the implementation. For OMH, the WAP implementation of MMS is supported.

Allowed Range:

* WAP
* SIP
* I-MAP

Typical Value: WAP

Note: Always WAP for OMH.

### Relay/Server Address

Definition: This parameter specifies the MMS Relay/Server address

Allowed Range: This is the URL

Typical Value: Operator specific

### WAP Domain Name

Definition: This parameter specifies MMS Connectivity Parameters: PXADDR-FQDN in WAP.

Allowed Range: Fully qualified domain name

Typical Value: Operator specific

Note: This may be used instead of Address & Address Type (i.e., enables DNS lookup of the WAP gateway IP address).

### WAP Address

Definition: This parameter specifies that PXADDR can store addresses of different kinds, for example an IP address or a SME number.

Allowed Range: Digits or characters

Typical Value: Operator specific

### WAP Address Type

Definition: The parameter PXADDRTYPE indicates the format and the interpretation of the PXADDR attribute. The PXADDRTYPE can indicate an IP address, a phone number according to the E164 scheme, or a generic alphanumeric address format. This parameter MUST be supported by the WAP client. This parameter is not needed if the Operator is using domain name.

Allowed Range:

* IPv4
* IPv6
* E164
* Alpha

Typical Value: IPv4

Note: This parameter is not needed if the operator is using domain name.

### WAP Port Number

Definition: This parameter contains the value of the port number. The port number must be given as a decimal number and must fit within the range of a 16-bit unsigned integer. The PORTNBR must be unique within its enclosed structure, i.e., within the PXLOGICAL or the PXPHYSICAL characteristic.

If the port number is well known, then the service behind the port is implied and the parameter SERVICE may be omitted. If the port number is not well known, then no service is implied and the service behind the port is defined in parameter SERVICE. If the port number is not well known and the parameter SERVICE is omitted, then the ME must assume a service according to its preferences.

If the parameter SERVICE is present, then the definition in the SERVICE parameter overrides the implicit meaning.

This parameter MUST be supported by the WAP client.

Allowed Range: 0–65535

Typical Value: Operator specific

### WAP Service

Definition: The SERVICE parameter specifies which service is available behind this particular port number. This parameter must be supported by the WAP client.

Allowed Range: 0 or more of the following:

* WAP connection-less
* WAP
* WAP secure connection-less
* WAP secure
* WAP WTA secure
* WAP WTA secure connection-less
* OTA-HTTP (push) TO-TCP
* OTA-HTTP secure (push)
* TO-TCP
* OTA-HTTP (push) PO-TCP
* OTA-HTTP secure (push) PO-TCP

Typical Value: WAP secure

### WAP Authentication Type

Definition: The PXAUTH-TYPE indicates the proxy authentication method: HTTP proxy authentication or WTLS methods.

This parameter does not indicate the actual authentication method to use when connecting to the proxy, but links the authentication parameters PXAUTH-ID and PXAUTH-PW to an authentication method. The PXAUTH-TYPE must be unique within its enclosed structure, i.e., within the PXLOGICAL characteristic.

Allowed Range:

* HTTP-BASIC
* HTTP-DIGEST
* WTLS-SS

Typical Value: HTTP-BASIC

### WAP Authentication ID [PXAUTH-ID]

Definition: The PXAUTH-ID indicates the proxy authentication identifier. If it is missing then the Global ID of the device should be used (see Section 6.4) of [[WAP-183](#WAP183)]. The global identifier can be defined, for example, using the ClientIdentity characteristic.

Allowed Range: Binary data

Typical Value: Operator specific

### WAP Authentication Password [PXAUTH-PW]

Definition: The PXAUTH-PW indicates the proxy authentication secret. The usage of the parameter is defined by the PXAUTH-TYPE.

Allowed Range: Binary data

Typical Value: Operator specific

### WAP Authentication Mechanism

Definition: This parameter specifies the MMS Connectivity Parameters: MMS Authentication Mechanism.

