.

.3GPP2 C.S0016-C

Version 2.0

Date: October 31, 2008

3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards

Release C

COPYRIGHT

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

Revision History

Revision	**Description**	**Date**
C.S0016-0	Release 0	May, 1998
C.S0016-A v2.0	Release A	December 7, 2001
C.S0016-B v1.0	Release B	October 25, 2002
C.S0016-C v1.0	Release C	October 22, 2004
C.S0016-C v2.0	Release C Version 2.0	October 31, 2008

CONTENTS

1 INTRODUCTION 1-1

1.1 General Description 1-1

1.2 Terms and Numeric Information 1-1

1.2.1 Terms 1-1

1.2.2 Numeric Information 1-6

2 MESSAGE TRANSPORT PROTOCOL 2-1

2.1 General 2-1

2.2 Analog Transport Protocol 2-1

2.2.1 *OTASP Data Message* Encapsulation 2-1

2.2.2 *OTASP Data Message* Segmentation 2-2

2.2.3 Mobile Station Procedures 2-4

2.2.3.1 *OTASP Transport Message* Acknowledgment and Re-transmission 2-4

2.2.3.2 Message Transmission 2-5

2.2.3.3 Message Reception 2-5

2.2.3.4 Reverse Voice Channel Message Format 2-8

2.2.3.4.1 *OTASP Transport Message* 2-8

2.2.3.4.2 *OTASP Transport Confirmation Message* 2-10

2.2.4 Base Station Procedures 2-11

2.2.4.1 Message Transmission 2-11

2.2.4.2 Message Reception 2-12

2.2.4.3 Forward Voice Channel Message Format 2-13

2.2.4.3.1 *OTASP Transport Message* 2-13

2.2.4.3.2 *OTASP Transport Confirmation Message* 2-16

2.3 CDMA Transport Protocol 2-17

3 MOBILE STATION PROCEDURES 3-1

3.1 Initial Values and NAM Parameters 3-1

3.2 Initiation of the Programming Procedures 3-2

3.2.1 User-Initiated Procedure 3-2

3.2.2 Network-Initiated Procedure 3-9

3.2.2.1 Initiation of OTAPA in the CDMA Mobile Station Idle State 3-10

3.2.2.2 Connection of the OTAPA Service Option 3-10

CONTENTS

3.2.2.3 Starting the OTAPA session 3-12
3.3 Programming Procedure 3-12
3.3.1 *OTASP Data Message* Processing 3-12
3.3.2 Mobile Station SSD Update and Re-authentication 3-40
3.3.3 Activation of Message Encryption 3-42
3.3.4 Activation of Voice Privacy 3-42
3.3.5 System Selection for Preferred Roaming 3-42
3.3.6 Service Programming Lock 3-42
3.3.7 Subscriber Parameter Administration Security Mechanism 3-43
3.3.8 Secure Mode 3-44
3.3.8.1 Generation of Secure Mode Ciphering Key 3-44
3.3.8.2 Encryption and Decryption of messages in Secure Mode 3-45
3.3.9 System Tag Indicator 3-45
3.3.10 Generation of Service Keys 3-46
3.3.10.1 Generation of Intermediate Key 3-46
3.3.10.2 Generation of Service Keys 3-46
3.4 Termination of the Programming Procedure 3-47
3.5 Reverse Link Message Formats 3-48
3.5.1 Message Contents 3-50
3.5.1.1 Configuration Response Message 3-50
3.5.1.2 Download Response Message 3-51
3.5.1.3 MS Key Response Message 3-55
3.5.1.4 Key Generation Response Message 3-55
3.5.1.5 Re-Authenticate Response Message 3-56
3.5.1.6 Commit Response Message 3-57
3.5.1.7 Protocol Capability Response Message 3-57
3.5.1.8 SSPR Configuration Response Message 3-61
3.5.1.9 SSPR Download Response Message 3-62
3.5.1.10 Validation Response Message 3-63
3.5.1.11 OTAPA Response Message 3-64
3.5.1.12 PUZL Configuration Response Message 3-65

CONTENTS

- 3.5.1.13 PUZL Download Response Message 3-66
- 3.5.1.14 3GPD Configuration Response Message 3-68
- 3.5.1.15 3GPD Download Response Message 3-69
- 3.5.1.16 Secure Mode Response Message 3-70
- 3.5.1.17 Extended Protocol Capability Response Message 3-70
- 3.5.1.18 MMD Configuration Response Message 3-76
- 3.5.1.19 MMD Download Response Message 3-78
- 3.5.1.20 System Tag Configuration Response Message 3-79
- 3.5.1.21 System Tag Download Response Message 3-80
- 3.5.1.22 Service Key Generation Response Message 3-81
- 3.5.1.23 MMS Configuration Response Message 3-81
- 3.5.1.24 MMS Download Response Message 3-83

3.5.2 NAM Parameter Blocks 3-83
- 3.5.2.1 CDMA/Analog NAM Parameter Block 3-84
- 3.5.2.2 Mobile Directory Number 3-87
- 3.5.2.3 CDMA NAM Parameter Block 3-88
- 3.5.2.4 IMSI_T Parameter Block 3-90

3.5.3 SSPR Parameter Blocks 3-91
- 3.5.3.1 Preferred Roaming List Dimensions Parameter Block 3-92
- 3.5.3.2 Preferred Roaming List Parameter Block 3-93
- 3.5.3.3 Extended Preferred Roaming List Dimensions Parameter Block 3-95

3.5.4 Reserved 3-96

3.5.5 Preferred Roaming List and Extended Preferred Roaming List 3-96
- 3.5.5.1 Preferred Roaming List CRC Calculation 3-101
- 3.5.5.2 Acquisition Records 3-101
  - 3.5.5.2.1 Acquisition Record Formats 3-103
    - 3.5.5.2.1.1 Cellular Analog System Acquisition Record 3-103
    - 3.5.5.2.1.2 Cellular CDMA and JTACS CDMA System Acquisition (Standard Channels) Record 3-103
    - 3.5.5.2.1.3 Cellular CDMA and JTACS CDMA System Acquisition (Custom Channels) Record 3-104
    - 3.5.5.2.1.4 Cellular CDMA Preferred System Acquisition Record 3-105

CONTENTS

3.5.5.2.1.5 PCS CDMA System Acquisition (Using Blocks) Record....................3-105
3.5.5.2.1.6 PCS CDMA and 2 GHz Band CDMA System Acquisition (Using Channels) Record...3-106
3.5.5.2.1.7 JTACS CDMA System Acquisition (Standard Channels) Record....3-107
3.5.5.2.1.8 JTACS CDMA System Acquisition (Custom Channels) Record 3-107
3.5.5.2.1.9 2 GHz Band CDMA System Acquisition (Using Channels) Record..3-108
3.5.5.2.2 Extended Acquisition Record Format...3-109
3.5.5.2.2.1 Cellular Analog System Acquisition Record 3-109
3.5.5.2.2.2 Cellular CDMA System Acquisition (Standard Channels) Record ..3-109
3.5.5.2.2.3 Cellular CDMA System Acquisition (Custom Channels) Record.....3-110
3.5.5.2.2.4 Cellular CDMA Preferred System Acquisition Record.....................3-111
3.5.5.2.2.5 PCS CDMA System Acquisition (Using Blocks) Record....................3-111
3.5.5.2.2.6 PCS CDMA System Acquisition (Using Channels) Record 3-112
3.5.5.2.2.7 JTACS CDMA System Acquisition (Standard Channels) Record....3-112
3.5.5.2.2.8 JTACS CDMA System Acquisition (Custom Channels) Record 3-113
3.5.5.2.2.9 2 GHz Band CDMA System Acquisition (Using Channels) Record..3-113
3.5.5.2.2.10 Generic Acquisition Record for IS-2000 and IS-95 3-114
3.5.5.2.2.11 Generic Acquisition Record for HRPD 3-114
3.5.5.3 System Record and Extended System Record Format 3-115
3.5.5.3.1 System Record Format 3-115
3.5.5.3.2 Extended System Record Format 3-117
3.5.5.3.2.1 Common Subnet Table for the HRPD Extended System Record....3-123
3.5.6 PUZL Parameter Blocks..3-123
3.5.6.1 PUZL Dimensions Parameter Block..3-124
3.5.6.2 PUZL Priorities Parameter Block 3-126
3.5.6.3 User Zone Parameter Block..3-127
3.5.6.4 Preferred User Zone List Parameter Block 3-128
3.5.7 Preferred User Zone List (PUZL) 3-130
3.5.7.1 User Zone Type Specific Fields 3-134
3.5.7.1.1 User Zone Type: Broadcast – RF Coverage Based 3-134
3.5.7.1.2 User Zone Type: Broadcast – Geo-based 3-135

CONTENTS

3.5.7.1.2.1 Circle 3-135
3.5.7.1.2.2 Segmented Linear 3-136
3.5.7.1.2.3 Polygon 3-137
3.5.7.1.3 User Zone Type: Mobile Specific – RF Coverage Based - Overhead Parameter Determined 3-139
3.5.7.1.3.1 SID Only....................3-139
3.5.7.1.3.2 SID and NID 3-140
3.5.7.1.3.3 SID and BASE_ID 3-140
3.5.7.1.3.4 Base Station Latitude and Longitude 3-141
3.5.7.1.3.5 User Zone Center Point and Radius 3-142
3.5.7.1.4 User Zone Type: Mobile Specific – Geo-Based....................3-143
3.5.7.1.5 User Zone Type: Mobile Specific – Geo-Based – Separate Carrier........3-143
3.5.8 3GPD Parameter Blocks 3-144
3.5.8.1 3GPD Operation Capability Parameters....................3-144
3.5.8.2 3GPD Operation Mode Parameters....................3-145
3.5.8.3 SimpleIP Capability Parameters 3-146
3.5.8.4 MobileIP Capability Parameters 3-147
3.5.8.5 SimpleIP User Profile Parameters....................3-149
3.5.8.6 Mobile IP User Profile Parameters 3-151
3.5.8.7 SimpleIP Status Parameters 3-155
3.5.8.8 MobileIP Status Parameters....................3-155
3.5.8.9 SimpleIP PAP SS Parameters 3-156
3.5.8.10 SimpleIP CHAP SS Parameters 3-157
3.5.8.11 MobileIP SS Parameters....................3-157
3.5.8.12 HRPD Access Authentication Capability Parameters 3-159
3.5.8.13 HRPD Access Authentication User Profile Parameters....................3-160
3.5.8.14 HRPD Access Authentication CHAP SS Parameters 3-161
3.5.9 MMD Parameter Block 3-161
3.5.9.1 MMD Application Parameters 3-161
3.5.10 System Tag Parameter Blocks....................3-163
3.5.10.1 Home System Tag 3-164

CONTENTS

3.5.10.2 Group Tag List Dimensions 3-165
3.5.10.3 Group Tag List Parameter Block 3-166
3.5.10.4 Specific Tag List Dimensions 3-167
3.4.10.5 Specific Tag List Parameter Block 3-167
3.4.10.6 Call Prompt List Dimensions 3-169
3.4.10.7 Call Prompt Tag List Parameter Block 3-169
3.5.11 Group Tag List, Specific Tag List and Call Prompt List 3-170
3.5.11.1 Group Tag List, Specific Tag List, and Call Prompt List CRC Calculation .3-174
3.5.11.2 Group Tag Records 3-174
3.5.11.2.1 Group Tag Record Format 3-175
3.5.11.2.1.1 Group Tag Record – Single Entry 3-175
3.5.11.2.1.2 Group Tag Record – Range 3-176
3.5.11.3 Specific Tag Records 3-178
3.5.11.3.1 Specific Tag Record Format 3-179
3.5.11.3.1.1 Specific Tag Record – Single Entry 3-179
3.5.11.3.1.2 Specific Tag Record – Range 3-180
3.5.11.4 Call Prompt Record Format 3-182
3.5.12 MMS Parameter Block 3-184
3.5.12.1 MMS URI Parameters 3-184
4 BASE STATION PROCEDURES 4-1
4.1 Reserved 4-1
4.2 Initiation of the Programming Procedures 4-1
4.2.1 User-Initiated Procedure 4-1
4.2.2 Network-Initiated Procedure. 4-2
4.3 Programming Data Download 4-2
4.3.1 OTA Data Message Processing 4-2
4.3.2 SSD Update and re-authentication 4-5
4.3.3 Activation of Message Encryption 4-6
4.3.4 Activation of Voice Privacy Mode 4-6
4.3.5 Secure Mode 4-6
4.3.5.1 Generation of Secure Mode Ciphering Key 4-7

CONTENTS

4.3.5.2 Encryption and Decryption of Messages in Secure Mode 4-8
4.3.6 Generation of Service Keys 4-8
4.3.6.1 Generation of Intermediate Key 4-8
4.3.6.2 Generation of Service Keys...4-8
4.4 Termination of the Programming Procedure 4-9
4.5 Forward Link Message Formats 4-9
4.5.1 Message Contents 4-11
4.5.1.1 Configuration Request Message 4-11
4.5.1.2 Download Request Message 4-12
4.5.1.3 MS Key Request Message 4-13
4.5.1.4 Key Generation Request Message 4-14
4.5.1.5 Re-Authenticate Request Message 4-14
4.5.1.6 Commit Request Message...4-15
4.5.1.7 Protocol Capability Request Message 4-15
4.5.1.8 SSPR Configuration Request Message..4-16
4.5.1.9 SSPR Download Request Message 4-16
4.5.1.10 Validation Request Message...4-18
4.5.1.11 OTAPA Request Message 4-18
4.5.1.12 PUZL Configuration Request Message 4-19
4.5.1.13 PUZL Download Request Message 4-21
4.5.1.14 3GPD Configuration Request Message 4-22
4.5.1.15 3GPD Download Request Message 4-23
4.5.1.16 Secure Mode Request Message 4-24
4.5.1.17 Reserved 4-25
4.5.1.18 MMD Configuration Request Message 4-25
4.5.1.19 MMD Download Request Message..4-25
4.5.1.20 System Tag Configuration Request Message 4-26
4.5.1.21 System Tag Download Request Message...4-27
4.5.1.22 Service Key Generation Request Message...4-28
4.5.1.23 MMS Configuration Request Message 4-28
4.5.1.24 MMS Download Request Message 4-29

CONTENTS

4.5.2 NAM Parameter Blocks 4-31
4.5.2.1 CDMA/Analog NAM Download 4-31
4.5.2.2 Mobile Directory Number 4-34
4.5.2.3 CDMA NAM Download 4-35
4.5.2.4 IMSI_T Parameter Block....................................4-37
4.5.3 SSPR Parameter Blocks 4-37
4.5.3.1 Preferred Roaming List Parameter Block....................................4-38
4.5.4 Validation Parameter Blocks 4-39
4.5.4.1 Verify SPC 4-39
4.5.4.2 Change SPC....................................4-40
4.5.4.3 Validate SPASM....................................4-41
4.5.5 Reserved....................................4-41
4.5.6 PUZL Parameter Blocks....................................4-41
4.5.6.1 User Zone Insert and User Zone Update 4-42
4.5.6.2 User Zone Delete 4-43
4.5.6.3 User Zone Priority Change 4-44
4.5.6.4 PUZL Flags 4-44
4.5.7 3GPD Parameter Blocks....................................4-45
4.5.7.1 3GPD Operation Mode Parameters....................................4-46
4.5.7.2 SimpleIP User Profile Parameters....................................4-47
4.5.7.3 Mobile IP User Profile Parameters 4-48
4.5.7.9 HRPD Access Authentication User Profile Parameters....................................4-55
4.5.7.10 HRPD Access Authentication CHAP SS Parameters 4-55
4.5.8 MMD Parameter Block....................................4-56
4.5.8.1 MMD Application Parameters 4-56
4.5.9 System Tag Parameter Blocks 4-58
4.5.9.1 Home System Tag Parameter Block....................................4-59
4.5.9.2 Group Tag List Parameter Block 4-60
4.5.9.3 Specific Tag List Parameter Block....................................4-61
4.5.9.4 Call Prompt List Parameter Block....................................4-62
4.5.10 MMS Parameter Block 4-63

CONTENTS

4.5.10.1 MMS URI Parameters 4-63
5 KEY EXCHANGE PROCEDURES 5-1
5.1 Mobile Station Requirements for A_KEY_P_REV < ‘00000011’....................5-1
5.1.1 Random Number Generation 5-1
5.1.2 Mobile Station Result....................5-1
5.1.3 A-key Computation....................5-1
5.2 Base Station Requirements for A_KEY_P_REV < ‘00000011’....................5-1
5.2.1 Generation of the Key Exchange Parameters....................5-1
5.2.2 Base Station Result....................5-2
5.2.3 A-key Computation....................5-2
5.3 Mobile Station Requirements for A_KEY_P_REV = ‘00000011’ or ‘00000100’....................5-2
5.3.1 Random Number Generation For Diffie-Hellman Key Exchange Procedure 5-2
5.3.2 Mobile Station Result....................5-3
5.3.3 A Key and Root Key Computation for A_KEY_P_REV = ‘00000011’....................5-3
5.3.4 Root Key Computation for A_KEY_P_REV = ‘00000100’....................5-3
5.4 Base Station Requirements for A_KEY_P_REV = ‘00000011’ or ‘00000100’....................5-3
5.4.1 Generation of the Key Exchange Parameters Root Key....................5-3
5.4.2 Base Station Result....................5-4
5.4.3 A Key and Root Key Computation for A_KEY_P_REV = ‘00000011’....................5-4
5.4.4 Root Key K Computation for A_KEY_P_REV = ‘00000100’....................5-5
5.5 Mobile Station Requirements for A_KEY_P_REV = ‘00000101’....................5-5
5.5.1 Random Number Generation and Key Generation Parameters....................5-5
5.5.2 Mobile Station Result....................5-5
5.5.3 Root Key Computation for A_KEY_P_REV = ‘00000101’....................5-6
5.6 Base Station Requirements for A_KEY_P_REV = ‘00000101’....................5-6
5.6.1 Random Number Generation and Key Generation Parameters....................5-6
5.6.2 Base Station Result....................5-7
5.6.3 3G Root Key K Computation....................5-7
ANNEX A RESERVED A-1
ANNEX B BIBLIOGRAPHY.................... B-1
ANNEX C SYSTEM SELECTION AND ACQUISITION C-1

CONTENTS

C.1 Introduction C-1
C.2 Accelerated System Selection C-2
  C.2.1 Using Positive and Negative Systems C-2
  C.2.2 PCS Block Mode System Selection C-3
  C.2.3 Special Cases and Considerations C-3
C.3 Preferred Roaming List Maintenance C-4
ANNEX D SYSTEM SELECTION AND THE PREFERRED USER ZONE LIST D-1

FIGURES

Figure 2.2.1-1 *OTASP Data Message* Encapsulation..2-1

Figure 2.2.1-2 *OTASP Data Message* CRC..2-2

Figure 2.2.2-1 *OTASP Data Message* Capsule Segmentation on the Forward Analog Voice Channel. 2-3

Figure 2.2.2-2 *OTASP Data Message* Capsule Segmentation on the Reverse Analog Voice Channel 2-4

TABLES

Table 3.2-1 System Selection Code. 3-3
Table 3.2.2.2-1 Valid Service Configuration Attributes for Service Option 18 3-11
Table 3.2.2.2-2 Valid Service Configuration Attributes for Service Option 19 3-11
Table 3.3.6-1 Service Programming Code Values 3-43
Table 3.3.10.2-1 Key Identifier Table 3-47
Table 3.5-1 Reverse Link Messages 3-48
Table 3.5.1.2-1 Result Codes 3-53
Table 3.5.1.7-1 Feature Identifier 3-59
Table 3.5.1.7-2 Band/mode Capability Information 3-61
Table 3.5.1.17.1-1 Capability Information Record Types 3-73
Table 3.5.1.17.1.1-1. OP_MODE..3-74
Table 3.5.1.17.1.3-1. MEID Field Setting..3-75
Table 3.5.1.17.1.5-1. EXT_UIM_ID Field Setting 3-76
Table 3.5.2-1 NAM Parameter Block Types 3-84
Table 3.5.3-1 SSPR Parameter Block Types 3-92
Table 3.5.5.2-1 Acquisition Record Type Values...3-102
Table 3.5.5.2-2 Extended Acquisition Record Type Values..3-102
Table 3.5.5.2.1.1-1 Cellular System A/B Selection Type Values 3-103
Table 3.5.5.2.1.2-1 Cellular CDMA and JTACS CDMA Standard Channel Selection Type Values 3-104
Table 3.5.5.2.1.5-1 PCS CDMA Frequency Blocks 3-106
Table 3.5.5.2.1.7-1 JTACS CDMA Standard Channel Selection Type Values 3-107
Table 3.5.5.3-1 NID_INCL Values 3-116
Table 3.5.5.3.2-1 Type-specific system ID record 3-118
Table 3.5.5.3.2-2 Type-specific system ID record 3-119
Table 3.5.5.3.2-3 NID_INCL Values...3-120
Table 3.5.6-1. PUZL Parameter Block Types 3-124
Table 3.5.7-1 User Zone Type Values 3-134
Table 3.5.7.1.2-1 Geo Type Values 3-135
Table 3.5.7.1.3-1 Overhead Parameter (OHP) Type Values 3-139
Table 3.5.8-1 3GPD Parameter Block Types...3-144

TABLES

Table 3.5.8.2-1 Operation Mode 3-146
Table 3.5.8.3-1 AUTH_ALGORITHM Parameter Values 3-147
Table 3.5.8.4-1 MN-AAA_AUTH_ALGORITHM Parameter Values..........3-148
Table 3.5.8.4-2 MN-HA_AUTH_ALGORITHM Parameter Values..........3-149
Table 3.5.8.5-1 Authentication Algorithm Parameter Values for SimpleIP 3-151
Table 3.5.8.6-1 Authentication Algorithm Parameter Values 3-154
Table 3.5.8.12-1 AUTH_ALGORITHM Parameter Values..........3-160
Table 3.5.8.13-1 Authentication Algorithm Parameter Values 3-160
Table 3.5.9-1 MMD Parameter Block Types 3-161
Table 3.5.10-1 System Tag Parameter Block Types..........3-164
Table 3.5.11.2-1 Group Tag Record Type Values 3-175
Table 3.5.11.3-1 Specific Tag Record Type Values..........3-179
Table 3.5.12-1 MMS Parameter Block Types..........3-184
Table 4.3.6.2-1 Key Identifier Table 4-9
Table 4.5-1 Forward Link Messages..........4-10
Table 4.5.1.22-1 Key Identifier Table 4-28
Table 4.5.2-1 NAM Parameter Block Types 4-31
Table 4.5.3-1 SSPR Parameter Block Types 4-38
Table 4.5.4-1 Validation Parameter Block Types 4-39
Table 4.5.4.1-1. BCD Mapping..........4-40
Table 4.5.6-1 PUZL Parameter Block Types..........4-42
Table 4.5.7-1 3GPD Parameter Block Types..........4-46
Table 4.5.8-1 MMD Parameter Block Types 4-56
Table 4.5.9-1 System Tag Parameter Block Types..........4-59
Table 4.5.10-1 MMS Parameter Block Types..........4-63
Table C.1-1 Preferred Roaming List.......... C-1
Table C.1-2 Acquisition Table.......... C-1
Table C.1-3 System Table C-2

FOREWORD

(This foreword is not part of this Standard)

These technical requirements form a standard for Over-the-Air Service Provisioning of mobile stations. A mobile station operating in either the analog or the spread spectrum (CDMA) mode conforming with various versions of the CDMA standards, such as TIA/EIA/IS-2000-A, TIA/EIA/IS-2000, TIA/EIA-95-B, TIA/EIA/IS-95-A (inclusive of TSB74), or ANSI J-STD-008 and this standard can be activated over the air in any system conforming with these standards.

The scope of this standard covers over-the-air provisioning of mobile station operational parameters. This standard does not address the quality or reliability of Over-the-Air Service Provisioning, nor does it cover equipment performance or measurement procedures.

SECTION SUMMARY

1. **Introduction.** This section defines the terms, references, protocols and network reference model used in this document.
2. **Message Transmission Procedures.** This section describes the lower-layer procedures used for transmission of messages for Over-the-Air Service Provisioning.
3. **Mobile Station Procedures.** This section describes the mobile station procedures for Over-the-Air Service Provisioning.
4. **Base Station Procedures.** This section describes the base station procedures for Over-the-Air Service Provisioning.
5. **Key Exchange Procedures.** This section describes the requirements for key exchange procedures.

NOTES

1. The following verbal forms are used: “Shall” and “shall not” identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others; that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the standard. “Can” and “cannot” are used for statements of possibility and capability, whether material, physical, or causal.
2. Footnotes appear at various points in this specification to elaborate and further clarify items discussed in the body of the specification.
3. Unless indicated otherwise, this document presents numbers in decimal form.

   Binary numbers are distinguished in the text by the use of single quotation marks. In some tables, binary values may appear without single quotation marks if table notation clearly specifies that values are binary. The character ‘x’ is used to represent a binary bit of unspecified value. For example ‘xxx00010’ represents any 8-bit binary value such that the least significant five bits equal ‘00010’.

   Hexadecimal numbers (base 16) are distinguished in the text by use of the form 0xh…h where h…h represents a string of hexadecimal digits. For example, 0x2fa1 represents a number whose binary value is ‘0010111110100001’ and whose decimal value is 12193. Note that the exact number of bits in the binary representation of a hexadecimal number strictly depends on the implementation requirements for the variable being represented.
4. Numeric information is used to describe the operation of the mobile station. The following subscripts are used in this document to clarify the use of the numeric information:
   - “s” indicates a value stored in a mobile station’s temporary memory.
   - “r” indicates a value received by a mobile station over a forward analog channel or a CDMA Forward Channel.
   - “p” indicates a value set in a mobile station’s permanent security and identification memory.
   - “s-p” indicates a value stored in a mobile station’s semi-permanent security and identification memory.
5. The term “mobile station” is equivalent to the term “personal station.”
6. IMSI_T Parameter Block does not apply for the mobile station conforming with TIA/EIA/IS-95-A (inclusive of TSB74) or ANSI J-STD-008.
7. IMSI_M in this document is equivalent to IMSI defined in TIA/EIA/IS-95-A (inclusive of TSB74) or ANSI J-STD-008.

NOTES

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

REFERENCES

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

– **Normative References:**

1. TIA-95-B, “*Mobile Station-Base Station Compatibility Standard for Wideband Spread Spectrum Cellular Systems*”, October 2004.
2. S.S0053, “*Common Cryptographic Algorithms*”, January 2002.
3. S.S0054, “*Interface Specification for Common Cryptographic Algorithms*”, January 2002.
4. Reserved.
5. C.S0002-D, “*Physical Layer Standard for cdma2000 Spread Spectrum Systems*”, March 2004.
6. C.S0004-D, “*Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems*”, March 2004.
7. C.S0005-D, “*Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*”, March 2004.
8. S.S0055 “*Enhanced Cryptographic Algorithms, Rev. A*”, January 2002.
9. C.S0024-A, “*cdma2000 High Rate Packet Data Air Interface Specification*”, April 2004.
10. IETF RFC 1334, “*PPP Authentication Protocols*”, October 1992.
11. IETF RFC 1994, “*PPP Challenge Handshake Authentication Protocol (CHAP)*”, August 1996.
12. IETF RFC 2002, “*IP Mobility Support*”, October 1996.
13. IETF RFC 2344, “*Reverse Tunneling for Mobile IP*”, August 1996.
14. IETF RFC 2486, “*The Network Access Interface*”, January 1999.
15. IETF RFC 3012, “*Mobile IPv4 Challenge/Response Extensions*”, November 1999.
16. National Bureau of Standards, Federal Information Processing Standards Publication 180-1; “*Secure Hash Standard*”, 1995.
17. X.S0013, “*ALL-IP Core Network Multimedia Domain*”, February 2004.
18. 3GPP TS 25.101, “*UE Radio Transmission and Reception (FDD)*”, March 2003.
19. X.S0016-310, “*MMS MM1 Stage 3 Using OMA/WAP*”, July 2004.
20. X.S0016-311, “*MMS MM1 Stage 3 Using M-IMAP for Message Submission and Retrieval*”, May 2003.

REFERENCES

21. X.S0016-312, “*MMS MM1 Using SIP*”, July 2004.

22. C.S0006-D, *“Analog Signaling Standard for cdma2000 Spread Spectrum Systems – Release D”*, March 2004.

23. C.S0057-0, “*Band Class Specification for cdma2000 Spread Spectrum Systems*”, February 2004.

24. *C.S0023-C, Removable User Identity Module for Spread Spectrum Systems, June 2006.*

– **Informative References:**

4. C.R1001-D, “*Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards, Release D*”, April 2003.

1 INTRODUCTION

1.1 General Description

Over-the-Air Service Provisioning (OTASP) consists of the following features provisioned over-the-air:

- Download of NAM operational parameters.
- Electronic Key Exchange for securely establishing the A-key and Root Key.
- System Selection for Preferred Roaming (SSPR) for providing mobile stations with information allowing acquisition of the preferred system in an area.
- Preferred User Zone List (PUZL) for providing mobile stations which support the optional User Zone feature with information allowing usage of the preferred user zone in an area.
- Download of 3G packet data operational parameters.

Service Programming Lock (SPL), if provided, prevents the over-the-air provisioning of certain mobile station parameters by an unauthorized network entity.

This document describes Over-the-Air Service Provisioning in CDMA and analog systems. The procedures defined are intended to be extendable and flexible enough to be used with future air interface specifications. The procedures in this document do not require support for continuation of the service provisioning process following a CDMA-to-analog handoff.

1.2 Terms and Numeric Information

1.2.1 Terms

3GPD. Third Generation Packet Data

AC. See Authentication Center.

Access Authentication. A procedure in which the Access Terminal (AT) is authenticated by the AN-AAA (Access Network Authentication, Authorization and Accounting entity).

Activation Code. A user-entered combination of a specified Feature Code (*FC) and defined group of at least two dialed digits (System Selection Code) that specify the user selection of a Band and a Block operated by the selected service provider.

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.

Analog Voice Channel. An analog channel on which a voice conversation occurs and on which brief digital messages may be sent from a base station to a mobile station or from a mobile station to a base station.

Authentication. A procedure used by a base station to validate a mobile station's identity.

Authentication Center (AC). An entity that manages the authentication information related to the mobile station.

Base Station. A fixed station used for communicating with mobile stations. Depending upon the context, the term base station may refer to a cell, a sector within a cell, an MSC, an OTAF, or other part of the wireless system. (See also MSC and OTAF.)

BCMCS Root Key. A secret 128-bit pattern used for BCMCS services.

CRC. See Cyclic Redundancy Code.

Cyclic Redundancy Code (CRC). A class of linear error detecting codes which generate parity check bits by finding the remainder of a polynomial division.

Electronic Serial Number (ESN). A 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.

ESN. See Electronic Serial Number.

Forward CDMA Channel. A CDMA Channel from a base station to mobile stations. The Forward CDMA Channel contains one or more code channels that are transmitted on a CDMA frequency assignment using a particular pilot PN offset.

Forward Analog Voice Channel (FVC). An analog voice channel used from a base station to a mobile station.

Forward Traffic Channel. A code channel used to transport user and signaling traffic from the base station to the mobile station.

FRESH. A 15-bit value used by the mobile station and the base station as the cryptographic synchronizer for encrypting parameter data in Secure Mode. FRESH may be set by the encrypting side to any value, including a monotonically incremented counter, as long as this value is not repeated for the duration of the Secure Mode in progress.

HLR. See Home Location Register.

Home Location Register (HLR). The location register to which a MIN/IMSI is assigned for record purposes such as subscriber information.

Home System. The cellular system in which the mobile station subscribes for service.

HRPD. High Rate Packet Data. See [9].

IMPI. IMS Private Identity. See [17].

IMPU. IMS Public Identity. See [17].

IMS Root Key. A secret 128-bit pattern used for IMS services.

IMSI. See International Mobile Station Identity.

IMSI_M. MIN based IMSI using the lower 10-digits to store the MIN.

IMSI_O. The operational value of IMSI used by the mobile station for operation with the base station.

IMSI_T. IMSI not associated with MIN. 15-digits or fewer.

International Mobile Station Identity (IMSI). A method of identifying stations in the land mobile service as specified in ITU-T Recommendation E.212.

Long Code Mask. A 42-bit binary number that creates the unique identity of the long code. See also Public Long Code, Private Long Code, Public Long Code Mask and Private Long Code Mask.

LSB. Least significant bit.

MCC. See Mobile Country Code.

MEID. See Mobile Equipment Identifier.

Mobile Country Code (MCC). A part of the E.212 IMSI identifying the home country. See ITU-T Recommendation E.212.

Mobile Equipment Identifier (MEID). A 56-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.

Mobile Directory Number. A dialable directory number which is not necessarily the same as the mobile station's air interface identification, i.e., MIN, IMSI_M or IMSI_T.

MIN. See Mobile Identification Number.

MMD. Multimedia Domain.

MMS. Multimedia Messaging Service.

MNC. See Mobile Network Code.

Mobile Identification Number (MIN). The 34-bit number that is a digital representation of the 10-digit number assigned to a mobile station.

Mobile Network Code (MNC). A part of the E.212 IMSI identifying the home network within the home country. See ITU-T Recommendation E.212.

Mobile Station. A station, fixed or mobile, which serves as the end user's wireless communication link with the base station. Mobile stations include portable units (e.g., hand-held personal units) and units installed in vehicles.

Mobile Station Originated Call. A call originating from a mobile station.

Mobile Station Terminated Call. A call received by a mobile station (not to be confused with a disconnect or call release).

Mobile Switching Center (MSC). A configuration of equipment that provides wireless radiotelephone service. Also called the Mobile Telephone Switching Office (MTSO).

MSB. Most significant bit.

MSC. See Mobile Switching Center.

NAM. See Number Assignment Module.

Network. A network is a subset of a wireless system, such as an area-wide wireless network, a private group of base stations, or a group of base stations set up to handle a special requirement. A network can be as small or as large as needed, as long as it is fully contained within a system. See also System.

Network Identification (NID). A number that uniquely identifies a network within a wireless system. See also System Identification.

NID. See Network Identification.

Number Assignment Module (NAM). A set of MIN/IMSI-related parameters stored in the mobile station.

OTAF. See Over-the-Air Service Provisioning Function.

Over-the-Air Service Provisioning Function (OTAF). A configuration of network equipment that controls OTASP functionality and messaging protocol.

OTAPA. See Over-the-Air Parameter Administration.

OTASP. See Over-the-Air Service Provisioning.

Over-the-Air Parameter Administration (OTAPA). Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.

Over-the-Air Service Provisioning (OTASP). A process of provisioning mobile station operational parameters over the air interface.

Parity Check Bits. Bits added to a sequence of information bits to provide error detection, correction, or both.

P-CSCF. Proxy Call Session Control Function.

Preferred User Zone List (PUZL). A list that provides the mobile station with the information for the User Zones to which the mobile user is subscribed.

PDSN. Packet Data Service Node.

Private Long Code. The long code characterized by the private long code mask.

Private Long Code Mask. The long code mask used to form the private long code.

Pseudo-ESN. A 32-bit number derived from MEID and used in place of ESN.

Public Long Code. The long code characterized by the public long code mask.

Public Long Code Mask. The long code mask used to form the public long code. The mask contains the ESN of the mobile station. See also Private Long Code Mask.

PUZL. See Preferred User Zone List.

Release. A process that the mobile station and base station use to inform each other of call disconnect.

Reverse CDMA Channel. The CDMA Channel from the mobile station to the base station. From the base station’s perspective, the Reverse CDMA Channel is the sum of all mobile station transmissions on a CDMA frequency assignment.

Roamer. A mobile station operating in a wireless system (or network) other than the one from which service was subscribed.

Secure Mode. Network initiated mode of communicating operational parameters between a mobile station and network based provisioning entity in an encrypted form.

SIP. Session Initiation Protocol.

SMCK. Secure Mode Ciphering Key.

Service Option. A service capability of the system. Service options may be applications such as voice, data, or facsimile. See [4].

Service Programming Code (SPC). A secret code assigned to the mobile station and known to the authorized network entity.

Service Programming Lock (SPL). A protection provided for preventing the over-the-air provisioning of certain mobile station parameters by unauthorized network entity by way of verifying the Service Programming Code (SPC).

Shared Secret Data (SSD). A 128-bit pattern stored in the mobile station (in semi-permanent memory) and known by the base station. SSD is a concatenation of two 64-bit subsets: SSD_A, which is used to support the authentication procedures, and SSD_B, which serves as one of the inputs to the process generating the encryption mask and private long code.

SID. See System Identification.

SPASM. See Subscriber Parameter Administration Security Mechanism.

SPC. See Service Programming Code.

SPL. See Service Programming Lock.

SSD. See Shared Secret Data.

SSPR. See System Selection for Preferred Roaming.

Subscriber Parameter Administration Security Mechanism (SPASM). Security mechanism protecting parameters and indicators of active NAM from programming by an unauthorized network entity during the OTAPA session.

System. A system is a wireless telephone service that covers a geographic area such as a city, metropolitan region, county, or group of counties. See also Network.

System Identification (SID). A number uniquely identifying a wireless system.

System Selection Code. A part of the Activation Code that specifies the user selection of a Band and a Block operated by the selected service provider.

System Selection for Preferred Roaming (SSPR). A feature that enhances the mobile station system acquisition process based on the set of additional parameters stored in the mobile station in the form of a Preferred Roaming List ($\text{PR\_LIST}_{\text{s-p}}$).

Traffic Channel. A communication path between a mobile station and a base station used for user and signaling traffic. The term Traffic Channel implies a Forward Traffic Channel and Reverse Traffic Channel pair. See also Forward Traffic Channel and Reverse Traffic Channel.

User Zone (UZ). CDMA Tiered Service Offerings are defined by User Zones that are geographical groupings of services.

UZ. See User Zone.

Voice Channel. See Analog Voice Channel.

Voice Privacy. The process by which user voice transmitted over a CDMA Traffic Channel is afforded a modest degree of protection against eavesdropping over the air.

WLAN Root Key. A secret 128-bit pattern used for WLAN services.

1.2.2 Numeric Information

Numeric information is used to describe the operation of the mobile station. The following subscripts are used to clarify the use of the numeric information:

- "s" indicates a value stored in a mobile station's temporary memory.
- "r" indicates a value received by a mobile station over a forward analog control channel or a CDMA Forward Channel.
- "p" indicates a value set in a mobile station's permanent security and identification memory.
- "s-p" indicates a value stored in a mobile station's semi-permanent security and identification memory.

This section defines numeric information specifically related to the OTASP.

A_KEY_P_REV$_p$ - Protocol revision of the mobile station Key Exchange procedure.

A_KEY_TEMP$_s$ - A secret 64-bit pattern temporarily stored in the mobile station.

AUTH_OTAPA$_s$ - The computed 18-bit result AUTH_SIGNATURE used for validating SPASM.

BCMCS_Kp - A secret 128-bit pattern permanently stored in the mobile station.

BS_PARAM – A variable used in the base station procedure for 3G Root Key computation.

BS_PW – A 128-bit user password that is stored in the base station. It has the same value as the MS_PW.

BS_PW_HASH – The computed 1152-bit hash of the base station user password BS_PW.

CUR_SSPR_P_REV$_{s\text{-}p}$ – Protocol revision of the mobile station's current preferred roaming list. This information is used to parse PR_LIST$_{s\text{-}p}$. Retained by the mobile station when the power is turned off.

DATA_P_REV$_p$ - Protocol revision of the mobile station NAM Download procedure.

IMS_Kp - A secret 128-bit pattern permanently stored in the mobile station.

ITM_KEY – An intermediate key used in the procedure for calculating service keys.

MS_PARAM – A variable used in the mobile station procedure for 3G Root Key computation.

MS_PW – A 128-bit user password that is stored in the mobile station. It has the same value as the BS_PW.

MS_PW_HASH – The computed 1152-bit hash of the mobile station user password MS_PW.

NAM_LOCK$_p$ - The locking indicator set in the mobile station by the base station that defines SPASM protection of the programmable parameters in the active NAM during the OTAPA session.

NULL - A value that is not in the specified range of the field or variable.

NAM_LOCK$_s$ - A network controlled status of the SPASM protection of the active NAM for the subsequent OTAPA session.

NAM_LOCK_STATE - a locking state of the mobile station programmable parameters for OTAPA. If the NAM_LOCK_STATE = ‘1’, the parameters are locked for network initiated programming.

PARAM_G$_s$ - Key exchange parameter G.

PARAM_P$_s$ - Key exchange parameter P.

PR_LIST$_{s-p}$ - Preferred Roaming List. Contains information to assist the mobile station system selection and acquisition process. Retained by the mobile station when the power is turned off.

PRL_BLOCK_ID_CURRENT$_s$ – Parameter Block Identifier for the current Preferred Roaming List temporarily stored in the mobile station.

PUZL$_{s-p}$ – Preferred User Zone List. Contains information to assist the mobile station during user zone selection and acquisition process. Retained by the mobile station when the power is turned off.

PUZL_P_REV$_p$ - Protocol revision of the mobile station PUZL Download procedure.

RAND_SEED – A secret 128-bit pattern temporarily stored in the mobile station.

RKp - A secret 128-bit pattern permanently stored in the mobile station.

RK_TEMP$_s$ - A secret 128-bit pattern temporarily stored in the mobile station.

SPC$_p$ - Service Programming Code. A secret code assigned to the mobile station and known to the authorized network entity. The base station uses the code equal to the SPC$_p$ for unlocking the mobile station parameters for programming or reprogramming.

SPC$_s$ - Service Programming Code temporarily stored in the mobile station.

SPL_P_REV$_p$ - Protocol revision of the mobile station Service Programming Lock.

SP_LOCK_STATE - A locking state of the mobile station programmable parameters. If the SP_LOCK_STATE = ‘1’, the parameters are locked for programming.

SSPR_P_REV$_p$ - Protocol revision of the mobile station SSPR Download procedure and the PRL format.

SECURE_MODE_IND$_s$- Secure Mode indicator. If SECURE_MODE_IND$_S$ = ‘1’, current programming session is in Secure Mode.

SMCK$_s$ – Secure Mode Ciphering Key.

WLAN_Kp - A secret 128-bit pattern permanently stored in the mobile station.

No text.

2 MESSAGE TRANSPORT PROTOCOL

2.1 General

OTASP Data Messages (see Sections 3 and 4) can be sent over the analog voice channel or the CDMA Traffic Channel. In either case, the *OTASP Data Messages* are sent using a Layer 2 protocol that provides reliable delivery and duplicate detection.

The delivery of *OTASP Data Messages* does not require sequential delivery of messages by the Layer 2 protocol because the Over-the-Air Service Provisioning procedures ensure that only one *OTASP Data Message* is outstanding at any time.

During the analog mode of operation, *OTASP Data Messages* are sent using the analog transport protocol (see 2.2). During the CDMA mode of operation, *OTASP Data Messages* are sent using the CDMA transport protocol (see 2.3).

2.2 Analog Transport Protocol

OTASP Data Messages are transmitted over an analog voice channel using the *OTASP Transport Message*. Signaling on the analog voice channel does not have a Layer 2 protocol defined in [1, 6]. Because of the large amount of data transported for Over-the-Air Service Provisioning, this standard defines a Layer 2 protocol to ensure *OTASP Data Message* integrity. This protocol provides message segmentation, segment acknowledgment, error detection and re-transmission.

2.2.1 *OTASP Data Message* Encapsulation

Each *OTASP Data Message* Unit transmitted on an analog voice channel shall consist of an 8-bit message length field (MSG_LENGTH), an *OTASP Data Message*, as defined in 3.5 and 4.5, and a 16-bit CRC, in that order (see Figure 2.2.1-1).

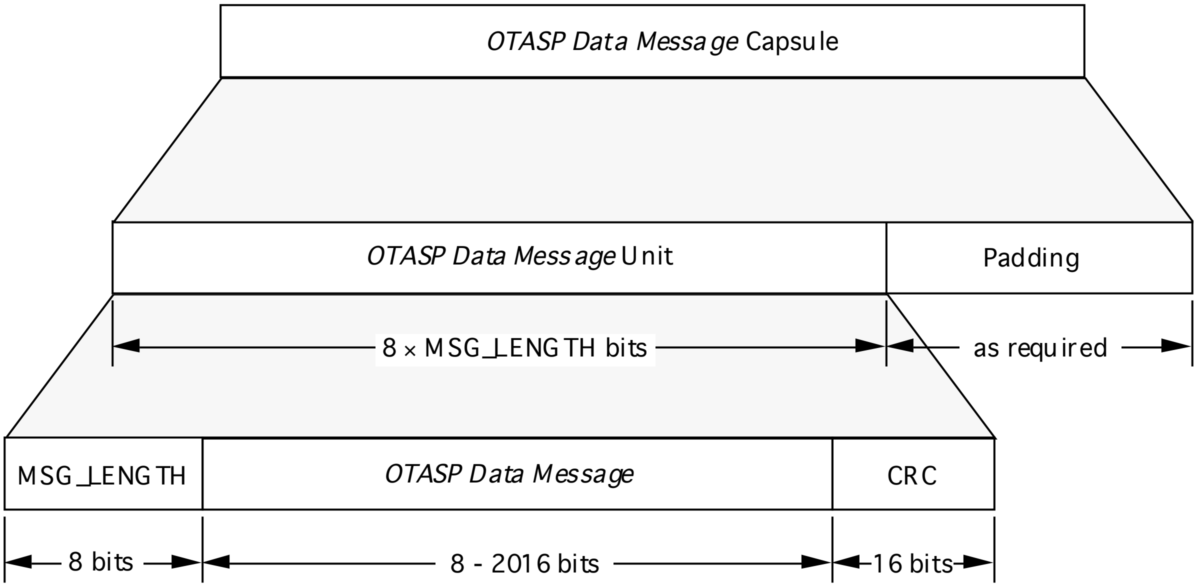

Figure 2.2.1-1 *OTASP Data Message* Encapsulation

The MSG_LENGTH field shall be set to the number of octets in the *OTASP Data Message* plus three.

The 16-bit CRC is calculated on the MSG_LENGTH field and the *OTASP Data Message* bits. The generator polynomial for this CRC shall be as follows:

$$g(x) = x^{16} + x^{12} + x^5 + x^0$$

The 16-bit CRC shall be computed according to the following procedure using the logic shown in Figure 2.2.1-2:

- Initially, all shift register elements shall be set to logical one and the switches shall be set in the position ‘A’.
- The register shall be clocked with each *OTASP Data Message* bit as an input, most significant bit first.
- The switches shall be set in the position ‘B’, and the register shall be clocked an additional 16 times. The 16 additional output bits shall be the CRC bits.
- The 16 CRC bits shall be transmitted in the order calculated.

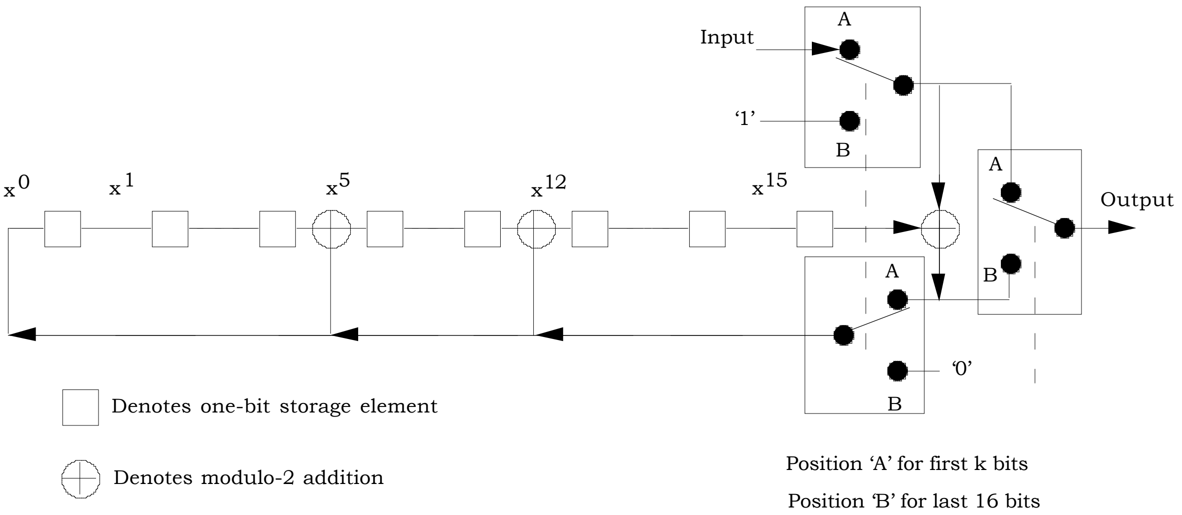
Input
A
‘1’
B
x^0
x^1
x^5
x^{12}
x^{15}
A
B
Output
A
B
‘0’
Denotes one-bit storage element
Denotes modulo-2 addition
Position ‘A’ for first k bits
Position ‘B’ for last 16 bits

Figure 2.2.1-2 *OTASP Data Message* CRC

Padding consisting of zero or more ‘0’ bits shall be added immediately following the *OTASP Data Message* Unit. The length of the padding shall be such that the resulting *OTASP Data Message* Capsule fits into the minimum possible integral number of *OTASP Transport Messages* (see 2.2.2).

2.2.2 *OTASP Data Message* Segmentation

Each *OTASP Data Message* Capsule (see 2.2.1) sent on an analog voice channel shall be segmented and transmitted in one or more *OTASP Transport Messages*, as defined in 2.2.3.4 and 2.2.4.3. Figures 2.2.2-1 and 2.2.2-2 illustrate the segmentation process for the forward and reverse analog voice channels, respectively.

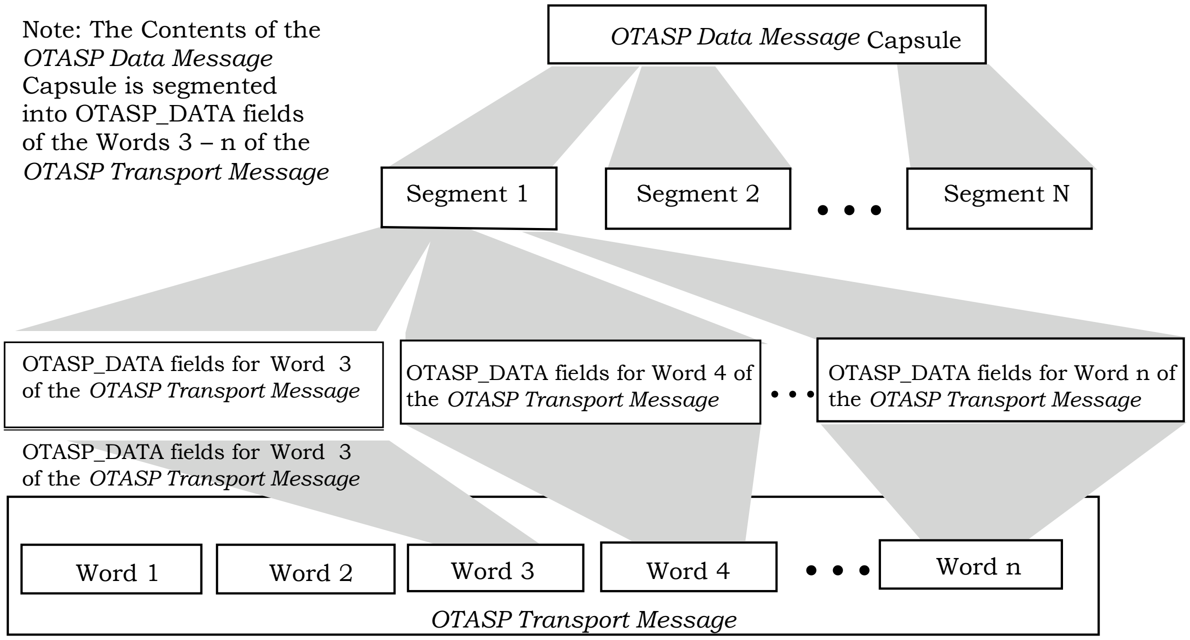
Note: The Contents of the *OTASP Data Message* Capsule is segmented into OTASP_DATA fields of the Words 3 – n of the *OTASP Transport Message*
OTASP Data Message Capsule
Segment 1
Segment 2
Segment N
OTASP_DATA fields for Word 3 of the *OTASP Transport Message*
OTASP_DATA fields for Word 4 of the *OTASP Transport Message*
OTASP_DATA fields for Word n of the *OTASP Transport Message*
OTASP_DATA fields for Word 3 of the *OTASP Transport Message*
Word 1
Word 2
Word 3
Word 4
Word n
OTASP Transport Message

Figure 2.2.2-1 *OTASP Data Message* Capsule Segmentation on the Forward Analog Voice Channel.

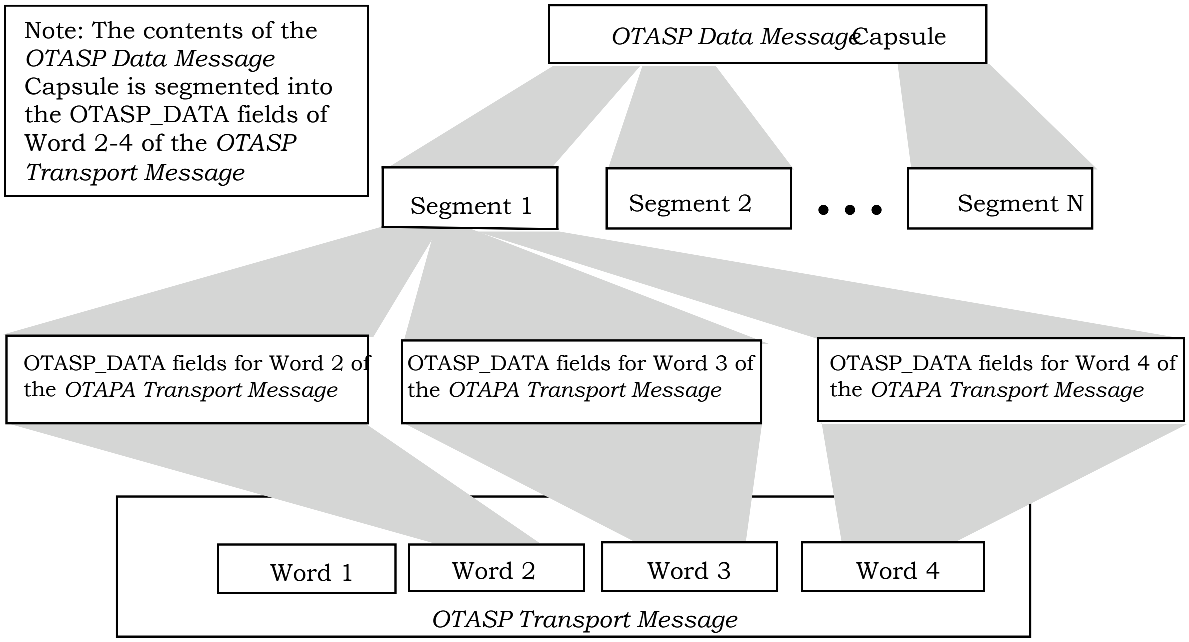
Note: The contents of the *OTASP Data Message* Capsule is segmented into the OTASP_DATA fields of Word 2-4 of the *OTASP Transport Message*
OTASP Data Message Capsule
Segment 1
Segment 2
• • •
Segment N
OTASP_DATA fields for Word 2 of the *OTAPA Transport Message*
OTASP_DATA fields for Word 3 of the *OTAPA Transport Message*
OTASP_DATA fields for Word 4 of the *OTAPA Transport Message*
Word 1
Word 2
Word 3
Word 4
OTASP Transport Message

Figure 2.2.2-2 *OTASP Data Message* Capsule Segmentation on the Reverse Analog Voice Channel

2.2.3 Mobile Station Procedures

OTASP Data Messages are sent and received on analog voice channels only when the mobile station is in the Conversation Task (see 2.6.4.4 of [1]). The mobile station shall transmit *OTASP Transport Messages* in accordance with the procedures in 2.7.2 of [1]. Mobile stations implementing the Over-the-Air Service Provisioning feature shall comply with the following requirements in addition to those of 2.6.4.4 of [1].

2.2.3.1 *OTASP Transport Message* Acknowledgment and Re-transmission

When the mobile station sends an *OTASP Transport Message*, it starts the OTASP acknowledgment timer. The timer is disabled when an *OTASP Transport Confirmation Message* is received.

After sending an *OTASP Transport Message*, the mobile station shall not send a new *OTASP Transport Message* until it has received an *OTASP Transport Confirmation Message* acknowledging the message that has been sent.

If the OTASP acknowledgment timer expires and the *OTASP Transport Message* has been sent fewer than three times, the mobile station shall resend the *OTASP Transport Message* and reset the OTASP acknowledgment timer to two seconds. If the OTASP acknowledgment timer expires and the *OTASP Transport Message* has been sent three times, the mobile station shall enter the Release Task (see 2.6.4.5 of [1]).

2.2.3.2 Message Transmission

While the mobile station is in the Conversation Task, the following messages can be sent in addition to those listed in 2.6.4.4 of [1]:

1. *OTASP Transport Message*:

   After sending the message, the mobile station shall set the OTASP acknowledgment timer to two seconds. The mobile station shall construct the *OTASP Transport Message* as follows:

   - If the OTASP_DATA field of the *OTASP Transport Message* contains an entire *OTASP Data Message* Capsule, the mobile station shall set $TX\_SEQ\_NUM_S$ to '00000', shall set the SEQ_NUM field equal to $TX\_SEQ\_NUM_S$, and shall set the value of the B/F field to '11'.
   - If the OTASP_DATA field of the *OTASP Transport Message* contains the first segment of the segmented *OTASP Data Message* Capsule, the mobile station shall set $TX\_SEQ\_NUM_S$ to '00000', shall set the SEQ_NUM field equal to $TX\_SEQ\_NUM_S$ and shall set the value of the B/F field to '10'.
   - If the OTASP_DATA field of the *OTASP Transport Message* contains a segment other than the first segment of the segmented *OTASP Data Message* Capsule, the mobile station shall perform the following:
     - If the OTASP_DATA field of the *OTASP Transport Message* contains a segment other than the final segment of the *OTASP Data Message* Capsule, the mobile station shall set $TX\_SEQ\_NUM_S$ to ($TX\_SEQ\_NUM_S$ + 1) modulo 32, shall set the SEQ_NUM field equal to $TX\_SEQ\_NUM_S$ and shall set the value of the B/F field to '00'.
     - If the OTASP_DATA field of the *OTASP Transport Message* contains the final segment of the *OTASP Data Message* Capsule, the mobile station shall set $TX\_SEQ\_NUM_S$ to ($TX\_SEQ\_NUM_S$ + 1) modulo 32, shall set the SEQ_NUM field equal to $TX\_SEQ\_NUM_S$ and shall set the value of the B/F field to '01'.

   The mobile station shall remain in the Conversation Task.

2. *OTASP Transport Confirmation Message:*

   The mobile station shall set the SEQ_ACK field and DMU_CRC_OK field as specified in 2.2.3.3. The mobile station shall remain in the Conversation Task.

2.2.3.3 Message Reception

While the mobile station is in the Conversation Task, the following messages can be received in addition to those listed in 2.6.4.4 of [1]. When any message is received, the mobile station shall perform all actions specified in 2.6.4.4 of [1] that apply to a message reception. The mobile station shall take the actions specified below for each message:

1. *OTASP Transport Message:*

   If the value of ESN_r received in the *OTASP Transport Message* does not match the ESN_p that identifies the mobile station, the mobile station shall turn off the transmitter and then enter the Serving-System Determination Task (see 2.6.3.12 of [1]).

If the value of ESN_r received in the *OTASP Transport Message* matches the ESN_p, the mobile station shall do the following:

- The mobile station shall send an *OTASP Transport Confirmation Message* within 750 ms after receiving the last bit of the *OTASP Transport Message*. The mobile station shall set the SEQ_ACK field equal to SEQ_NUM_r received in the *OTASP Transport Message*. The mobile station shall set the DMU_CRC_OK field as specified below.

- If the value of the B/F field of the received message is '11', the OTASP_DATA field of the received message contains an *OTASP Data Message* Capsule in its entirety (i.e., contains an unsegmented *OTASP Data Message* Capsule). The mobile station shall discard any incomplete *OTASP Data Message* Capsule being reassembled. If the CRC of the *OTASP Data Message* Unit checks (see 2.2.1), the mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '1', and shall process the *OTASP Data Message* as specified in Section 3; otherwise, the mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0', and shall discard the *OTASP Data Message* Capsule.

- If the value of the B/F field of the received message is '10', the mobile station shall discard any incomplete *OTASP Data Message* Capsule being reassembled, and shall store the OTASP_DATA field of the received message as the first segment of an *OTASP Data Message* Capsule to be reassembled. The mobile station shall set $RX\_SEQ\_NUM_s$ to the value of the SEQ_NUM field of the received message. The mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0'.

- If the value of the B/F field of the received message is '00' and a segmented *OTASP Data Message* Capsule is being reassembled, the mobile station shall perform the following:
    - If ($RX\_SEQ\_NUM_s$ + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the mobile station shall store the OTASP_DATA field of the received message as the next segment of the *OTASP Data Message* Capsule being reassembled, and shall increment $RX\_SEQ\_NUM_s$, modulo 32.
    - If $RX\_SEQ\_NUM_s$ is equal to the value of the SEQ_NUM field of the received message, the mobile station shall discard the OTASP_DATA field of the received message.
    - If neither $RX\_SEQ\_NUM_s$ nor ($RX\_SEQ\_NUM_s$ + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the mobile station shall discard the OTASP_DATA field of the received message and shall discard the incomplete *OTASP Data Message* Capsule being reassembled.

  - The mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0'.

- If the value of the B/F field of the received message is '00', and if no segmented *OTASP Data Message* Capsule is being reassembled, the mobile station shall discard the OTASP_DATA field of the received message. The mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0'.

- If the value of the B/F field of the received message is '01' and if a segmented *OTASP Data Message* Capsule is being reassembled, the mobile station shall perform the following:
  - If ($RX\_SEQ\_NUM_S$ + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the mobile station shall store the OTASP_DATA field of the received message as the last segment of the *OTASP Data Message* Capsule being reassembled and shall increment $RX\_SEQ\_NUM_S$, modulo 32. If the CRC of the *OTASP Data Message* Unit checks (see 2.2.1), the mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '1' and shall process the *OTASP Data Message* as specified in Section 3; otherwise, the mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0' and shall discard the *OTASP Data Message* Capsule.
  - If $RX\_SEQ\_NUM_S$ is equal to the value of the SEQ_NUM field of the received message, the mobile station shall discard the OTASP_DATA field of the received message. If the CRC of the *OTASP Data Message* Unit checks (see 2.2.1), the mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '1'; otherwise, the mobile station shall set the DMU_CRC_OK field to '0'.
  - If neither $RX\_SEQ\_NUM_S$ nor ($RX\_SEQ\_NUM_S$ + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the mobile station shall discard the OTASP_DATA field of the received message and shall discard the incomplete *OTASP Data Message* Capsule being reassembled. The mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0'.

- If the value of the B/F field of the received message is '01', and if no segmented *OTASP Data Message* Capsule is being reassembled, the mobile station shall discard the OTASP_DATA field of the received message. The mobile station shall set the DMU_CRC_OK field of the *OTASP Transport Confirmation Message* to '0'.

The mobile station shall remain in the Conversation Task.

2. *OTASP Transport Confirmation Message:*

   If the SEQ_ACK field is equal to $TX\_SEQ\_NUM_S$, the mobile station shall disable the OTASP acknowledgment timer; otherwise, the mobile station shall ignore the message. The mobile station shall remain in the Conversation Task.

2.2.3.4 Reverse Voice Channel Message Format

2.2.3.4.1 *OTASP Transport Message*

When the mobile station sends the *OTASP Transport Message* on the Reverse Voice Channel (RVC), it shall use the following format:

- Word 1 of the *OTASP Transport Message*:

Information Element	**Length (bits)**
F=1	1
NAWC	2
T=1	1
MSG_TYPE=00000	5
ORDQ=000	3
ORDER=11010	5
SEQ_NUM	5
B/F	2
ESN_4	8
RSVD=0000	4
P	12

- Word 2 of the *OTASP Transport Message:*

Information Element	**Length (bits)**
F=0	1
NAWC	2
T=1	1
ESN_3	8
ESN_2	8
ESN_1	8
OTASP_DATA	8
P	12

- Words 3 and 4 of the *OTASP Transport Message:*

Information Element	Length (bits)
F=0	1
NAWC	2
T=1	1
OTASP_DATA	32
P	12

F - First word field. The mobile station shall set this field to '1' in the first word of the message, and to '0' in all other words.

NAWC - Number of additional words coming field. The mobile station shall set this field in each word of the message to the number of remaining words not including the current word.

T - T field. The mobile station shall set this field to '1'.

MSG_TYPE - Message Type field. The mobile station shall set this field to '00000'.

ORDQ - Order qualifier field. The mobile station shall set this field to '000'.

ORDER - Order field. The mobile station shall set this field to '11010'.

SEQ_NUM - Message Sequence Number. The mobile station shall set this field to the message sequence number of this *OTASP Transport Message*.

B/F - Begin/Final. This field is used to specify whether the *OTASP Data Message* Capsule has been segmented into multiple *OTASP Transport Messages.* If the *OTASP Data Message* Capsule is completely contained in a single *OTASP Transport Message,* the mobile station shall set this field to '11'. For an *OTASP Data Message* Capsule contained in multiple *OTASP Transport Messages,* the mobile station shall set the value of this field in the first segment to '10', the value of this field in all intermediate segments to '00', and the value of this field in the final segment to '01'.

ESN_4 - The mobile station shall set this field to the most significant octet (bits d31-d24) of the mobile station ESN.

ESN_3 - The mobile station shall set this field to the next to the most significant octet (bits d23-d16) of the mobile station ESN.

ESN_2 - The mobile station shall set this field to the next to the least significant octet (bits d15-d8) of the mobile station ESN.

ESN_1 - The mobile station shall set this field to the least significant octet (bits d7-d0) of the mobile station ESN.

RSVD - Reserved for future use; the mobile station shall set all bits as indicated.

OTASP_DATA - The mobile station shall set these fields to the corresponding octets of the *OTASP Data Message* Capsule.

P - Parity field. The mobile station shall set this field as specified in 2.7.2 of [1].

2.2.3.4.2 *OTASP Transport Confirmation Message*

The mobile station Reverse Voice Channel (RVC) *OTASP Transport Confirmation Message* has the following format:

Information Element	**Length (bits)**
F=1	1
NAWC=00	2
T=1	1
MSG_TYPE=00001	5
ORDQ=000	3
ORDER=11010	5
SEQ_ACK	5
DMU_CRC_OK	1
RSVD=0000000000000	13
P	12

F - First word field. The mobile station shall set this field to ‘1’.

NAWC - Number of additional words coming field. The mobile station shall set this field to ‘00’.

T - T field. The mobile station shall set this field to ‘1’.

MSG_TYPE - Message Type field. The mobile station shall set this field to ‘00001’.

ORDQ - Order qualifier field. The mobile station shall set this field to ‘000’.

ORDER - Order field. The mobile station shall set this field to ‘11010’.

SEQ_ACK - Sequence Number for Acknowledgment by the *OTASP Transport Confirmation Message*. The mobile station shall set this field to the value of SEQ_NUM in the *OTASP Transport Message* being acknowledged.

DMU_CRC_OK - *OTASP Data Message* Unit CRC status flag. The mobile station shall set this field as specified in 2.2.3.2 to indicate whether or not the *OTASP Data Message* Unit CRC checks.

RSVD - Reserved for future use; the mobile station shall set all bits as indicated.

P - Parity field. The mobile station shall set this field as specified in 2.7.2 of [1].

2.2.4 Base Station Procedures

OTASP Data Messages are sent and received on the analog voice channel only when the base station is in the Conversation Task (see 3.6.4.4 of [1]). The base station shall transmit *OTASP Transport Messages* as specified in 3.7.2 of [1]. Base stations implementing the Over-the-Air Service Provisioning feature should comply with the following requirements in addition to those of 3.6.4.4 of [1].

2.2.4.1 Message Transmission

While the base station is in the Conversation Task, the following messages can be sent in addition to those listed in 3.6.4.4 of [1]:

1. *OTASP Transport Message:*

   The base station should construct the *OTASP Transport Message* as follows:

   - If the OTASP_DATA field of the *OTASP Transport Message* contains an entire *OTASP Data Message* Capsule, the base station should set the value of the SEQ_NUM field to ‘00000’ and the value of the B/F field to ‘11’.
   - If the OTASP_DATA field of the *OTASP Transport Message* contains the first segment of the segmented *OTASP Data Message* Capsule, the base station should set the value of the SEQ_NUM field to ‘00000’ and the value of the B/F field to ‘10’.
   - If the OTASP_DATA field of the *OTASP Transport Message* contains a segment other than the first segment of the segmented *OTASP Data Message* Capsule, the base station should perform the following:
     - If the OTASP_DATA field of the *OTASP Transport Message* contains a segment other than the final segment of the *OTASP Data Message* Capsule, the base station should increment SEQ_NUM modulo 32 and should set the value of the B/F field to ‘00’.
     - If the OTASP_DATA field of the *OTASP Transport Message* contains the final segment of the *OTASP Data Message*, the base station should increment SEQ_NUM modulo 32 and should set the value of the B/F field to ‘01’.

   The base station should remain in the Conversation Task.

2. *OTASP Transport Confirmation Message*:

   The base station should set the SEQ_ACK field to the value of the SEQ_NUM field received in the *OTASP Transport Message* being acknowledged, and should remain in the Conversation Task.

2.2.4.2 Message Reception

While the base station is in the Conversation Task, the following messages can be received autonomously from the mobile station, in addition to those listed in 3.6.4.4 of [1]. When any message is received, the base station should perform all actions specified in 3.6.4.4 of [1] that apply to a message reception. The base station shall take the actions specified below for each message:

1. *OTASP Transport Message*:

   If the value of ESN received in the *OTASP Transport Message* does not match the ESN that identifies the mobile station being activated, the base station should ignore the message.

   If the value of ESN received in the *OTASP Transport Message* matches the ESN that identifies the mobile station being activated, the base station should do the following:

   - The base station should send an *OTASP Transport Confirmation Message*.
   - If the value of the B/F field of the received message is '11', the OTASP_DATA field of the received message contains the *OTASP Data Message* Capsule in its entirety. The base station may discard any incomplete *OTASP Data Message* being reassembled, and should process the *OTASP Data Message* as specified in Section 4.
   - If the value of the B/F field of the received message is '10', the base station may discard any incomplete *OTASP Data Message* being reassembled, and should store the OTASP_DATA field of the received message as the first segment of an *OTASP Data Message* Capsule to be reassembled. The base station should store the value of the SEQ_NUM field of the received message in RX_SEQ_NUM.
   - If the value of the B/F field of the received message is '00' and a segmented *OTASP Data Message* Capsule is being reassembled, the base station should perform the following:
     - If (RX_SEQ_NUM + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the base station should store the OTASP_DATA field of the received message as the next segment of the *OTASP Data Message* being reassembled, and increment RX_SEQ_NUM modulo 32.
     - If RX_SEQ_NUM is equal to the value of the SEQ_NUM field of the received message, the base station may discard the OTASP_DATA field of the received message.
     - If neither RX_SEQ_NUM nor (RX_SEQ_NUM + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the base station may discard the OTASP_DATA field of the received message and may discard the incomplete *OTASP Data Message* being reassembled.

- If the value of the B/F field of the received message is ‘00’, and no segmented *OTASP Data Message* Capsule is being reassembled, the base station may discard the OTASP_DATA field of the received message.
- If the value of the B/F field of the received message is ‘01’ and a segmented *OTASP Data Message* Capsule is being reassembled, the base station should perform the following:
  - If (RX_SEQ_NUM + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the base station should store the OTASP_DATA field of the received message as the last segment of the *OTASP Data Message* Capsule being reassembled, should increment RX_SEQ_NUM modulo 32, and should process the *OTASP Data Message* as specified in Section 4.
  - If RX_SEQ_NUM is equal to the value of the SEQ_NUM field of the received message, the base station may discard the OTASP_DATA field of the received message.
  - If neither RX_SEQ_NUM nor (RX_SEQ_NUM + 1) modulo 32 is equal to the value of the SEQ_NUM field of the received message, the base station may discard the OTASP_DATA field of the received message and may discard the incomplete *OTASP Data Message* Capsule being reassembled.
- If the value of the B/F field of the received message is ‘01’, and no segmented *OTASP Data Message* Capsule is being reassembled, the base station may discard the OTASP_DATA field of the received message.

The base station should remain in the Conversation Task.

2. *OTASP Transport Confirmation Message:*

If SEQ_ACK is equal to the sequence number of the last *OTASP Transport Message* sent, the base station may transmit the next *OTASP Transport Message*; otherwise, the base station should ignore the message. If the DMU_CRC_OK field indicates that the CRC of the *OTASP Data Message* Unit did not check at the mobile station (see 2.2.3.3), the base station should resend the *OTASP Data Message*. The base station should remain in the Conversation Task.

2.2.4.3 Forward Voice Channel Message Format

2.2.4.3.1 *OTASP Transport Message*

When the base station sends an *OTASP Transport Message* on the Forward Voice Channel (FVC), it shall use the following variable-length message format:

- Word 1 of the *OTASP Transport Message:*

Information Element	Length (bits)
T_1T_2 = 10	2
SCC=11	2
PSCC	2
EF=0	1
SEQ_NUM	5
DATA_WORDS	3
MSG_TYPE=00000	5
ORDQ=000	3
ORDER=11010	5
P	12

- Word 2 of the *OTASP Transport Message:*

Information Element	Length (bits)
T_1T_2 = 01	2
B/F	2
ESN_4	8
ESN_3	8
ESN_2	8
P	12

- Word 3 of the *OTASP Transport Message:*

Information Element	Length (bits)
T_1T_2 = 01	2
RSVD=00	2
ESN_1	8
OTASP_DATA	16
P	12

- Word 4 through N of the *OTASP Transport Message:*

Information Element	**Length (bits)**
T_1T_2 = 01	2
RSVD=00	2
OTASP_DATA	24
P	12

T_1T_2	-	Type field. The base station shall set this field to '10' in the first word of the message, and to '01' in all other words.
SCC	-	SAT color code for new channel. The base station shall set this field to '11'.
PSCC	-	Present SAT color code. The base station shall set this field to indicate the SAT color code associated with the present channel as specified in the Table 3.7.1.1-2 of [1].
EF	-	Extended Protocol Forward Channel Indicator. The base station shall set this field to '0'.
SEQ_NUM	-	Message Sequence Number. The base station shall set this field to the message sequence number of this *OTASP Transport Message*.
DATA_WORDS	-	The number of words in the *OTASP Transport Message* containing the OTASP_DATA field. The base station shall set this field to the number of words in the *OTASP Transport Message,* not including Word 1 and Word 2.
MSG_TYPE	-	Message Type field. The base station shall set this field to '00000'.
ORDQ	-	Order qualifier field. The base station shall set this field to '000'.
ORDER	-	Order field. The base station shall set this field to '11010'.
B/F	-	Begin/Final. This field is used to specify whether the *OTASP Data Message* Capsule has been segmented into multiple *OTASP Transport Messages.* If the *OTASP Data Message* Capsule is completely contained in a single *OTASP Transport Message,* the base station shall set this field to '11'. For an *OTASP Data Message* Capsule contained in multiple *OTASP Transport Messages,* the base station shall set the value of this field in the first segment to '10', the value of this field in all intermediate segments to '00', and the value of this field in the final segment to '01'.
ESN_4	-	The base station shall set this field to the most significant octet (bits d31-d24) of the mobile station ESN.
ESN_3	-	The base station shall set this field to the next to the most significant octet (bits d23-d16) of the mobile station ESN.

ESN_2	-	The base station shall set this field to the next to the least significant octet (bits d15-d8) of the mobile station ESN.
ESN_1	-	The base station shall set this field to the least significant octet (bits d7-d0) of the mobile station ESN.
OTASP_DATA	-	The base station shall set these fields to the corresponding octets of the *OTASP Data Message* Capsule.
RSVD	-	Reserved for future use; the base station shall set all bits as indicated.
P	-	Parity field. The base station shall set this field as specified in 3.7.2 of [1].

2.2.4.3.2 *OTASP Transport Confirmation Message*

When the base station sends an *OTASP Transport Confirmation Message* on the Forward Voice Channel (FVC), it shall use the following fixed-length message format:

Information Element	Length (bits)
T_1T_2 = 10	2
SCC=11	2
PSCC	2
EF=0	1
SEQ_ACK	5
RSVD=000	3
MSG_TYPE=00001	5
ORDQ=000	3
ORDER=11010	5
P	12

T_1T_2	-	Type field. The base station shall set this field to ‘10’.
SCC	-	SAT color code for new channel. The base station shall set this field to ‘11’.
PSCC	-	Present SAT color code. The base station shall set this field to indicate the SAT color code associated with the present channel as specified in the Table 3.7.1.1-2 of [1].
EF	-	Extended Protocol Forward Channel Indicator. The base station shall set this field to ‘0’.

SEQ_ACK	-	Sequence Number for Acknowledgment by the *OTASP Transport Confirmation Message*. The base station shall set this field to the value of SEQ_NUM in the *OTASP Transport Message* being acknowledged.
MSG_TYPE	-	Message Type field. The base station shall set this field to '00001'.
ORDQ	-	Order qualifier field. The base station shall set this field to '000'.
ORDER	-	Order field. The base station shall set this field to '11010'.
RSVD	-	Reserved for future use; the base station shall set all bits as indicated.
P	-	Parity field. The base station shall set this field as specified in 3.7.2 of [1].

2.3 CDMA Transport Protocol

The messages defined in 3.5 and 4.5 shall be sent in the CHARi fields of *Data Burst Messages* (see 6.7.2.3.2.4 and 7.7.3.3.2.4 of [1] and 2.7.2.3.2.4 and 3.7.3.3.2.4 of [7]). The BURST_TYPE field of *Data Burst Messages* carrying *OTASP Data Messages* shall be set to '000100' (as assigned in [4]). The MSG_NUMBER and NUM_MSGS fields shall be set to 1 and the NUM_FIELDS field shall be set to the number of octets in the *OTASP Data Message.*

The base station should send *Data Burst Messages* carrying *OTASP Data Messages* only on CDMA Traffic Channels. Mobile stations shall ignore *Data Burst Messages* with the BURST_TYPE field equal to '000100' that are received on CDMA channels other than CDMA Traffic Channels. *Data Burst Messages* carrying *OTASP Data Messages* shall be sent as messages requiring Layer 2 acknowledgment (see 6.6.4.1.3.1 and 7.6.4.1.3.1 of [1] or as messages requiring delivery in assured mode see 1.3.2.1 and 1.3.2.2 of [7]).

No text.

3 MOBILE STATION PROCEDURES

3.1 Initial Values and NAM Parameters

Mobile stations support one or more Number Assignment Modules (NAM). The NAM includes certain numeric indicators, as defined in Annex F of [1, 7]. The standard NAM indicators, stored in the mobile station's permanent and semi-permanent memory, are defined in F.3 of [1, 7]. Manufacturer-specific NAM parameters may be defined within a Parameter Block Type reserved for manufacturer-specific parameter definitions (see Tables 3.5.2-1 and 4.5.2-1).

Mobile stations supporting Service Programming Lock shall maintain a single additional indicator, SPC_p (see 3.3.6).

Mobile stations supporting the Over-the-Air Parameter Administration (OTAPA) shall maintain an additional indicator for each NAM, NAM_LOCK_p (see 3.2.2).

The NAM indicators and parameters that can be assigned values using Over-the-Air Service Provisioning are specified in 4.5.2, 4.5.3, 4.5.4 and 4.5.6.

A mobile station shall have a single NAM selected for use at all times. If a mobile station supports more than one NAM, the mobile station manufacturer shall provide a means for the user to select the NAM to be activated.

When a mobile station is manufactured, and whenever a NAM is created or cleared:

- $IMSI\_M\_CLASS_p$ shall be set to 0.
- MCC_M_p, $IMSI\_M\_11\_12_p$ and $IMSI\_M\_S_p$ shall be set to the coded value of the IMSI_M with the four least-significant digits set to ESN_p, converted directly from binary to decimal, modulo 10000. The other digits shall be set to 0.
- $IMSI\_M\_ADDR\_NUM_p$ shall be set to '000'.
- $IMSI\_T\_CLASS_p$ shall be set to 0.
- MCC_T_p, $IMSI\_T\_11\_12_p$ and $IMSI\_T\_S_p$ shall be set to the coded value of the IMSI_T with the four least-significant digits set to ESN_p, converted directly from binary to decimal, modulo 10000. The other digits shall be set to 0.
- $IMSI\_T\ \_ADDR\_NUM_p$ shall be set to '000'.
- $ACCOLC_p$ shall be set as specified in 6.3.5 of [1] or 2.3.5 of [7].
- $HOME\_SID_p$, if present, shall be set to 0.
- All other indicators of the selected NAM may be set to manufacturer-defined default values. All configuration indicator values shall be set within their valid range (see F.3 of [1, 7]).