Allowed Range:

* CRAM-MD5
* HTTP Digest (MD5)
* HTTP Digest (MD5-sess)
* HTTP Digest (AKAv1-MD5)
* HTTP Digest (AKAv1-MD5-sess)
* SASL DIGEST
* SASL OTP
* SASL GSSAPI

Typical Value: HTTP Digest (MD5)

## EFMMSConfig [6F7E]

Definition: This EF specifies the operator-specific configuration that the MMS client on the device is to use when connecting to the MMS service.

Size (bytes): 8 (fixed)

### MMS Max Message Size

Definition: This parameter specifies the maximum MMS message size allowed by the operator.

Allowed Range: 0 to 232-1 bytes

Typical Value: 300–600 Kbytes

### MMS Retry Times

Definition: This parameter specifies the number of retries for sending MMS.

Allowed Range: 0–255 retries

Typical Value: 3

### MMS Retry Interval

Definition: This parameter specifies the MMS Retry interval before the next retry can be made.

Allowed Range: 0–255 seconds

Typical Value: 20–30 seconds

### MMS Center Timeout

Definition: This parameter specifies the number of seconds for the device to wait for response from the Mobile Messaging Service Center (MMSC) before declaring it as an MMSC timeout.

Allowed Range: 0–65535 seconds

Typical Value: 30 – 60 seconds

<page left blank intentionally>

# Java Catalog

## EFJDL [6F7F]

Definition: This EF specifies the JAVA download portal URL.

Size (bytes): Variable

Typical EF Size (bytes): 70 bytes

### Java Download URL

Definition: This parameter specifies the URL of the Java download portal.

**Allowed Range:** URL text string

Typical Value: N/A

Note: If WAP Browser Home URL is used for Java download, the same URL should be provisioned here.

<page left blank intentionally>

# BREW Catalog

## EFBREWDownload [6F81]

Definition: This EF specifies the configuration for enabling BREW download services.

The operator should allocate n21 in EF\_CST and provision the following parameters, if BREW service is supported on its network.

Size (bytes): 207 (fixed)

### BREW Carrier ID

Definition: This parameter specifies the BREW Carrier ID.

Allowed Range: 32-bit unsigned integer

Typical Value: Operator specific

### BREW A-Key

Definition: This parameter specifies the BREW A-key to be used.

Allowed Range: 64-bit binary data

Typical Value: False

### BREW Download Server

Definition: This parameter specifies either the IP Address or Domain Name associated with the BREW Download Server. The device automatically identifies whether the contents of this field are an IP address or domain name; in the case of domain name, DNS resolution is performed to obtain the IP address. If there is more than one server address, they may be specified with comma delimiters (e.g., address1,address2).

Allowed Range: Up to 64 bytes of ASCII characters

Typical Value: Operator specific

### BREW Use A-Key Flag

Definition: This flag indicates to the BREW downloader (for example, MobileShop) whether to use AKEY or BKEY for mutual authentication/validation with the ADS server.

Allowed Range:

* True
* False

Typical Value: False

### BREW Use MIN for SID Flag

Definition: This flag informs MobileShop to use the MIN for the SID as the default. This allows the operator to avoid the provisioning of the SID at the point of sale. Instead, the value of the SID will be that of the MIN, so any existing mechanism for setting the MIN (operator keying it in by hand, OTASP, etc.) will effectively set the SID as well.

Allowed Range:

* True
* False

Typical Value: True

### BREW Prepaid Flag

Definition: This flag informs BREW that this is a prepay phone and that purchases made by using MobileShop need to have the device user’s account balance checked for sufficient funds before allowing him or her to download an application. When the application downloads successfully, the device user’s account is debited.

Allowed Range:

* True
* False

Typical Value: False

### BREW No Auto Ack Flag

Definition: If true, do not force ACKs until the user runs MobileShop.