Mobile stations may perform any function allowable by applicable standards, including system accesses, whether the selected NAM is activated or not.

3.2 Initiation of the Programming Procedures

Over-the-air service provisioning (OTASP) can be initiated in two ways: by the user and by the network.

The user-initiated procedure provides a tool for the mobile station user to select a wireless service provider, to activate a mobile station, and to update NAM indicators and parameters.

The network-initiated procedure, also known as Over-The-Air Parameter Administration (OTAPA), is also built upon the over-the-air programming protocol and procedures that support the OTASP feature. OTAPA provides a tool for the wireless service provider to update NAM indicators and parameters.

3.2.1 User-Initiated Procedure

The mobile station shall initiate programming procedures only when directed to do so by the user. The procedure for user initiation of the programming procedure is manufacturer-defined. Upon initiation of the programming procedure, the mobile station shall set $\text{PRL\_BLOCK\_ID\_CURRENT}_S$ to NULL. As part of this procedure, the mobile station shall permit the user to enter a choice of the service provider. At a minimum, the mobile station shall permit the user to manually enter the activation code for the selected system using the following sequence:

- *FC + XX + SEND

*FC - Feature Code (*ACT or *228). This feature code indicates the activation call type to the base station.

XX - System Selection Code. This code indicates the system selected by the user. See Table 3.2-1.

Table 3.2-1 System Selection Code.

Selected System	Code
800 MHz, A-Band	00
800 MHz, B-Band	01
1.9 GHz, A Block	02
1.9 GHz, B Block	03
1.9 GHz, C Block	04
1.9 GHz, D Block	05
1.9 GHz, E Block	06
1.9 GHz, F Block	07
TACS, A-Band	08
TACS, B-Band	09
JTACS, A-Band	10
JTACS, B-Band	11
Korean PCS, A-Band	12
Korean PCS, B-Band	13
Korean PCS, C-Band	14
450 MHz, A-Band	15
450 MHz, B-Band	16
450 MHz, C-Band	17
450 MHz, D-Band	18
450 MHz, E-Band	19
450 MHz, F-Band	20
450 MHz, G-Band	21
450 MHz, H-Band	22
2 GHz Band	23
700 MHz, A-Band	24
700 MHz, B-Band	25
700 MHz, C-Band	26
700 MHz, D-Band	27
1800 MHz Band	28
900 MHz Band	29
Secondary 800 MHz, A-Band	30
Secondary 800 MHz, B-Band	31

Secondary 800 MHz, C-Band	32
Secondary 800 MHz, D-Band	33
Secondary 800 MHz, E-Band	34
400 MHz European PAMR, A-Band	35
400 MHz European PAMR, B-Band	36
400 MHz European PAMR, C-Band	37
400 MHz European PAMR, D-Band	38
400 MHz European PAMR, E-Band	39
400 MHz European PAMR, F-Band	40
800 MHz PAMR, A-Band	41
800 MHz PAMR, B-Band	42
Reserved	43 through 99

The user may append additional digits after the System Selection Code.

The activation code consists of the Feature Code, the System Selection Code and any additional digits that the user appends.

The mobile station shall use the preferred roaming list to select the system if either of the following sets of conditions hold:

- Set #1:
    - The mobile station supports the Service Programming Lock feature, and
    - The SPC$_p$ is set to any value other than the default value (see 3.3.6), and
    - The mobile station supports SSPR and the PR_LIST_SIZE is greater than zero (see 3.5.5).
- Set #2:
    - The user has entered the feature code (*FC) only (no system selection code or any additional digits have been entered), and
    - The mobile station supports SSPR and the PR_LIST_SIZE is greater than zero (see 3.5.5).

Otherwise, the mobile station shall use the system selection code (see Table 3.2-1) to acquire the system.

When the user directs the mobile station to begin the programming procedure, and if the mobile station is not already monitoring a selected system, the mobile station shall enter the *System Determination Substate* of the *Mobile Station Initialization State* with a provisioning indication.

If the mobile station enters the *System Determination Substate* of the *Mobile Station Initialization State* with a provisioning indication the mobile station shall perform the following:

- If an 800 MHz system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00000'.
  - If the user selects System A, the mobile station shall set SERVSYS_S to SYS_A. If the user selects System B, the mobile station shall set SERVSYS_S to SYS_B.
  - The mobile station shall set CDMACH_S to either the Primary or the Secondary CDMA Channel number (see 6.1.1.1.1 of [1] or 2.1.1.1.1 of [5]) for the selected system (A or B)- and shall attempt to acquire the system as specified in 6.6.1.1.3 of [1] or 2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should attempt to acquire on the alternate CDMA Channel (Primary or Secondary) before attempting other alternatives.
  - If the mobile station fails to acquire a CDMA system on either the Primary or Secondary CDMA Channel, the mobile station may attempt to acquire an analog system as specified in 6.6.1.1.3 of [1] or 2.6.1.1.3 of [7], using the current setting of SERVSYS_S.
- If a 1.9 GHz system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S = '00001'.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 6.1.1.1-4 of [1] or Table 2.1.1.1-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 6.6.1.1.3 of [1] or 2.6.1.1.3 of [7].
  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.
- If a TACS system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00010'.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.3-6 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 2.6.1.1.3 of [7].

  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.

- If a JTACS system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00011'.
  - If the user selects System A, the mobile station shall set SERVSYS_S to SYS_A. If the user selects System B, the mobile station shall set SERVSYS_S to SYS_B.
  - The mobile station shall set CDMACH_S to either the Primary or the Secondary CDMA Channel number (see 2.1.1.1.4 of [5]) for the selected system (A or B)- and shall attempt to acquire the system as specified in 2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should attempt to acquire a CDMA system on the alternate CDMA Channel (Primary or Secondary) in the same band before attempting other alternatives.

- If a Korean PCS Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00100'.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.5-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 2.6.1.1.3 of [7].
  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.

- If a 450 MHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00101'.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.6-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 2.6.1.1.3 of [7].

  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.

- If a 2GHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00110'.
  - The mobile station shall set CDMACH_S to a preferred CDMA channel number (see 2.1.1.1.7 of [5]) and shall attempt to acquire the system as specified in 2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should continue attempting to acquire different preferred CDMA channels until it acquires a CDMA system or until it exhausts all preferred CDMA channels within the CDMA Preferred Set.

- If the mobile station fails to acquire a system, or if the selected band is not supported by the mobile station, the mobile station shall terminate the programming procedure and shall retain the NAM indicator values and parameters specified in 3.1, in effect prior to the initiation of the programming procedure.

- If a 700MHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '00111'.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.8-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 2.6.1.1.3 of [5].
  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.

- If a 1800MHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to '01000'.
  - The mobile station shall set CDMACH_S to a preferred CDMA channel number (see 2.1.1.1.9 of [5]) and shall attempt to acquire the system as specified in 2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should continue attempting to acquire different preferred CDMA channels until it acquires a CDMA system or until it exhausts all preferred CDMA channels within the CDMA Preferred Set.

- If a 900MHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to ‘01001’.
  - The mobile station shall set CDMACH_S to a preferred CDMA channel number (see 2.1.1.1.10 of [5]) and shall attempt to acquire the system as specified in 2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should continue attempting to acquire different preferred CDMA channels until it acquires a CDMA system or until it exhausts all preferred CDMA channels within the CDMA Preferred Set.
- If a Secondary 800MHz Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to ‘01010’.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.11-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified in 2.6.1.1.3 of [7].
  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.
- If a 400MHz European PAMR Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to ‘01011’.
  - The mobile station shall set CDMACH_S to a preferred CDMA Channel number (see Table 2.1.1.1.12-5 of [5]) within the selected frequency block and shall attempt to acquire a CDMA system as specified 2.6.1.1.3 of [7].
  - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel it tries, the mobile station should set CDMACH_S to an alternate preferred CDMA Channel number within the selected frequency block and should attempt to acquire a CDMA system. The mobile station should continue attempting to acquire different preferred CDMA Channels until it acquires a CDMA system or until it exhausts all preferred CDMA Channels within the selected frequency block.
- If an 800MHz PAMR Band system is selected for provisioning, the mobile station shall perform the following:
  - The mobile station shall set CDMABAND_S to ‘01100’.
  - The mobile station shall set CDMACH_S to a preferred CDMA channel number (see 2.1.1.1.13 of [5]) and shall attempt to acquire the system as specified in

2.6.1.1.3 of [7]. If the mobile station fails to acquire a CDMA system on the first CDMA Channel it tries, the mobile station should continue attempting to acquire different preferred CDMA channels until it acquires a CDMA system or until it exhausts all preferred CDMA channels within the CDMA Preferred Set.

Once the selected system is acquired, the mobile station shall originate a call as follows:

- If the mobile station is in the CDMA mode, the mobile station shall perform the *Mobile Station Origination Operation*, as defined in 6.6.2.5 of [1] or 2.6.2.5 of [7], using the activation code as the dialed digits. The mobile station should request either a voice or an async data service option in the *Origination Message*. The mechanism used for the service option selection (either voice or async data) is vendor specific. The mobile station shall format each message sent on the CDMA Access Channel, Enhanced Access Channel, or Reverse Common Control Channel using an MSID field format that contains the mobile station's ESN or MEID.[1]
- If the mobile station is in the analog mode, the mobile station shall enter the System Access Task with an "origination" indication, using the activation code as the dialed digits. Regardless of the value of the S_S bit, the mobile station shall send Serial Number Word C in all Reverse Analog Control Channel messages.

If the mobile station responds to a page and the mobile station does not support concurrent services, the mobile station shall terminate the programming procedure and shall retain the NAM indicator values and parameters, specified in 3.1, in effect prior to the initiation of the programming procedure.

If the mobile station does not support Service Programming Lock, the mobile station shall set mobile station locking state SP_LOCK_STATE to '0'.

If the mobile station supports Service Programming Lock, and if SPC_p is equal to '0' (the default value), the mobile station shall set SP_LOCK_STATE to '0'; otherwise, the mobile station shall set SP_LOCK_STATE to '1'.

The mobile station shall set $SPC_s = SPC_p$.

When the mobile station supports OTAPA and the programming session was initiated by the user, the mobile station shall set the NAM_LOCK_STATE to '0' to indicate that SPASM does not protect access to the NAM parameters and indicators.

3.2.2 Network-Initiated Procedure

An OTAPA-capable mobile station should support a manufacturer-specific means by which the user may disable and enable OTAPA for a given NAM. OTAPA should be enabled by default. When enabled, OTAPA may be initiated by the network.

---

[1] For systems defined in [1] or [7], this means the MSID_TYPE field must be set to '000' or '011'. For systems defined in [1] or [7], the use of a pseudo ESN can potentially conflict with another pseudo ESN in the network performing the mobile provisioning. The system should implement protective procedures to guard against this case.

OTAPA procedures can be conducted when the mobile station is in the CDMA *Conversation Substate* or the analog Conversation Task (see 3.2.2.3). All *OTASP Data Messages* during the OTAPA session are exchanged between the base station and the mobile station using signaling traffic.

If the mobile station is in the CDMA *Mobile Station Idle State* the base station can place the mobile station on the CDMA Traffic Channel for the purpose of conducting OTAPA procedure (see 3.2.2.1).

3.2.2.1 Initiation of OTAPA in the CDMA Mobile Station Idle State

The network can initiate OTAPA by placing a mobile terminated call to the mobile station indicating the OTAPA service option in the *General Page Message.* The OTAPA Service Option when using Multiplex Option 1 is called Service Option 18. The OTAPA Service Option when using Multiplex Option 2 is called Service Option 19. The mobile station shall respond to paging as defined in 6.6 of [1] or 2.6 of [7] and perform service negotiation.

3.2.2.2 Connection of the OTAPA Service Option

A service option is connected when primary traffic data are being processed in accordance with the requirements of the service option.

The negotiated service configuration shall include only valid attributes for the negotiated service option consistent with those specified in Tables 3.2.2.2-1 and 3.2.2.2-2.

Table 3.2.2.2-1 Valid Service Configuration Attributes for Service Option 18

Service Configuration Attribute	Valid Selections
Forward Multiplex Option	Multiplex Option 1
Reverse Multiplex Option	Multiplex Option 1
Forward Transmission Rates	Rate Set 1 with all four rates enabled
Reverse Transmission Rates	Rate Set 1 with all four rates enabled
Forward Traffic Type	None. This service option does not use nor generate any forward traffic other than signaling.
Reverse Traffic Type	None. This service option does not use nor generate any reverse traffic other than signaling.

Table 3.2.2.2-2 Valid Service Configuration Attributes for Service Option 19

Service Configuration Attribute	Valid Selections
Forward Multiplex Option	Multiplex Option 2
Reverse Multiplex Option	Multiplex Option 2
Forward Transmission Rates	Rate Set 2 with all four rates enabled
Reverse Transmission Rates	Rate Set 2 with all four rates enabled
Forward Traffic Type	None. This service option does not use nor generate any forward traffic other than signaling.
Reverse Traffic Type	None. This service option does not use nor generate any reverse traffic other than signaling.

If the mobile station accepts a service configuration, as specified in a *Service Connect Message*, that includes a service option connection using Service Option 18 or 19, then the service option connection shall become part of the current service configuration at the action time associated with the *Service Connect Message*. Service Option 18 or 19 is considered connected when the current service configuration includes a service option connection for it.

If Service Option 18 or 19 is connected when the mobile station enters the *Waiting for Mobile Station Answer Substate*, or while the mobile station is in the *Waiting for Mobile Station Answer Substate*, the mobile station shall send a *Connect Order* to the base station as a message requiring acknowledgment without waiting for the user to explicitly command the call to be answered. The mobile station shall enter the *Conversation Substate*.

When Service Option 18 or 19 is connected, the Service Option shall discard all primary traffic data bits received from the multiplex sublayer, and the mobile station shall transmit null traffic channel data.

3.2.2.3 Starting the OTAPA session

If the mobile station supports OTAPA and OTAPA is enabled (see 3.2.2), the mobile station shall start the OTAPA session when it receives the *OTAPA Request Message* with the $START\_STOP_r$ equal to '1', while in the CDMA *Conversation Substate* or the analog Conversation Task.

Upon starting the OTAPA session, the mobile station shall set $PRL\_BLOCK\_ID\_CURRENT_s$ to NULL.

During the OTAPA session, access to individual parameters of the active NAM is controlled by the Subscriber Parameter Administration Security Mechanism (SPASM).

If the programming session was initiated by the user as described in 3.2.1, SPASM does not protect access to the NAM parameters and indicators; otherwise, upon invocation of the OTAPA session the mobile station shall set the $NAM\_LOCK_s = NAM\_LOCK_p$ and $NAM\_LOCK\_STATE = NAM\_LOCK_p$. The NAM_LOCK_STATE being set to '0' indicates that SPASM protection of the mobile station's active NAM is disabled. The NAM_LOCK_STATE being set to '1' indicates that SPASM protection of the mobile station's active NAM is enabled.

If the mobile station does not support Service Programming Lock, the mobile station shall set mobile station locking state SP_LOCK_STATE to '0'.

If the mobile station supports Service Programming Lock, and if SPC_p is equal to '0' (the default value), the mobile station shall set SP_LOCK_STATE to '0'; otherwise, the mobile station shall set SP_LOCK_STATE to '1'.

The mobile station shall set $SPC_s = SPC_p$.

3.3 Programming Procedure

3.3.1 *OTASP Data Message* Processing

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

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

1. *Configuration Request Message:* The mobile station shall send a *Configuration Response Message* within 750 ms after receiving the message.
    - If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall set the RESULT_CODE in all corresponding returned confirmation blocks to '00001010', "Rejected - Mobile station locked." The mobile station shall include all requested parameter blocks with the BLOCK_LEN field set to '00000000'.
    - If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:

  - If the mobile station does not support a requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000111’, “Rejected - BLOCK_ID value not supported.” The mobile station shall include the parameter block with the BLOCK_LEN field set to ‘00000000’.

  - If the requested data blocks exceed the allowable message length, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the message. The mobile station shall include data blocks, in the order requested, up to the maximum number of blocks that fit into the message. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *Configuration Response Message*. All the encrypted Parameter Blocks and FRESH field shall fit into the *Configuration Response Message.*

  - Otherwise, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the corresponding confirmation block. The mobile station shall include complete data blocks, in the order requested, in the *Configuration Response Message*. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *Configuration Response Message*.

2. *Download Request Message:* The mobile station shall respond to the message with a *Download Response Message* within 750 ms.

   - If FRESH_INCL$_r$ = ‘1’ and the SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set FRESH$_S$ = FRESH$_r$ and decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *Download Request Message.*

   - If the *Download Request Message* contains an OTASP Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000111’, “Rejected - BLOCK_ID value not supported;”

   - If the *Download Request Message* contains an OTASP Parameter Block having a size different from that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000010’, “Rejected - Data size mismatch;”

- If the *Download Request Message* contains an OTASP Parameter Block with a parameter value that is out-of-range, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000100', "Rejected - Invalid parameter;"

- If the *Download Request Message* contains an OTASP Parameter Block with MAX_SID_NID larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000101', "Rejected - SID/NID length mismatch;"

- If the *Download Request Message* is not accepted for any other reason, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000001', "Rejected - Unknown reason;"

- Otherwise, the mobile station shall store the message data in temporary memory, set BLOCK_ID to the received parameter block identifier and set RESULT_CODE to '00000000', "Accepted - Operation successful." Then, if the mobile station supports the optional NAM indicators (see F.3 of [1, 7]), the mobile station should also store values for CDMA_PREF_SERV_p and $\text{ANALOG\_PREF\_SERV}_p$ equal to the serving system selected for activation in temporary memory. If more than one *Download Request Message* or parameter block is received containing values for the same indicators, the mobile station shall retain only the most recently received values. If the received data includes SID/NID pairs, the mobile station shall retain only the SID/NID pairs from the most recently received message.

3. *Commit Request Message:* The mobile station shall send a *Commit Response Message* within 10 seconds after receiving the message.

- If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall not move data from temporary memory to permanent memory. The mobile station shall set RESULT_CODE to '00001010', "Rejected - Mobile station locked;" otherwise,
  - If the mobile station is able to move data from temporary memory to permanent memory successfully, the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful."
  - If the mobile station is not able to move data from temporary memory to permanent memory for any other reason, the mobile station shall set the RESULT_CODE to '00000001', "Rejected - Unknown reason."
  - If the mobile station has received configuration parameters in one or more *Download Request Messages*, it shall set the NAM indicators to the values contained in the received configuration parameters data. The mobile station shall not change the value of any NAM indicator for which no data has been received.

- If the mobile station has received Preferred Roaming List parameters in one or more *SSPR Download Request Messages*, it shall set the permanent Preferred Roaming List parameters to the values contained in the received data. The mobile station shall set the CUR_SSPR_P_REV$_{s\text{-}p}$ according to the following rules:

    If PRL_BLOCK_ID_CURRENT$_s$ is set to ‘00000000’ (Preferred Roaming List Parameter Block), then the mobile station shall set the CUR_SSPR_P_REV$_{s\text{-}p}$ to ‘00000001’.

    - If PRL_BLOCK_ID_CURRENT$_s$ is set to ‘00000001’ (Extended Preferred Roaming List Parameter Block), then the mobile station shall set the CUR_SSPR_P_REV$_{s\text{-}p}$ to the value of CUR_SSPR_P_REV in the Extended Preferred Roaming List (see Section 3.5.5).

- If the mobile station has received 3GPD parameters in one or more *3GPD Download Request Messages*, it shall set the permanent 3GPD parameters to the values contained in the received data.

- If the mobile station has received Preferred User Zone List parameters in one or more *PUZL Download Request Messages*, it shall set the permanent Preferred User Zone List parameters to the values contained in the received data.

- If the mobile station has received User Zone Delete parameter blocks in one or more *PUZL Download Request Messages*, it shall remove the identified user zone entry(s) from the current Preferred User Zone List.

- If the received data includes SID/NID pairs, the mobile station shall set the NAM indicators to include only the SID/NID pairs received.

- If the mobile station has stored A_KEY_TEMP$_s$ after receiving a *Key Generation Request Message*, it shall set the value of the A_KEY$_p$ NAM indicator equal to A_KEY_TEMP$_s$.

- If the mobile station has stored RK_TEMP$_s$ after receiving a *Key Generation Request Message*, it shall set the value of the RK$_p$ NAM indicator equal to RK_TEMP$_s$.

- If the mobile station has generated the SSD$_s$ as a result of an SSD update procedure based on the A_KEY_TEMP$_s$, the mobile station shall store the SSD$_s$ in SSD$_{s\text{-}p}$.

- If the mobile station has stored temporary service keys after receiving a *Service KeyGeneration Request Message*, it shall store the service keys to permanent memory.

- If the mobile station has stored the SPC$_s$ after receiving a *Validation Request Message*, it shall set the value of the SPC$_p$ parameter equal to SPC$_s$.

- If the mobile station has stored the NAM_LOCK_s after receiving a *Validation Request Message*, it shall set the value of the NAM_LOCK_p parameter equal to NAM_LOCK_s.

- If the mobile station has received System Tag List parameters in one or more *System Tag Download Request Messages*, it shall set the permanent System Tag List parameters to the values contained in the received data. The mobile station shall set the $TAG\_P\_REV_{s-p}$ to $TAG\_P\_REV_r$.

4. *Re-Authenticate Request Message:* The mobile station shall send a *Re-Authenticate Response Message* within 750 ms after receiving the message. The mobile station shall set $RAND_s = RAND_r$. The mobile station shall perform the re-authentication procedures specified in 3.3.2.

5. *MS Key Request Message:* The mobile station shall set $PARAM\_P_s = PARAM\_P_r$ and $PARAM\_G_s = PARAM\_G_r$ if A_KEY_P_REV received in the *MS Key Request Message* = ‘00000010’.

   If A_KEY_P_REV received in the *MS Key Request Message* = ‘00000011’, ‘00000100’ or ‘00000101’, the mobile station shall set $PARAM\_P_s$ and $PARAM\_G_s$ to the values as specified in 5.3.1, respectively.

   - If the value of A_KEY_P_REV in the *MS Key Request Message* is not supported by the mobile station, the mobile station shall indicate the error condition by setting RESULT_CODE to ‘00000011’, “Rejected - Protocol version mismatch.” The mobile station shall send an *MS Key Response Message* within 750 ms after receiving this message.

   - If the value of A_KEY_P_REV in the *MS Key Request Message* is supported by the mobile station, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful.” The mobile station shall compute the MS_RESULT value according to the value of A_KEY_P_REV received in the *MS Key Request Message* as follows:

     ‘00000010’, calculate MS_RESULT in accordance with 5.1.2;

     ‘00000011’, calculate MS_RESULT in accordance with 5.3.2;

     ‘00000100’, calculate MS_RESULT in accordance with 5.3.2;

     ‘00000101’, calculate MS_RESULT in accordance with 5.5.2.

     The mobile station shall send an *MS Key Response Message* within 30 seconds after receiving this message.

   - If the mobile station is unable to compute the MS_RESULT value in accordance with 5.1.2, 5.3.2 or 5.5.2, the mobile station shall set RESULT_CODE to ‘00000001’, “Rejected - Unknown reason.” The mobile station shall send an *MS Key Response Message* within 30 seconds after receiving this message.

6. *Key Generation Request Message:*

- If the mobile station has not received an *MS Key Request Message,* the mobile station shall indicate the error condition by setting RESULT_CODE to ‘00000110’, “Rejected - Message not expected in this mode.” The mobile station shall send a *Key Generation Response Message* within 750 ms after receiving this message.

- If the mobile station has received an *MS Key Request Message* and returned RESULT CODE other then ‘00000000’, “Accepted - Operation successful,” the mobile station shall indicate the error condition by setting RESULT_CODE to ‘00000110’, “Rejected - Message not expected in this mode.” The mobile station shall send a *Key Generation Response Message* within 750 ms after receiving this message.

- If the mobile station has received an *Key Generation Request Message* with the value of BS_RESULT equal to 0, the mobile station shall set RESULT_CODE to ‘00000001’, “Rejected - Unknown reason.” The mobile station shall then send a *Key Generation Response Message* within 750 ms after receiving this message.

- Otherwise, the mobile station shall compute the value of the A-key, A-key and Root Key combination, or Root Key if the value of A_KEY_P_REV received in the *MS Key Request Message* equals to:

  ‘00000010’, calculate A-key in accordance with 5.1.3;

  ‘00000011’, calculate A-key and Root Key in accordance with 5.3.3;

  ‘00000100’, calculate Root Key in accordance with 5.3.4;

  ‘00000101’, calculate Root Key in accordance with 5.5.3.

- If the mobile station has not successfully calculated the A-key, A-key and Root Key combination, or Root Key in accordance with 5.1.3, 5.3.3, 5.3.4 and 5.5.3 respectively, the mobile station shall set RESULT_CODE to ‘00000001’, “Rejected - Unknown reason.” The mobile station shall then send a *Key Generation Response Message* within 30 seconds after receiving this message.

- If the mobile station has successfully calculated the A-key, A-key and Root Key combination, or Root Key in accordance with 5.1.3, 5.3.3, 5.3.4 and 5.5.3 respectively, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful”. The mobile station shall then send a *Key Generation Response Message* ~~or an *Extended Protocol Capability Response Message*~~ within 30 seconds after receiving this message. ~~If the Protocol Capability Request Message contains the OTASP_P_REV field and the mobile station is able to parse it, then the mobile station shall send the *Extended Protocol Capability Response Message*; otherwise, the mobile station shall send the *Protocol Capability Response Message.*~~

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

8. *SSPR Configuration Request Message:* The mobile station shall send an *SSPR Configuration Response Message* within 750 ms after receiving the message.

   - If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall set RESULT_CODE in the *SSPR Configuration Response Message* to '00001010', "Rejected - Mobile station locked". The mobile station shall include the requested parameter block with the BLOCK_LEN field set to zero.

   - If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:

     - If the mobile station does not support the requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned parameter block to '00000111', "Rejected - BLOCK_ID value not supported." The mobile station shall include the parameter block with the BLOCK_LEN field set to zero.

     - If the *SSPR Configuration Request Message* contains the request for the Preferred Roaming List Dimension Parameter Block (BLOCK_ID = '00000000') and if the mobile station supports SSPR_P_REV greater than or equal to '00000011' and stores preferred roaming list associated with SSPR_P_REV greater than or equal to '00000011', then, the mobile station shall set the RESULT_CODE in the *SSPR Configuration Response Message* to '00100011', "Rejected – PRL format mismatch." The mobile station shall include the parameter block with the BLOCK_LEN field set to zero.

     - If the REQUEST_OFFSET_r received in the message specifies an offset which is invalid for the current preferred roaming list, the mobile station shall set the RESULT_CODE in the corresponding returned parameter block to '00000010', "Rejected - Data size mismatch."

       The mobile station shall set the BLOCK_ID to the corresponding parameter block identifier, the SEGMENT_OFFSET in the returned Parameter Block to the value of the REQUEST_OFFSET_r, the SEGMENT_SIZE to '00000000', and shall include no octets of the preferred roaming list in the returned Parameter Block.

     - Otherwise, if the *SSPR Configuration Request Message* contains the request for the Preferred Roaming List Parameter Block (BLOCK_ID = '00000001'), and if the REQUEST_OFFSET_r received in the message is valid for the current preferred roaming list, the mobile station shall set the RESULT_CODE in the *SSPR Configuration Response Message* to '00000000', "Accepted - Operation successful" for the Parameter Block included in the message.

       The mobile station shall include the preferred roaming list data (PR_LIST_{s-p}) starting at the offset corresponding to the REQUEST_OFFSET_r and not exceeding a maximum number of octets corresponding to the $\text{REQUEST\_MAX\_SIZE}_r$ received in the message.

The mobile station shall set the SEGMENT_OFFSET in the returned Parameter Block to the value of the REQUEST_OFFSET$_r$ received in the message.

The mobile station shall set the SEGMENT_SIZE field to the number of octets of the preferred roaming list included in the returned Parameter Block. If the Parameter Block contains the last segment of the preferred roaming list data, the mobile station shall set the LAST_SEGMENT field to '1'; otherwise the mobile station shall set the LAST_SEGMENT field to '0' in the returned Parameter Block.

9. *SSPR Download Request Message:* The mobile station shall respond to the message with an *SSPR Download Response Message* within 750 ms.

- If FRESH_INCL$_r$ = '1' and the SECURE_MODE_IND$_S$ = '1', the mobile station shall set FRESH$_s$ = FRESH$_r$ and decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *SSPR Download Request Message*.
- If the *SSPR Download Request Message* contains an SSPR Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set the RESULT_CODE in the *SSPR Download Response Message* to '00000111', "Rejected - BLOCK_ID value not supported" and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall set the SEGMENT_OFFSET and the SEGMENT_SIZE in the *SSPR Download Response Message* to '00000000'.
- If the *SSPR Download Request Message* contains an SSPR Parameter Block having a size different from that supported by the mobile station, the mobile station shall set the RESULT_CODE in the *SSPR Download Response Message* to '00000010', "Rejected - Data size mismatch" and shall set the BLOCK_ID to the received parameter block identifier.

  The mobile station shall set SEGMENT_OFFSET to the value of SEGMENT_OFFSET received in the message. The mobile station shall set SEGMENT_SIZE to the value of SEGMENT_SIZE received in the message.
- If the SSPR Download Request Message does not contain an SSPR Parameter Block with a BLOCK_ID of either '00000000' (Preferred Roaming List) or '00000001' (Extended Preferred Roaming List), the mobile station shall omit the SEGMENT_OFFSET and SEGMENT_SIZE.• Otherwise, if the BLOCK_ID field in the *SSPR Download Request Message* is equal to '00000000' or '00000001' (Preferred Roaming List Parameter Block or Extended Preferred Roaming List Parameter Block, respectively), the mobile station shall perform the following:
  - The mobile station shall set SEGMENT_OFFSET to the value of SEGMENT_OFFSET received in the message. The mobile station shall set SEGMENT_SIZE to the value of SEGMENT_SIZE received in the message.

- If $\text{PRL\_BLOCK\_ID\_CURRENT}_S$ is not NULL and the value of the BLOCK_ID_r field is not equal to $\text{PRL\_BLOCK\_ID\_CURRENT}_S$, the mobile station shall perform the following:
    - + Set the RESULT_CODE in the *SSPR Download Response Message* to '00100010', "Rejected – Unexpected PRL BLOCK_ID change".
    - + In the *SSPR Download Response Message*, set the BLOCK_ID to the received parameter block identifier and set the SEGMENT_OFFSET and the SEGMENT_SIZE to '00000000'.
    - + Discard all the SEGMENT_DATA octets that have been received in an *SSPR Download Request Message* with the BLOCK_ID field set to '00000000' or '00000001'.
    - + Set the $\text{PRL\_BLOCK\_ID\_CURRENT}_S$ to NULL.
- Otherwise, the mobile station shall perform the following:
    - + Set the $\text{PRL\_BLOCK\_ID\_CURRENT}_S$ to the value of the BLOCK_ID field received in the *SSPR Download Request Message*.
    - + If SEGMENT_OFFSET in conjunction with SEGMENT_SIZE are inconsistent with the preferred roaming list storage capabilities of the mobile station, the mobile station shall set the RESULT_CODE to '00001000', "Rejected - Preferred roaming list length mismatch" and shall set the BLOCK_ID to the received parameter block identifier.
    - + Otherwise, if SEGMENT_OFFSET in conjunction with SEGMENT_SIZE are consistent with the preferred roaming list storage capabilities of the mobile station, the mobile station shall store the SEGMENT_DATA octets in temporary memory.
        - o If LAST_SEGMENT is equal to '0', the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful" and shall set the BLOCK_ID to the received parameter block identifier.
        - o If LAST_SEGMENT is equal to '1', the mobile station shall calculate the CRC, as specified in Section 3.5.5.1 for the preferred roaming list stored in temporary memory. If the CRC checks, the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful;" otherwise, the mobile station shall set the RESULT_CODE to '00001001', "Rejected - CRC error" and shall discard this segment and all previously assembled segments of the preferred roaming list from the temporary memory. The mobile station shall set the BLOCK_ID to the received parameter block identifier.

10. *Validation Request Message:* The mobile station shall send a *Validation Response Message* within 750 ms after receiving the message.

  - If the *Validation Request Message* contains a Validation Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set the BLOCK_ID to the received parameter block identifier and shall set the RESULT_CODE to '00000111', "Rejected - BLOCK_ID value not supported;"
  - If the *Validation Request Message* contains a Validation Parameter Block having a size different from that supported by the mobile station, the mobile station shall set the RESULT_CODE to '00000010', "Rejected - Data size mismatch" and shall set the BLOCK_ID to the received parameter block identifier.
  - If the *Validation Request Message* contains a Validation Parameter Block with a parameter value that is out-of-range, the mobile station shall set the RESULT_CODE to '00000100', "Rejected - Invalid parameter" and the BLOCK_ID to the received parameter block identifier.
  - If the *Validation Request Message* is not accepted for any other reason, the mobile station shall set the RESULT_CODE to '00000001', "Rejected - Unknown reason" and shall set the BLOCK_ID to the received parameter block identifier.

- If the *Validation Request Message* contains the Verify SPC Parameter Block, the mobile station shall compare the SPC_r received in the message with the SPC_s.
  - If the comparison results in a mismatch, the mobile station shall set the RESULT_CODE to '00001011', "Rejected - Invalid SPC" and shall set the BLOCK_ID to the received parameter block identifier.
  - Otherwise, if the comparison results in a match, the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful" and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall set the SP_LOCK_STATE to '0'.
- If the *Validation Request Message* contains the Change SPC Parameter Block, the mobile station shall do the following:
  - If SP_LOCK_STATE = '1', the mobile station shall set the RESULT_CODE to '00001010', "Rejected - Mobile station locked" and shall set the BLOCK_ID to the received parameter block identifier.
  - If SP_LOCK_STATE = '0' and SPC_s is set to the default value, the mobile station shall do the following:
    - + If the mobile station is programmed by the user to accept SPC change (see 3.3.6), the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful" and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall set SPC_s to SPC_r received in the message.
    - + If the mobile station is programmed by the user to deny SPC change, the mobile station shall set the RESULT_CODE to '00001100', "Rejected - SPC change denied by the user" and shall set the BLOCK_ID to the received parameter block identifier.

  - Otherwise, if SP_LOCK_STATE = ‘0’ and if the SPC_s is not set to the default value, the mobile station shall set $SPC_s = SPC_r$ received in the message and shall set the RESULT_CODE to ‘00000000’, “Accepted - Operation successful” and the BLOCK_ID to the received parameter block identifier.

- If the *Validation Request Message* contains both the Verify SPC Parameter Block and the Change SPC Parameter Block, the mobile station shall process the Verify SPC Parameter Block first.

- If the *Validation Request Message* contains the Validate SPASM Parameter Block, the mobile station shall do the following:

  - If the programming session was initiated by the user as described in 3.2.1, the mobile station shall set the RESULT_CODE to ‘00001110’, “Rejected - BLOCK_ID not expected in this mode” and shall set the BLOCK_ID to the received parameter block identifier.

  - If the NAM_LOCK_STATE = ‘0’, the mobile station shall set the RESULT_CODE to ‘00000000’, “Accepted - Operation successful” and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall set $NAM\_LOCK_s = NAM\_LOCK_r$ received in the message.

  - If the NAM_LOCK_STATE = ‘1’, the mobile station shall compare the $AUTH\_OTAPA_r$ received in the message with the $AUTH\_OTAPA_s$ calculated using SPASM Validation Procedure defined in 3.3.7.

    + If the comparison results in a mismatch, the mobile station shall set the RESULT_CODE to ‘00001101’, “Rejected - Invalid SPASM” and shall set the BLOCK_ID to the received parameter block identifier.

    + If the comparison results in a match, the mobile station shall set the RESULT_CODE to ‘00000000’, “Accepted - Operation successful” and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall set the NAM_LOCK_STATE to ‘0’ and the $NAM\_LOCK_s = NAM\_LOCK_r$.

11. *OTAPA Request Message*: The mobile station shall send the *OTAPA Response Message* within 750 ms after receiving the message.

- If the programming session was initiated by the user as described in 3.2.1, the mobile station shall indicate the error condition by setting RESULT_CODE to ‘00000110’, “Rejected - Message not expected in this mode.” The mobile station shall set the NAM_LOCK_IND field to ‘0’ and shall omit the RAND_OTAPA field in the *OTAPA Response Message*.

- If the mobile station does not support OTAPA, or if the OTAPA was disabled by the user as described in 3.2.2, the mobile station shall indicate the error condition by setting RESULT_CODE to ‘00000110’, “Rejected - Message not expected in this mode.” The mobile station shall set the NAM_LOCK_IND field to ‘0’ and shall omit the RAND_OTAPA field in the *OTAPA Response Message*.

- If the START_STOP$_r$ field received in the message is equal to '1', the mobile station shall do the following:
  - If the NAM_LOCK_STATE = '1', the mobile station shall set the NAM_LOCK_IND field to '1', RAND_OTAPA field to a randomly generated 32-bit value, and shall set the RESULT_CODE to the '00000000', "Accepted - Operation successful" in the *OTAPA Response Message*. The mobile station shall generate the AUTH_OTAPA$_s$ as specified in 3.3.7.
  - If the NAM_LOCK_STATE = '0', the mobile station shall set the NAM_LOCK_IND field to '0', the RESULT_CODE to the '00000000', "Accepted - Operation successful", and shall omit the RAND_OTAPA field in the *OTAPA Response Message*.
  - The mobile station shall start the OTAPA session (see 3.2.2.3).
- If the START_STOP$_r$ field received in the message is equal to '0', the mobile station shall set the NAM_LOCK_IND field to '0', the RESULT_CODE to the '00000000', "Accepted - Operation successful", and shall omit the RAND_OTAPA field in the *OTAPA Response Message*. The mobile station shall terminate the OTAPA session (see 3.4).

12. *PUZL Configuration Request Message*: The mobile station shall send a *PUZL Configuration Response Message* within 750 ms after receiving the message.
    - If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00001010', "Rejected - Mobile station locked". The mobile station shall set BLOCK_ID to the received value and set BLOCK_LEN to zero.
    - If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:
      - If the mobile station does not support the requested parameter block, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00000111', "Rejected - BLOCK_ID value not supported". The mobile station shall set BLOCK_ID to the received value and set BLOCK_LEN to zero.
      - If the *PUZL Configuration Request Message* contains the request for the PUZL Priorities Parameter Block (BLOCK_ID = '00000001'), and the REQUEST_INDEX value received in the message specifies an index that is invalid for the current preferred user zone list, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00000010', "Rejected – Data size mismatch".

        The mobile station shall set BLOCK_ID to the received parameter block identifier, set SEGMENT_INDEX in the returned parameter block to the value of the REQUEST_INDEX, set NUM_ENTRIES to '00000000' and include no UZ_ID, UZ_SID and UZ_PRIORITY field data.

- Otherwise, if the *PUZL Configuration Request Message* contains the request for the PUZL Priorities Parameter Block (BLOCK_ID = ‘00000001’), and the REQUEST_INDEX value received in the message specifies an index which is valid for the current preferred user zone list, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to ‘00000000’, “Accepted – Operation successful” and shall set BLOCK_ID to the received parameter block identifier.

  The mobile station shall include the UZ_ID, UZ_SID and UZ_PRIORITY values starting at the user zone entry in the current preferred user zone list corresponding to the REQUEST_INDEX value and not exceeding the maximum number of user zone entries specified by the REQUEST_MAX_ENTRIES value received in the message.

  The mobile station shall set SEGMENT_INDEX in the returned parameter block to the value of the REQUEST_INDEX received in the message.

  The mobile station shall set the NUM_ENTRIES field to the number of user zone entries for which ID, SID and priority information has been included in the returned parameter block. If the parameter block contains the information for the last user zone entry of the current preferred user zone list, the mobile station shall set the LAST_SEGMENT field to ‘1’; otherwise, the mobile station shall set the LAST_SEGMENT field to ‘0’ in the returned parameter block.

- If the *PUZL Configuration Request Message* contains the request for the User Zone Parameter Block (BLOCK_ID = ‘00000010’), and if the user zone entry identified by the UZ_ID and UZ_SID values received in the message is not present in the current preferred user zone list, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to ‘00010000’, “Rejected – User Zone not in PUZL”. The mobile station shall set BLOCK_ID to the received value and set BLOCK_LEN to zero.

- If the *PUZL Configuration Request Message* contains the request for the User Zone Parameter Block (BLOCK_ID = ‘00000010’), and if the REQUEST_OFFSET value received in the message specifies an offset which is invalid for the user zone entry, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to ‘00000010’, “Rejected – Data size mismatch”.

  The mobile station shall set BLOCK_ID to the received parameter block identifier, set SEGMENT_OFFSET in the returned parameter block to the value of the REQUEST_OFFSET, set UZ_ID and UZ_SID to the values received in the message, set SEGMENT_SIZE to ‘00000000’ and include no octets of the user zone entry in the returned parameter block.

- Otherwise, if the *PUZL Configuration Request Message* contains the request for the User Zone Parameter Block (BLOCK_ID = '00000010'), and if the REQUEST_OFFSET value received in the message specifies an offset which is valid for the specified user zone entry, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00000000', "Accepted – Operation successful", and shall set BLOCK_ID to the received parameter block identifier.

  The mobile station shall include the user zone entry of the preferred user zone list starting at the offset corresponding to the REQUEST_OFFSET and not exceeding a maximum number of octets corresponding to the REQUEST_MAX_SIZE received in the message.

  The mobile station shall set SEGMENT_OFFSET in the returned parameter block to the value of the REQUEST_OFFSET received in the message and set UZ_ID and UZ_SID to the values received in the message.

  The mobile station shall set SEGMENT_SIZE to the number of octets of the user zone entry included in the returned parameter block. If the parameter block contains the last segment of the user zone entry, the mobile station shall set the LAST_SEGMENT field to '1'; otherwise, the mobile station shall set the LAST_SEGMENT field to '0' in the returned parameter block.

- If the *PUZL Configuration Request Message* contains the request for the Preferred User Zone List Parameter Block (BLOCK_ID = '00000011'), and if the REQUEST_INDEX value received in the message specifies an index which is invalid for the current preferred user zone list, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00000010', "Rejected – Data size mismatch".

  The mobile station shall set BLOCK_ID to the received parameter block identifier, set NUM_ENTRIES to '1' in the returned parameter block, set SEGMENT_INDEX to the value of the REQUEST_INDEX, set SEGMENT_OFFSET to the value of REQUEST_OFFSET, set SEGMENT_SIZE to '00000000' and include no octets of the preferred user zone list in the returned parameter block.

- If the *PUZL Configuration Request Message* contains the request for the Preferred User Zone List Parameter Block (BLOCK_ID = '00000011'), and if the REQUEST_OFFSET value received in the message specifies an offset which is invalid for user zone entry identified by REQUEST_INDEX of the current preferred user zone list, the mobile station shall set RESULT_CODE in the *PUZL Configuration Response Message* to '00000010', "Rejected – Data size mismatch".

The mobile station shall set BLOCK_ID to the received parameter block identifier, set NUM_ENTRIES to ‘1’ in the returned parameter block, set SEGMENT_INDEX to the value of the REQUEST_INDEX, set SEGMENT_OFFSET to the value of REQUEST_OFFSET, set SEGMENT_SIZE to ‘00000000’ and include no octets of the preferred user zone list in the returned parameter block.

- Otherwise, if the *PUZL Configuration Request Message* contains the request for the Preferred User Zone List Parameter Block (BLOCK_ID = ‘00000011’), and if the REQUEST_INDEX value received in the message specifies an index which is valid for the current preferred user zone list, and if the REQUEST_OFFSET value received in the message specifies an offset which is valid for the user zone entry identified by REQUEST_INDEX, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted – Operation successful”, and shall set BLOCK_ID to the received parameter block identifier.

  The mobile station shall include the user zone entry specified by REQUEST_INDEX of the preferred user zone list starting at the offset corresponding to REQUEST_OFFSET and not exceeding a maximum number of octets corresponding to REQUEST_MAX_SIZE received in the message.

  The mobile station shall set SEGMENT_INDEX in the returned parameter block to the value of REQUEST_INDEX received in the message and shall set SEGMENT_OFFSET to the value of REQUEST_OFFSET.

  The mobile station shall set SEGMENT_SIZE to the number of octets of the user zone entry included in the returned parameter block. If the parameter block contains the last segment of the user zone entry, the mobile station shall set the LAST_SEGMENT field to ‘1’; otherwise, the mobile station shall set the LAST_SEGMENT field to ‘0’ in the returned parameter block.

  If the last segment of a user zone entry is included in the returned parameter block and if the REQUEST_MAX_SIZE number of octets has not been included, the mobile station shall include a segment of the next user zone entry of the preferred user zone list. When including the start of a subsequent user zone entry, the mobile shall set the SEGMENT_OFFSET to ‘00000000’ and shall not include a segment of less than four octets. The SEGMENT_INDEX shall be set appropriately and the LAST_SEGMENT and SEGMENT_SIZE shall be set as described above.

  The mobile station shall set NUM_ENTRIES to the number of user zone entry segments included in the returned parameter block.

  - If the *PUZL Configuration Request Message* contains the request for a valid parameter block and if there is no entry in the current preferred user zone list, the mobile station shall set the RESULT_CODE in the *PUZL Configuration Response Message* to ‘00010001’, “Rejected – No entries in PUZL”, and shall set the BLOCK_ID to the received parameter block identifier

  - Otherwise, if SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, and include the FRESH field set to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *PUZL Configuration Response Message*.

13. *PUZL Download Request Message*: The mobile station shall send a *PUZL Download Response Message* within 750 ms after receiving the message.

    - If FRESH_INCL$_r$ = ‘1’ and the SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set FRESH$_S$ = FRESH$_r$ and decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *PUZL Download Request Message*.

    - If the *PUZL Download Request Message* contains a PUZL Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000111’, “Rejected - BLOCK_ID value not supported”, and set IDS_PRESENT to ‘0’. The UZ_ID and UZ_SID fields shall not be included in the returned parameter block.

    - If the *PUZL Download Request Message* contains a PUZL Parameter Block having a size different from that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000010’, “Rejected - Data size mismatch”, and set IDS_PRESENT to ‘0’. The UZ_ID and UZ_SID fields shall not be included in the returned parameter block.

    - If the *PUZL Download Request Message* contains a PUZL Parameter Block with a parameter value that is out-of-range, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000100’, “Rejected - Invalid parameter” and shall set IDS_PRESENT to ‘0’. The UZ_ID and UZ_SID fields shall not be included in the returned parameter block.

    - If the *PUZL Download Request Message* is not accepted for any other reason, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000001’, “Rejected - Unknown reason”, and set IDS_PRESENT to ‘0’. The UZ_ID and UZ_SID fields shall not be included in the returned parameter block.

- If the *PUZL Download Request Message* contains the User Zone Insert Parameter Block and the User Zone ID/System ID pair already exists in the current preferred user zone list, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00001111’, “Rejected – User Zone already in PUZL”, and set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received.
  - Otherwise, the mobile station shall store the parameter block data in temporary memory, set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000000’, “Accepted - Operation successful”, and set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received. If more than one *PUZL Download Request Message* or parameter block is received containing the same user zone entry segment, the mobile station shall retain only the most recently received data.
- If the *PUZL Download Request Message* contains the User Zone Update Parameter Block and the User Zone ID/System ID pair does not exist in the current preferred user zone list, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00010000’, “Rejected – User Zone not in PUZL”, and set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received.
  - Otherwise, the mobile station shall store the parameter block data in temporary memory, set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000000’, “Accepted - Operation successful”, and set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received. If more than one *PUZL Download Request Message* or parameter block is received containing the same user zone entry segment, the mobile station shall retain only the most recently received data.
- If the *PUZL Download Request Message* contains the User Zone Delete Parameter Block, and if the User Zone ID/System ID pair does not exist in the current preferred user zone list, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00010000’, “Rejected – User Zone not in PUZL”, and shall set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received.
  - Otherwise, the mobile station shall mark the specified user zone entry to be deleted, set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to ‘00000000’, “Accepted - Operation successful”, and set IDS_PRESENT to ‘1’. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received.

- If the *PUZL Download Request Message* contains the User Zone Priority Change Parameter Block and the User Zone ID/System ID pair does not exist in the current preferred user zone list, the mobile station shall set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to '00010000', "Rejected – User Zone not in PUZL", and set IDS_PRESENT to '1'. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received.
  - Otherwise, the mobile station shall store the parameter block data in temporary memory, set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to '00000000', "Accepted - Operation successful", and set IDS_PRESENT to '1'. The mobile station shall include the UZ_ID and UZ_SID fields in the returned parameter block containing the values received. If more than one *PUZL Download Request Message* or parameter block is received for the same user zone, the mobile station shall retain only the most recently received data.
- If the *PUZL Download Request Message* contains the PUZL Flags Parameter Block, the mobile station shall store the parameter block data in temporary memory, set BLOCK_ID to the received parameter block identifier, set RESULT_CODE to '00000000', "Accepted - Operation successful", and set IDS_PRESENT to '0'. The UZ_ID and UZ_SID fields shall not be included in the returned parameter block. If more than one *PUZL Download Request Message* or parameter block is received, the mobile station shall retain only the most recently received data.

14. *3GPD Configuration Request Message:* The mobile station shall send a *3GPD Configuration Response Message* within 750 ms after receiving the message.

- If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall set the RESULT_CODE in the corresponding returned confirmation blocks to '00001010', "Rejected - Mobile station locked." The mobile station shall include all requested parameter blocks with the BLOCK_LEN field set to '00000000'.
- If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:
  - If the mobile station does not support a requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to '00000111', "Rejected - BLOCK_ID value not supported." The mobile station shall include the parameter block with the BLOCK_LEN field set to '00000000'.

  - If the requested data blocks exceed the allowable message length, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the message. The mobile station shall include data blocks, in the order requested, up to the maximum number of blocks that fit into the message. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *3GPD Configuration Response Message*. All the encrypted Parameter Blocks and FRESH field shall fit into the *3GPD Configuration Response Message.*

  - Otherwise, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the corresponding confirmation block. The mobile station shall include complete data blocks, in the order requested, in the 3GPD *Configuration Response Message*. . If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, and include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *3GPD Configuration Response Message*.

15. *3GPD Download Request Message:* The mobile station shall respond to the message with a *3GPD Download Response Message* within 750 ms.

    - If FRESH_INCL$_r$ = ‘1’, the mobile station shall set FRESH$_S$ = FRESH$_r$. If the SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *3GPD Download Request Message*.

    - If the *3GPD Download Request Message* contains an 3GPD Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000111’, “Rejected - BLOCK_ID value not supported;”

    - If the *3GPD Download Request Message* contains an 3GPD Parameter Block having a size different from that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000010’, “Rejected - Data size mismatch;”

    - If the *3GPD Download Request Message* contains an 3GPD Parameter Block with a parameter value that is out-of-range, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000100’, “Rejected - Invalid parameter;”

    - If the *3GPD Download Request Message* contains an Operation Mode Parameter Block with a OP_MODE not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00010010’, “Rejected – Operation Mode mismatch;”

- If the *3GPD Download Request Message* contains a SimpleIP User Profile Parameter Block with a NUM_NAI or any NAI_ENTRY_INDEX greater than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00010011', "Rejected – SimpleIP MAX_NUM_NAI mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP User Profile Parameter Block with any NAI_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00010100', "Rejected – SimpleIP MAX_NAI_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP User Profile Parameter Block with a NUM_NAI or any NAI_ENTRY_INDEX greater than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00010101', "Rejected – MobileIP MAX_NUM_NAI mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP User Profile Parameter Block with any NAI_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00010110', "Rejected – MobileIP MAX_NAI_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP PAP SS Parameter Block with a SS_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00010111', "Rejected – SimpleIP PAP MAX_SS_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP CHAP SS Parameter Block with a SS_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011000', "Rejected – SimpleIP CHAP MAX_SS_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP SS Parameter Block with a MN-AAA_SS_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011001', "Rejected – MAX_MN-AAA_SS_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP SS Parameter Block with a MN-HA_SS_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011010', "Rejected – MAX_MN-HA_SS_LENGTH mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP User Profile Parameter Block with any MN-AAA_AUTH_ALGORITHM not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011011', "Rejected – MN-AAA_AUTH_ALGORITHM mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP User Profile Parameter Block with any MN-HA_AUTH_ ALGORITHM not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011100', "Rejected – MN-HA_AUTH_ ALGORITHM mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP Status Parameter Block with an ACT_NAI_ENTRY_INDEX not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011101', "Rejected – SimpleIP ACT_NAI_ENTRY_INDEX mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP Status Parameter Block with an ACT_NAI_ENTRY_INDEX not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011110', "Rejected – MobileIP ACT_NAI_ENTRY_INDEX mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP PAP SS Parameter Block with an NAI_ENTRY_INDEX not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00011111', "Rejected – SimpleIP PAP NAI_ENTRY_INDEX mismatch;"

- If the *3GPD Download Request Message* contains a SimpleIP CHAP SS Parameter Block with an NAI_ENTRY_INDEX not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100000', "Rejected – SimpleIP CHAP NAI_ENTRY_INDEX mismatch;"

- If the *3GPD Download Request Message* contains a MobileIP SS Parameter Block with an NAI_ENTRY_INDEX not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100001', "Rejected – MobileIP NAI_ENTRY_INDEX mismatch;"

- If the *3GPD Download Request Message* contains a HRPD Access Authentication User Profile Parameter Block with any NAI_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100100', "Rejected – HRPD Access Authentication MAX_NAI_LENGTH mismatch;"

  - If the *3GPD Download Request Message* contains a HRPD Access Authentication CHAP SS Parameter Block with a SS_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100101', "Rejected – HRPD Access Authentication CHAP_MAX_SS_LENGTH mismatch;"
  - If the *3GPD Download Request Message* is not accepted for any other reason, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000001', "Rejected – Unknown reason;"
- Otherwise, the mobile station shall store the message data in temporary memory, set BLOCK_ID to the received parameter block identifier and set RESULT_CODE to '00000000', "Accepted – Operation successful." If more than one *3GPD Download Request Message* or parameter block is received containing values for the same indicators, the mobile station shall retain only the most recently received values.

16. *Secure Mode Request Message*: The mobile station shall send the *Secure Mode Response Message* within 750 ms after receiving the message.
    - If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall indicate the error condition by setting the RESULT_CODE to '00001010', "Rejected - Mobile station locked" in the *Secure Mode Response Message*.
    - If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:
      - If the mobile station does not support Secure Mode, the mobile station shall indicate the error condition by setting RESULT_CODE to '00000110', "Rejected - Message not expected in this mode", in the *Secure Mode Response Message*; otherwise
      - If the START_STOP_r field received in the message is equal to '1', the mobile station shall do the following:
        - + The mobile station shall set SECURE_MODE_IND_S = '1'.
        - + The mobile station shall generate SMCK_s (see 3.8.2).
        - + The mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful", in the *Secure Mode Response Message*.
      - If the START_STOP_r field received in the message is equal to '0', the mobile station shall set the RESULT_CODE to the '00000000', "Accepted - Operation successful", in the *OTAPA Response Message*. If the Secure Mode is active, the mobile station shall terminate the Secure Mode. The mobile station shall set SECURE_MODE_IND_S = '0' and SMCK_s to NULL.

17. *MMD Configuration Request Message:* The mobile station shall send a *MMD Configuration Response Message* within 750 ms after receiving the message.

- If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to ‘1’, the mobile station shall set the RESULT_CODE in the corresponding returned confirmation blocks to ‘00001010’, “Rejected - Mobile station locked.” The mobile station shall include all requested parameter blocks with the BLOCK_LEN field set to ‘00000000’.
- If both SP_LOCK_STATE and NAM_LOCK_STATE are set to ‘0’, then:
    - If the mobile station does not support a requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000111’, “Rejected - BLOCK_ID value not supported.” The mobile station shall include the parameter block with the BLOCK_LEN field set to ‘00000000’.
    - If the requested data blocks exceed the allowable message length, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the message. The mobile station shall include data blocks, in the order requested, up to the maximum number of blocks that fit into the message. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *MMD Configuration Response Message*. All the encrypted Parameter Blocks and FRESH field shall fit into the *MMD Configuration Response Message.*
    - Otherwise, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the corresponding confirmation block. The mobile station shall include complete data blocks, in the order requested, in the *MMD Configuration Response Message*. . If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, and include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *MMD Configuration Response Message*.

18. *MMD Download Request Message:* The mobile station shall respond to the message with a *MMD Download Response Message* within 750 ms.
    - If FRESH_INCL$_r$ = ‘1’, the mobile station shall set FRESH$_S$ = FRESH$_r$. If the SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *MMD Download Request Message*.
    - If the *MMD Download Request Message* contains an MMD Application Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000111’, “Rejected - BLOCK_ID value not supported;”

- If the *MMD Download Request Message* contains an MMD Application Parameter Block having a size different from that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000010', "Rejected - Data size mismatch;"
- If the *MMD Download Request Message* contains an MMD Application Parameter Block with a parameter value that is out-of-range, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000100', "Rejected - Invalid parameter;"
- If the *MMD Download Request Message* contains a MMD Application Parameter Block with a NUM_IMPU or any IMPU_ENTRY_IDX greater than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100110', "Rejected – MMD MAX_NUM_IMPU mismatch;"
- If the *MMD Download Request Message* contains a MMD Application Parameter Block with any IMPU_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00100111', "Rejected – MMD MAX_IMPU_LENGTH mismatch;"
- If the *MMD Download Request Message* contains a MMD Application Parameter Block with a NUM_P-CSCF or any P-CSCF_ENTRY_IDX greater than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00101000', "Rejected – MMD MAX_NUM_P-CSCF mismatch;"
- If the *MMD Download Request Message* contains a MMD Application Parameter Block with any P-CSCF_LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00101001', "Rejected – MMD MAX_P-CSCF_LENGTH mismatch;"
- If the *MMD Download Request Message* is not accepted for any other reason, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000001', "Rejected – Unknown reason;"
    - Otherwise, the mobile station shall store the message data in temporary memory, set BLOCK_ID to the received parameter block identifier and set RESULT_CODE to '00000000', "Accepted – Operation successful." If more than one *MMD Download Request Message* or parameter block is received containing values for the same indicators, the mobile station shall retain only the most recently received values.

19. *System Tag Configuration Request Message:* The mobile station shall send a *System Tag Configuration Response Message* within 750 ms after receiving the message.

- If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to ‘1’, the mobile station shall set RESULT_CODE in the *System Tag Configuration Response Message* to ‘00001010’, “Rejected - Mobile station locked”. The mobile station shall include the requested parameter block with the BLOCK_LEN field set to zero.
- If both SP_LOCK_STATE and NAM_LOCK_STATE are set to ‘0’, then:
  - If the mobile station does not support the requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned parameter block to ‘00000111’, “Rejected - BLOCK_ID value not supported.” The mobile station shall include the parameter block with the BLOCK_LEN field set to zero.
  - If the REQUEST_OFFSET$_r$ received in the message specifies an offset which is invalid for the current system tag list, the mobile station shall set the RESULT_CODE in the corresponding returned parameter block to ‘00000010’, “Rejected - Data size mismatch.”

    The mobile station shall set the BLOCK_ID to the corresponding parameter block identifier, the SEGMENT_OFFSET in the returned Parameter Block to the value of the REQUEST_OFFSET$_r$, the SEGMENT_SIZE to ‘00000000’, and shall include no octets of the system tag list in the returned Parameter Block.
  - Otherwise, if the REQUEST_OFFSET$_r$ received in the message is valid for the current system tag list, the mobile station shall set the RESULT_CODE in the *System Tag Configuration Response Message* to ‘00000000’, “Accepted - Operation successful” for the Parameter Block included in the message.

    The mobile station shall include the system tag data starting at the offset corresponding to the REQUEST_OFFSET$_r$ and not exceeding a maximum number of octets corresponding to the REQUEST_MAX_SIZE$_r$ received in the message.

    The mobile station shall set the SEGMENT_OFFSET in the returned Parameter Block to the value of the REQUEST_OFFSET$_r$ received in the message.

    The mobile station shall set the SEGMENT_SIZE field to the number of octets of the system tag list included in the returned Parameter Block. If the Parameter Block contains the last segment of the system tag list data, the mobile station shall set the LAST_SEGMENT field to ‘1’; otherwise the mobile station shall set the LAST_SEGMENT field to ‘0’ in the returned Parameter Block.

20. *System Tag Download Request Message:* The mobile station shall respond to the message with a *System Tag Download Response Message* within 750 ms.

    - If the *System Tag Download Request Message* contains a System Tag Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set the RESULT_CODE in the *System Tag Download Response*

Message to ‘00000111’, “Rejected - BLOCK_ID value not supported” and shall set the BLOCK_ID to the received parameter block identifier. The mobile station shall omit the SEGMENT_OFFSET and the SEGMENT_SIZE fields in the *System Tag Download Response Message*.

- If the *System Tag Download Request Message* contains a System Tag Parameter Block having a size different from that supported by the mobile station, the mobile station shall set the RESULT_CODE in the *System Tag Download Response Message* to ‘00000010’, “Rejected - Data size mismatch” and shall set the BLOCK_ID to the received parameter block identifier.

  If the *System Tag Download Request Message* does not contain a System tag Parameter Block having a BLOCK_ID of ‘00000001’, ‘00000010’, or ‘00000011’, the mobile station shall omit the SEGMENT_OFFSET and SEGMENT_SIZE fields.

- Otherwise, the mobile station shall perform the following:
  - If the *System Tag Download Request Message* contains a System tag Parameter Block having a BLOCK_ID of ‘00000001’, ‘00000010’, or ‘00000011’, the mobile station shall set SEGMENT_OFFSET to the value of SEGMENT_OFFSET received in the message. The mobile station shall set SEGMENT_SIZE to the value of SEGMENT_SIZE received in the message.
  - If $\text{SYS\_TAG\_BLOCK\_ID\_CURRENT}_s$ is not NULL and the value of the BLOCK_ID_r field is not equal to $\text{SYS\_TAG\_BLOCK\_ID\_CURRENT}_s$, the mobile station shall perform the following:
    - + Set the RESULT_CODE in the *System Tag Download Response Message* to ‘00101010’, “Rejected – Unexpected System Tag BLOCK_ID change”.
    - + In the *System Tag Download Response Message*, set the BLOCK_ID to the received parameter block identifier and set the SEGMENT_OFFSET and the SEGMENT_SIZE to ‘00000000’.
    - + Discard all the SEGMENT_DATA octets that have been received in a *System Tag Download Request Message* with the BLOCK_ID field set to ‘00000001’.
    - + Set the $\text{SYS\_TAG\_BLOCK\_ID\_CURRENT}_s$ to NULL.
  - Otherwise, the mobile station shall perform the following:
    - + Set the $\text{SYS\_TAG\_BLOCK\_ID\_CURRENT}_s$ to the value of the BLOCK_ID field received in the *System Tag Download Request Message*.
    - + If SEGMENT_OFFSET in conjunction with SEGMENT_SIZE are inconsistent with the system tag list storage capabilities of the mobile station, the mobile station shall set the RESULT_CODE to ‘00101011’, “Rejected – System Tag format mismatch” and shall set the BLOCK_ID to the received parameter block identifier.

  + Otherwise, if SEGMENT_OFFSET in conjunction with SEGMENT_SIZE are consistent with the system tag list storage capabilities of the mobile station, the mobile station shall store the SEGMENT_DATA octets in temporary memory.
    - If LAST_SEGMENT is equal to '0', the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful" and shall set the BLOCK_ID to the received parameter block identifier.
    - If LAST_SEGMENT is equal to '1' or if BLOCK_ID is equal to '00000000' (Home System Tag), the mobile station shall calculate the CRC, as specified in Section 3.5.10.1 for the system tag list stored in temporary memory. If the CRC checks, the mobile station shall set the RESULT_CODE to '00000000', "Accepted - Operation successful;" otherwise, the mobile station shall set the RESULT_CODE to '00001001', "Rejected - CRC error" and shall discard this segment and all previously assembled segments of the system tag list from the temporary memory. The mobile station shall set the BLOCK_ID to the received parameter block identifier.

21. *Service Key Generation Request Message:*

- The mobile station shall compute the value of the service root key, for each service root key requested, in accordance with 3.3.9.
- If the mobile station has not successfully calculated the service key(s) in accordance with 3.3.9, the mobile station shall set RESULT_CODE to '00000001', "Rejected - Unknown reason." The mobile station shall then send a *Service Key Generation Response Message* within 750 ms after receiving this message.
- If the mobile station has successfully calculated the services root key(s) in accordance with 3.3.9, the mobile station shall set RESULT_CODE to '00000000', "Accepted - Operation successful." The mobile station shall then send a *Service Key Generation Response Message* within 750 ms after receiving this message.

22. *MMS Configuration Request Message:* The mobile station shall send a *MMS Configuration Response Message* within 750 ms after receiving the message.

- If either SP_LOCK_STATE, or NAM_LOCK_STATE, or both are set to '1', the mobile station shall set the RESULT_CODE in the corresponding returned confirmation blocks to '00001010', "Rejected - Mobile station locked." The mobile station shall include all requested parameter blocks with the BLOCK_LEN field set to '00000000'.
- If both SP_LOCK_STATE and NAM_LOCK_STATE are set to '0', then:

  - If the mobile station does not support a requested parameter block, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000111’, “Rejected - BLOCK_ID value not supported.” The mobile station shall include the parameter block with the BLOCK_LEN field set to ‘00000000’.

  - If the requested data blocks exceed the allowable message length, the mobile station shall set RESULT_CODE in the corresponding returned confirmation block to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the message. The mobile station shall include data blocks, in the order requested, up to the maximum number of blocks that fit into the message. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *MMS Configuration Response Message*. All the encrypted Parameter Blocks and FRESH field shall fit into the *MMS Configuration Response Message*.

  - Otherwise, the mobile station shall set RESULT_CODE to ‘00000000’, “Accepted - Operation successful” for each Parameter Block included in the corresponding confirmation block. The mobile station shall include complete data blocks, in the order requested, in the *MMS Configuration Response Message*. If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set the FRESH_INCL field to ‘1’, and include the FRESH field and set it to a 15-bit value selected according to 3.3.8. The mobile station shall encrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks included in the *MMS Configuration Response Message*.

23. *MMS Download Request Message:* The mobile station shall respond to the message with a *MMS Download Response Message* within 750 ms.

- If FRESH_INCL$_r$ = ‘1’, the mobile station shall set FRESH$_S$ = FRESH$_r$. If the SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall decrypt as specified in 3.3.8 each PARAM_DATA field of all Parameter Blocks received in the *MM*S *Download Request Message*.

- If the *MMS Download Request Message* contains an MMS URI Parameter Block with a BLOCK_ID that is not supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000111’, “Rejected - BLOCK_ID value not supported”

- If the *MMS Download Request Message* contains an MMS URI Parameter Block having a size different from that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to ‘00000010’, “Rejected - Data size mismatch”

- If the *MMS Download Request Message* contains an MMS URI Parameter Block with a parameter value that is out-of-range, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000100', "Rejected - Invalid parameter"
- If the *MMS Download Request Message* contains a MMS URI Parameter Block with a NUM_MMS_URI greater than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00101100', "Rejected – NUM_MMS_URI mismatch"
- If the *MMS Download Request Message* contains a MMS URI Parameter Block with any MMS_URI _LENGTH larger than that supported by the mobile station, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00101101', "Rejected – MMS_URI _LENGTH mismatch;"
- If the *MMS Download Request Message* contains a MMS URI Parameter Block with an invalid MMS_URI, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00101110', "Rejected – Invalid MMS_URI"
- If the *MMS Download Request Message* is not accepted for any other reason, the mobile station shall set BLOCK_ID to the received parameter block identifier and RESULT_CODE to '00000001', "Rejected – Unknown reason;"
- Otherwise, the mobile station shall store the message data in temporary memory, set BLOCK_ID to the received parameter block identifier and set RESULT_CODE to '00000000', "Accepted – Operation successful." If more than one *MMS Download Request Message* or parameter block is received containing values for the same indicators, the mobile station shall retain only the most recently received values.

If the mobile station receives an *OTASP Data Message* that it does not recognize or which requires a capability that is not supported, the mobile station shall discard the message and shall send a *Mobile Station Reject Order* with ORDQ set to '00000110' within T_{56m} seconds.

3.3.2 Mobile Station SSD Update and Re-authentication

Re-authentication is the process by which the mobile station is instructed to perform authentication and generate the Private Long Code Mask (CDMA only) and Message Encryption parameters while on the CDMA Traffic channel or analog voice channel. The authentication key, A-key, may be generated by the mobile station during the programming session. Shared Secret Data, SSD, is generated prior to performing re-authentication.

If the mobile station has not generated an A-key during the present programming session via the *Key Generation Request Message*, the mobile station shall follow the procedures specified in 6.3.12 of [1] or 2.3.12 of [7] when performing an SSD update.

If the mobile station has correctly generated an A-key during the present programming session, the mobile station shall follow the procedures specified in 6.3.12 of [1] or 2.3.12 of [7] when performing an SSD update with the following exceptions:

- The mobile station shall use A_KEY_TEMP$_S$ as the A-key input.
- The mobile station shall store the SSD_A_NEW and SSD_B_NEW outputs in SSD_A$_S$ and SSD_B$_S$, respectively, rather than in SSD_A$_{S-p}$ and SSD_B$_{S-p}$.

Once SSD has been generated from A_KEY_TEMP$_S$, the mobile station shall use SSD$_S$ instead of SSD$_{S-p}$ until SSD$_S$ is stored into SSD$_{S-p}$ after receiving a *Commit Request Message*.

The authentication algorithms are described in "Common Cryptographic Algorithms." The interface for the algorithms is described in "Interface Specification for Common Cryptographic Algorithms." Re-authentication should be performed as follows:

In the mobile station,

- Set the input parameters of the Auth_Signature procedure (see 2.3 of "Interface Specification for Common Cryptographic Algorithms") as follows
  - If the programming session was initiated by the network as described in 3.2.2, the input parameters shall be set as defined in 6.3.12.1.7 of TIA/EIA-95B.
  - If the programming session was initiated by the user as described in 3.2.1, the input parameters shall be set as defined in 6.3.12.1.6 of TIA/EIA-95B.
- Execute the Auth_Signature procedure;
- Set AUTHR$_S$ equal to the 18-bit output AUTH_SIGNATURE;
- Send AUTHR$_S$, RANDC (eight most significant bits of RAND$_S$), AUTH_DATA$_S$ and COUNT$_{S-p}$ to the base station in the *Re-Authenticate Response Message*.

At the base station,

- Compare the received values for RANDC, and optionally COUNT, with the internally stored values associated with the mobile station being activated;
- Compute AUTHR as described above, except use the internally stored value of SSD_A;
- Compare the value for AUTHR computed internally with the value of AUTHR received from the mobile station.

If the comparisons executed at the base station are successful, the base station may activate Message Encryption (see 3.3.3) and may also activate Voice Privacy (see 3.3.4). The base station may issue a *Parameter Update Order* to the mobile station on the Forward Voice Channel or on the Forward Traffic Channel, updating the value of COUNT$_{S-p}$ in the mobile station.

If any of the comparisons fail, the base station may deny activation, initiate the Unique Challenge-Response Procedure (see 6.3.12.1.5 of [1] or 2.3.12.1.4 of [7]) or commence the process of updating SSD (see 6.3.12.1.5 of [1] or 2.3.12.1.9 of [7]).

3.3.3 Activation of Message Encryption

To enhance the security of the programming session and to protect sensitive subscriber information, a method is provided to encrypt certain fields of selected OTASP Traffic Channel and Forward and Reverse Voice Channel messages (see [7] for details].

Message encryption is controlled on a per-call basis.

If message encryption was activated (see 2.3.12.2.1 and 6.3.12.2 of [1] or 2.3.12.2 of [7]) or transition to the Private Long Code Mask was made (see 6.3.12.3 of [1] or 2.3.12.3 of [7]) before the re-authentication operation, the message encryption parameters active at that time shall remain unchanged for the duration of the call.

Otherwise, the message encryption parameters are re-calculated during the re-authentication operation. In this case, the data used to initialize the algorithm for calculating the message encryption parameters is computed based on parameters in effect at the time the AUTHR included in *Re-Authenticate Response Message* was computed.

3.3.4 Activation of Voice Privacy

To enhance the security of the programming session and to protect sensitive subscriber information, voice privacy is provided in the CDMA system (see 6.3.12.3 of [1] or 2.3.12.3 of [7]) by means of the Private Long Code Mask used for PN spreading.

The generation of the Private Long Code Mask is specified in [1, 7].

If transition to the Private Long Code Mask was made (see 6.3.12.3 of [1] or 2.3.12.3 of [7]), or if signaling message encryption was activated (see 2.3.12.2.1 and 6.3.12.2 of [1] or 2.3.12.2 of [7]) before the re-authentication operation, the Private Long Code Mask active at that time shall remain unchanged for the duration of the call.

Otherwise, the Private Long Code Mask shall be recalculated during the re-authentication operation. In this case, the data used to initialize the algorithm for calculating the Private Long Code Mask is computed based on parameters in effect at the time the AUTHR included in the *Re-Authenticate Response Message* was computed.

3.3.5 System Selection for Preferred Roaming

The goal of System Selection for Preferred Roaming (SSPR) is for the mobile station to acquire the most preferred system using the information from the preferred roaming list (PR_LIST_{S-P}) stored in the mobile station (see 3.5.5). Annex C contains information on the recommended use of the preferred roaming list.

3.3.6 Service Programming Lock

Access to the mobile station programming module containing NAM indicators and parameters (see 4.5.2, 4.5.3 and 4.5.4) that can be assigned values using Over-the-Air Service Provisioning is protected by the service programming lock. The service programming lock parameter contains the Service Programming Code (SPC) used for unlocking the mobile station parameters for programming or reprogramming.

The service programming lock based on a single SPC protects parameters of all NAMs in the mobile station.

The SPC has values defined in the Table 3.3.6-1.

Table 3.3.6-1 Service Programming Code Values

Service Programming Code Type	SPC Value
Default	0
Active	1 through 999,999

The mobile station should provide the user a means to program the mobile station to accept or deny the SPC change from the default value to a non-default value. The mobile station should be programmed by default to deny the SPC change from the default value to a non-default value.

When SPC is set to the default value, all programmable modules in the mobile station are unlocked, unless protected by SPASM (see 3.3.7). When programmable modules are unlocked, access and programming of all NAM indicators and parameters are allowed.

When SPC is set to any value other than the default value, the programming module in the mobile station is locked, and access to NAM indicators and parameters can be allowed only if correct value of the SPC is received from the base station within the current OTASP session.

3.3.7 Subscriber Parameter Administration Security Mechanism

In order to validate SPASM, the mobile station shall set the input parameters of the Auth_Signature procedure (see “Interface Specifications for Common Cryptographic Algorithms, section 2.3) as follows:

The mobile station shall set the RAND_CHALLENGE input parameter to the 32-bit random value that is sent to the base station in the RAND_OTAPA field of the *OTAPA Response Message*, the AUTH_DATA input parameter as defined in 6.3.12.1.7 of TIA/EIA-95B, the SSD_AUTH input parameter to the exclusive OR of $\text{SSD\_A}_{\text{S-p}}$ and A_KEY, the ESN input parameter to the mobile station ESN and the SAVE_REGISTERS input parameter to FALSE. If the mobile station only supports MEID, then Pseudo-ESN shall be used as the ESN.

The mobile station shall execute the Auth_Signature procedure. The $\text{AUTH\_OTAPA}_{\text{S}}$ is set to the computed 18-bit result AUTH_SIGNATURE.

Upon receiving the RAND_OTAPA from the mobile station in the *OTAPA Response Message*, the base station shall compute AUTH_OTAPA as described above with the exception of using the SSD_AUTH input parameter set to the exclusive OR of the internally stored value of SSD_A and A_KEY.

The AUTH_OTAPA is set to the computed 18-bit result AUTH_SIGNATURE and is sent to the mobile station in the Validate SPASM Parameter Block of the *Validation Request Message*.

The mobile station validates SPASM by comparing the $\text{AUTH\_OTAPA}_{\text{r}}$ received in the message to its locally computed value of the $\text{AUTH\_OTAPA}_{\text{S}}$.

3.3.8 Secure Mode

To enhance security of the programming session and to protect sensitive subscriber information, a method is provided to encrypt PARAM_DATA fields of Parameter Blocks in OTASP messages irrespective of the air interface message encryption described in 3.3.3. This method allows setting up a secure "tunnel" between the mobile station and the network based Over-The-Air Service Provisioning entity.

If the mobile station supports Secure Mode, it shall indicate it to the base station in the *Protocol Capability Response Message* by setting appropriate feature-related fields.

When the mobile station is unlocked, i.e. when both SP LOCK_STATE$_S$ and NAM_LOCK_STATE$_S$ are equal to '0', the base station can initiate the Secure Mode by sending the *Secure Mode Request Message* to the mobile station with the START_STOP field set to '1'.

The mobile station shall use the RAND_SM$_r$ received in the message and the SSD$_{s-p}$ to compute the Secure Mode Ciphering Key SMCK$_s$ as specified in 3.3.8.1.

The mobile station shall use the SMCK$_s$ as a key for encryption and decryption, as specified in 3.3.8.2, of all PARAM-DATA of all Parameter Blocks sent and received by the mobile station in the OTASP Data Messages while the Secure mode is active.

When encrypting the message, the mobile station shall select a value of FRESH associated with this message and unique for the duration of Secure Mode session. The value of FRESH can be selected at random, or can be set to a monotonically increasing counter.

When decrypting the message, the mobile station shall use the value of FRESH$_r$ received in the message.

The base station can terminate the Secure Mode by sending the *Secure Mode Request Message* to the mobile station with the START_STOP field set to '0'. When Secure Mode session is terminated, the mobile station shall reset the SMCK$_s$ to NULL.

3.3.8.1 Generation of Secure Mode Ciphering Key

The Secure Mode Ciphering Key Generation SMCK$_s$ is generated by the algorithmic function specified in Section 2.2.2.6 of [8].

If KEY_IN_USE = '0000', the input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to SSD-A$_{s-p}$ | SSD-B$_{s-p}$.
- The fi parameter shall be set to 0x45.
- The RAND parameter shall be set to RAND_SM$_r$ | RAND_SM$_r$.
- The Fmk parameter shall be set to 0x41484147.

If KEY_IN_USE = '0001', the input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to the 128-bit Root Key K.
- The fi parameter shall be set to 0x45.

- The RAND parameter shall be set to $RAND\_SM_r$|$RAND\_SM_r$.
- The Fmk parameter shall be set to 0x41484147.

The mobile station shall execute the Ciphering Key Generation Procedure as specified in 2.2.2.6 of [8]. The mobile station shall set $SMCK_s$ to the computed 128-bit output of *f3*.

The mobile station shall set input parameter to the *ESP_privacykey Procedure* as follows:

- The *key* parameter shall be set to $SMCK_{s.}$

The mobile station shall execute the *ESP_privacykey Procedure.*

3.3.8.2 Encryption and Decryption of messages in Secure Mode

Encryption and decryption of PARAM_DATA information is performed by the Enhanced Privacy Algorithm specified in 2.3.2.2 of [8].

The mobile station shall set input parameters to the Enhanced Privacy Algorithm as follows:

- If the mobile station presents the data for encryption, the mobile station shall set the *fresh* parameter to FRESH|' 0'|BLOCK_ID; otherwise, if the mobile station presents the data for decryption, the mobile station shall set the *fresh* parameter to $FRESH_r$|' 1'|BLOCK_ID;
- The *freshsize* parameter shall be set to 3;
- The *buf* parameter shall be set to address of the octet containing the first bit of the buffer that contains the data to be encrypted or decrypted.
- The *bit_offset* parameter shall be set to the offset between the bit position of the most significant bit of the data to be encrypted/decrypted and the bit position of the most significant bit of the buffer (e.g., if the bit position of the most significant bit of the data to be encrypted/decrypted and the bit position of the most significant bit of the buffer are equal, *bit_offset* shall be set to 0).
- The *bit_count* parameter shall be set to the number of bits of the data to be encrypted/decrypted.

The mobile station shall execute the *ESP_maskbits Procedure*.

3.3.9 System Tag Indicator

The goal of the System Tag capability is to increase the functionality of the Roaming Indicators (ROAM_IND) listed within the Preferred Roaming List. This capability allows the downloading and synchronization of a file of operator-customizable roaming indicators, tailored to the specific capabilities of the mobile station, representing the operator-specific roaming indicators.

Once configured with a compatible System Tag file associated with the Preferred Roaming List stored within the mobile station, the mobile station shall determine the roaming indicator (ROAM_IND) listed within the System Record or Extended System Record entry (see 3.5.5.3.1 and 3.5.5.3.2, respectively) corresponding to the SID of the system in which the mobile station is operating. The mobile station shall then use this ROAM_IND to determine the appropriate user interface actions (graphical and/or textual display) to take as defined by the corresponding ROAM_IND entry within the System Tag file.

3.3.10 Generation of Service Keys

Generation of service keys consists of generating an intermediate key and using the intermediate key to generate service keys.

3.3.10.1 Generation of Intermediate Key

The Intermediate value ITM_RAND is generated by the algorithmic function specified in Section 2.2.2.2 of [8].