Allowed Range:

* True
* False

Typical Value: False

### BREW App Encoding Flag

Definition: This flag indicates whether to use Subscriber ID or ESN for application encoding. Before executing applications, BREW will ensure that the SID of the current handset matches the SID for which this application was downloaded.

Allowed Range:

* Use SID
* Use ESN

Typical Value: Use SID

Note: This should not be set for handsets with R-UIM cards.

### BREW Validate All Apps Flag

Definition: This parameter specifies whether the subscription applications only or both subscription and non-subscription applications will be verified; that is, a check is performed to determine if the SID or ESN of the current handset matches the handset on which the application was downloaded.

Allowed Range:

* True
* False

Typical Value: True

Note: If true, all applications are validated, not just SSN applications. With this flag set to False, only the subscription applications will be verified; that is, a check is performed to determine if the SID or ESN of the current handset matches the SID or ESN of the handset on which the application was downloaded.

### BREW RUIM Delete Override Flag

Definition: This flag allows the user to delete applications owned by another user. By default, BREW will allow deletion of BREW applications only by the original owner; that is, the owner who downloaded the applications. To override this behavior and to allow one R-UIM user to delete applications owned by another, this flag must be set.

Allowed Range:

* True
* False

Typical Value: True

### BREW Auto Upgrade Flag

Definition: This parameter specifies whether to perform an automatic upgrade when new uses are purchased.

Allowed Range:

* True
* False

Typical Value: True

Note: If a user buys an application and the need arises for it to be renewed, any available, new upgrade to this software will automatically be upgraded.

### BREW Launch when MOD\_ACK\_DISABLED Is Set Flag

Definition: This parameter determines whether an application starts, If true, an application with flag MOD\_ACK\_DISABLE set is not started.

Allowed Range:

* True (do not start)
* False

Typical Value: False

### BREW Download Auth Policy

Definition: This parameter specifies the operator’s authentication policy for BREW Download.

Allowed Range:

* No authentication required
* SID sent to ADS
* Prompt user for text “key”
* Prompt user for numeric “key”

Typical Value: SID sent to ADS

## EFBREWTSID [6F82]

Definition: This EF specifies the Teleservice ID to be used in BREW-directed SMS messages.

Size (bytes): 4 (fixed)

### **BREW Teleservice ID**

Definition: This parameter specifies the Teleservice ID to be used in BREW-directed SMS messages.

Allowed Range: 32-bit number

Typical Value: 4098 (CMT-95)

## EFBREWSID [6F83]

Definition: This EF specifies information about the BREW Subscriber ID.

Size (bytes):

* Typical EF Size (bytes): 32 bytes
* Maximum EF Size (bytes): 128 bytes

### BREW SID

Definition: This parameter specifies information about the BREW Subscriber ID.

Allowed Range: ASCII string

Typical Value: Operator specific

## EFBREWAEP [6F89]

Definition: This EF specifies the BREW Application Execution Policy.

Size (bytes): 1 (fixed)

### **BREW App Execution Policy**

Definition: This parameter specifies the BREW Application Execution Policy.

Allowed Range:

* TRUE-BREW signed applet only
* Carrier-signed applet only
* TRUE-BREW and carrier-signed
* TRUE-BREW or carrier-signed

Typical Value: TRUE-BREW or carrier-signed

<page left blank intentionally>

# Location Based Services

## EFLBSXTRAConfig [6F84]

Definition: This EF contains the configuration of the LBS XTRA client on the device. If service n24 (LBS) is allocated, this EF shall be present.

The operator should always allocate n24 in EF\_CST and provision the following parameters, whether LBS service is supported on its network or not, for XTRA to still work.

Size (bytes): 4 (fixed)

### Allow gpsOne XTRA Flag

Definition: This parameter specifies whether gpsOne XTRA is allowed or not. If this feature is enabled, an application resident on the mobile downloads a small data file from gpsOne Xtra server that contains forecasted satellite data valid for up to seven days. This data file is refreshed if it becomes stale. The mobile uses the downloaded data file to make fast(er) GPS fixes.