The input parameters to the algorithmic function *f0* shall be set as follows:

- The K parameter shall be set to RK_P.
- The fi parameter shall be set to 0x41.
- The Fmk parameter shall be set to 0x534B474B.

The mobile station shall execute f0 twice. ITM_RAND is set to the 128-bit output of f0.

3.3.10.2 Generation of Service Keys

For each bit in the bitmap as illustrated in Table 4.5.1.17-1 that is turned on, the base station shall generate the service key by invoking the key generation function as specified in Section 2.2.2.6 of [8].

The input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to ITM_RAND.
- The fi parameter shall be set to 0x45.
- The RAND parameter shall be set according to table 4.3.6.2-1, with remaining least significant bits padded with ‘0’, for each service requested.
- The Fmk parameter shall be set to 0x534B474B.

The mobile station shall execute f3 to produce 128-bit service root key.

Table 3.3.10.2-1 Key Identifier Table

Service Key Requested	RAND Value
IMS ROOT KEY	0x494D53
BCMCS ROOT KEY	0x42434D4353
WLAN ROOT KEY	0x574C414E

3.4 Termination of the Programming Procedure

If the mobile station does not support concurrent services, if the mobile station enters any substate or task other than the CDMA *Conversation Substate* or the analog Conversation Task, the mobile station shall terminate the programming session.

Following a CDMA-to-analog handoff, the mobile station may terminate the programming session; however, the mobile station shall not autonomously release the call.

If the mobile station receives more than five *Validation Request Messages* during the same programming session with the SPC_r value not equal to the SPC_p, the mobile station should terminate the programming session and should not begin another session until after the mobile station power is cycled.

If more than five validations of SPASM (see 3.3.7) result in a mismatch during the same programming session, the mobile station should terminate the programming session and should not begin another session until after the mobile station power is cycled.

The mobile station shall provide a means for the user to end the programming session. If the user directs the mobile station to end the programming process, the mobile station shall release the call and shall terminate the programming session.

If the programming session was initiated by the network as described in 3.2.2, and if the mobile station is directed by the user to initiate a call during the OTAPA session, the mobile station may initiate the call by sending an Enhanced Origination Message if both mobile station and the base station supports concurrent service; otherwise, the mobile station shall terminate the OTAPA session and release the OTAPA call prior to proceeding with the origination procedure.

If the mobile station receives the *OTAPA Request Message* with the $START\_STOP_r$ equal to '0', it shall terminate the OTAPA session.

If the programming session is terminated, the mobile station shall discard all the NAM indicator values that are not stored in permanent memory.

3.5 Reverse Link Message Formats

The reverse link *OTASP Data Messages* are summarized in Table 3.5-1.

Table 3.5-1 Reverse Link Messages

Message Name	OTASP_MSG_TYPE	Reference
Configuration Response Message	‘00000000’	3.5.1.1
Download Response Message	‘00000001’	3.5.1.2
MS Key Response Message	‘00000010’	3.5.1.3
Key Generation Response Message	‘00000011’	3.5.1.4
Re-Authenticate Response Message	‘00000100’	3.5.1.5
Commit Response Message	‘00000101’	3.5.1.6
Protocol Capability Response Message	‘00000110’	3.5.1.7
SSPR Configuration Response Message	‘00000111’	3.5.1.8
SSPR Download Response Message	‘00001000’	3.5.1.9
Validation Response Message	‘00001001’	3.5.1.10
OTAPA Response Message	‘00001010’	3.5.1.11
PUZL Configuration Response Message	‘00001011’	3.5.1.12
PUZL Download Response Message	‘00001100’	3.5.1.13
3GPD Configuration Response Message	'00001101'	3.5.1.14
3GPD Download Response Message	'00001110'	3.5.1.15
Secure Mode Response Message	‘00001111’	3.5.1.16
Extended Protocol Capability Response Message	‘00010000’	3.5.1.17
MMD Configuration Response Message	‘00010001’	3.5.1.18
MMD Download Response Message	‘00010010’	3.5.1.19
System Tag Configuration Response Message	‘00010011’	3.5.1.20

System Tag Download Response Message	‘00010100’	3.5.1.21
Service Key Generation Response Message	‘00010101’	3.5.1.22
MMS Configuration Response Message	‘00010110’	3.5.1.23
MMS Download Response Message	‘00010111’	3.5.1.24
Reserved for future standardization	‘00011000’ through ‘10111111’	
Available for manufacturer-specific *OTASP Data Message* definition	‘11000000’ through ‘11111110’	See [4]
Reserved	‘11111111’	

3.5.1 Message Contents

3.5.1.1 Configuration Response Message

The *Configuration Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000000’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
NUM_BLOCKS occurrences of the following field	
RESULT_CODE	8
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE -	*OTASP Data Message* type. The mobile station shall set this field to ‘00000000’.
NUM_BLOCKS -	Number of parameter blocks. The mobile station shall set this field to the number of parameter blocks contained in the *Configuration Response Message*.
BLOCK_ID -	Parameter block identifier. The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *Configuration Request Message* that is being confirmed (see Table 3.5.2-1).
BLOCK_LEN -	Parameter block length. The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.
PARAM_DATA -	Parameter data fields. The mobile station shall include the parameter block (see 3.5.2) specified by the BLOCK_ID field. If SECURE_MODE_IND_S = ‘1’, PARAM_DATA fields shall be encrypted as specified in 3.3.8.

RESULT_CODE - Configuration result code.

The mobile station shall include one instance of this field for each parameter block included in the message, in the same order of appearance. The mobile station shall set this field to indicate acceptance or rejection status of the request for the corresponding parameter block in the *Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

FRESH_INCL - FRESH included indicator.

If SECURE_MODE_IND$_S$ = '1', the mobile station shall set this field to '1'; otherwise the mobile station shall set this field to '0'.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = '1', the mobile station shall include this field and set it to a 15-bit value chosen according to requirements set in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = '1', the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to '0'.

3.5.1.2 Download Response Message

The *Download Response Message* has the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE ('00000001')	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following confirmation block:

BLOCK_ID	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to '00000001'.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *Download Request Message* that is being confirmed.

BLOCK_ID - Parameter block identifier.

		The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *Download Request Message* that is being confirmed (see Table 4.5.2-1).
RESULT_CODE	-	Download result code. The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

Table 3.5.1.2-1 Result Codes

RESULT_CODE	Message Parameter Description
‘00000000’	Accepted - Operation successful
‘00000001’	Rejected - Unknown reason
‘00000010’	Rejected - Data size mismatch
‘00000011’	Rejected - Protocol version mismatch
‘00000100’	Rejected - Invalid parameter
‘00000101’	Rejected - SID/NID length mismatch
‘00000110’	Rejected - Message not expected in this mode
‘00000111’	Rejected - BLOCK_ID value not supported
‘00001000’	Rejected - Preferred roaming list length mismatch
‘00001001’	Rejected - CRC error
‘00001010’	Rejected - Mobile station locked
‘00001011’	Rejected - Invalid SPC
‘00001100’	Rejected - SPC change denied by the user
‘00001101’	Rejected - Invalid SPASM
‘00001110’	Rejected - BLOCK_ID not expected in this mode
‘00001111’	Rejected – User Zone already in PUZL
‘00010000’	Rejected – User Zone not in PUZL
‘00010001’	Rejected – No entries in PUZL
'00010010'	Rejected - Operation Mode mismatch
'00010011'	Rejected - SimpleIP MAX_NUM_NAI mismatch
'00010100'	Rejected - SimpleIP MAX_NAI_LENGTH mismatch
'00010101'	Rejected - MobileIP MAX_NUM_NAI mismatch
'00010110'	Rejected - MobileIP MAX_NAI_LENGTH mismatch
'00010111'	Rejected - SimpleIP PAP MAX_SS_LENGTH mismatch
'00011000'	Rejected - SmpleIP CHAP MAX_SS_LENGTH mismatch
'00011001'	Rejected - MobileIP MAX_MN-AAA_SS_LENGTH mismatch
'00011010'	Rejected - MobileIP MAX_MN-HA_SS_LENGTH mismatch

'00011011'	Rejected - MobileIP MN-AAA_AUTH_ALGORITHM mismatch
'00011100'	Rejected - MobileIP MN-HA_AUTH_ALGORITHM mismatch
'00011101'	Rejected - SimpleIP ACT_NAI_ENTRY_INDEX mismatch
'00011110'	Rejected - MobileIP ACT_NAI_ENTRY_INDEX mismatch
'00011111'	Rejected - SimpleIP PAP NAI_ENTRY_INDEX mismatch
'00100000'	Rejected - SimpleIP CHAP NAI_ENTRY_INDEX mismatch
'00100001'	Rejected - MobileIP NAI_ENTRY_INDEX mismatch
'00100010'	Rejected – Unexpected PRL_BLOCK_ID change
'00100011'	Rejected – PRL format mismatch
'00100100'	Rejected – HRPD Access Authentication MAX_NAI_LENGTH mismatch
'00100101'	Rejected – HRPD Access Authentication CHAP MAX_SS_LENGTH mismatch

‘00100110’	Rejected – MMD MAX_NUM_IMPU mismatch
‘00100111’	Rejected – MMD MAX_IMPU_LENGTH mismatch
‘00101000’	Rejected – MMD MAX_NUM_P-CSCF mismatch
‘00101001’	Rejected – MMD MAX_P-CSCF_LENGTH mismatch
‘00101010’	Rejected – Unexpected System Tag BLOCK_ID Change
‘00101011’	Rejected – System Tag Format mismatch
‘00101100’	Rejected – NUM_MMS_URI mismatch
‘00101101’	Rejected – MMS_URI _LENGTH mismatch
‘00101110’	Rejected – Invalid MMS_URI
'00101111' - ‘01111111’	Reserved for future standardization
‘10000000’ - ‘11111110’	Available for manufacturer-specific Result Code definitions. See [4].
‘11111111’	Reserved

3.5.1.3 MS Key Response Message

The *MS Key Response Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000010’)	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00000010’.

RESULT_CODE - Key exchange result code.

The mobile station shall set this field to indicate acceptance or rejection status, using the values defined in Table 3.5.1.2-1.

3.5.1.4 Key Generation Response Message

The *Key Generation Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000011’)	8
RESULT_CODE	8
MS_RESULT_LEN	8
MS_RESULT	8 × MS_RESULT_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00000011’.

RESULT_CODE - Key exchange result code.

The mobile station shall set this field to indicate acceptance or rejection status, using the values defined in Table 3.5.1.2-1.

MS_RESULT_LEN - Length of MS_RESULT field.

The mobile station shall set this field to the number of octets in the MS_RESULT field.

MS_RESULT - Mobile station calculation result.

If A_KEY_P_REV received in the *MS Key Request Message* is equal to ‘00000010’, the mobile station shall set this field equal to the value of MS_RESULT as described in 5.1.2. If A_KEY_P_REV received in the *MS Key Request Message* is equal to ‘00000011’ or ‘00000100’, the mobile station shall set this field equal to the value of MS_RESULT as described in 5.3.2. If A_KEY_P_REV received in the *MS Key Request Message* is equal to ‘00000101’, the mobile station shall set this field to the value of MS_RESULT as described in 5.5.2.

3.5.1.5 Re-Authenticate Response Message

The *Re-Authenticate Response Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000100’)	8
AUTHR	18
RANDC	8
COUNT	6
AUTH_DATA	24

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00000100’.

AUTHR - Authentication signature data.

The mobile station shall set this field as specified in 3.3.2.

RANDC - Random challenge value.

The mobile station shall set this field as specified in 3.3.2.

COUNT - Call history parameter.

The mobile station shall set this field as specified in 3.3.2.

AUTH_DATA - Authentication Data input parameter.

The mobile station shall set this field as specified in 3.3.2.

3.5.1.6 Commit Response Message

The *Commit Response Message* has the following fixed-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00000101’)	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00000101’.

RESULT_CODE - Data commit result code.

The mobile station shall set this field to indicate acceptance or rejection status of the *Commit Request Message*, using values defined in Table 3.5.1.2-1.

3.5.1.7 Protocol Capability Response Message

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

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00000110’)	8
MOB_FIRM_REV	16
MOB_MODEL	8
NUM_FEATURES	8

NUM_FEATURES occurrences of the following features:

FEATURE_ID	8
FEATURE_P_REV	8

ADD_LENGTH	8
Additional fields	8 × ADD_LENGTH

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00000110’.

MOB_FIRM_REV - Mobile station firmware revision number.

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

MOB_MODEL - Mobile station manufacturer’s model number.

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

NUM_FEATURES - Number of Features.

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

FEATURE_ID - Feature Identifier.

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

FEATURE_P_REV - Feature protocol version.

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

Table 3.5.1.7-1 Feature Identifier

Features	FEATURE_ID	FEATURE_P_REV	FEATURE_P_REV Description
NAM Download (DATA_P_REV)	‘00000000’	‘00000010’	NAM Download as specified in this document
Key Exchange (A_KEY_P_REV)	‘00000001’	‘00000010’	A key provisioning as specified in this document
		‘00000011’	A key and 3G Root Key provisioning as specified in this document
		‘00000100’	3G Root Key provisioning as specified in this document
		‘00000101’	Enhanced 3G Root Key provisioning as specified in this document
		‘00000110’	Service Key Generation as specified in this document
System Selection for Preferred Roaming (SSPR_P_REV)	‘00000010’	‘00000001’	System Selection for Preferred Roaming using Preferred Roaming List
		‘00000010’	Reserved
		‘00000011’	System Selection for Preferred Roaming using Extended Preferred Roaming List associated with SSPR_P_REV of ‘00000011’
Service Programming Lock (SPL_P_REV)	‘00000011’	‘00000001’	Service Programming Lock as specified in this document
Over-The-Air Parameter Administration (OTAPA_P_REV)	‘00000100’	‘00000001’	Over-The-Air Parameter Administration as specified in this document
Preferred User Zone List (PUZL_P_REV)	‘00000101’	‘00000001’	Preferred User Zone List as specified in this document

3G Packet Data (3GPD)	'00000110'	'00000010'	3G Packet Data as specified in this document
Secure MODE (SECURE_MODE_P_REV)	‘00000111’	‘00000001’	Secure Mode as specified in this document when root key K is not available
		‘00000010’	Secure Mode as specified in this document when root key K is available
Multimedia Domain (MMD)	‘00001000’	‘00000001’	MMD as specified in this document
System Tag Download (TAG_P_REV)	‘00001001’	‘00000001’	System Tag Download as specified in this document
Multimedia Messaging Service (MMS)	‘00001010’	‘00000001’	MMS as specified in this document
Reserved for future standardization	‘000001011’ through ‘10111111’		
Available for manufacturer-specific features	‘11000000’ through ‘11111110’	See [4]	
Reserved	‘11111111’		

ADD_LENGTH - Number of octets in the additional fields.

The mobile station shall set this field to the number of octets included in the Additional fields.

Additional fields - Additional fields.

The mobile station shall include the following field as the first octet of the additional fields.

Field	Length (bits)
BAND_MODE_CAP	8

BAND_MODE_CAP - Band/mode Capability Information.

The mobile station shall set this field to indicate band and mode capabilities supported by the mobile station. This field consists of the fields as shown in Table 3.5.1.7-2. The mobile station shall set each field to '1' if the corresponding band/mode is supported by the mobile station; otherwise, the mobile station shall set the corresponding field to '0'. All bits of the RESERVED field of the BAND_MODE_CAP field shall be set to '0'.

Table 3.5.1.7-2 Band/mode Capability Information

Description	Length (bits)
Band Class 0 Analog	1
Band Class 0 CDMA	1
Band Class 1 CDMA	1
Band Class 3 CDMA	1
Band Class 6 CDMA	1
RESERVED	3

3.5.1.8 SSPR Configuration Response Message

The *SSPR Configuration Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00000111')	8
BLOCK_ID	8
RESULT_CODE	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to '00000111'.

BLOCK_ID - Parameter Block identifier.

The mobile station shall set this field to the value of the BLOCK_ID of the parameter block being returned in this message (see Table 3.5.3-1).

RESULT_CODE - SSPR Configuration result code.

The mobile station shall set this field to indicate acceptance or rejection status of the request for corresponding parameter block in the *SSPR Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter block data.

The mobile station shall include the parameter block specified by the BLOCK_ID field. If SECURE_MODE_IND$_S$ = '1', PARAM_DATA fields shall be encrypted as specified in 3.3.8.

FRESH_INCL - FRESH included indicator.

If SECURE_MODE_IND$_S$ = '1', the mobile station shall set this field to '1'; otherwise the mobile station shall set this field to '0'.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = '1', the mobile station shall include this field and set it to a 15-bit value chosen according to requirements set in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = '1', the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to '0'.

3.5.1.9 SSPR Download Response Message

The *SSPR Download Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00001000')	8
BLOCK_ID	8
RESULT_CODE	8

If the BLOCK_ID being confirmed is either '00000000' (Preferred Roaming List) or '00000001' (Extended Preferred Roaming List), the mobile station shall also include the following fields:

SEGMENT_OFFSET	16
SEGMENT_SIZE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001000’.

BLOCK_ID SSPR Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the parameter block in the *SSPR Download Request Message* that is being confirmed (see Table 4.5.3-1).

RESULT_CODE - SSPR Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the parameter block in the *SSPR Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

SEGMENT_OFFSET - Segment offset.

If the BLOCK_ID is either ‘00000000’ (Preferred Roaming List) or ‘00000001’ (Extended Preferred Roaming List), the mobile station shall include and set this field to the value of SEGMENT_OFFSET from the *SSPR Download Request Message* that is being confirmed; otherwise, the mobile station shall omit this field (See *SSPR Download Request Message* processing in 3.3.1 for more details).

SEGMENT_SIZE - Segment size.

If the BLOCK_ID is either ‘00000000’ (Preferred Roaming List) or ‘00000001’ (Extended Preferred Roaming List), the mobile station shall include and set this field to the number of octets of the preferred roaming list ($\text{PR\_LIST}_{\text{s-p}}$) included in SEGMENT_DATA of the *SSPR Download Request Message* that is being confirmed; otherwise, the mobile station shall omit this field (See *SSPR Download Request Message* processing in 3.3.1 for more details).

3.5.1.10 Validation Response Message

The *Validation Response Message* shall have the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001001’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001001’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *Validation Request Message* that is being confirmed.

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *Validation Request Message* that is being confirmed (see Table 4.5.4-1).

RESULT_CODE - Service programming lock result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *Validation Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

3.5.1.11 OTAPA Response Message

The *OTAPA Response Message* shall have the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001010’)	8
RESULT_CODE	8
RESERVED	7
NAM_LOCK_IND	1
RAND_OTAPA	0 or 32

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001010’.

RESULT_CODE - OTAPA result code.

The mobile station shall set this field using the values defined in Table 3.5.1.2-1.

RESERVED - Reserved field.

The mobile station shall set this field to ‘0000000’

NAM_LOCK_IND - NAM_LOCK indicator.

If the mobile station is sending this message in response to the *OTAPA Request Message* containing the START_STOP field equal to ‘1’, the mobile station shall set this field to ‘1’ if the indicators and parameters of the active NAM are secured by SPASM (see 3.3.7); otherwise, the mobile station shall set this field to ‘0’.

If the mobile station is sending this message in response to the *OTAPA Request Message* containing the START_STOP field equal to ‘0’, the mobile station shall set this field to ‘0’.

RAND_OTAPA - SPASM random challenge.

If the NAM_LOCK_IND is equal to ‘1’, the mobile station shall set this field as specified in 3.3.7; otherwise, the mobile station shall omit this field.

3.5.1.12 PUZL Configuration Response Message

The *PUZL Configuration Response Message* shall have the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00001011’)	8
BLOCK_ID	8
RESULT_CODE	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001011’.

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *PUZL Configuration Request Message* that is being confirmed (see Table 3.5.6-1).

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The mobile station shall include the parameter block specified by the BLOCK_ID field. If SECURE_MODE_IND$_S$ = ‘1’, PARAM_DATA field shall be encrypted as specified in 3.3.8.

FRESH_INCL - FRESH included indicator.

If the mobile station supports Secure Mode and if SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set this field to ’1’; otherwise the mobile station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If the mobile station supports Secure Mode, SECURE_MODE_IND$_S$ = ‘1’, and FRESH_INCL = ‘1’, the mobile station shall include this field and set it to a 15-bit value chosen according to requirements set in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = ‘1’, the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to ‘0’.

RESULT_CODE - Configuration result code.

The mobile station shall include one instance of this field for each parameter block included in the message, in the same order of appearance. The mobile station shall set this field to indicate acceptance or rejection status of the request for the corresponding parameter block in the *PUZL Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

3.5.1.13 PUZL Download Response Message

The *PUZL Download Response Message* shall have the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00001100')	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
RESULT_CODE	8
IDS_PRESENT	1
UZ_ID	0 or 16
UZ_SID	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to '00001100'.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *PUZL Download Response Message*.

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *PUZL Download Request Message* that is being confirmed (see Table 4.5.6-1).

RESULT_CODE - PUZL Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *PUZL Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

IDS_PRESENT - Identifiers present flag.

The mobile station shall set this field to indicate whether or not the UZ_ID and UZ_SID fields are included in the parameter block. If the UZ_ID and UZ_SID fields are included, IDS_PRESENT = '1'; otherwise, IDS_PRESENT = '0'.

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

RESERVED - Reserved bits.

3.5.1.14 3GPD Configuration Response Message

The *3GPD Configuration Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001101’)	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following parameter block:

BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
RESULT_CODE	8

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001101’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *3GPD Configuration Response Message*.

The mobile station shall set NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *3GPD Configuration Request Message* that is being confirmed (see Table 3.5.8-1).

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The mobile station shall include the parameter block (see 3.5.8) specified by the BLOCK_ID field. If SECURE_MODE_IND$_S$ = '1', PARAM_DATA fields shall be encrypted as specified in 3.3.8.

RESULT_CODE - Configuration result code.

The mobile station shall set this field to indicate acceptance or rejection status of the request for the corresponding parameter block in the *3GPD Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

FRESH_INCL - FRESH included indicator.

If SECURE_MODE_IND$_S$ = '1', the mobile station shall set this field to SECURE_MODE_IND; otherwise the mobile station shall set this field to '0'.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = '1', the mobile station shall include this field and set it to a 15-bit value chosen according to requirements set in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = '1', the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to '0'.

3.5.1.15 3GPD Download Response Message

The *3GPD Download Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE ('00001110')	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following confirmation block:	
BLOCK_ID	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to '00001110'.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the 3GPD *Download Request Message* that is being confirmed.

The mobile station shall set NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *3GPD Download Request Message* that is being confirmed (see Table 4.5.7-1).

RESULT_CODE - Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *3GPD Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

3.5.1.16 Secure Mode Response Message

The *Secure Mode Response Message* shall have the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00001111’)	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00001111’.

RESULT_CODE - Secure Mode result code.

The mobile station shall set this field using the values defined in Table 3.5.1.2-1.

The mobile station shall add reserved bits, if necessary, in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0000000’.

3.5.1.17 Extended Protocol Capability Response Message

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

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

NUM_FEATURES occurrences of the following features:

FEATURE_ID	8
FEATURE_P_REV	8

NUM_CAP_RECORDS	8

NUM_CAP_RECORDS occurrences of the following records:

CAP_RECORD_TYPE	8
CAP_RECORD_LEN	8
Type-specific field	8 × RECORD_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

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

OTASP_MOB_P_REV - OTASP Mobile Protocol Revision.

The mobile station shall set this field to '00000100'.

MOB_FIRM_REV - Mobile station firmware revision number.

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

MOB_MODEL - Mobile station manufacturer's model number.

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

NUM_FEATURES - Number of Features.

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

FEATURE_ID - Feature Identifier.

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

FEATURE_P_REV - Feature protocol version.

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

NUM_CAP_RECORDS - Number of Capability Records.

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

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

CAP_RECORD_TYPE - Capability Record Type.

The mobile station shall set this field to the record type value shown in Table 3.5.1.*1*7.1-1 corresponding to the type of this information record.

CAP_RECORD_LEN - Capability Record Length.

The mobile station shall set this field to the number of octets included in the type-specific fields of this information record. If the mobile station doesn’t support a requested CAP_REC*ORD*_TYPE or supports a requested CAP_REC*ORD*_TYPE, but doesn’t have a value, the mobile station shall include the CAP_REC*ORD*_TYPE with the CAP_RECORD_LEN field set to ‘00000000’.

Type-specific field - Type-specific field.

The mobile station shall set these fields to the information as specified in 3.5.1.*1*7.1 for the specific type of records.

3.5.1.17.1 Capability Information Record

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

Table 3.5.1.17.1-1 Capability Information Record Types

Capability Information Record	**Record Type (binary)**
Operating Mode Information	‘00000000’
CDMA Band Class Information	‘00000001’
MEID	‘00000010’
ICCID	*‘00000011’*
EXT_UIM_ID	*‘00000100’*
MEID_ME	*‘00000101’*
All other values are reserved.	

3.5.1.17.1.1 Operating Mode Information

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

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

OP_MODE_INFO – Operating mode information.

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

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

Table 3.5.1.17.1.1-1. OP_MODE

Subfield	Length (bits)	Subfield Description	Standards
OP_MODE0	1	Analog mode	[22]
OP_MODE1	1	CDMA mode	[7]
OP_MODE2	1	HRPD mode	[9]
RESERVED	5	–	–

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

RESERVED – Reserved bits.

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

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

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

3.5.1.17.1.2 CDMA Band Class Information

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

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

BAND_CLASS_INFO – Band class information.

This field indicates which band classes are supported by the mobile station.

The mobile station shall set the Nth significant bit of this field to ‘1’ if the Nth band class defined in [23] is supported by the mobile station; otherwise, the mobile station shall set the Nth most significant bit of this field to ‘0’.

The mobile station shall add reserved bits as needed in order to make the length of the entire information record equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.1.17.1.3 MEID

This capability information record is used to return the mobile station MEID *or R-UIM’s SF_EUIMID based on the SF_EUIMID Usage Indicator as defined in [24]*.

Type-Specific Field	**Length (bits)**
MEID	56

MEID – Mobile Equipment Identifier.

The mobile station shall set this field ~~to its Mobile Equipment Identifier.~~*according to Table 3.5.1.17.1.3-1.*

Table 3.5.1.17.1.3-1. MEID Field Setting

SF_EUIMID Usage Indicator	***MEID***
0	*MEID*
1	*SF_EUIMID*

3.5.1.17.1.4 ICCID

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

Type-Specific Field	***Length (bits)***
ICCID	*80*

ICCID – Integrated Circuit Card Identifier.

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

3.5.1.17.1.5 EXT_UIM_ID

This capability information record is used to return the EXT_UIM_ID in the R-UIM based on the SF_EUIMID-based EUIMID service as defined in [24].

Type-Specific Field	***Length (bits)***
EXT_UIM_ID	*8 × CAP_RECORD_LEN*

EXT_UIM_ID – *Mobile station Extended User Identity Module identifier.*

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

Table 3.5.1.17.1.5-1. EXT_UIM_ID Field Setting

SF_EUIMID-based EUIMID	***EXT_UIM_ID***	***Length (bits)***
0	*LF_EUIMID*	*80*
1	*SF_EUIMID*	*56*

3.5.1.17.1.6 MEID_ME

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

Type-Specific Field	***Length (bits)***
MEID_ME	*56*

MEID_ME – *Mobile Equipment Identifier of ME.*

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

3.5.1.18 MMD Configuration Response Message

The *MMD Configuration Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010001’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
RESULT_CODE	8

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010001’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *MMD Configuration Response Message*.

The mobile station shall set NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *MMD Configuration Request Message* that is being confirmed (see Table 3.5.9-1).

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The mobile station shall include the parameter block (see 3.5.9) specified by the BLOCK_ID field. If $SECURE\_MODE\_IND_S$ = ‘1’, PARAM_DATA fields shall be encrypted as specified in 3.3.8.

RESULT_CODE - Configuration result code.

The mobile station shall set this field to indicate acceptance or rejection status of the request for the corresponding parameter block in the *MMD Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

FRESH_INCL - FRESH included indicator.

If SECURE_MODE_IND$_S$ = ‘1’, the mobile station shall set this field to SECURE_MODE_IND; otherwise the mobile station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1’, the mobile station shall include this field and set it to a 15-bit value chosen according to requirements set in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = ‘1’, the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to ‘0’.

3.5.1.19 MMD Download Response Message

The *MMD Download Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010010’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following confirmation block:	
BLOCK_ID	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010010’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *MMD Download Request Message* that is being confirmed.

The mobile station shall set NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *MMD Download Request Message* that is being confirmed (see Table 4.5.8-1).

RESULT_CODE - Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *MMD Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

3.5.1.20 System Tag Configuration Response Message

The *System Tag Configuration Response Message* shall have the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00010011’)	8
BLOCK_ID	8
RESULT_CODE	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010011’.

BLOCK_ID - The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *System Tag Configuration Request Message* that is being confirmed (see Table 3.5.10-1).

RESULT_CODE - System Tag result code.

The mobile station shall set this field to indicate acceptance or rejection status of the request for corresponding parameter block in the *System Tag Configuration Request Message*, using the values defined in Table 3.5.1.2-1.

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter block data.

The mobile station shall include the parameter block specified by the BLOCK_ID field.

3.5.1.21 System Tag Download Response Message

The *System Tag Download Response Message* shall have the following format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010100’)	8
BLOCK_ID	8
RESULT_CODE	8

If the BLOCK_ID being confirmed is ‘00000001’ (Group Tag List),’00000010’ (Specific Tag List), or ‘00000011’ (Call Prompt List), the mobile station shall also include the following fields:

SEGMENT_OFFSET	16
SEGMENT_SIZE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010100’.

BLOCK_ID System Tag Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the parameter block in the *System Tag Download Request Message* that is being confirmed (see Table 4.5.9-1).

RESULT_CODE - System Tag Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the parameter block in the *System Tag Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

SEGMENT_OFFSET - Segment offset.

If the BLOCK_ID being confirmed is ‘00000001’ (Group Tag List),’00000010’ (Specific Tag List), or ‘00000011’ (Call Prompt List), the mobile station shall include and set this field to the value of SEGMENT_OFFSET from the *System Tag Download Request Message* that is being confirmed; otherwise, the mobile station shall omit this field

SEGMENT_SIZE - Segment size.

If the BLOCK_ID being confirmed is ‘00000001’ (Group Tag List),’00000010’ (Specific Tag List), or ‘00000011’ (Call Prompt List), the mobile station shall set this field to the number of octets of the group tag list (GROUP_TAG_LIST$_{s\text{-}p}$), specific tag list (SPEC_TAG_LIST$_{s\text{-}p}$), or call prompt list (CALL_PRMPT_ LIST$_{s\text{-}p}$) included in SEGMENT_DATA of the *System Tag Download Request Message* that is being confirmed; otherwise, the mobile station shall omit this field.

3.5.1.22 Service Key Generation Response Message

The *Service Key Generation Response Message* shall have the following format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010101’)	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010101’.

RESULT_CODE - Service Key Generation result code.

The mobile station shall set this field using the values defined in Table 3.5.1.2-1.

3.5.1.23 MMS Configuration Response Message

The *MMS Configuration Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010110’)	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following parameter block:

BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
RESULT_CODE	*8*

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010110’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *MMS Configuration Response Message*.

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the parameter block type being included in the message (see Table 3.5.12-1).

BLOCK_LEN - Parameter block length.

The mobile station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The mobile station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active, PARAM_DATA fields shall be encrypted as specified in 3.3.8.

RESULT_CODE - Configuration result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the MMS Configuration Request Message that is being confirmed, using the values defined in Table 3.5.1.2-1.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 3.3.8), the mobile station shall set this field to ‘1’; otherwise the mobile station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1’, the mobile station shall include this field and set it to a 15-bit value chosen as specified in 3.3.8 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the mobile station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL= ‘1’, the mobile station shall omit this field; otherwise, the mobile station shall set all the bits of this field to ‘0’.

3.5.1.24 MMS Download Response Message

The *MMS Download Response Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010111’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following confirmation block:	
BLOCK_ID	8
RESULT_CODE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The mobile station shall set this field to ‘00010111’.

NUM_BLOCKS - Number of parameter blocks.

The mobile station shall set this field to the number of parameter blocks contained in the *MMS Download Request Message* that is being confirmed.

The mobile station shall set NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The mobile station shall set this field to the value of the BLOCK_ID field of the corresponding parameter block in the *MMS Download Request Message* that is being confirmed (see Table 4.5.10-1).

RESULT_CODE - Download result code.

The mobile station shall set this field to indicate acceptance or rejection status of the corresponding parameter block in the *MMS Download Request Message* that is being confirmed, using the values defined in Table 3.5.1.2-1.

3.5.2 NAM Parameter Blocks

Table 3.5.2-1 lists the types of parameter blocks used in the *Configuration Request Message* and the *Configuration Response Message*.

Table 3.5.2-1 NAM Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
CDMA/Analog NAM	'00000000'	3.5.2.1
Mobile Directory Number	'00000001'	3.5.2.2
CDMA NAM	'00000010'	3.5.2.3
IMSI_T	'00000011'	3.5.2.4
Reserved for future standardization	'00000100' through '01111111'	
Available for manufacturer-specific parameter block definitions	'10000000' through '11111110'	See [4]
Reserved	'11111111'	

3.5.2.1 CDMA/Analog NAM Parameter Block

The PARAM_DATA field of this Parameter Block consists of the following fields:

Field	Length (bits)
FIRSTCHP	11
HOME_SID	15
EX	1
SCM	8
MOB_P_REV	8
IMSI_M_CLASS	1
IMSI_M_ADDR_NUM	3
MCC_M	10
IMSI__M_11_12	7
IMSI_M_S	34
ACCOLC	4
LOCAL_CONTROL	1
MOB_TERM_HOME	1
MOB_TERM_FOR_SID	1
MOB_TERM_FOR_NID	1
MAX_SID_NID	8
STORED_SID_NID	8

STORED_SID_NID occurrences of the following SID/NID pair:

SID	15
NID	16

The parameter block ends with the following field:

RESERVED	0 to 7 (as needed)

FIRSTCHP - First paging channel used in the home system.

The mobile station shall set this field to the value of the FIRSTCHP_p NAM indicator (see F.3 of [1, 7]).

HOME_SID - Home system identification.

The mobile station shall set this field to the value of the HOME_SID_p NAM indicator (see F.3 of [1, 7]).

EX - Extended address indicator.

The mobile station shall set this field to the value of the Ex_p NAM indicator (see F.3 of [1, 7]).

SCM - Station class mark.

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

MOB_P_REV - Mobile station protocol revision number.

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

IMSI_M_CLASS - IMSI_M Class assignment of the mobile station.

If the mobile station's IMSI_M is a class 0 IMSI, the mobile station shall set this field to '0'; otherwise, the mobile station shall set this field to '1'.

IMSI_M_ADDR_NUM - Number of IMSI_M address digits.

If the mobile station has been assigned a class 1 IMSI_M (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]), the mobile station shall set this field to four less than the number of digits in the NMSI; otherwise, the mobile station shall set this field to '000'.

MCC_M - Mobile country code.

The mobile station shall set this field to the value of the MCC_M$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI__M_11_12 - 11th and 12th digits of the IMSI_M.

The mobile station shall set this field to the value of the IMSI_M_11_12$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_S - The least significant 10 digits of the IMSI_M.

The mobile station shall set this field to the value of the IMSI_M_S$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

ACCOLC - Access overload class.

The mobile station shall set this field to the value of the ACCOLC$_p$ NAM indicator (see F.3 of [1, 7]).

LOCAL_CONTROL - Local control status.

If the local control status is enabled (see 2.6.1.2.2 of [1]), the mobile station shall set this field to '1'; otherwise, the mobile station shall set this field to '0'.

MOB_TERM_HOME - Termination indicator for the home system.

The mobile station shall set this field to the value of the MOB_TERM_HOME$_p$ NAM indicator (see F.3 of [1, 7]).

MOB_TERM_FOR_SID - Termination indicator for SID roaming.

The mobile station shall set this field to the value of the MOB_TERM_FOR_SID$_p$ NAM indicator (see F.3 of [1, 7]).

MOB_TERM_FOR_NID - Termination indicator for NID roaming.

The mobile station shall set this field to the value of the $\text{MOB\_TERM\_FOR\_NID}_p$ NAM indicator (see F.3 of [1, 7]).

MAX_SID_NID - Maximum stored SID/NID pairs.

The mobile station shall set this field to the maximum number of SID/NID pairs that it can store in the NAM.

STORED_SID_NID - Number of stored SID/NID pairs.

The mobile station shall set this field to the number of SID/NID pairs stored in the NAM. All SID/NID pairs stored in the NAM shall be included in the parameter block.

SID - System identification.

The mobile station shall include one occurrence of this field for each SID/NID pair stored in the NAM. The mobile station shall set this field to the value of the SID_p NAM indicator (see F.3 of [1, 7]).

NID - Network identification.

The mobile station shall include one occurrence of this field for each SID/NID pair stored in the NAM. The mobile station shall set this field to the value of the NID_p NAM indicator (see F.3 of [1, 7]).

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to '0'.

3.5.2.2 Mobile Directory Number

The PARAM_DATA field of the Mobile Directory Number Parameter Block consists of the following fields:

Field	Length (bits)
N_DIGITS	4
N_DIGITS occurrences of the following field:	
DIGITn	4
The parameter block ends with the following field:	
RESERVED	0 or 4

N_DIGITS - Number of digits.

The mobile station shall set this field to the number of digits included in the parameter block.

DIGITn - Digit.

The mobile station shall set these fields to the digits of the mobile station directory number. Each digit shall be encoded according to Table 6.7.1.3.2.4-4 of [1] or Table 2.7.1.3.2.4-4 of [7].

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.2.3 CDMA NAM Parameter Block

The PARAM_DATA field of this Parameter Block consists of the following fields:

Field	**Length (bits)**
RESERVED	2
SLOTTED_MODE	1
RESERVED	5
MOB_P_REV	8
IMSI_M_CLASS	1
IMSI_M_ADDR_NUM	3
MCC_M	10
IMSI_M_11_12	7
IMSI_M_S	34
ACCOLC	4
LOCAL CONTROL	1
MOB_TERM_HOME	1
MOB_TERM_FOR_SID	1
MOB_TERM_FOR_NID	1
MAX_SID_NID	8
STORED_SID_NID	8

STORED_SID_NID occurrences of the following SID/NID pair:

SID	15
NID	16

The parameter block ends with the following field:

RESERVED	0 to 7 (as needed)

RESERVED - Reserved bits.

The mobile station shall set this field to ‘00’.

SLOTTED_MODE - Slotted mode.

If the mobile station is operating in the slotted mode, the mobile station shall set this field to ‘1’; otherwise, the mobile station shall set this field to ‘0’.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘00000’.

MOB_P_REV - Mobile station protocol revision number.

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

IMSI_M_CLASS - IMSI_M Class assignment of the mobile station.

If the mobile station’s IMSI_M is a class 0 IMSI, the mobile station shall set this field to ‘0’; otherwise, the mobile station shall set this field to ‘1’.

IMSI_ M_ADDR_NUM - Number of IMSI_M address digits.

If the mobile station has been assigned a class 1 IMSI_M (see F.3 [1, 7]), the mobile station shall set this field to four less than the number of digits in the NMSI; otherwise, the mobile station shall set this field to ‘000’.

MCC_M - Mobile country code.

The mobile station shall set this field to the value of the MCC_M$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_11_12 - 11th and 12th digits of the IMSI.

The mobile station shall set this field to the value of the IMSI_M_11_12$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_S - The least significant 10 digits of the IMSI.

The mobile station shall set this field to the value of the IMSI_M_S$_p$ NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

ACCOLC - Access overload class.

The mobile station shall set this field to the value of the ACCOLC$_p$ NAM indicator (see F.3 of [1, 7]).

LOCAL CONTROL - Local control status.

If the local control status is enabled (see 6.3.9 of [1] or 2.3.9 of [7]), the mobile station shall set this field to ‘1’; otherwise, the mobile station shall set this field to ‘0’.

MOB_TERM_HOME - Termination indicator for the home system.

The mobile station shall set this field to the value of the MOB_TERM_HOME$_p$ NAM indicator (see F.3 of [1, 7]).

MOB_TERM_FOR_SID - Termination indicator for SID roaming.

The mobile station shall set this field to the value of the MOB_TERM_FOR_SID$_p$ NAM indicator (see F.3 of [1, 7]).

MOB_TERM_FOR_NID - Termination indicator for NID roaming.

The mobile station shall set this field to the value of the MOB_TERM_FOR_NID$_p$ NAM indicator (see F.3 of [1, 7]).

MAX_SID_NID - Maximum stored SID/NID pairs.

The mobile station shall set this field to the maximum number of SID/NID pairs that it can store in the NAM.

STORED_SID_NID - Number of stored SID/NID pairs.

The mobile station shall set this field to the number of SID/NID pairs stored in the NAM. All SID/NID pairs stored in the NAM shall be included in the parameter block.

SID - System identification.

The mobile station shall include one occurrence of this field for each SID/NID pair stored in the NAM. The mobile station shall set this field to the value of the SID$_p$ NAM indicator (see F.3 of [1, 7]).

NID - Network identification.

The mobile station shall include one occurrence of this field for each SID/NID pair stored in the NAM. The mobile station shall set this field to the value of the NID$_p$ NAM indicator (see F.3 of [1, 7]).

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.2.4 IMSI_T Parameter Block

The PARAM_DATA field of the IMSI_T Parameter Block consists of the following fields:

Field	Length (bits)
IMSI_T_CLASS	1
IMSI_T_ADDR_NUM	3
MCC_T	10
IMSI_T_11_12	7
IMSI_T_S	34
RESERVED	1

IMSI_T_CLASS - IMSI_T Class assignment of the mobile station.

If the mobile station's IMSI_T is a class 0 IMSI, the mobile station shall set this field to '0'; otherwise, the mobile station shall set this field to '1'.

IMSI_T_ADDR_NUM - Number of IMSI_T address digits.

If the mobile station has been assigned a class 1 IMSI_T (see 6.3.1 of [1] or 2.3.1 of [7]), the mobile station shall set this field to four less than the number of digits in the NMSI; otherwise, the mobile station shall set this field to '000'.

MCC_T - Mobile country code.

The mobile station shall set this field to the value of the MCC_T_p NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI__T_11_12 - 11th and 12th digits of the IMSI_T.

The mobile station shall set this field to the value of the IMSI_T_11_12_p NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_T_S - The least significant 10 digits of the IMSI_T.

The mobile station shall set this field to the value of the IMSI_T_S_p NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

RESERVED - Reserved bits.

The mobile station shall set this field to '0'.

3.5.3 SSPR Parameter Blocks

Table 3.5.3-1 lists the types of parameter blocks used in the *SSPR Configuration Request Message* and the *SSPR Configuration Response Message*.

Table 3.5.3-1 SSPR Parameter Block Types

SSPR Parameter Block Type	BLOCK_ID	Reference
Preferred Roaming List Dimensions	‘00000000’	3.5.3.1
Preferred Roaming List	‘00000001’	3.5.3.2
Extended Preferred Roaming List Dimensions	‘00000010’	3.5.3.3
Reserved for future standardization	‘00000011’ - ’01111111’	
Available for manufacturer-specific parameter block definitions	‘10000000’- ‘11111110’	See [4]
Reserved	‘11111111’	

3.5.3.1 Preferred Roaming List Dimensions Parameter Block

The PARAM_DATA field of the Preferred Roaming List Dimensions Parameter Block consists of the following fields:

Field	Length (bits)
MAX_PR_LIST_SIZE	16
CUR_PR_LIST_SIZE	16
PR_LIST_ID	16
RESERVED	1
NUM_ACQ_RECS	9
NUM_SYS_RECS	14

MAX_PR_LIST_SIZE - Maximum preferred roaming list size.

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_LIST_{S-p}).

CUR_PR_LIST_SIZE - Current preferred roaming list size.

The mobile station shall set this field to the size, in octets, of the current preferred roaming list.

PR_LIST_ID Preferred Roaming List Identification.

The mobile station shall set this field to the value of the Preferred Roaming List Identification assigned for the preferred roaming list (PR_LIST_{S-p}) by the base station.

RESERVED - Reserved bit.

The mobile station shall set this field to ‘0’.

NUM_ACQ_RECS	-	Number of acquisition records. The mobile station shall set this field to the number of acquisition records contained in the ACQ_TABLE field of the current preferred roaming list.
NUM_SYS_RECS	-	Number of system records. The mobile station shall set this field to the number of system records contained in the SYS_TABLE field of the current preferred roaming list.

3.5.3.2 Preferred Roaming List Parameter Block

The PARAM_DATA field of the Preferred Roaming List Parameter Block consists of the following fields:

Field	Length (bits)
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	8 × SEGMENT_SIZE

RESERVED	-	Reserved bits. The mobile station shall set this field to ‘0000000’.
LAST_SEGMENT	-	Last segment indicator bit. The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the preferred roaming list (PR_LIST_{S-P}); otherwise, the mobile station shall set this field to ‘0’.
SEGMENT_OFFSET	-	Segment offset. The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *SSPR Configuration Request Message*.
SEGMENT_SIZE	-	Segment size. The mobile station shall set this field to the number of octets of the preferred roaming list (PR_LIST_{S-P}) included in SEGMENT_DATA.
SEGMENT_DATA	-	Segment of the preferred roaming list (PR_LIST_{S-P}) data.

If REQUEST_OFFSET from the corresponding *SSPR Configuration Request Message* specifies an offset that is invalid for the current preferred roaming list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current preferred roaming list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the preferred roaming list in this field. The octets shall be equal to the octets starting at the offset within the preferred roaming list specified by SEGMENT_OFFSET.

3.5.3.3 Extended Preferred Roaming List Dimensions Parameter Block

The PARAM_DATA field of the Extended Preferred Roaming List Dimensions Parameter Block consists of the following fields:

Field	**Length (bits)**
MAX_PR_LIST_SIZE	16
CUR_PR_LIST_SIZE	16
PR_LIST_ID	16
CUR_SSPR_P_REV	8
CUR_SSPR_P_REV-specific fields	variable

If CUR_SSPR_P_REV is ‘00000001’ the CUR_SSPR_P_REV-specific fields also include the following fields:

RESERVED	1
NUM_ACQ_RECS	9
NUM_SYS_RECS	14

If CUR_SSPR_P_REV is ‘00000011’ the CUR_SSPR_P_REV-specific fields also include the following fields:

NUM_ACQ_RECS	9
NUM_COMMON_SUBNET_RECS	9
NUM_EXT_SYS_RECS	14

MAX_PR_LIST_SIZE - Maximum preferred roaming list size.

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_LIST$_{s-p}$).

CUR_PR_LIST_SIZE - Current preferred roaming list size.

The mobile station shall set this field to the size, in octets, of the current preferred roaming list.

PR_LIST_ID Preferred Roaming List Identification.

The mobile station shall set this field to the value of the Preferred Roaming List Identification assigned for the preferred roaming list (PR_LIST$_{s-p}$) by the base station.

CUR_SSPR_P_REV - Protocol revision of the mobile station’s current preferred roaming list.

The mobile station shall set this field to the value of the SSPR_P_REV associated with its current preferred roaming list.

RESERVED - Reserved bit.

The mobile station shall set this field to ‘0’.

NUM_ACQ_RECS - Number of acquisition records.

The mobile station shall set this field to the number of acquisition records contained in the ACQ_TABLE field of the current preferred roaming list.

NUM_SYS_RECS - Number of system records.

The mobile station shall set this field to the number of system records contained in the SYS_TABLE field of the current preferred roaming list.

NUM_COMMON_SUBNET_RECS

- Number of records in the Common Subnet Table.

This field is set to the number of records contained in the Common Subnet Table.

NUM_EXT_SYS_RECS - Number of extended system records.

The mobile station shall set this field to the number of extended system records contained in the EXT_SYS_TABLE field of the current preferred roaming list.

3.5.4 Reserved

Reserved.

3.5.5 Preferred Roaming List and Extended Preferred Roaming List

The preferred roaming list (PR_LIST$_{s\text{-}p}$) contains information to assist the mobile station system selection and acquisition process, particularly when the mobile station is roaming. The preferred roaming list can be sent to the mobile station using Over-the-Air Service Provisioning (OTASP). The preferred roaming list is retained by the mobile station when power is turned off. Two categories of the preferred roaming list are defined: The Preferred Roaming List and the Extended Preferred Roaming List.

The Preferred Roaming List is associated with SSPR_P_REV equal to ‘00000001’ and has the following variable length format:

Preferred Roaming List Field	**Length (bits)**
PR_LIST_SIZE	16
PR_LIST_ID	16
PREF_ONLY	1
DEF_ROAM_IND	8
NUM_ACQ_RECS	9
NUM_SYS_RECS	14
ACQ_TABLE	variable
SYS_TABLE	variable
RESERVED	0 to 7
PR_LIST_CRC	16

PR_LIST_SIZE - Preferred roaming list size.

This field is set to the total size, in octets, of the preferred roaming list, including the PR_LIST_SIZE and PR_LIST_CRC fields.

PR_LIST_ID Preferred Roaming List Identification.

The mobile station shall set this field to the value of the Preferred Roaming List Identification assigned for the preferred roaming list ($PR\_LIST_{s\text{-}p}$) by the base station.

PREF_ONLY - Preferred only.

This field is set to ‘1’ if the mobile station is to operate only on systems that are specified in SYS_TABLE with PREF_NEG set to ‘1’. This field is set to ‘0’ if the mobile station is to operate on systems that are specified in SYS_TABLE with PREF_NEG set to ‘1’ or on systems that are not specified in SYS_TABLE[2].

DEF_ROAM_IND - Default roaming indication.

This field is set to the roaming indication value the mobile station is to use when operating on systems not specified in SYS_TABLE (see [4]).

NUM_ACQ_RECS - Number of acquisition records.

This field is set to the number of acquisition records contained in ACQ_TABLE (see Table 3.5.5.2-1).

NUM_SYS_RECS - Number of system records.

---

[2] For emergency access (911) the mobile station may ignore restrictions set by the PREF_ONLY and PREF_NEG fields and access any available system.

This field is set to the number of system records contained in SYS_TABLE.

ACQ_TABLE - Acquisition Table.

This field contains the Acquisition Records. The number of acquisition records is specified by NUM_ACQ_RECS. The acquisition record formats are specified in 3.5.5.2.1.

SYS_TABLE - System Table.

This field contains system records. The number of system records is specified by NUM_SYS_RECS. The system record format is specified in 3.5.5.3.1.

RESERVED - Reserved bits.

This field is populated with '0' bits as necessary to make the length of the entire preferred roaming list equal to an integer number of octets.

PR_LIST_CRC - CRC for preferred roaming list.

This field is set to the 16-bit CRC calculated according to 3.5.5.1.

The Extended Preferred Roaming List is associated with SSPR_P_REV greater than or equal to '00000010' and has the following variable length format:

Extended Preferred Roaming List Field	**Length (bits)**
PR_LIST_SIZE	16
PR_LIST_ID	16
CUR_SSPR_P_REV	8
CUR_SSPR_P_REV-specific	variable

PR_LIST_SIZE - Extended Preferred Roaming List size.

This field is set to the total size, in octets, of the Extended Preferred Roaming List, including the PR_LIST_SIZE and PR_LIST_CRC fields.

PR_LIST_ID Preferred Roaming List Identification.

The mobile station shall set this field to the value of the Extended Preferred Roaming List identification assigned for the preferred roaming list ($PR\_LIST_{s\text{-}p}$) by the base station.

CUR_SSPR_P_REV - Protocol revision for the PRL format.

This field is used to specify the format of the rest of the Extended Preferred Roaming List.

The format of the Extended Preferred Roaming List associated with the SSPR_P_REV equal to '00000011' has the following format:

Extended Preferred Roaming List Field	**Length (bits)**
PR_LIST_SIZE	16
PR_LIST_ID	16
CUR_SSPR_P_REV	8
PREF_ONLY	1
DEF_ROAM_IND	8
NUM_ACQ_RECS	9
NUM_COMMON_SUBNET_RECS	9
NUM_SYS_RECS	14
RESERVED	7
EXT_ACQ_TABLE	variable
COMMON_SUBNET_TABLE	variable
EXT_SYS_TABLE	variable
RESERVED	As needed
PR_LIST_CRC	16

PR_LIST_SIZE - Preferred roaming list size.

This field is set to the total size, in octets, of the preferred roaming list, including the PR_LIST_SIZE and PR_LIST_CRC fields.

PR_LIST_ID Preferred Roaming List Identification.

The mobile station shall set this field to the value of the Preferred Roaming List Identification assigned for the preferred roaming list (PR_LIST$_{s-p}$) by the base station.

CUR_SSPR_P_REV - Protocol revision of the mobile station SSPR Download procedure and the PRL format.

This field is set to the value of the SSPR_P_REV corresponding this preferred roaming list (PR_LIST$_{s-p}$) structure. This field determines the parsing rules for the Preferred Roaming List. The base station shall set this field to ‘00000011’ for this PRL structure.

PREF_ONLY - Preferred only.

This field is set to ‘1’ if the mobile station is to operate only on systems that are specified in SYS_TABLE with PREF_NEG set to ‘1’. This field is set to ‘0’ if the mobile station is to operate on systems that are specified in SYS_TABLE with PREF_NEG set to ‘1’ or on systems that are not specified in SYS_TABLE[3].

DEF_ROAM_IND - Default roaming indication.

This field is set to the roaming indication value the mobile station is to use when operating on systems not specified in SYS_TABLE (see TSB58).

NUM_ACQ_RECS - Number of acquisition records.

This field is set to the number of acquisition records contained in ACQ_TABLE (see Table 3.5.5.2-1).

NUM_COMMON_SUBNET_RECS

- Number of records in the Common Subnet Table.

This field is set to the number of records contained in the Common Subnet Table.

NUM_SYS_RECS - Number of system records.

This field is set to the number of Extended System Records contained in EXT_SYS_TABLE.

EXT_ACQ_TABLE - Extended Acquisition Table.

This field contains the Extended Acquisition Records. The number of acquisition records is specified by NUM_ACQ_RECS. The Extended Acquisition Record format is specified in 3.5.5.2.2.

COMMON_SUBNET_TABLE -

Common Subnet Table.

This field contains the Common Subnet Records defined in 3.5.5.3.2.1. The number of acquisition records is specified by NUM_COMMON_SUBNET_RECS.

EXT_SYS_TABLE - Extended System Table.

This field contains Extended System Records. The number of Extended system records is specified by NUM_SYS_RECS. The Extended system record format is specified in 3.5.5.3.2.

RESERVED - Reserved bits.

---

[3] For emergency access (911) the mobile station may ignore restrictions set by the PREF_ONLY and PREF_NEG fields and access any available system.

This field is populated with ‘0’ bits as necessary to make the length of the entire preferred roaming list equal to an integer number of octets. This field may be extended for future use. The mobile station shall be able to parse the entire Extended PRL even if this field is more than 7 bits.

PR_LIST_CRC - CRC for preferred roaming list.

This field is set to the 16-bit CRC calculated according to 3.5.5.1.

3.5.5.1 Preferred Roaming List CRC Calculation

The 16-bit preferred roaming list CRC field PR_LIST_CRC is calculated on all bits of the Preferred Roaming List/Extended Preferred Roaming List excluding the bits of the PR_LIST_CRC field itself. The generator polynomial for this CRC is $g(x) = x^{16} + x^{12} + x^{5} + x^{0}$.

The 16-bit CRC is calculated according to the following procedure using the logic shown in Figure 2.2.1-2:

- Initially, all shift register elements are set to logical one and the switches are set in the position A.
- The register is clocked with each preferred roaming list bit as an input, from the most significant bit of the PR_LIST_SIZE field through the least significant bit of the RESERVED field.
- The switches are set in the position B, and the register is clocked an additional 16 times. The 16 additional output bits constitute the CRC.

3.5.5.2 Acquisition Records

An acquisition record contains parameters that the mobile station can use to acquire a system. Each type of acquisition record is tailored for use in acquiring a particular kind of system.

Two categories of acquisition records are defined; Acquisition Records and Extended Acquisition Records. Table 3.5.5.2-1 defines the types of Acquisition Records. The Acquisition Records shall be used only in a Preferred Roaming List associated with the SSPR_P_REV equal to ‘00000001’.

Table 3.5.5.2-1 Acquisition Record Type Values

Acquisition Record Type	Value
Reserved	‘0000’
Cellular Analog	‘0001’
Cellular CDMA (Standard Channels)	‘0010’
Cellular CDMA (Custom Channels)	‘0011’
Cellular CDMA Preferred	‘0100’
PCS CDMA (Using Blocks)	‘0101’
PCS CDMA (Using Channels)	‘0110’
JTACS CDMA (Standard Channels)	'0111'
JTACS CDMA (Custom Channels)	'1000'
2GHz Band (Using Channels)	'1001'
Reserved	‘1010’ - ‘1111’

Table 3.5.5.2-2 defines the types of Extended Acquisition Records. The Extended Acquisition Records shall be used only in an Extended Preferred Roaming List associated with the SSPR_P_REV equal to ‘00000011’.

Table 3.5.5.2-2 Extended Acquisition Record Type Values

Acquisition Record Type	Value
Reserved	‘00000000’
Cellular Analog	‘00000001’
Cellular CDMA (Standard Channels)	‘00000010’
Cellular CDMA (Custom Channels)	‘00000011’
Cellular CDMA Preferred	‘00000100’
PCS CDMA (Using Blocks)	‘00000101’
PCS CDMA (Using Channels)	‘00000110’
JTACS CDMA (Standard Channels)	'00000111'
JTACS CDMA (Custom Channels)	'00001000'
2GHz Band (Using Channels)	'00001001'
Generic Acquisition Record for IS-2000 and IS-95	‘00001010’
Generic Acquisition Record for HRPD	‘00001011’
Reserved	All other values

If ACQ_TABLE contains more than one acquisition record, these records should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

3.5.5.2.1 Acquisition Record Formats

3.5.5.2.1.1 Cellular Analog System Acquisition Record

This acquisition record type is for use in acquiring a cellular analog system, and has the following fixed length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘0001’)	4
A_B	2

ACQ_TYPE - Acquisition record type.
This field is set to ‘0001’ (see Table 3.5.5.2-1).

A_B - System A/B selection type.
The values for this field are specified in Table 3.5.5.2.1.1-1.

Table 3.5.5.2.1.1-1 Cellular System A/B Selection Type Values

System A/B Selection Type	Value
System A	‘00’
System B	‘01’
Reserved	‘10’
System A or B	‘11’

3.5.5.2.1.2 Cellular CDMA and JTACS CDMA System Acquisition (Standard Channels) Record

This acquisition record type is for use in acquiring a cellular CDMA and JTACS CDMA system on the primary or secondary CDMA channels, and has the following fixed length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘0010’)	4
A_B	2
PRI_SEC	2

ACQ_TYPE - Acquisition record type.
This field is set to ‘0010’ (see Table 3.5.5.2-1).

A_B - System A/B selection type.
The values for this field are specified in Table 3.5.5.2.1.1-1.

PRI_SEC - Standard CDMA Channel selection type.
The values for this field are specified in Table 3.5.5.2.1.2-1.

Table 3.5.5.2.1.2-1 Cellular CDMA and JTACS CDMA Standard Channel Selection Type Values

Standard Channel Selection Type	Value
Reserved	‘00’
Primary CDMA Channel	‘01’
Secondary CDMA Channel	‘10’
Primary or Secondary CDMA Channel	‘11’

3.5.5.2.1.3 Cellular CDMA and JTACS CDMA System Acquisition (Custom Channels) Record

This acquisition record type is for use in acquiring a cellular CDMA and JTACS CDMA system using a list of CDMA channels, and has the following variable length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘0011’)	4
NUM_CHANS	5
NUM_CHANS occurrences of the following field:	
CHAN	11

ACQ_TYPE - Acquisition record type.

This field is set to ‘0011’ (see Table 3.5.5.2-1).

NUM_CHANS - Number of CDMA channels.

This field is set to the number of cellular CDMA and JTACS CDMA channels included in this record.

CHAN - Cellular CDMA and JTACS CDMA channel.

This field specifies a cellular CDMA and JTACS CDMA channel number (see 6.1.1.1 of [1] or 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

3.5.5.2.1.4 Cellular CDMA Preferred System Acquisition Record

This acquisition record type is for use in acquiring a cellular system (CDMA first, then Analog), and has the following fixed length format:

Acquisition Record Field	**Length (bits)**
ACQ_TYPE (‘0100’)	4
A_B	2

ACQ_TYPE - Acquisition record type.

This field is set to ‘0100’ (see Table 3.5.5.2-1).

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

3.5.5.2.1.5 PCS CDMA System Acquisition (Using Blocks) Record

This acquisition record type is for use in acquiring a PCS CDMA system using a list of CDMA frequency blocks, and has the following variable length format:

Acquisition Record Field	**Length (bits)**
ACQ_TYPE (‘0101’)	4
NUM_BLOCKS	3
NUM_BLOCKS occurrences of the following field:	
BLOCK	3

ACQ_TYPE - Acquisition record type.

This field is set to ‘0101’ (see Table 3.5.5.2-1).

NUM_BLOCKS - Number of frequency blocks.

This field is set to the number of PCS frequency blocks included in this record.

BLOCK - PCS frequency block.

The values for this field are specified in Table 3.5.5.2.1.5-1. The BLOCK fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

Table 3.5.5.2.1.5-1 PCS CDMA Frequency Blocks

PCS CDMA Frequency Block	Value
Block A	'000'
Block B	'001'
Block C	'010'
Block D	'011'
Block E	'100'
Block F	'101'
Reserved	'110'
Any Block	'111'

3.5.5.2.1.6 PCS CDMA and 2 GHz Band CDMA System Acquisition (Using Channels) Record

This acquisition record type is for use in acquiring a PCS CDMA and a 2 GHz Band CDMA system using a list of CDMA channels, and has the following variable length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE ('0110')	4
NUM_CHANS	5
NUM_CHANS occurrences of the following field:	
CHAN	11

ACQ_TYPE - Acquisition record type.

This field is set to '0110' (see Table 3.5.5.2-1).

NUM_CHANS - Number of CDMA channels.

This field is set to the number of PCS CDMA and 2 GHz band CDMA channels included in this record.

CHAN - PCS CDMA channel.

This field specifies a PCS CDMA and a 2 GHz Band CDMA channel number (see 6.1.1.1 of [1] or 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

3.5.5.2.1.7 JTACS CDMA System Acquisition (Standard Channels) Record

This acquisition record type is for use in acquiring a JTACS CDMA system on the primary or secondary CDMA channels, and has the following fixed length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘0111’)	4
A_B	2
PRI_SEC	2

ACQ_TYPE - Acquisition record type.

This field is set to ‘0111’ (see Table 3.5.5.2-1).

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

PRI_SEC - Standard CDMA Channel selection type.

The values for this field are specified in Table 3.5.5.2.1.7-1.

Table 3.5.5.2.1.7-1 JTACS CDMA Standard Channel Selection Type Values

Standard Channel Selection Type	Value
Reserved	‘00’
Primary CDMA Channel	‘01’
Secondary CDMA Channel	‘10’
Primary or Secondary CDMA Channel	‘11’

3.5.5.2.1.8 JTACS CDMA System Acquisition (Custom Channels) Record

This acquisition record type is for use in acquiring a JTACS CDMA system using a list of custom CDMA channels, and has the following variable length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘1000’)	4
NUM_CHANS	5

NUM_CHANS occurrences of the following field:

CHAN	11

ACQ_TYPE - Acquisition record type.

This field is set to ‘1000’ (see Table 3.5.5.2-1).

NUM_CHANS - Number of CDMA channels.

This field is set to the number of JTACS CDMA channels included in this record.

CHAN - JTACS CDMA channel.

This field specifies a JTACS CDMA channel number (2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

3.5.5.2.1.9 2 GHz Band CDMA System Acquisition (Using Channels) Record

This acquisition record type is for use in acquiring a 2 GHz Band CDMA system using a list of CDMA channels, and has the following variable length format:

Acquisition Record Field	Length (bits)
ACQ_TYPE (‘1001’)	4
NUM_CHANS	5

NUM_CHANS occurrences of the following field:

CHAN	11

ACQ_TYPE - Acquisition record type.

This field is set to ‘1001’ (see Table 3.5.5.2-1).

NUM_CHANS - Number of CDMA channels.

This field is set to the number of 2 GHz Band CDMA channels included in this record.

CHAN - 2 GHz Band CDMA channel.

This field specifies a PCS CDMA channel number (see 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

3.5.5.2.2 Extended Acquisition Record Format

The format of the Extended Acquisition Record is as follows:

Type-specific Record	Length (bits)
ACQ_TYPE	8
LENGTH	8
Type-specific	8 × LENGTH

ACQ_TYPE - Acquisition record type.

This field is set to the Extended Acquisition Record type (see Table 3.5.5.2-2) and identifies the type-specific fields.

LENGTH - Length of the Type-specific fields.

This field is set to the length of the Type-specific record in octets.

The contents of the type-specific fields determined by the ACQ_TYPE field and are specified as follows.

3.5.5.2.2.1 Cellular Analog System Acquisition Record

If the ACQ_TYPE field is set to ‘00000001’, the type-specific record specifies the acquisition record for use in acquiring a cellular analog system. The type-specific record has the following fixed-length format:

Type-specific Record	Length (bits)
A_B	2
RESERVED	6

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

RESERVED - The value of this field shall be set to zero.

3.5.5.2.2.2 Cellular CDMA System Acquisition (Standard Channels) Record

If the ACQ_TYPE field is set to ‘00000010’, the type-specific record specifies the acquisition record for use in acquiring a cellular CDMA system on the primary or secondary CDMA channels. The type-specific record has the following fixed-length format:

Type-specific Record	Length (bits)
A_B	2
PRI_SEC	2
RESERVED	4

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

PRI_SEC - Standard CDMA Channel selection type.

The values for this field are specified in Table 3.5.5.2.1.2-1.

RESERVED - The value of this field shall be set to zero.

3.5.5.2.2.3 Cellular CDMA System Acquisition (Custom Channels) Record

If the ACQ_TYPE field is set to '00000011', the type-specific record specifies the acquisition record for use in acquiring a cellular CDMA system using a list of CDMA channels. The type-specific record has the following variable-length format:

Type-specific Record	Length (bits)
NUM_CHANS	5
NUM_CHANS occurrences of the following field:	
CHAN	11
RESERVED	As required

NUM_CHANS - Number of CDMA channels.

This field is set to the number of cellular CDMA channels included in this record.

CHAN - Cellular CDMA channel.

This field specifies a cellular CDMA channel number (see 6.1.1.1 of [1] or 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

RESERVED - The length of this field shall be the smallest number of bits that is required to make the total length of the Type-specific record and integer multiple of octets. The value of this field shall be set to zero.

3.5.5.2.2.4 Cellular CDMA Preferred System Acquisition Record

If the ACQ_TYPE field is set to '00000100', the type-specific record specifies the acquisition record for use in acquiring a cellular system (CDMA first, then Analog). The type-specific record has the following fixed-length format:

Type-specific Record	Length (bits)
A_B	2
RESERVED	6

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

RESERVED - The value of this field shall be set to zero.

3.5.5.2.2.5 PCS CDMA System Acquisition (Using Blocks) Record

If the ACQ_TYPE field is set to '00000101', the type-specific record specifies the acquisition record for use in acquiring a PCS CDMA system using a list of CDMA frequency blocks. The type-specific record has the following variable-length format:

Type-specific Record	Length (bits)
NUM_BLOCKS	3
NUM_BLOCKS occurrences of the following field:	
BLOCK	3
RESERVED	As required

NUM_BLOCKS - Number of frequency blocks.

This field is set to the number of PCS frequency blocks included in this record.

BLOCK - PCS frequency block.

The values for this field are specified in Table 3.5.5.2.1.5-1. The BLOCK fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

RESERVED - The length of this field shall be the smallest number of bits that is required to make the total length of the Type-specific record and integer multiple of octets. The value of this field shall be set to zero.

3.5.5.2.2.6 PCS CDMA System Acquisition (Using Channels) Record

If the ACQ_TYPE field is set to ‘00000110’, the type-specific record specifies the acquisition record for use in acquiring a PCS CDMA system using a list of CDMA channels. The type-specific record has the following variable-length format:

Type-specific Record	Length (bits)
NUM_CHANS	5
NUM_CHANS occurrences of the following field:	
CHAN	11
RESERVED	As required

NUM_CHANS - Number of CDMA channels.

This field is set to the number of PCS CDMA channels included in this record.

CHAN - PCS CDMA channel.

This field specifies a PCS CDMA channel number (see 6.1.1.1 of [1] or 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

RESERVED - The length of this field shall be the smallest number of bits that is required to make the total length of the Type-specific record and integer multiple of octets. The value of this field shall be set to zero.

3.5.5.2.2.7 JTACS CDMA System Acquisition (Standard Channels) Record

If the ACQ_TYPE field is set to ‘00000111’, the type-specific record specifies the acquisition record for use in acquiring a JTACS CDMA system on the primary or secondary CDMA channels. The type-specific record has the following fixed-length format:

Type-specific Record	Length (bits)
A_B	2
PRI_SEC	2
RESERVED	4

A_B - System A/B selection type.

The values for this field are specified in Table 3.5.5.2.1.1-1.

PRI_SEC - Standard CDMA Channel selection type.

The values for this field are specified in Table 3.5.5.2.1.7-1.

RESERVED - The value of this field shall be set to zero.

3.5.5.2.2.8 JTACS CDMA System Acquisition (Custom Channels) Record

If the ACQ_TYPE field is set to '00001000', the type-specific record specifies the acquisition record for use in acquiring a JTACS CDMA system using a list of custom CDMA channels. The type-specific record has the following variable-length format:

Type-specific Record	**Length (bits)**
NUM_CHANS	5
NUM_CHANS occurrences of the following field:	
CHAN	11
RESERVED	As required

NUM_CHANS - Number of CDMA channels.

This field is set to the number of JTACS CDMA channels included in this record.

CHAN - JTACS CDMA channel.

This field specifies a JTACS CDMA channel number (2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

RESERVED - The length of this field shall be the smallest number of bits that is required to make the total length of the Type-specific record and integer multiple of octets. The value of this field shall be set to zero.

3.5.5.2.2.9 2 GHz Band CDMA System Acquisition (Using Channels) Record

If the ACQ_TYPE field is set to '00001001', the type-specific record specifies the acquisition record for use in acquiring a 2 GHz Band CDMA system using a list of CDMA channels. The type-specific record has the following variable-length format:

This acquisition record type is for use in acquiring, and has the following variable length format:

Type-specific Record	**Length (bits)**
NUM_CHANS	5

NUM_CHANS occurrences of the following field:	
CHAN	11

RESERVED	As required

NUM_CHANS - Number of CDMA channels.

This field is set to the number of 2 GHz Band CDMA channels included in this record.

CHAN - 2 GHz Band CDMA channel.

This field specifies a PCS CDMA channel number (see 2.1.1.1 of [5]). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

RESERVED - The length of this field shall be the smallest number of bits that is required to make the total length of the Type-specific record and integer multiple of octets. The value of this field shall be set to zero.

3.5.5.2.2.10 Generic Acquisition Record for IS-2000 and IS-95

If the ACQ_TYPE field is set to '00001010', the type-specific record specifies the acquisition record for use in acquiring IS-2000 and IS-95 systems using band-class and channel number. The type-specific record has the following variable-length format:

This acquisition record type is for use in acquiring, and has the following variable length format:

Type-specific Record	**Length (bits)**
LENGTH/2 occurrences of the following two fields:	
BAND_CLASS	5
CHANNEL_NUMBER	11

BAND_CLASS - This field is set to the Band Class number corresponding to the frequency assignment of the channel specified by this record.

CHANNEL_NUMBER - This field is set to the channel number corresponding to the Band Class specified by this record.

3.5.5.2.2.11 Generic Acquisition Record for HRPD

If the ACQ_TYPE field is set to '00001011', the type-specific record specifies the acquisition record for use in acquiring HRPD systems using band-class and channel number. The type-specific record has the following variable-length format:

This acquisition record type is for use in acquiring, and has the following variable length format:

Type-specific Record	Length (bits)
LENGTH/2 occurrences of the following two fields:	
BAND_CLASS	5
CHANNEL_NUMBER	11

BAND_CLASS - This field is set to the Band Class number corresponding to the frequency assignment of the channel specified by this record.

CHANNEL_NUMBER - This field is set to the channel number corresponding to the Band Class specified by this record.

3.5.5.3 System Record and Extended System Record Format

A system record contains parameters that the mobile station can use for identifying an acquired system, for determining whether an acquired system is the optimal system on which to operate and for determining the mobile station's roaming status.

Two categories of system records are defined: System Records and Extended System Records. A System Record defined in section 3.5.5.3.1 shall be included only in a Preferred Roaming List associated with the SSPR_P_REV equal to '00000001'. An Extended System Record defined in section 3.5.5.3.2 shall be included only in an Extended Preferred Roaming List associated with the SSPR_P_REV equal to or greater than '00000011'.

3.5.5.3.1 System Record Format

Each System Record has the following variable length format:

System Record Field	Length (bits)
SID	15
NID_INCL	2
NID	0 or 16
PREF_NEG	1
GEO	1
PRI	0 or 1
ACQ_INDEX	9
ROAM_IND	0 or 8

SID - System identification.

This field is set to the SID of the system associated with this record.

The value ‘000000000000000’ denotes a system with any SID (i.e., serves as a SID wildcard) not specifically included elsewhere in SYS_TABLE, provided that the system is found on a channel or in a block specified in the acquisition record corresponding to ACQ_INDEX. Any other value of this field denotes a system with that specific SID found on any channel.

NID_INCL - NID included.

This field is set to the value defined in Table 3.5.5.3-1.

Table 3.5.5.3-1 NID_INCL Values

NID_INCL Value	Parameter Description
‘00’	NID not included. Assume NID value ‘1111111111111111’
‘01’	NID included
‘10’	NID not included. Assume NID value ‘0000000000000000’
‘11’	Reserved

NID - Network identification.

If the NID_INCL field of this record is equal to ‘01’, this field is included and is set to the NID of the network associated with this record; otherwise, this field is omitted.

The value ‘1111111111111111’ denotes any NID (i.e., serves as a NID wildcard). Not including the NID field is equivalent to including it and setting it to ‘1111111111111111’.

The value ‘0000000000000000’ denotes a NID of the public system (see 6.6.5.2 of [1] or 2.6.5.2 of [7])

PREF_NEG - Preferred/negative system.

This field is set to ‘1’ if the mobile station is allowed to operate on the system associated with this record. This field is set to ‘0’ if the mobile station is not allowed to operate on the system associated with this record.

GEO - Geographical region indicator.

If this is the first system record, this field is set to ‘0’.

If this is not the first system record, then this field is set as follows: If the system associated with this record is in the same geographical region as the system associated with the previous system record, this field is set to ‘1’; otherwise, this field is set to ‘0’.

PRI - Relative priority indicator.

If the PREF_NEG field of this system record is equal to ‘0’, this field is omitted; otherwise this field is included and is set as follows:

If this is the last system record in the specific geographical region, or if the PREF_NEG field in the next system record is equal to’0’, this field is set to ‘0’ and has no meaning.

If the system associated with this system record is more desirable than the system associated with the next system record, this field is set to ‘1’.

If the system associated with this system record is as desirable as the system associated with the next system record, this field is set to ‘0’.

ACQ_INDEX - Acquisition record index.

This field is set to the index of the acquisition record that specifies the acquisition parameters for the system associated with this record.

Note: The index of the n^{th} acquisition record is n-1. For example, the index of the first acquisition record in ACQ_TABLE is 0, and the index for the fourth acquisition record is 3.

ROAM_IND - If the PREF_NEG field of this record is equal to ‘1’, this field is included and is set to the roaming indication value (see [4]) for the system associated with this record; otherwise, this field is omitted.

3.5.5.3.2 Extended System Record Format

Each Extended System Record has the following variable length format:

System Record Field	Length (bits)
SYS_RECORD_LENGTH	5
SYS_RECORD_TYPE	4
SYS_RECORD_TYPE specific fields	variable

SYS_RECORD_LENGTH - Extended System Record Length.

This field is set to the length of the Extended System Record in octets.

SYS_RECORD_TYPE - Extended System Record Type.

The value of this field specifies the format of the rest of this record.

The following table specifies the format of the Extended System Record for the values of the SYS_RECORD_TYPE specified in Table 3.5.5.3.2-1. All other values for the SYS_RECORD_TYPE are reserved.

System Record Field	Length (bits)
SYS_RECORD_LENGTH	5
SYS_RECORD_TYPE	4
PREF_NEG	1
GEO	1
PRI	1
ACQ_INDEX	9
Type-specific system ID record	variable
ROAM_IND	0 or 8
ASSOCIATION_INC	1
ASSOCIATION_TAG	0 or 8
PN_ASSOCIATION	0 or 1
DATA_ASSOCIATION	0 or 1
RESERVED	As required

SYS_RECORD_LENGTH - Extended System Record Length.

This field is set to the length of the Extended System Record in octets.

SYS_RECORD_TYPE - Extended System Record Type.

This field is set to the type of this Extended System Record (see Table 3.5.5.3.2-1).

Table 3.5.5.3.2-1 Type-specific system ID record

SYS_RECORD_TYPE	Parameter Description
‘0000’	IS-2000 and IS-95 Systems
‘0001’	HRPD System

PREF_NEG - Preferred/negative system.

This field is set to ‘1’ if the mobile station is allowed to operate on the system associated with this record. This field is set to ‘0’ if the mobile station is not allowed to operate on the system associated with this record.

GEO - Geographical region indicator.

If this is the first system record, this field is set to ‘0’.

If this is not the first system record, then this field is set as follows: If the system associated with this record is in the same geographical region as the system associated with the previous system record, this field is set to ‘1’; otherwise, this field is set to ‘0’.

PRI - Relative priority indicator.

This field is set as follows:

If this is the last system record in the specific geographical region, or if the PREF_NEG field in the next system record is equal to‘0’, this field is set to ‘0’ and has no meaning.

If the system associated with this system record is more desirable than the system associated with the next system record, this field is set to ‘1’.

If the system associated with this system record is as desirable as the system associated with the next system record, this field is set to ‘0’.

ACQ_INDEX - Acquisition record index.

This field is set to the index of the acquisition record that specifies the acquisition parameters for the system associated with this record.

Note: The index of the n^{th} acquisition record is n-1. For example, the index of the first acquisition record in ACQ_TABLE is 0, and the index for the fourth acquisition record is 3.

RESERVED - This field shall be set to zero.

The type-specific system ID record is set according to the value of the SYS_RECORD_TYPE field as follows:

If the SYS_RECORD_TYPE is set to ‘0000’, the type-specific system ID is as specified in Table 3.5.5.3.2-2:

Table 3.5.5.3.2-2 Type-specific system ID record

System ID Record Field	Length (bits)
RESERVED	1
NID_INCL	2
SID	15
NID	0 or 16

RESERVED - This field shall be set to zero.

NID_INCL - NID included.

This field is set to the value defined in Table 3.5.5.3.2-3.

Table 3.5.5.3.2-3 NID_INCL Values

NID_INCL Value	Parameter Description
‘00’	NID not included. Assume NID value ‘1111111111111111’
‘01’	NID included
‘10’	NID not included. Assume NID value ‘0000000000000000’
‘11’	Reserved

SID - System identification.

This field is set to the SID of the system associated with this record.

The value ‘000000000000000’ denotes a system with any SID (i.e., serves as a SID wildcard) not specifically included elsewhere in SYS_TABLE, provided that the system is found on a channel or in a block specified in the acquisition record corresponding to ACQ_INDEX. Any other value of this field denotes a system with that specific SID found on any channel.

NID - Network identification.

If the NID_INCL field of this record is equal to ‘01’, this field is included and is set to the NID of the network associated with this record; otherwise, this field is omitted.

The value ‘1111111111111111’ denotes any NID (i.e., serves as a NID wildcard). Not including the NID field is equivalent to including it and setting it to ‘1111111111111111’.

The value ‘0000000000000000’ denotes a NID of the public system (see 6.6.5.2 of [1])

If the SYS_RECORD_TYPE is set to ‘0001’, the type-specific system ID is as specified in Table 3.5.5.3.2-4:

Table 3.5.5.3.2-4 Type-specific System ID Record

System ID Record Field	Length (bits)
RESERVED	3
SUBNET_COMMON_INCLUDED	1
SUBNET_LSB_LENGTH	7
SUBNET_LSB	SUBNET_LSB_LENGTH
SUBNET_COMMON_OFFSET	0 or 12

RESERVED - This field shall be set to zero.

SUBNET_COMMON_INCLUDED

- Common part of the HRPD subnet included indicator.

This field is set to ‘1’ if the SUBNET_COMMON_OFFSET field is included. Otherwise this field is set to ‘0’.

SUBNET_LSB_LENGTH - This field is set to the length of the least significant bits of the HRPD subnet. If SUBNET_COMMON_INCLUDED is set to ‘0’, this field is set to the length of the HRPD subnet associated with this system record.

SUBNET_LSB - This field is set to the least significant bits of the HRPD subnet of length specified by SUBNET_LSB_LENGTH. If SUBNET_COMMON_INCLUDED is set to ‘0’, this field is set to the entire HRPD subnet associated with this system record.