Allowed Range:

* True
* False

Typical Value: True

### Allow gpsOne XTRA Automatic Download

Definition: This parameter indicates whether to allow gpsOne XTRA Automatic Download or not.

Allowed Range:

* True
* False

Typical Value: False

### gpsOne XTRA Download Interval

Definition: This parameter specifies the number of hours between automatic retrievals of gpsOneXTRAAssistance data from the Internet.

Allowed Range: 1–168 hours

Typical Value: 24 hours

### gpsOne XTRA Download Retries

Definition: This parameter specifies the number of unsuccessful attempts (i.e., retries) made to retrieve gpsOneXTRAAssistance data from the Internet before giving up.

Allowed Range: 0–10

Typical Value: 3

### gpsOne XTRA Download Retry Interval

Definition: This parameter specifies the time (in minutes) between unsuccessful download attempts (i.e., retries).

Allowed Range: 1–120 minutes

Typical Value: 10 minutes

## EFLBSXSURL [6F85]

Definition: This EF contains the XTRA Server URLs for LBS. If service n24 (LBS) is allocated, this EF shall be present.

Size (bytes): Typical EF Size (bytes): 300 bytes (assumes 100 bytes for each URL TLV object)

### Primary XTRA Server URL

Definition: This parameter specifies the XTRA Server URLs for LBS.

Allowed Range: URL text string

Typical Value: <http://xtra1.gpsOneXTRA.net/xtra.bin>

### Primary XTRA Server Name

Definition: This parameter specifies the name for the Primary XTRA Server.

Allowed Range: ASCII text string

Typical Value: Operator specific

### Secondary XTRA Server URL

Definition: This parameter specifies the URL for the Secondary XTRA Server.

Allowed Range: URL text string

Typical Value: <http://xtra2.gpsOneXTRA.net/xtra.bin>

### Secondary XTRA Server Name

Definition: This parameter specifies the name for the Secondary XTRA Server.

Allowed Range: ASCII text string

Typical Value: Operator specific

### Tertiary XTRA Server URL

Definition: This parameter specifies the URL for the Tertiary XTRA Server.

Allowed Range: URL text string

Typical Value: <http://xtra3.gpsOneXTRA.net/xtra.bin>

### Tertiary XTRA Server Name

Definition: This parameter specifies the name for the Tertiary XTRA Server.

Allowed Range: ASCII Text string

Typical Value: Operator specific

## EFLBSV2Config [6F86]

Definition: This parameter specifies the configuration of the LBS V2 client on the device. If service n24 (LBS) is allocated, this EF shall be present.

Size (bytes): 1 (fixed)

### LBS V2 Allow Sending System Parameter Info Message

Definition: This parameter indicates whether to enable the Allow Sending System Parameter Info Message. The System Parameter Info message contains the serving base station information (SID, NID, Base ID, Frequency, PN, etc.).

Allowed Range:

* True
* False

Typical Value: True

### LBS V2 Allow Seed Position Use

Definition: This parameter indicates whether to allow Seed Position Use. If this item is enabled, the gpsOne engine will trust and use the broadcasted tower location as a seed position.

Allowed Range:

* True
* False

Typical Value: True

### LBS V2 Allow Dynamic Mode

Definition: This parameter indicates whether to allow Dynamic Mode. If this item is enabled, fallback from MS-Based to Standalone mode, and vice versa, is allowed.

Allowed Range:

* True
* False

Typical Value: True

## EFLBSV2PDEADDR [6F87]

Definition: This EF specifies information pertaining to the Position Determination Entity (PDE) Server IP address and Port Number for V2 LBS. If service n24 (LBS) is allocated, this EF shall be present.

Size (bytes): Typical EF Size (bytes): 100 bytes (assumes a 96-byte Domain Name)

### LBS V2 Address Type

Definition: This parameter identifies the type of address contained in the V2 LBS PDE Address Information field.