SUBNET_COMMON_OFFSET

- Common part of the HRPD subnet.

If included, this field is set to the offset into the Common Subnet Table (see Table 3.5.5.3.2.1-1), in octets, that specifies the most significant bits of the subnet associated with this system record (e.g., a value of zero for this field points to the beginning of the Common Subnet Table).

ROAM_IND - If the PREF_NEG field of this record is equal to ‘1’, this field is included and is set to the roaming indication value (see TSB58) for the system associated with this record; otherwise, this field is omitted.

ASSOCIATION_INC - Association tag included flag.

This field is set to ‘1’ if the next three fields are included. Otherwise, this field is set to ‘0’.

ASSOCIATION_TAG - If included, this field is set to the 8-bit number that specifies the set to which this system record belongs. The value of the ASSOCIATION_TAG field is only unique within a GEO. The set is defined as a set of systems (specified by the system records) for which at least one the following two conditions hold:

- The members of the set have the same PN offset assignment (i.e., collocated), or
- The members of the set can reach the same set of PDSNs (i.e., associated).

PN_ASSOCIATION - PN association flag.

This field is only included if the ASSOCIATION_INC field is set to ‘1’. If included, this field shall be set to ‘1’ if the system identified by this system record has the same PN assignment as other systems in the same GEO that are members of the set identified by ASSOCIATION_TAG and whose PN_ASSOCIATION field is also set to ‘1’. Otherwise, this field shall be set to ‘0’.

DATA_ASSOCIATION - Data association flag.

This field is only included if the ASSOCIATION_INC field is set to ‘1’. If included, this field shall be set to ‘1’ if the system identified by this system record can reach the same set of PDSNs as other systems in the same GEO that are members of the set identified by ASSOCIATION_TAG and whose DATA_ASSOCIATION field is also set to ‘1’. Otherwise, this field shall be set to ‘0’. [4]

RESERVED - The size of this field is such that the total length of this Extended System Record (including the RESERVED field) is an integer number of octets. This field is set to all zeros.

---

[4] The mobile station may use the value of this field to limit the set of systems in the GEO that it should attempt to acquire. For example, the mobile station may choose to only acquire systems that can reach the same set of PDSNs (in order to avoid establishing two separate PPP session).

3.5.5.3.2.1 Common Subnet Table for the HRPD Extended System Record

The Common Subnet Table for the HRPD Extended System Record consists of records with the following format:

Table 3.5.5.3.2.1-1 Common Subnet Record

System ID Record Field	Length (bits)
RESERVED	4
SUBNET_COMMON_LENGTH	4
SUBNET_COMMON	8 × SUBNET_COMMON_LENGTH

SUBNET_COMMON_LENGTH

- Length of the common part of the HRPD subnet.

This field is set to the length of the most significant bits of the HRPD subnet which is included in this record.

SUBNET_COMMON - Common part of the HRPD subnet.

This field is set to the most significant bits of the HRPD subnet which is included in this record.

RESERVED - The size of this field is such that the total length of this record (including the RESERVED field) is an integer number of octets. This field is set to all zeros.

3.5.6 PUZL Parameter Blocks

Table 3.5.6-1 lists the types of parameter blocks used in the *PUZL Configuration Request Message* and the *PUZL Configuration Response Message*.

Table 3.5.6-1. PUZL Parameter Block Types

PUZL Parameter Block Type	BLOCK_ID	Reference
PUZL Dimensions	‘00000000’	3.5.6.1
PUZL Priorities	‘00000001’	3.5.6.2
User Zone	‘00000010’	3.5.6.3
Preferred User Zone List	‘00000011’	3.5.6.4
Reserved for future standardization	‘00000100’ through ‘01111111	
Available for manufacturer-specific parameter block definitions	‘10000000’ through ‘11111110’	See [4]
Reserved	‘11111111’	

3.5.6.1 PUZL Dimensions Parameter Block

The PARAM_DATA field of the PUZL Dimensions Parameter Block consists of the following fields:

Field	Length (bits)
MAX_UZ_LIST_SIZE	24
CUR_UZ_LIST_SIZE	24
MAX_UZ	12
CUR_UZ	12
UZ_ORIG_ONLY	1
UZ_TEMP_SUBSC	1
UZ_CIRCLE_FLAG	1
UZ_POLYGON_FLAG	1
UZ_LINEAR_FLAG	1
RESERVED	3

MAX_UZ_LIST_SIZE - Maximum preferred user zone list size.

The mobile station shall set this field to the maximum size, in octets, that the mobile station can support for the preferred user zone list ($PUZL_{s-p}$).

CUR_UZ_LIST_SIZE - Current preferred user zone list size.

The mobile station shall set this field to the size, in octets, of the current preferred user zone list.

MAX_UZ - Maximum number of User Zone entries.

The mobile station shall set this field to the maximum number of user zone entries that the mobile station can support.

CUR_UZ - Current number of User Zone entries.

The mobile station shall set this field to the number of user zone entries currently stored in the preferred user zone list in the mobile station.

UZ_ORIG_ONLY - User Zone Origination Only Flag.

The mobile station shall set this field corresponding to its current setting to indicate whether or not the mobile station is permitted to originate calls only when within the serving area of a currently assigned User Zone. If call origination is only allowed within an assigned user zone, UZ_ORIG_ONLY = ‘1’; otherwise, UZ_ORIG_ONLY = ‘0’.

UZ_TEMP_SUBSC - User Zone Temporary Subscription Flag.

The mobile station shall set this field corresponding to its current setting to indicate whether or not it is permitted to access User Zones that offer temporary subscription. If allowed, UZ_TEMP_SUBSC = ‘1’; otherwise, UZ_TEMP_SUBSC = ‘0’.

UZ_CIRCLE_FLAG - User Zone Circle Flag.

The mobile station shall set this field corresponding to its capability to support the Circle User Zone Type. If supported, UZ_CIRCLE_FLAG = ‘1’; otherwise, UZ_CIRCLE_FLAG = ‘0’.

UZ_POLYGON_FLAG - User Zone Polygon Flag.

The mobile station shall set this field corresponding to its capability to support the Polygon User Zone Type. If supported, UZ_POLYGON_FLAG = ‘1’; otherwise, UZ_POLYGON_FLAG = ‘0’.

UZ_LINEAR_FLAG - User Zone Segmented Linear Flag.

The mobile station shall set this field corresponding to its capability to support the Segmented Linear User Zone Type. If supported, UZ_LINEAR_FLAG = ‘1’; otherwise, UZ_LINEAR_FLAG = ‘0’.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘000’.

3.5.6.2 PUZL Priorities Parameter Block

The PARAM_DATA field of the PUZL Priorities Parameter Block consists of the following fields:

Field	Length (bits)
LAST_SEGMENT	1
SEGMENT_INDEX	12
NUM_ENTRIES	8
NUM_ENTRIES occurrences of the following parameters:	
UZ_ID	16
UZ_SID	15
UZ_PRIORITY	4
The parameter block ends with the following field:	
RESERVED	0 to 7

LAST_SEGMENT - Last segment indicator bit.

The mobile station shall set this field to '1' if this parameter block contains the user zone ID, SID and priority information for the last entry of the current preferred user zone list ($PUZL_{s-p}$); otherwise, the mobile station shall set this field to '0'.

SEGMENT_INDEX - Segment index.

The mobile station shall set this field to the value of REQUEST_INDEX from the corresponding *PUZL Configuration Request Message*.

NUM_ENTRIES - Number of entries.

The mobile station shall set this field to the number of user zone entries included in the parameter block.

If REQUEST_INDEX from the corresponding *PUZL Configuration Request Message* specifies an index that is invalid for the current preferred user zone list, the mobile station shall set this field to zero. No UZ_ID, UZ_SID and UZ_PRIORITY fields shall be included.

If REQUEST_INDEX from the corresponding *PUZL Configuration Request Message* specifies an index that is valid for the current preferred user zone list, the mobile station shall include the UZ_ID, UZ_SID and UZ_PRIORITY values from at most REQUEST_MAX_ENTRIES user zone entries from the current preferred user zone list.

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

UZ_PRIORITY - User Zone priority.

The priority by which User Zones are selected by the mobile station when more than one User Zone is present. A priority of null indicates that a User Zone is for manual selection only. A mobile station will never automatically select a User Zone of priority ‘null’ unless initiated manually by the user. Note that the value of User Zone Priority is non-exclusive. Normally two User Zones of the same priority would not occupy the same geographical area. When two User Zones of the same priority overlap and they are the highest priority to be selected, the mobile station shall offer the user a choice of the user zones via the Mobile Station's user interface.

RESERVED - Reserved bits.

The mobile station shall add reserved bits in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.6.3 User Zone Parameter Block

The PARAM_DATA field of the User Zone Parameter Block consists of the following fields:

Field	Length (bits)
UZ_ID	16
UZ_SID	15
LAST_SEGMENT	1
SEGMENT_OFFSET	12
RESERVED	4
SEGMENT_SIZE	8
SEGMENT_DATA	8 × SEGMENT_SIZE

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID	-	User Zone System ID. The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.
LAST_SEGMENT	-	Last segment indicator bit. The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the user zone entry; otherwise, the mobile station shall set this field to ‘0’.
SEGMENT_OFFSET	-	Segment offset. The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *PUZL Configuration Request Message*.
RESERVED	-	Reserved bits. The mobile station shall set this field to ‘0000’.
SEGMENT_SIZE	-	Segment size. The base station shall set this field to the number of octets of the user zone entry included in SEGMENT_DATA.
SEGMENT_DATA	-	Segment of the specified user zone entry of the PUZL. Refer to Section 3.5.7. If REQUEST_OFFSET from the corresponding *PUZL Configuration Request Message* specifies an offset that is invalid for the user zone entry of the current preferred user zone list, the mobile station shall include no octets in this field. If REQUEST_OFFSET specifies an offset that is valid for the specified user zone entry of the preferred user zone list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the user zone entry from the preferred user zone list in this field. The octets shall be equal to the octets starting at the offset within the user zone entry of the preferred user zone list specified by SEGMENT_OFFSET.

3.5.6.4 Preferred User Zone List Parameter Block

The PARAM_DATA field of the Preferred User Zone List Parameter Block consists of the following fields:

Field	Length (bits)
NUM_ENTRIES	8
NUM_ENTRIES occurrences of the following:	
RESERVED	7
LAST_SEGMENT	1
SEGMENT_INDEX	12
SEGMENT_OFFSET	12
SEGMENT_SIZE	8
SEGMENT_DATA	8 × SEGMENT_SIZE

NUM_ENTRIES -	Number of entries. The mobile station shall set this field to the number of user zone entries included in the parameter block.
RESERVED -	Reserved bits. The mobile station shall set this field to ‘0000000’.
LAST_SEGMENT -	Last segment indicator bit. The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the user zone entry; otherwise, the mobile station shall set this field to ‘0’.
SEGMENT_INDEX -	Segment index. The mobile station shall set this field to the index value of the user zone entry in the PUZL.
SEGMENT_OFFSET -	Segment offset. The mobile station shall set this field to the value of offset, in octets, from the beginning of the user zone entry in the PUZL.
SEGMENT_SIZE -	Segment size. The mobile station shall set this field to the number of octets of the user zone entry included in SEGMENT_DATA.
SEGMENT_DATA -	Segment of the PUZL data for Preferred User Zone List Parameter Block. Refer to Section 3.5.7 for more details. If REQUEST_OFFSET from the corresponding *PUZL Configuration Request Message* specifies an offset that is invalid for the current user zone entry of the preferred user zone list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the specified user zone entry of the preferred user zone list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the user zone entry from the preferred user zone list in this field. The octets shall be equal to the octets starting at the offset within the user zone entry of the preferred user zone list specified by SEGMENT_OFFSET.

3.5.7 Preferred User Zone List (PUZL)

The Preferred User Zone List provides the mobile station with the priority and characteristics of the User Zones to which the mobile station is subscribed. The PUZL is used after the mobile station has completed system acquisition using the PRL or other techniques. Once a mobile station has found its preferred system, the PUZL is used to select the most preferred User Zone on that system. It should be noted that PUZL could have up to 4095 User Zone entries. A User Zone entry includes all of the information associated with the definition of a single user zone that is uniquely identified by the combination of User Zone ID and User Zone SID.

The following sections define the parameters that are stored in the PUZL:

Field	Length (bits)
RESERVED	2
UZ_TEMP_SUBSC	1
UZ_ORIG_ONLY	1
NUM_UZ_ENTRIES	12
NUM_UZ_ENTRIES occurrences of the following User Zone entry:	
UZ_PRIORITY	4
UZ_ID	16
UZ_SID	15
UZ_NAME_ENCODING	8
N_OCTETS	5
UZ_NAME	8 × N_OCTETS
ACTIVE_FLAG	1
PRIORITY_CONTROL	3
NOTIFICATION_FLAG	1
UZ_REVISION	4
UZ_TYPE	3
NUM_ELEMENTS	4
NUM_ELEMENTS occurrences of the following:	
UZ Type Specific Fields	Variable
The User Zone entry ends with the following field:	
RESERVED	0 to 7

RESERVED - Reserved bits.

The mobile station shall set this field to ‘00’.

UZ_TEMP_SUBSC - User Zone Temporary Subscription Flag.

This flag indicates whether or not the mobile station is permitted to access User Zones that offer temporary subscription. This field does not apply to a specific User Zone and is per MS. If allowed, UZ_TEMP_SUBSC = ‘1’; otherwise, UZ_TEMP_SUBSC = ‘0’.

UZ_ORIG_ONLY - User Zone Origination Only Flag.

This flag indicates whether or not the mobile station is permitted to originate calls only when within the serving area of a currently assigned User Zone. If call origination is only allowed within an assigned user zone, UZ_ORIG_ONLY = '1'; otherwise, UZ_ORIG_ONLY = '0'.

NUM_UZ_ENTRIES - Current number of User Zone entries.

Number of User Zone entries currently in the mobile's PUZL.

UZ_PRIORITY - User Zone priority.

The priority by which User Zones are selected by the mobile station when more than one User Zone is present. A priority of null indicates that a User Zone is for manual selection only. A mobile station will never automatically select a User Zone of priority 'null' unless initiated manually by the user. Note that the value of User Zone Priority is non-exclusive. Normally two User Zones of the same priority would not occupy the same geographical area. When two User Zones of the same priority overlap and they are the highest priority to be selected, the mobile station shall offer the user a choice of the user zones via the Mobile Station's user interface.

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

UZ_NAME_ENCODING - User Zone name encoding.

A field indicating the character set the User Zone Name is encoded in as per ANSI-41 (TSB-58).

N_OCTETS - Number of octets.

Number of octets in the User Zone name.

UZ_NAME - User Zone name.

Up to 12-character field used in the mobile station to indicate to the mobile station the Name of the User Zone the mobile station is currently subscribed to. Encoded as per the previous field.

ACTIVE_FLAG - Active flag.

With this flag set to '1', the mobile station must register upon entering or exiting this particular User Zone. If allowed, ACTIVE_FLAG = '1'; otherwise, ACTIVE_FLAG = '0'.

PRIORITY_CONTROL - Priority Control.

A 3 bit field that controls the ability of the user to modify PUZL priorities using the user interface of the mobile. The following states are defined at this time:

State	Value	Description
No changes permitted	'000'	The user may not modify or override the PUZL priorities in any way.
Manual	'001'	Permitted to select manually amongst the User Zones present. Upon exiting the User Zone the Mobile will revert back to the PUZL priorities.
Manual and Temporary	'010'	The user is also permitted to change the priorities of the PUZL for this User Zone. The change will remain in effect until the next power down.
Reserved	'011' through '111'	

NOTIFICATION_FLAG - Notification flag.

When this flag is set to '1' and a mobile station moves within the coverage area of a User Zone, this flag can be used to indicate to the user that the User Zone is present. This flag would typically be used for User Zones that are set for manual selection only (User Zone Priority = null) but that the subscriber wishes to be informed of its presence.

UZ_REVISION - User Zone revision.

This indicates the current revision of this entry in the PUZL. For Broadcast User Zones, the mobile station uses this value to determine if the network has more current information about the particular User Zone.

UZ_TYPE - User Zone type.

This field is used to distinguish between the following types of User Zones:

Table 3.5.7-1 User Zone Type Values

User Zone Type	Value
Broadcast – RF Coverage Based	‘000’
Broadcast – Geo-Based	‘001’
Mobile Specific – RF Coverage Based - Overhead Parameter Determined	‘010’
Mobile Specific – Geo-Based	‘011’
Mobile Specific - Geo Based - Separate Carrier	‘100’
Reserved	‘101’ through ‘111’

NUM_ELEMENTS - Number of elements.

This is the number of User Zone type specific fields that follow according to the following table.

User Zone Type	NUM_ELEMENTS	Type of Elements
000	0	None
001	Variable	Geo Types
010	Variable	OHP Types
011	Variable	Geo Types
100	1	Geo-Based – Separate Carrier

UZ Type Specific Fields - User Zone type specific fields.

Refer to Section 3.5.7.1.

3.5.7.1 User Zone Type Specific Fields

This section describes User Zone Type specific fields associated with a User Zone.

3.5.7.1.1 User Zone Type: Broadcast – RF Coverage Based

No data required.

3.5.7.1.2 User Zone Type: Broadcast – Geo-based

Table 3.5.7.1.2-1 below lists all the supporting Geo Types and corresponding values.

Table 3.5.7.1.2-1 Geo Type Values

Geo Type	Value
Circle	‘000’
Segmented Linear	‘001’
Polygon	‘010’
Reserved	‘011’ through ‘100’

For Geo Type Specific Fields see 3.5.7.1.2.1 – 3.5.7.1.2.3.

3.5.7.1.2.1 Circle

The “Circle” Geo Type has the following format:

Geo Type Field	Length (bits)
GEO_TYPE (‘000’)	3
ANCHOR_LATITUDE	23
ANCHOR_LONGITUDE	22
RADIUS	10
HYSTERESIS	4

GEO_TYPE - Geo Type.

This field is set to ‘000’ (see Table 3.5.7.1.2-1).

ANCHOR_LATITUDE - Anchor latitude.

Latitude of the center of the circle in units of 0.25 second, expressed as a two’s complemented signed number with positive numbers signifying North latitudes. Values over the range of -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°) are valid.

ANCHOR_LONGITUDE - Anchor longitude.

Longitude of the center of the circle in units of 0.25 second, expressed as a two's complemented signed number with positive numbers signifying East longitude. Values over the range of -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°) are valid.

RADIUS - Radius.

Radius of the circle in units of 0.25 second. The 10 bits are divided into a 7-bit mantissa and a 3-bit exponent providing a range of 0 to 127 x 2^7 x 0.25 seconds.

HYSTERESIS - Hysteresis.

Hysteresis value expressed in units of 0.25 second. The mantissa is defined as '1' and the 4 bits represent the exponent. This provides hysteresis values of 1, 2 , 4, 8 ...128 x 0.25 sec. The hysteresis value delays the exiting of a user zone by a distance offset determined by the value of the hysteresis. The entry point for a user zone is the radius value.

3.5.7.1.2.2 Segmented Linear

The segmented linear user zone is defined by an anchor point and a series of points offset relative to each other. The area is formed by defining a distance (radius) offset from the line.

The "Segmented Linear" Geo Type has the following format:

Geo Type Field	Length (bits)
GEO_TYPE ('001')	3
ANCHOR_LATITUDE	23
ANCHOR_LONGITUDE	22
RADIUS	10
HYSTERESIS	4
N_POINTS	5
N_POINTS of the following:	
LAT_OFFSET	11
LONG_OFFSET	11

GEO_TYPE - Geo Type.

This field is set to '001' (see Table 3.5.7.1.2-1).

ANCHOR_LATITUDE - Anchor latitude.

Latitude of the anchor point for the line in units of 0.25 second, expressed as a two's complemented signed number with positive numbers signifying North latitudes. Values over the range of -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°) are valid.

ANCHOR_LONGITUDE - Anchor longitude.

Longitude of the anchor point for the line in units of 0.25 second, expressed as a two's complemented signed number with positive numbers signifying East longitude. Values over the range of -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°) are valid.

RADIUS - Radius.

Distance away from the line that the User Zone covers in units of 0.25 second. The 10 bits are divided into a 7-bit mantissa and a 3-bit exponent providing a range of 0 to 127 x 2^7 x 0.25 seconds.

HYSTERESIS - Hysteresis.

Hysteresis value expressed in units of 0.25 second. The mantissa is defined as '1' and the 4 bits represent the exponent. This provides hysteresis values of 1, 2, 4, 8 ...128 x 0.25 sec. The hysteresis value delays the exiting of a user zone by a distance offset from the radius determined by the value of the hysteresis. The entry point for a user zone is the radius value.

N_POINTS - Number of points.

Number of points of the following two values.

LAT_OFFSET - Latitude offset.

Latitude offset distance from the previous point in units of 0.25 seconds. The 11 bits are divided into an 8 bit mantissa (2's complement representation) and a 3 bit exponent providing a range of ± 0 to 127 x 2^7 x 0.25 seconds.

LONG_OFFSET - Longitude offset.

Longitude offset distance from the previous point in units of 0.25 seconds. The 11 bits are divided into an 8 bit mantissa (2's complement representation) and a 3 bit exponent providing a range of ± 0 to 127 x 2^7 x 0.25 seconds.

3.5.7.1.2.3 Polygon

The polygon is defined by an anchor vertex and a series of vertices offset from the anchor. The polygon is formed by lines formed between the vertices in the order they are provisioned starting with the anchor as the first vertex. A line is formed between the last point provisioned and the anchor to close the polygon.

The "Polygon" Geo Type has the following format:

Geo Type Field	Length (bits)
GEO_TYPE (‘010’)	3
ANCHOR_LATITUDE	23
ANCHOR_LONGITUDE	22
HYSTERESIS	4
N_POINTS	5
N_POINTS of the following:	
LAT_OFFSET	11
LONG_OFFSET	11

GEO_TYPE - Geo Type.

This field is set to ‘010’ (see Table 3.5.7.1.2-1).

ANCHOR_LATITUDE - Anchor latitude.

Latitude of the anchor point for one vertex on the polygon in units of 0.25 second, expressed as a two’s complement signed number with positive numbers signifying North latitudes. Values over the range of -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°) are valid.

ANCHOR_LONGITUDE - Anchor longitude.

Longitude of the anchor point for one vertex on the polygon in units of 0.25 second, expressed as a two’s complement signed number with positive numbers signifying East longitude. Values over the range of -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°) are valid.

HYSTERESIS - Hysteresis.

Hysteresis value expressed in units of 0.25 second. The mantissa is defined as '1' and the 4 bits represent the exponent. This provides hysteresis values of 1, 2 , 4, 8 …128 x 0.25 sec. The hysteresis value delays the exiting of a user zone by a distance offset from the polygon edge determined by the value of the hysteresis. The entry point for the polygon as defined by the lines joining the points on the polygon.

N_POINTS - Number of points.

Number of points of the following two values.

LAT_OFFSET - Latitude offset.

Latitude offset distance from the anchor point in units of 0.25 seconds. The 11 bits are divided into an 8 bit mantissa (2's complement representation) and a 3 bit exponent providing a range of ± 0 to 127 x 2^7 x 0.25 seconds.

LONG_OFFSET - Longitude offset.

Longitude offset distance from the anchor point in units of 0.25 seconds. The 11 bits are divided into an 8 bit mantissa (2's complement representation) and a 3 bit exponent providing a range of ± 0 to 127 x 2^7 x 0.25 seconds.

3.5.7.1.3 User Zone Type: Mobile Specific – RF Coverage Based - Overhead Parameter Determined

For this type of user zone, the mobile station matched parameters on the overhead channel with information in the PUZL.

Below describes all the supporting Overhead Parameter (OHP) Types and corresponding values:

Table 3.5.7.1.3-1 Overhead Parameter (OHP) Type Values

OHP Type	Value
SID Only	‘000’
SID and NID	‘001’
SID and BASE_ID	‘010’
Base station Latitude and Longitude	‘011’
User Zone Center Point and Radius	‘100’
Reserved	‘101’ through ‘111’

3.5.7.1.3.1 SID Only

The SID comes from the common parameters defining the User Zone.

The “SID Only” OHP Type has the following format:

OHP Type Field	Length (bits)
OHP_TYPE (‘000’)	3
HYSTERESIS	4

OHP_TYPE - Overhead Parameter Type.
This field is set to ‘000’ (see Table 3.5.7.1.3-1).

HYSTERESIS - Hysteresis.

Expressed in dB. See Section 2.6.9 of [7] for definition of hysteresis relative to CDMA Tiered Services.

3.5.7.1.3.2 SID and NID

The SID comes from the common parameters defining the User Zone.

The “SID and NID” OHP Type has the following format:

OHP Type Field	Length (bits)
OHP_TYPE (‘001’)	3
N_ITEMS	5
N_ITEMS occurrences of the following:	
NID	16
HYSTERESIS	4

OHP_TYPE - Overhead Parameter Type.

This field is set to ‘001’ (see Table 3.5.7.1.3-1).

N_ITEMS - Number of items.

Number of entries of the following two values.

NID - Network ID.

See [7].

HYSTERESIS - Hysteresis.

Expressed in dB. See Section 2.6.9 of [7] for definition of hysteresis relative to CDMA Tiered Services for RF coverage based user zones.

3.5.7.1.3.3 SID and BASE_ID

The SID comes from the common parameters defining the User Zone.

The “SID and BASE_ID” OHP Type has the following format:

OHP Type Field	Length (bits)
OHP_TYPE (‘010’)	3
N_ITEMS	5
N_ITEMS occurrences of the following:	
BASE_ID	16
HYSTERESIS	4

OHP_TYPE - Overhead Parameter Type.

This field is set to ‘010’ (see Table 3.5.7.1.3-1).

N_ITEMS - Number of items.

Number of entries of the following two values.

BASE_ID - Base Station ID.

See [7].

HYSTERESIS - Hysteresis.

Expressed in dB. See Section 2.6.9 of [7] for definition of hysteresis relative to CDMA Tiered Services for RF coverage based user zones.

3.5.7.1.3.4 Base Station Latitude and Longitude

The “Base Station Latitude and Longitude “ OHP Type has the following format:

OHP Type Field	Length (bits)
OHP_TYPE (‘011’)	3
N_POINTS	5
N_POINTS occurrences of the following:	
BASE_LAT	22
BASE_LONG	23
HYSTERESIS	4

OHP_TYPE - Overhead Parameter Type.

This field is set to ‘011’ (see Table 3.5.7.1.3-1).

N_POINTS - Number of points.

Number of points of the following three values.

BASE_LAT - Base Station latitude.

See [7].

BASE_LONG - Base Station longitude.

See [7].

HYSTERESIS - Hysteresis.

Expressed in dB. See Section 2.6.9 of [7] for definition of hysteresis relative to CDMA Tiered Services for RF coverage based user zones.

3.5.7.1.3.5 User Zone Center Point and Radius

In this case, a circle is used to define the user zone. Any base station whose BASE_LAT and BASE_LONG fall within the circle are considered to define the user zone. The coverage area of these sites constitute the user zone.

The "User Zone Center Point and Radius " HP Type has the following format:

OHP Type Field	**Length (bits)**
OHP_TYPE ('100')	3
CENTER_POINT_LAT	23
CENTER_POINT_LONG	22
RADIUS	10
HYSTERESIS	4

OHP_TYPE - Overhead Parameter Type.

This field is set to '100' (see Table 3.5.7.1.3-1).

CENTER_POINT_LAT - Center point latitude.

Latitude of the center of the circle in units of 0.25 second, expressed as a two's complemented signed number with positive numbers signifying North latitudes. Values over the range of -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°) are valid.

CENTER_POINT_LONG - Center point longitude.

Longitude of the center of the circle in units of 0.25 second, expressed as a two's complemented signed number with positive numbers signifying East longitude. Values over the range of -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°) are valid.

RADIUS - Radius.

Radius of the circle in units of 0.25 second. The 10 bits are divided into a 7-bit mantissa and a 3-bit exponent providing a range of 0 to $127 \times 2^7 \times 0.25$ seconds.

HYSTERESIS - Hysteresis.

Expressed in dB. See Section 2.6.9 of [7] for definition of hysteresis relative to CDMA Tiered Services for RF coverage based user zones.

3.5.7.1.4 User Zone Type: Mobile Specific – Geo-Based

See section 3.5.7.1 2. The parameters are identical.

3.5.7.1.5 User Zone Type: Mobile Specific – Geo-Based – Separate Carrier

This user zone type has the following format:

Field	Length (bits)
SID	15
NID	16
PN_INCLUDED	1
PRI_NGHBR_PN	0 or 9
BAND_CLASS	5
NGHBR_FREQ	5
NUM_ENTRIES	4

NUM_ENTRIES occurrences of the following:

Geo Type Specific Fields	Variable

SID - System ID.

The SID of the separate RF carrier.

NID - Network ID.

The NID of the separate RF carrier.

PN_INCLUDED - Private neighbor PN included indicator.

Set to ‘1’ if the Private Neighbor PN is included. Otherwise the mobile should due a full search of the frequency.

PRI_NGHBR_PN - Private neighbor PN offset.

The PN offset of the private RF carrier.

BAND_CLASS - Private neighbor band class.

The Band Class of the private RF carrier.

NGHBR_FREQ - Private neighbor frequency.

The frequency of the private RF carrier.

NUM_ENTRIES - Number of entries.

The number of Geo Type specific fields that follow.

Geo Type Specific Fields - Geo Type specific fields.

One or more Geo Type specific fields (see Sections 3.5.7.1.2.1 – 3.5.7.1.2.3).

3.5.8 3GPD Parameter Blocks

Table 3.5.8-1 lists the types of parameter blocks used in the *3GPD Configuration Request Message* and the *3GPD Configuration Response Message.*

Table 3.5.8-1 3GPD Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
3GPD Operation Capability Parameters	‘00000000’	3.5.8.1
3GPD Operation Mode Parameters	‘00000001’	3.5.8.2
SimpleIP Capability Parameters	‘00000010’	3.5.8.3
MobileIP Capability Parameters	‘00000011’	3.5.8.4
SimpleIP User Profile Parameters	‘00000100’	3.5.8.5
Mobile IP User Profile Parameters	‘00000101’	3.5.8.6
SimpleIP Status Parameters	‘00000110’	3.5.8.7
MobileIP Status Parameters	‘00000111’	3.5.8.8
SimpleIP PAP SS Parameters[1]	‘00001000’	3.5.8.9
SimpleIP CHAP SS Parameters[1]	‘00001001’	3.5.8.10
MobileIP SS Parameters[1]	‘00001010’	3.5.8.11
HRPD Access Authentication Capability Parameters	‘00001011’	3.5.8.12
HRPD Access Authentication User Profile Parameters	‘00001100’	3.5.8.13
HRPD Access Authentication CHAP SS Parameters[1]	‘00001101’	3.5.8.14
Reserved	‘00001110’ through ‘11111111’	
[1] The shared secret parameters shall not be transmitted over the air unencrypted.		

3.5.8.1 3GPD Operation Capability Parameters

The PARAM_DATA field of the 3GPD Operation Capability Parameters Block consists of the following fields:

Field	Length
OP_MODE	8

OP_ MODE - Operation Mode Bitmap to indicate which operation modes are supported by the mobile station.

The mobile station shall set this field to the value in the form of bitmap as follows:

Subfield	Length (bits)	Subfield Description
SimpleIP	1	SimpleIP Supported
MobileIP	1	MobileIP Supported
MobileIP with SimpleIP fallback	1	MobileIP with SimpleIP fallback Supported
Reserved	5	-

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

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set this field to '00000'.

3.5.8.2 3GPD Operation Mode Parameters

The PARAM_DATA field of the 3GPD Operation Mode Parameters Block consists of the following fields:

Field	Length
OP_MODE	2
RESERVED	6

OP_ MODE - Active operation mode in the mobile station.

The mobile station shall set this field to the active operation mode in the mobile station as specified in Table 3.5.8.2-1.

Table 3.5.8.2-1 Operation Mode

Operation Mode	Binary Value
SimpleIP only	00
MobileIP with SimpleIP Fallback	01
MobileIP only	10
RESERVED	11

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set this field to ‘000000’.

3.5.8.3 SimpleIP Capability Parameters

The PARAM_DATA field of the SimpleIP Capability Parameters Block consists of the following fields:

Field	**Length (bits)**
MAX_NUM_NAI	4
MAX_NAI_LENGTH	8
MAX_SS_LENGTH	5
AUTH_ALGORITHM	8
RESERVED	7

MAX_NUM_NAI - Maximum SimpleIP NAI Entries.

The mobile station shall set this field to the maximum number of SimpleIP NAI entries supported by the mobile station.

MAX_NAI_LENGTH - Maximum SimpleIP NAI length.

The mobile station shall set this field to the maximum length, in units of octets, of the SimpleIP NAIs supported by the mobile station. The mobile station shall support an NAI length of at least 72 octets. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the NAI lengths allocated for the supported algorithms.

MAX_SS_LENGTH - Maximum Length of the Shared Secret Data.

The mobile station shall set this field to the maximum length, in units of octets, of the shared secret data supported by the mobile station. The mobile station shall support an SS length of at least 16 octets long. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the SS lengths allocated for the supported algorithms.

AUTH_ALGORITHM - SimpleIP Authentication Algorithm supported by the mobile station.

The mobile station shall set this field to the SimpleIP authentication algorithms supported by the mobile station in the form of bitmap. The Authentication Algorithm is encoded as follows:

Table 3.5.8.3-1 AUTH_ALGORITHM Parameter Values

Subfield	**Length (bits)**	**Subfield Description**
PPP CHAP	1	CHAP mode-[11]
PPP_PAP	1	PAP mode- [10]
RESERVED	6	

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set all bits of this field to ‘0’.

3.5.8.4 MobileIP Capability Parameters

The PARAM_DATA field of the 3GPD MobileIP Capability Parameters Block consists of the following fields:

Field	Length (bits)
MAX_NUM_NAI	4
MAX_NAI_LENGTH	8
MAX_MN-AAA_SS_LENGTH	5
MN-AAA_AUTH_ALGORITHM	8
MAX_MN-HA_SS_LENGTH	5
MN-HA_AUTH_ALGORITHM	8
RESERVED	2

MAX_NUM_NAI - Maximum MobileIP NAI Entries.

The mobile station shall set this field to the maximum number of MobileIP NAI entries supported by the mobile station.

MAX_NAI_LENGTH - Maximum MobileIP NAI length.

The mobile station shall set this field to the maximum length, in units of octets, of the MobileIP NAIs supported by the mobile station. The mobile station shall support an NAI length of at least 72 octets. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the NAI lengths allocated for the supported algorithms.

MAX_MN-AAA_SS_LENGTH - Maximum Length of the Shared Secret Data (MN-AAA).

The mobile station shall set this field to the maximum length, in units of octet, of the shared secret data (MN-AAA) supported by the mobile station. The mobile station shall support shared secret data of at least 16 octets long. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the MN-AAA SS lengths allocated for the supported algorithms.

MN-AAA_AUTH_ALGORITHM - Authentication Algorithm (MN-AAA) supported by the mobile station.

The mobile station shall set this field to the MobileIP authentication algorithms (MN-AAA) supported by the mobile station in the form of bitmap. The Authentication Algorithm is encoded as follows:

Table 3.5.8.4-1 MN-AAA_AUTH_ALGORITHM Parameter Values

Subfield	Length (bits)	Subfield Description
MD5	1	[15]
RESERVED	7	

MAX_MN-HA_SS_LENGTH - Maximum Length of the Shared Secret Data (MN-HA).

The mobile station shall set this field to the maximum length, in units of octet, of the shared secret data (MN-HA) supported by the mobile station. The mobile station shall set the shared secret data of at least 16 octets long. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the MN-HA SS lengths allocated for the supported algorithms.

MN-HA_AUTH_ALGORITHM - Authentication Algorithm (MN-HA) supported by the mobile station.

The mobile station shall set this field to the MobileIP authentication algorithms (MN-HA) supported by the mobile station in the form of bitmap. The Authentication Algorithm is encoded as follows:

Table 3.5.8.4-2 MN-HA_AUTH_ALGORITHM Parameter Values

Subfield	Length (bits)	Subfield Description
MD5	1	[12]
RESERVED	7	

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set all bits of this field to ‘0’.

3.5.8.5 SimpleIP User Profile Parameters

The PARAM_DATA field of the SimpleIP User Profile Parameters Block consists of the following fields:

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
AUTH_ALGORITHM	4
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The mobile station shall set this field to the number of SimpleIP NAI entries.

The mobile station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The mobile station shall set this field to the index in the SimpleIP NAI Table.

NAI_LENGTH - SimpleIP NAI length.

The mobile station shall set this field to the length of the NAI in units of octet.

NAI - Network Access Identifier.

The mobile station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.

AUTH_ALGORITHM - Authentication Algorithm for SimpleIP.

The mobile station shall set this field to the authentication algorithm used to calculate the Simple IP Authentication. The Authentication Algorithm is specified in Table 3.5.8.5-1.

Table 3.5.8.5-1 Authentication Algorithm Parameter Values for SimpleIP

AUTH_ALGORITHM	Binary Value
None	‘0000’
PPP CHAP	‘0001’
PPP PAP	‘0010’
PPP CHAP to PAP fallback	‘0011’
RESERVED	‘0100’ to ‘1111’

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.8.6 Mobile IP User Profile Parameters

The PARAM_DATA field of the Mobile IP User Profile Parameters Block consists of the following fields:

Field	Length (bits)
RETRY_INFO_INCLUDED	1
MAX_NUM_RETRY	0 or 2
FIRST_RETRY_TIMEOUT	0 or 3
REREG_THRESHOLD	0 or 6
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
T_BIT	1
HOME_ADDRESS	32
PRIMARY_HOME_AGENT	32
SECONDARY_HOME_AGENT	32
MN-AAA_AUTH_ALGORITHM	4
MN-AAA-SPI_INDICATOR	1
MN-AAA_SPI	0 or 32
MN-HA_AUTH_ALGORITHM	4
MN-HA_SPI_INDICATOR	1
MN-HA_SPI	0 or 32
RESERVED	0 to 7 (as needed)

RETRY_INFO_INCLUDED - Indicate if the retry information is included or not.

If MAX_NUM_RETRY, FIRST_RETRY_TIMEOUT and REREG_THRESHOLD are included in this block, the mobile station shall set this field to ‘1’; otherwise, the mobile station shall set this field to ‘0’.

MAX_NUM_RETRY - Maximum Number of Retry for the MobileIP Registration.

If RETRY_INFO_INCLUDED is set to ‘0’, the mobile station shall omit this field; otherwise, the mobile station shall set this field as follows:

The mobile station shall set this field to the maximum number of retries for MobileIP registration.

FIRST_RETRY_TIMEOUT - The amount of time elapsed between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply.

If RETRY_INFO_INCLUDED is set to ‘0’, this field shall be omitted; otherwise, this field shall be set as follows:

This field shall be set to one less than the number of amount of time elapsed, in units of 250ms, between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply.

REREG_THRESHOLD -Re-Registration Threshold.

If RETRY_INFO_INCLUDED is set to ‘0’, the mobile station shall omit this field; otherwise, the mobile station shall set this field as follows:

The mobile station shall set this field to the time, in units of minute, before the expiration of the registration lifetime that the mobile will try to reregister.

NUM_NAI - Number of MobileIP NAI Entries.

The mobile station shall set this field to the number of MobileIP NAI entries.

The mobile station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - MobileIP NAI entry index.

The mobile station shall set this field to the index in the MobileIP NAI Table.

NAI_LENGTH - MobileIP NAI length.

The mobile station shall set this field to the length of the MobileIP NAI, in units of octet.

NAI - Network Access Identifier.

The mobile station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.

T_BIT - Reverse Tunneling.

The mobile station shall set this field to ‘1’ if the reverse tunneling is required or set to ‘0’ if reverse tunneling is not required, see [13].

HOME_ADDRESS - Home Address.

The mobile station shall set this field to the IP address of the mobile node in the form of network byte code.

PRIMARY_HOME_AGENT - Primary Home Agent.

The mobile station shall set this field to the IP address of the mobile node's primary home agent in the form of network byte code.

SECONDARY_HOME_AGENT - Secondary Home Agent.

The mobile station shall set this field to the IP address of the mobile node's back-up/secondary home agent in the form of network byte code.

MN-AAA_AUTH_ALGORITHM - Authentication Algorithm (MN-AAA)

The mobile station shall set this field to the authentication algorithm used to calculate the Mobile IP MN-AAA Authentication Extension as defined in [15]. The Authentication Algorithm is encoded corresponding to Table 3.5.8.6-1.