Allowed Range:

* Domain name
* IPv4 address
* IPv6 address

Typical Value: IPv4

### LBS V2 PDE Address

Definition: This parameter specifies the address of the PDE server. The type of PDE server address contained in this field is determined by the Address Type field above.

Allowed Range: ASCII string

Typical Value: Operator specific

### LBS V2 PDE Port Number

Definition: This parameter specifies the port Number for the V2 LBS PDE Server.

Allowed Range: 0–65535

Typical Value: Operator specific

## EFLBSV2MPCADDR [6F88]

Definition: This parameter specifies the MPC Server IP address and Port Number for V2 LBS. If service n24 (LBS) is allocated, this EF shall be present.

Size (bytes): Typical EF Size (bytes): 100 bytes (assumes a 96-byte Domain Name)

### LBS V2 MPC Address Type

Definition: This specifies the type of address contained in the V2 LBS MPC Address Information field.

Allowed Range:

* Domain name (gpsOne needs to perform DNS resolution)
* IPv4 address
* IPv6 address

Typical Value: Operator specific

### LBS V2 MPC Address

Definition: This parameter specifies the type of MPC server address contained in this field, as determined by the Address Type field above.

Allowed Range: 8-bit ASCII (one octet per character) string

Typical Value: Operator specific

### LBS V2 MPC Port Number

Definition: This parameter specifies the Port Number for the V2 LBS MPC Server.

Allowed Range: 0–65535

Typical Value: Operator specific

<page left blank intentionally>

# Terminology

|  |  |
| --- | --- |
| ***Term*** | ***Meaning*** |
| 3GPD | Third Generation Packet Data |
| AAA | Authentication, Authorization and Accounting |
| A-Key | A secret, 64-bit pattern stored in the mobile station and HLR/AC. It is used to generate/update the mobile station’s Shared Secret Data and to validate SPASM. |
| Authentication | A procedure used by a base station to validate a mobile station’s identity. |
| BCD | Binary-Coded Decimal |
| BREW | Binary Runtime Environment for Windows |
| CAVE | Cellular Algorithms for Validation and Encryption |
| CHAP | Challenge Handshake Authentication Protocol |
| DNS | Domain Name Server. Provides translation between domain names and IP addresses |
| EF | Elementary File |
| EMS | Enhanced Short Message Service |
| ESN | Electronic Serial Number |
| FA | Foreign Agent |
| FC | Feature Code |
| GID | Group ID |
| HA | Home Agent |
| HRPD | High Rate Packet Data |
| IID | Interface ID |
| IMSI | International Mobile Station Identity |
| ITU | International Telecommunication Union |
| ITU | International Telecommunication Union |
| LCM | Local Use Mark |
| LMS | Long SMS |
| MCC | Mobile Country Code |
| MDN | Mobile Directory Number |
| ME | Mobile Equipment |
| MIN | Mobile Identification Number |
| MIP | MobileIP |
| MMS | Multimedia Messaging Service |
| MMSC | Multimedia Messaging Service Center |
| MN | Mobile Node |
| MNC | Mobile Network Code |
| MO | Mobile Originated |
| MS | Mobile Station |
| NA | Not Applicable |
| NAI | Network Address Identifier |
| NAM | Number Assignment Module |
| NID | Network Identifier |
| NMSI | National Mobile Subscriber Identity |
| OTA | Over The Air |
| OTAPA | Over-the-Air Parameter Administration. Network initiated OTASP process of provisioning mobile station operational parameters over the air interface |
| OTASP | Over-the-Air Service Provisioning. A process of provisioning mobile station operational parameters over the air interface |
| PAP | Password Authentication Protocol |
| PDSN | Packet Data Serving Node |
| PPP | Point-to-Point |
| RA | Router Advertisement |
| RRP | Registration Reply |
| RRQ | Registration Request |
| RS | Router Solicitation |
| R-UIM | Removable User Identity Module |
| SID | System Identification |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SPASM | Subscriber Parameter Administration Security Mechanism |
| SPC | Service Programming Code |
| SPC | Service Programming Code |
| SPI | Security Parameter Index |
| SPN | Service Provider Name |
| TCP | Transmission Control Protocol |
| WAP | Wireless Application Protocol |
| WTLS | Wireless Transport Layer Security |

<page left blank intentionally>

# 

# References

|  |  |
| --- | --- |
| **[CDG101]** | CDG Reference Document 101, “CDMA Mobile Station LBS Requirements *- V2*,” v1.0, August 22, 2005. See [www.cdg.org](http://www.cdg.org) |
| **[CDG167]** | CDG Reference Document 167, “Open Market Handset (OMH) Device and Network Specification,” v2.0, May 2008. See [www.cdg.org](http://www.cdg.org) |
| **[CDG169]** | CDG Reference Document 169, “Open Market Handsets (OMH) PRI,” v2.1, May 2009. See [www.cdg.org](http://www.cdg.org) |
| **[CR1001-F]** | 3GPP2 C.R1001-F, “Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards,” v1.0. Download at <http://www.3gpp2.org/Public_html/specs/C.R1001-F_v1.0_061211.pdf> |
| **[CS0015-B]** | 3GPP2 C.S0015-B, “Short Message Service (SMS) for Wideband Spread Spectrum Systems,” v2.0, September 2005. Download at <http://www.3gpp2.org/Public_html/specs/C.S0015-B_v2.0_051006.pdf> |
| **[CS0005-A]** | 3GPP2 C.S0005-A, “Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems – Release A Addendum 2,” v6.0, February 2002. Download at <http://www.3gpp2.org/Public_html/specs/C.S0005-A_v6.0.pdf> |
| **[CS0016-B]** | 3GPP2 C.S0016-B, “Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards,” v.1.0, October 25, 2002. Download at <http://www.3gpp2.org/Public_html/specs/C.S0016-B_v1.0.pdf> |
| **[CS0016-C]** | 3GPP2 C.S0016-C (TIA-683C), “Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*,”* v1.0, October 31, 2008. Download at <http://www.3gpp2.org/Public_html/specs/C.S0016-C_v2.0_081031.pdf> |
| **[CS0023-D]** | C.S0023-D, “Removable User Identity Module for Spread Spectrum Systems,” v1.0, June 2009. Download at <http://www.3gpp2.org/Public_html/specs/C.S0023-D_v1.0_R-UIM-090720.pdf> |
| **[CS0024-D]** | C.S0024-D, “cdma2000 High Rate Packet Data Air Interface Specification,” v.3.0, December 2001. Download at <http://www.3gpp2.org/Public_html/specs/C.S0024-0_v3.0.pdf> |
| **[RFC2002]** | IETF RFC 2002, “IP Mobility Support,” October 1996. Go to <http://www.apps.ietf.org/rfc/rfc2002.html> |
| **[RFC2462]** | RFC 2462, “IPv6 Stateless Address Autoconfiguration,” December 1998. Go to <http://www.ietf.org/rfc/rfc2462.txt> |
| **[RFC2472]** | RFC 2472, “IP Version 6 over PPP,” September 2007. Go to <http://tools.ietf.org/rfc/rfc5072.txt> |
| **[RFC3041]** | IETF RFC 3041, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” January 2001. Go to <http://www.apps.ietf.org/rfc/rfc3041.html> |
| **[WAP-183]** | WAP-183-ProvCont-20010724-a, “WAP Provisioning Content,” July 2001. Download at <http://www.openmobilealliance.org/tech/affiliates/wap/wap-183-provcont-20010724-a.pdf> |
| **[XS0016-310-0]** | 3GPP2 X.S0016-310-0 (TIA-934-310), “MMS MM1 Stage 3 Using OMA/WAP,” June 2004. Download at <http://www.3gpp2.org/Public_html/specs/X.S0016-310-0_v2.0_040617.pdf> |

1. Billing, Routing, etc. [↑](#footnote-ref-1)