Table 3.5.8.6-1 Authentication Algorithm Parameter Values

MN-AAA_AUTH_ALGORITHM/ MA-HA_AUTH_AlGORITHM	**Binary Value**
None	‘0000’
MD5	‘0001’
RESERVED	‘0010’ to ‘1111’

MN-AAA_SPI_INDICATOR - Indicator of SPI between MN and AAA.

The mobile station shall set this field to ‘1’ if the Security Parameter Index is included; otherwise, the mobile station shall set this field to ‘0’.

MN-AAA_SPI - SPI between MN and AAA.

If the MN-AAA_SPI_INDICATOR field is set to ‘1’, the mobile station shall set this field to the Security Parameter Index (MN-AAA); otherwise, the mobile station shall omit this field.

MN-HA_AUTH_ALGORITHM - Authentication Algorithm (MN-HA)

The mobile station shall set this field to the authentication algorithm used to calculate the Mobile IP MN-HA Authentication Extension as defined in [12]. The Authentication Algorithm is encoded according to Table 3.5.8.6-1.

MN-HA_SPI_INDICATOR - Indicator of SPI between MN and HA.

The mobile station shall set this field to ‘1’ if Security Parameter Index is included; otherwise, the mobile station shall set this field to ‘0’.

MN-HA_SPI - SPI between MN and HA.

If the MN-HA_SPI_INDICATOR field is set to ‘1’, the mobile station shall set this field to the Security Parameter Index between MN and HA; otherwise, mobile station shall omit this field.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.8.7 SimpleIP Status Parameters

Field	Length (bits)
ACT_NAI_ENTRY_INDEX	4
RESERVED	4

ACT_NAI_ENTRY_INDEX - Active SimpleIP NAI entry index.

The mobile station shall set this field to the active SimpleIP NAI entry index.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set this field to ‘0000’.

3.5.8.8 MobileIP Status Parameters

Field	Length (bits)
ACT_NAI_ENTRY_INDEX	4
NUM_ADD_ACT_NAI	4
NUM_ADD_ACT_NAI occurrences of the following field:	
ADD_ACT_NAI_ENTRY_INDEX	4
RESERVED	0 or 4 (as needed)

ACT_NAI_ENTRY_INDEX - Active MobileIP NAI entry index.

The mobile station shall set this field to the active MobileIP NAI entry index.

NUM_ADD_ACT_NAI - Number of additional Active MobileIP NAI entries.

The mobile station shall set this field to the number of additional active MobileIP NAI entries.

ADD_ACT_NAI_ENTRY_INDEX - Additonal Active MobileIP NAI entry index.

The mobile station shall set this field to the active MobileIP NAI entry index.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set this field to '0000'.

3.5.8.9 SimpleIP PAP SS Parameters

Field	**Length (bits)**
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The mobile station shall set this field to the number of SimpleIP NAI entries.

The mobile station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The mobile station shall set this field to the index in the SimpleIP NAI Table.

SS_LENGTH - Shared Secret Data Length.

The mobile station shall set this field to the length, in units of octet, of the shared secret data. The mobile station shall support the shared secret data of at least 16 octets long.

SS - Shared Secret Data.

The mobile station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to '0'.

3.5.8.10 SimpleIP CHAP SS Parameters

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The mobile station shall set this field to the number of SimpleIP NAI entries.

The mobile station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The mobile station shall set this field to the index in the SimpleIP NAI Table.

SS_LENGTH - Shared Secret Data Length.

The mobile station shall set this field to the length, in units of octet, of the shared secret data. The mobile station shall support the shared secret data of at least 16 octets long.

SS - Shared Secret Data

The mobile station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.8.11 MobileIP SS Parameters

Field	Length (bits)
NUM_NAI	4

NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX	4
MN-AAA_SS_LENGTH	5
MN-AAA_SS	8 × MN-AAA_SS_LENGTH
MN-HA_SS_LENGTH	5
MN-HA_SS	8 × MN-FA_SS_LENGTH

RESERVED	0 to 7 (as needed)

NUM_NAI - Number of MobileIP NAI Entries.

The mobile station shall set this field to the number of MobileIP NAI entries.

The mobile station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - MobileIP NAI entry index.

The mobile station shall set this field to the index in the MobileIP NAI Table.

MN-AAA_SS_LENGTH - Shared Secret Data Length between MN and AAA.

The mobile station shall set this field to the length, in units of octet, of the shared secret data between MN and AAA. The mobile station shall support the shared secret data of at least 16 octets long.

MN-AAA_SS - Shared Secret Data between MN and AAA.

The mobile station shall set this field to the Shared Secret Data between MN and AAA.

MN-HA_SS_LENGTH - Shared Secret Data Length between MN and HA.

The mobile station shall set this field to the length, in units of octet, of the shared secret data. The mobile station shall support the shared secret data of at least 16 octets long.

MN-HA_SS - Shared Secret Data between MN and HA.

The mobile station shall set this field to the Shared Secret Data between MN and HA.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to ‘0’.

3.5.8.12 HRPD Access Authentication Capability Parameters

The PARAM_DATA field of the HRPD [9] Access Authentication Capability Parameters Block consists of the following fields:

Field	Length (bits)
MAX_NAI_LENGTH	8
MAX_SS_LENGTH	5
RESERVED	3
AUTH_ALGORITHM	8

MAX_NAI_LENGTH - Maximum Access Authentication NAI length.

The mobile station shall set this field to the maximum length, in units of octets, of the NAIs supported by the mobile station. The mobile station shall support an NAI length of at least 72 octets. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the NAI length allocated for the supported algorithms.

MAX_SS_LENGTH - Maximum Length of the Shared Secret Data.

The mobile station shall set this field to the maximum length, in units of octets, of the shared secret data supported by the mobile station. The mobile station shall support an SS length of at least 16 octets long. If multiple authentication algorithms support is indicated, the mobile station shall set this field to the maximum of the SS length allocated for the supported algorithms.

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

The mobile station shall set this field to ‘000’.

AUTH_ALGORITHM - HRPD Access Authentication Algorithm supported by the mobile station.

The mobile station shall set this field to the HRPD access authentication algorithms supported by the mobile station in the form of bitmap. The Authentication Algorithm is encoded as follows:

Table 3.5.8.12-1 AUTH_ALGORITHM Parameter Values

Subfield	Length (bits)	Subfield Description
PPP CHAP	1	CHAP mode-[11]
RESERVED	7	

The mobile station shall set each subfield to ‘1’, if the corresponding authentication algorithm is supported by the mobile station; otherwise, the mobile station shall set the subfield to ‘0’.

3.5.8.13 HRPD Access Authentication User Profile Parameters

The PARAM_DATA field of the HRPD Access Authentication User Profile Parameters Block consists of the following fields:

Field	Length (bits)
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
AUTH_ALGORITHM	4
RESERVED	4

NAI_LENGTH - NAI length.

The mobile station shall set this field to the length of the NAI in units of octet.

NAI - Network Access Identifier.

The mobile station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.

AUTH_ALGORITHM - Authentication Algorithm for HRPD Access Authentication.

The mobile station shall set this field to the authentication algorithm used to calculate the HRPD Access Authentication. The Authentication Algorithm is specified in Table 3.5.8.13-1.

Table 3.5.8.13-1 Authentication Algorithm Parameter Values

AUTH_ALGORITHM	Binary Value
None	‘0000’
PPP CHAP	‘0001’
RESERVED	‘0010’ to ‘1111’

RESERVED - Reserved bits.

The mobile station shall set these bits to ‘0’.

3.5.8.14 HRPD Access Authentication CHAP SS Parameters

Field	**Length (bits)**
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	3

SS_LENGTH - Shared Secret Data Length.

The mobile station shall set this field to the length, in units of octet, of the shared secret data. The mobile station shall support the shared secret data of at least 16 octets long.

SS - Shared Secret Data

The mobile station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to '0'.

3.5.9 MMD Parameter Block

Table 3.5.9-1 lists the types of parameter blocks used in the *MMD Configuration Request Message* and the *MMD Configuration Response Message.*

Table 3.5.9-1 MMD Parameter Block Types

Parameter Block Type	**BLOCK_ID**	**Reference**
MMD Application Parameters	'00000000'	3.5.9.1
Reserved	'00000001' through '11111111'	

3.5.9.1 MMD Application Parameters

The PARAM_DATA field of the MMD Application Parameters Block consists of the following fields:

Field	**Length (bits)**
IMPI_LENGTH	8
IMPI	8 × IMPI_LENGTH
NUM_IMPU	4
NUM_IMPU occurrences of the following fields:	
IMPU_ENTRY_IDX	4
IMPU_LENGTH	8
IMPU	8 × IMPU_LENGTH
SIP_URI_LENGTH	8
SIP_DOMAIN_URI	8 × SIP_URI_LENGTH
NUM_P-CSCF	4
NUM_P-CSCF occurrences of the following fields:	
P-CSCF_ENTRY_IDX	4
P-CSCF_LENGTH	8
P-CSCF_ADDRESS	8 × P-CSCF_LENGTH
RESERVED	0 to 7

IMPI_LENGTH - IMS Private Identity length

The mobile station shall set this field to the length of the IMPI in units of octets

IMPI - IMS Private Identity.

The mobile station shall set this field to the IMS Private Identity, encoded in ASCII string, refer to [17].

NUM_IMPU - Number of IMS Public Identity entries.

The mobile station shall set this field to the number of IMS Public Identity entries.

The mobile station shall include NUM_IMPU occurrences of the following fields:

IMPU_ENTRY_IDX - IMPU entry index.

The mobile station shall set this field to the index in the IMPU Table.

IMPU_LENGTH - IMS Public Identity length.

The mobile station shall set this field to the length of the IMPU in units of octet.

IMPU - IMS Public Identity.

		The mobile station shall set this field to the IMS Public Identity (IMPU), encoded in ASCII string, refer to [17].
SIP_URI_LENGTH	-	SIP Domain URI length. The mobile station shall set this field to the length of the SIP Domain URI.
SIP_DOMAIN_URI	-	SIP Domain URI. The mobile station shall set this field to the SIP Domain URI, encoded in ASCII string, refer to [17].
NUM_P-CSCF	-	Number of P-CSCF entries The mobile station shall set this field to the number of P-CSCF entries.

The mobile station shall include NUM_P-CSCF occurrences of the following fields:

P-CSCF_ENTRY_IDX	-	P-CSCF entry index. The mobile station shall set this field to the index in the P-CSCF Table.
P-CSCF_LENGTH	-	P-CSCF length. The mobile station shall set this field to the length of the P-CSCF in units of octet.
P-CSCF_ADDRESS	-	P-CSCF address. The mobile station shall set this field to the P-CSCF address, encoded in ASCII string, refer to [17]
RESERVED	-	Reserved bits. The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

3.5.10 System Tag Parameter Blocks

Table 3.5.10-1 lists the types of parameter blocks used in the *System Tag Configuration Request Message* and the *System Tag Configuration Response Message.*

Table 3.5.10-1 System Tag Parameter Block Types

System Tag Parameter Block Type	BLOCK_ID	Reference
Home System Tag	‘00000000’	3.5.10.1
Group Tag List Dimensions	‘00000001’	3.5.10.2
Group Tag List	‘00000010’	3.5.10.3
Specific Tag List Dimensions	‘00000011’	3.5.10.4
Specific Tag List	‘00000100’	3.5.10.5
Call Prompt List Dimensions	‘00000101’	3.5.10.6
Call Prompt List	‘00000110’	3.5.10.7
Reserved	‘00000111’ through ‘11111111’	

3.5.10.1 Home System Tag

The PARAM_DATA field of the Home System Tag Block consists of the following fields:

Field	Length (bits)
CALL_PRMPT_INCL	1
CALL_PRMPT	0 or 5
RESERVED	0 or 5
TAG_ENCODING	5
TAG_LEN	5
TAG	TAG_LEN × 8

CALL_PRMPT_INCL - Call Prompt Included Flag.

The mobile station shall set this field to ‘1’ if the CALL_PRMPT field is included in this parameter block. Otherwise, the mobile station shall set this field to ‘0’

CALL_PRMPT - Call prompt identifier.

If a Call Prompt is associated with the Home System Tag, the mobile station shall set this field to the associated Call Prompt Identifier (see 3.5.10.4). Otherwise, this field shall be omitted.

RESERVED - Reserved bits.

If CALL_PRMPT_INCL is set to ‘0’, the mobile station shall set this field to ‘00000’. Otherwise, this field shall be omitted.

TAG_ENCODING - Home system tag encoding.

See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.

TAG_LEN - Length of home system tag.

The mobile system shall set this field to the length of the home system tag in octets.

TAG - Home system tag.

The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING.

3.5.10.2 Group Tag List Dimensions

The PARAM_DATA field of the Group Tag List Dimensions Block consists of the following fields:

Field	**Length (bits)**
MAX_GROUP_TAG_LIST_SIZE	16
CUR_GROUP_TAG_LIST_SIZE	16
GROUP_TAG_LIST_ID	16
CUR_TAG_P_REV	8
NUM_GROUP_TAG_RECS	8

MAX_GROUP_TAG_LIST_SIZE - Maximum group system tag list size.

The mobile station shall set this field to the maximum size, in octets, that the mobile station can support for the group system tag list (GROUP_TAG_LIST$_{s-p}$).

CUR_GROUP_TAG_LIST_SIZE - Current group system tag list size.

The mobile station shall set this field to the size, in octets, of the current group system tag list.

GROUP_TAG_LIST_ID Group System Tag List Identification.

The mobile station shall set this field to the value of the Group System Tag List Identification assigned for the group system tag indicator list (GROUP_TAG_LIST$_{s-p}$) by the base station.

CUR_TAG_P_REV - Protocol revision of the mobile station’s current group tag list.

The mobile station shall set this field to the value of the TAG_P_REV associated with its current group tag list.

NUM_GROUP_TAG_RECS - Number of Group System Tag Records.

The mobile station shall set this field to the number of group system tag records contained within the GROUP_TAG_TABLE field of the current group tag list.

3.5.10.3 Group Tag List Parameter Block

The PARAM_DATA field of the Group Tag List Block consists of the following fields:

Field	**Length (bits)**
CUR_TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag. The mobile station shall set this field to the value of the TAG_P_REV associated with its current group tag list.

RESERVED - Reserved bits.

The mobile station shall set this field to '0000000'.

LAST_SEGMENT - Last segment indicator bit.

The mobile station shall set this field to '1' if SEGMENT_DATA contains the last octet of the group tag list; otherwise, the mobile station shall set this field to '0'.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the group tag list included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the group tag list data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current group tag list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current group tag list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the group tag list in this field. The octets shall be equal to the octets starting at the offset within the group tag list specified by SEGMENT_OFFSET.

3.5.10.4 Specific Tag List Dimensions

The PARAM_DATA field of the Specific Tag List Dimensions Block consists of the following fields:

Field	**Length (bits)**
MAX_SPEC_TAG_LIST_SIZE	16
CUR_SPEC_TAG_LIST_SIZE	16
SPEC_TAG_LIST_ID	16
CUR_TAG_P_REV	8
NUM_SPEC_TAG_RECS	14
RESERVED	2

MAX_SPEC_TAG_LIST_SIZE - Maximum specific system tag list size.

The mobile station shall set this field to the maximum size, in octets, that the mobile station can support for the specific system tag list ($SPEC\_TAG\_LIST_{s-p}$).

CUR_SPEC_TAG_LIST_SIZE - Current specific system tag list size.

The mobile station shall set this field to the size, in octets, of the current specific system tag list.

SPEC_TAG_LIST_ID Specific System Tag List Identification.

The mobile station shall set this field to the value of the Specific System Tag List Identification assigned for the specific system tag indicator list ($SPEC\_TAG\_LIST_{s-p}$) by the base station.

CUR_TAG_P_REV - Protocol revision of the mobile station's current group tag list.

The mobile station shall set this field to the value of the TAG_P_REV associated with its current specific tag list.

NUM_SPEC_TAG_RECS - Number of Specific System Tag Records.

The mobile station shall set this field to the number of specific system tag records contained within its SPEC_TAG_TABLE field of the current specific tag list

RESERVED - Reserved bits.

The mobile station shall set this field to '00'.

3.4.10.5 Specific Tag List Parameter Block

The PARAM_DATA field of the Specific Tag List Block consists of the following fields:

Field	Length (bits)
CUR_TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag. The mobile station shall set this field to the value of the TAG_P_REV associated with its current specific tag list.

RESERVED - Reserved bits.

The mobile station shall set this field to '0000000'.

LAST_SEGMENT - Last segment indicator bit.

The mobile station shall set this field to '1' if SEGMENT_DATA contains the last octet of the specific tag list; otherwise, the mobile station shall set this field to '0'.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the specific tag list included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the specific tag list data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current specific tag list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current specific tag list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the specific tag list in this field. The octets shall be equal to the octets starting at the offset within the specific tag list specified by SEGMENT_OFFSET.

3.4.10.6 Call Prompt List Dimensions

The PARAM_DATA field of the Call Prompt List Dimensions Block consists of the following fields:

Field	**Length (bits)**
MAX_CALL_PRMPT_LIST_SIZE	16
CUR_CALL_PRMPT_LIST_SIZE	16
CALL_PRMPT_LIST_ID	16
CUR_TAG_P_REV	8
NUM_CALL_PRMPT_RECS	8

MAX_CALL_PRMPT_LIST_SIZE - Maximum call prompt list size.

The mobile station shall set this field to the maximum size, in octets, that the mobile station can support for the call prompt list (CALL_PRMPT_LIST$_{s\text{-}p}$).

CUR_CALL_PRMPT_LIST_SIZE - Current call prompt list size.

The mobile station shall set this field to the size, in octets, of the current call prompt list.

CALL_PRMPT_LIST_ID Call Prompt List Identification.

The mobile station shall set this field to the value of the Call Prompt List Identification assigned for the call prompt list (CALL_PRMPT_LIST$_{s\text{-}p}$) by the base station.

CUR_TAG_P_REV - Protocol revision for the system tag.

The mobile station shall set this field to the value of the TAG_P_REV associated with its current call prompt list.

NUM_CALL_PRMPT_RECS - Number of Call Prompt Records.

The mobile station shall set this field to the number of call prompt records contained within its CALL_PRMPT_TABLE field of the call prompt list

3.4.10.7 Call Prompt Tag List Parameter Block

The PARAM_DATA field of the Call Prompt List Block consists of the following fields:

Field	Length (bits)
TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag. The mobile station shall set this field to the value of the TAG_P_REV associated with its current specific tag list.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘0000000’.

LAST_SEGMENT - Last segment indicator bit.

The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the call prompt list; otherwise, the mobile station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the call prompt list included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the group tag list data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current call prompt list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current call prompt list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the call prompt list in this field. The octets shall be equal to the octets starting at the offset within the call prompt list specified by SEGMENT_OFFSET.

3.5.11 Group Tag List, Specific Tag List and Call Prompt List

The group tag list (GROUP_TAG_LIST$_{s\text{-}p}$) and the specific tag list (SPEC_TAG_LIST$_{s\text{-}p}$) contain information to be displayed on the mobile station when the mobile station is obtaining a service in the roaming network. These information can be associated with some parameters in the system record in the preferred roaming list.

The Group Tag List is associated with TAG_P_REV equal to '00000001' and has the following variable length format:

Group Tag List Field	Length (bits)
GROUP_TAG_LIST_SIZE	16
GROUP_TAG_LIST_ID	16
TAG_P_REV	8
DEF_TAG_ENCODING	8
NUM_GROUP_TAG_RECS	8
GROUP_TAG_TABLE	variable
GROUP_TAG_CRC	16

GROUP_TAG_LIST_SIZE - Group tag list size.

This field is set to the total size, in octets, of the group tag list, including the GROUP_TAG_LIST_SIZE and GROUP_TAG_LIST_CRC fields.

GROUP_TAG_LIST_ID Group Tag List Identification.

The mobile station shall set this field to the value of the Group Tag List Identification assigned for the group tag list ($\text{GROUP\_TAG\_LIST}_{\text{s-p}}$) by the base station.

TAG_P_REV - Protocol revision of the Group Tag format.

This field is set to the value of the TAG_P_REV corresponding this group tag list ($\text{GROUP\_TAG\_LIST}_{\text{s-p}}$) structure. This field determines the parsing rules for the Group Tag List. The base station shall set this field to '00000001' for this Group Tag List structure.

DEF_TAG_ENCODING - Default tag encoding.

This field is set to the tag encoding method the mobile station is to use when operating on group tags not specified in GROUP_TAG_TABLE.

NUM_GROUP_TAG_RECS - Number of group tag records.

This field is set to the number of group tag records contained in GROUP_TAG_TABLE (see Table 3.5.10.2-1).

GROUP_TAG_TABLE - Group Tag Table.

This field contains the Group Tag Records. The number of group tag records is specified by NUM_GROUP_TAG_RECS. The group tag record formats are specified in 3.5.10.2.1.

GROUP_TAG_LIST_CRC - CRC for group tag list.

This field is set to the 16-bit CRC calculated according to 3.5.10.1.

The Specific Tag List is associated with TAG_P_REV equal to '00000001' and has the following variable length format:

Specific Tag List Field	Length (bits)
SPEC_TAG_LIST_SIZE	16
SPEC_TAG_LIST_ID	16
TAG_P_REV	8
DEF_TAG_ENCODING	8
NUM_SPEC_TAG_RECS	14
RESERVED	2
SPEC_TAG_TABLE	variable
SPEC_TAG_CRC	16

SPEC_TAG_LIST_SIZE - Specific tag list size.

This field is set to the total size, in octets, of the specific tag list, including the SPEC_TAG_LIST_SIZE and SPEC_TAG_LIST_CRC fields.

SPEC_TAG_LIST_ID Specific Tag List Identification.

The mobile station shall set this field to the value of the Specific Tag List Identification assigned for the specific tag list (SPEC_TAG_LIST$_{s\text{-}p}$) by the base station.

TAG_P_REV - Protocol revision of the Specific Tag format.

This field is set to the value of the TAG_P_REV corresponding this specific tag list (SPEC_TAG_LIST$_{s\text{-}p}$) structure. This field determines the parsing rules for the Specific Tag List. The base station shall set this field to '00000001' for this Specific Tag List structure.

DEF_TAG_ENCODING - Default tag encoding.

This field is set to the tag encoding method the mobile station is to use when operating on specific tags not specified in SPEC_TAG_TABLE.

NUM_SPEC_TAG_RECS - Number of specific tag records.

This field is set to the number of specific tag records contained in SPEC_TAG_TABLE (see Table 3.5.10.3-1).

RESERVED - Reserved bits.

This field shall be set to '00'.

SPEC_TAG_TABLE - Specific Tag Table.

This field contains the Specific Tag Records. The number of specific tag records is specified by NUM_SPEC_TAG_RECS. The specific tag record formats are specified in 3.5.10.3.1.

SPEC_TAG_LIST_CRC - CRC for group tag list.

This field is set to the 16-bit CRC calculated according to 3.5.10.1.

The Call Prompt List is associated with TAG_P_REV equal to ‘00000001’ and has the following variable length format:

Call Prompt List Field	**Length (bits)**
CALL_PRMPT_LIST_SIZE	16
CALL_PRMPT_LIST_ID	16
TAG_P_REV	8
DEF_TAG_ENCODING	8
NUM_CALL_PRMPT_RECS	14
RESERVED	2
CALL_PRMPT_TABLE	variable
CALL_PRMPT_CRC	16

CALL_PRMPT_LIST_SIZE - Call prompt list size.

This field is set to the total size, in octets, of the specific tag list, including the CALL_PRMPT_LIST_SIZE and CALL_PRMPT_LIST_CRC fields.

CALL_PRMPT_LIST_ID Call Prompt List Identification.

The mobile station shall set this field to the value of the Call Prompt List Identification assigned for the call prompt list ($\text{CALL\_PRMPT\_LIST}_{\text{s-p}}$) by the base station.

TAG_P_REV - Protocol revision of the Call Prompt format.

This field is set to the value of the TAG_P_REV corresponding this call prompt list ($\text{CALL\_PRMPT\_LIST}_{\text{s-p}}$) structure. This field determines the parsing rules for the Call Prompt List. The base station shall set this field to ‘00000001’ for this Call Prompt List structure.

DEF_TAG_ENCODING - Default tag encoding.

This field is set to the tag encoding method the mobile station is to use when operating on call prompts not specified in CALL_PRMPT_TABLE.

NUM_CALL_PRMPT_RECS - Number of call prompt records.

This field is set to the number of call prompt records contained in CALL_PRMPT_TABLE (see Table 3.5.10.3-1).

RESERVED - Reserved bits.

This field shall be set to ‘00’.

CALL_PRMPT_TABLE - Call Prompt Table.

This field contains the Call Prompt Records. The number of call prompt records is specified by NUM_CALL_PRMPT_RECS. The call prompt record formats are specified in 3.5.10.3.1.

CALL_PRMPT_LIST_CRC - CRC for call prompt list.

This field is set to the 16-bit CRC calculated according to 3.5.10.1.

3.5.11.1 Group Tag List, Specific Tag List, and Call Prompt List CRC Calculation

The 16-bit group tag list, specific tag list, and call prompt list CRC fields (GROUP_TAG_LIST_CRC, SPEC_TAG_LIST_CRC, CALL_PRMPT_LIST_CRC, respectively) are calculated on all bits of the Group Tag List, Specific Tag List, or Call Prompt List (as appropriate) excluding the bits of the GROUP_TAG_LIST_CRC, SPEC_TAG_LIST_CRC, and CALL_PRMPT_LIST_CRC fields. The generator polynomial for this CRC is $g(x) = x^{16} + x^{12} + x^{5} + x^{0}$.

The 16-bit CRC is calculated according to the following procedure using the logic shown in Figure 2.2.1-2:

- Initially, all shift register elements are set to logical one and the switches are set in the position A.
- The register is clocked with each preferred roaming list bit as an input, from the most significant bit of the GROUP_TAG_LIST_SIZE/SPEC_TAG_LIST_SIZE/CALL_PRMPT_LIST_SIZE field through the least significant bit of the GROUP_TAG_TABLE/SPEC_TAG_TABLE/CALL_PRMPT_TABLE field.
- The switches are set in the position B, and the register is clocked an additional 16 times. The 16 additional output bits constitute the CRC.

3.5.11.2 Group Tag Records

A group tag record contains parameters that the mobile station can use to display a system tag. Each type of group tag record is tailored for use in determining a particular system tag.

Table 3.5.11.2-1 Group Tag Record Type Values

Acquisition Record Type	Value
Group Tag Record – Single Entry	‘000’
Group Tag Record – Range	‘001’
Reserved	‘010’ - ‘111’

3.5.11.2.1 Group Tag Record Format

3.5.11.2.1.1 Group Tag Record – Single Entry

This group tag record type is for use in displaying a system tag in associated with a roaming indicator in the system record of the preferred roaming list, and has the following variable length format:

Group Tag Record Field	Length (bits)
GROUP_TAG_TYPE (‘000’)	3
ROAM_DISP_IND	4
ENCODING_INCL	1
TAG_ENCODING	0 or 5
ROAM_IND	8
CALL_PRMPT_INCL	1
CALL_PRMPT	0 or 5
TAG_LEN	5
TAG	TAG_LEN × 8
RESERVED	0, 2 or 5

GROUP_TAG_TYPE - Group tag record type.

This field is set to ‘000’ (see Table 3.5.10.2-1).

ROAM_DISP_IND - Roaming display indicator.

The mobile station shall set this field to the value of the action for displaying the default roaming indicator on the mobile station’s display. The values are:

ROAM_DISP_IND	Action
‘0000’	Default Roaming Indicator off.
‘0001’	Default Roaming indicator on.
‘0010’	Default Roaming Indicator flashing.

‘0011’ – ‘1111’	Reserved

ENCODING_INCL - Tag encoding field included flag.

The mobile station shall set this field to ‘1’ if the TAG_ENCODING field is included. Otherwise, the mobile station shall set this field to ‘0’.

TAG_ENCODING - Group tag encoding format.

See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.

ROAM_IND - Roaming indicator

The mobile station shall set this field to the roaming indicator value (see [4]) for which this Group Tag Record is associated.

CALL_PRMPT_INCL - Call Prompt Included Flag

The mobile station shall set this field to ‘1’ if the CALL_PRMPT field is included in this parameter block. Otherwise, the mobile station shall set this field to ‘0’

CALL_PRMPT - Call prompt identifier

If a Call Prompt is associated with the Home System Tag, the mobile station shall set this field to the associated Call Prompt Identifier (see 3.5.10.4). Otherwise, this field shall be omitted.

TAG_LEN - Group tag length indicator.

The mobile station shall set this field to the number of octets in the TAG field.

TAG - Group tag.

The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘00’ if ENCODING_INCL = ‘0’ and CALL_PRMPT_INCL = ‘0’. The mobile station shall set this field to ‘00000’ if either ENCODING_INCL = ‘1’ or CALL_PRMPT_INCL = ‘1’. If ENCODING_INCL = ‘1’ and CALL_PRMPT = ‘1’, this field shall be omitted.

3.5.11.2.1.2 Group Tag Record – Range

This group tag record type is for use in displaying a system tag in associated with roaming indicators in the system records of the preferred roaming list, and has the following variable length format:

Group Tag Record Field	Length (bits)
GROUP_TAG_TYPE (‘000’)	3
ROAM_DISP_IND	4
ENCODING_INCL	1
TAG_ENCODING	0 or 5
CALL_PRMPT_INCL	1
CALL_PRMPT	0 or 5
LOW_ROAM_IND	8
HIGH_ROAM_IND	8
ROAM_INC	3
TAG_LEN	5
TAG	TAG_LEN × 8
RESERVED	2, 5 or 7

GROUP_TAG_TYPE - Group tag record type.

This field is set to ‘000’ (see Table 3.5.10.2-1).

ROAM_DISP_IND - Roaming display indicator.

The mobile station shall set this field to the value of the action for displaying the default roaming indicator on the mobile station’s display. The values are:

ROAM_DISP_IND	Action
‘0000’	Default Roaming Indicator off.
‘0001’	Default Roaming indicator on.
‘0010’	Default Roaming Indicator flashing.
‘0011’ – ‘1111’	Reserved

ENCODING_INCL - Tag encoding field included flag.

The mobile station shall set this field to ‘1’ if the TAG_ENCODING field is included. Otherwise, the mobile station shall set this field to ‘0’.

TAG_ENCODING - Group tag encoding format.

See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.

CALL_PRMPT_INCL - Call Prompt Included Flag

The mobile station shall set this field to ‘1’ if the CALL_PRMPT field is included in this parameter block. Otherwise, the mobile station shall set this field to ‘0’

CALL_PRMPT - Call prompt identifier

If a Call Prompt is associated with the Home System Tag, the mobile station shall set this field to the associated Call Prompt Identifier (see 3.5.10.4). Otherwise, this field shall be omitted.

LOW_ROAM_IND - Low roaming indicator

The mobile station shall set this field to the roaming indicator (ROAM_IND, see [4]) having the lowest value over the range of ROAM_IND values for which this Group Tag Record is associated.

HIGH_ROAM_IND - High roaming indicator

The mobile station shall set this field to the roaming indicator (ROAM_IND, see [4]) having the highest value over the range of ROAM_IND values for which this Group Tag Record is associated.

ROAM_INC - Roaming indicator increment

The mobile station shall set this field to the increment used to construct the set of ROAM_INDs associated with this record. ROAM_INDs associated with this record are multiples of this value between LOW_ROAM_IND and HIGH_ROAM_IND inclusive. This field shall be set to a value in the range 1 to 7 inclusive.

TAG_LEN - Group tag length indicator.

The mobile station shall set this field to the number of octets in the TAG field.

TAG - Group tag.

The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘00’ if either ENCODING_INCL = ‘1’ or CALL_PRMPT_INCL = ‘1’. If ENCODING_INCL = ‘1’ and CALL_PRMPT_INCL = ‘1’, the mobile station shall set this field to ‘00000’. If ENCODING_INCL = ‘0’ and CALL_PRMPT_INCL = ‘0’, the mobile station shall set this field to ‘0000000’.

3.5.11.3 Specific Tag Records

A specific tag record contains parameters that the mobile station can use to display a system tag. Each type of group tag record is tailored for use in determining a particular system tag.

Table 3.5.11.3-1 Specific Tag Record Type Values

Acquisition Record Type	Value
Specific Tag Record – Single Entry	‘000’
Specific Tag Record – Range	‘001’
Reserved	‘010’ - ‘111’

3.5.11.3.1 Specific Tag Record Format

3.5.11.3.1.1 Specific Tag Record – Single Entry

This specific tag record type is for use in displaying a system tag in associated with a SID in the system record of the preferred roaming list, and has the following variable length format:

Specific Tag Record Field	Length (bits)
SPEC_TAG_TYPE (‘000’)	3
ROAM_DISP_IND	4
ENCODING_INCL	1
TAG_ENCODING	0 or 5
CALL_PRMPT_INCL	1
CALL_PRMPT	0 or 5
SID	15
TAG_LEN	5
TAG	TAG_LEN × 8
RESERVED	1, 3 or 6

SPEC_TAG_TYPE - Specific tag record type.

This field is set to ‘000’ (see Table 3.5.10.2-1).

ROAM_DISP_IND - Roaming display indicator.

The mobile station shall set this field to the value of the action for displaying the default roaming indicator on the mobile station’s display. The values are:

ROAM_DISP_IND	Action
‘0000’	Default Roaming Indicator off.
‘0001’	Default Roaming indicator on.

‘0010’	Default Roaming Indicator flashing.
‘0011’ – ‘1111’	Reserved

ENCODING_INCL	-	Tag encoding indicator flag. The mobile station shall set this field to ‘1’ if the TAG_ENCODING field is included. Otherwise, the mobile station shall set this field to ‘0’.
TAG_ENCODING	-	Tag encoding format. See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.
CALL_PRMPT_INCL	-	Call Prompt Included Flag The mobile station shall set this field to ‘1’ if the CALL_PRMPT field is included in this parameter block. Otherwise, the mobile station shall set this field to ‘0’
CALL_PRMPT	-	Call prompt identifier If a Call Prompt is associated with the Home System Tag, the mobile station shall set this field to the associated Call Prompt Identifier (see 3.5.10.4). Otherwise, this field shall be omitted.
SID	-	System Identification The mobile station shall set this field to the System Identification (SID) corresponding to this Specific Tag Record. (See [7]).
TAG_LEN	-	Tag length The mobile station shall set this field to the number of octets in the TAG field.
TAG	-	Specific Tag. The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING.
RESERVED	-	Reserved bits. The mobile station shall set this field to ‘0’ if ENCODING_INCL = ‘1’ and CALL_PRMPT_INCL = ‘1’. The mobile station shall set this field to ‘000’ if ENCODING_INCL = ‘0’ and CALL_PRMPT_INCL = ‘0’. Otherwise, the mobile station shall set this field to ‘000000’.

3.5.11.3.1.2 Specific Tag Record – Range

This specific tag record type is for use in displaying a system tag in associated with SIDs in the system records of the preferred roaming list, and has the following variable length format:

Specific Tag Record Field	**Length (bits)**
SPEC_TAG_TYPE (‘000’)	3
ROAM_DISP_IND	4
ENCODING_INCL	1
TAG_ENCODING	0 or 5
CALL_PRMPT_INCL	1
CALL_PRMPT	0 or 5
LOW_SID	15
HIGH_SID	15
SID_INC	3
TAG_LEN	5
TAG	TAG_LEN × 8
RESERVED	1, 4 or 7

SPEC_TAG_TYPE - Specific tag record type.

This field is set to ‘000’ (see Table 3.5.10.2-1).

ROAM_DISP_IND - Roaming display indicator.

The mobile station shall set this field to the value of the action for displaying the default roaming indicator on the mobile station’s display. The values are:

ROAM_DISP_IND	Action
‘0000’	Default Roaming Indicator off.
‘0001’	Default Roaming indicator on.
‘0010’	Default Roaming Indicator flashing.
‘0011’ – ‘1111’	Reserved

ENCODING_INCL - Tag encoding indicator flag.

The mobile station shall set this field to ‘1’ if the TAG_ENCODING field is included. Otherwise, the mobile station shall set this field to ‘0’.

TAG_ENCODING - Tag encoding format.

See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.

CALL_PRMPT_INCL - Call Prompt Included Flag

		The mobile station shall set this field to ‘1’ if the CALL_PRMPT field is included in this parameter block. Otherwise, the mobile station shall set this field to ‘0’
CALL_PRMPT	-	Call prompt identifier
		If a Call Prompt is associated with the Home System Tag, the mobile station shall set this field to the associated Call Prompt Identifier (see 3.5.10.4). Otherwise, this field shall be omitted.
LOW_SID	-	Lowest applicable System Identification
		The mobile station shall set this field to the System Identification (SID) having the lowest value over the range of SID values for which this Specific Tag Record is associated. (See [7]).
HIGH_SID	-	Highest applicable System Identification
		The mobile station shall set this field to the System Identification (SID) having the highest value over the range of SID values for which this Specific Tag Record is associated. (See [7]).
SID_INC	-	System identifier increment
		The mobile station shall set this field to the increment to be used to construct SIDs of the systems associated with this record. SIDs of the systems associated with this record are multiples of this value between LOW_SID and HIGH_SID inclusive. This field shall be set to a value in the range 1 to 7 inclusive.
TAG_LEN	-	Tag length
		The mobile station shall set this field to the number of octets in the TAG field.
TAG	-	Specific Tag.
		The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING.
RESERVED	-	Reserved bits.
		The mobile station shall set this field to ‘0’ if ENCODING_INCL = ‘0’ and CALL_PRMPT_INCL = ‘0’. The mobile station shall set this field to ‘0000’ if either ENCODING_INCL = ‘1’ or CALL_PRMPT_INCL = ‘1’. The mobile station shall set this field to ‘0000000’ if ENCODING_INCL = ‘1’ and CALL_PRMPT_INCL = ‘1’.

3.5.11.4 Call Prompt Record Format

Each Call Prompt Record has the following format:

Call Prompt Record Field	**Length (bits)**
CALL_PRMPT	5
CALL_PRMPT_TEXT_STATE	2
ENCODING_INCL	1
PRMPT_ENCODING	0 or 5
PRMPT_LEN	5
PRMPT	PRMPT_LEN × 8
RESERVED	3 or 6

CALL_PRMPT - Call prompt identifier.

The mobile station shall set this field to the call prompt identifier for the given record entry.

CALL_PRMPT_TEXT_STATE - Call Prompt Text State

The mobile station shall set this field to the text state for the text to be displayed by the mobile station according to the following table:

CALL_PROMPT_TEXT_STATE	Action
‘00’	Call Prompt text on.
‘01’	Call Prompt text flashing.
‘10’ – ‘11’	Reserved

ENCODING_INCL - Call prompt character encoding included flag.

The mobile station shall set this field to ‘1’ if the PRMPT_ENCODING field is included. Otherwise, the mobile station shall set this field to ‘0’.

PRMPT_ENCODING - Character Encoding.

See [4]. This field shall be set to indicate the character set used in the PRMPT field included in this parameter block.

PRMPT_LEN - Call prompt length indicator

The mobile station shall set this field to indicate the number of octets of the PRMPT field.

PRMPT - Call prompt.

The mobile station shall set this field to the characters based on the encoding method defined in PRMPT_ENCODING.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘000’ if ENCODING_INCL = ‘0’. Otherwise, the mobile station shall set this field to ‘000000’.

3.5.12 MMS Parameter Block

Table 3.5.12-1 lists the types of parameter blocks used in the *MMS Configuration Request Message* and the *MMS Configuration Response Message.*

Table 3.5.12-1 MMS Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
MMS URI Parameters	‘00000000’	3.5.12.1
MMS URI Capability Parameters	‘00000001’	3.5.12.2
Reserved	‘00000010’ through ‘11111111’	

3.5.12.1 MMS URI Parameters

The PARAM_DATA field of the MMS URI Parameters Block consists of the following fields:

Field	Length (bits)
NUM_MMS_URI	4
NUM_MMS_URI occurrences of the following fields:	
MMS_URI_ENTRY_IDX	4
MMS_URI_LENGTH	8
MMS URI	8 x MMS_URI_LENGTH
RESERVED	0 to 7

NUM_MMS_URI - Number of MMS URIs

The mobile station shall set this field to the number of MMS URIs stored on the mobile, encoded in ASCII string, refer to [16], [17] and [18].

The mobile station shall include NUM_MMS_URI occurrences of the following fields:

MMS_URI_ENTRY_IDX - MMS URI entry index.

The mobile station shall set this field to the index in the MMS URI Table, refer to [16], [17] and [18].

MMS_URI_LENGTH - MMS URI length.

The mobile station shall set this field to the length of the URI associated with the MMS Relay/Server in units of octet

MMS_URI - MMS_URI

The mobile station shall set this field to the URI of the MMS Relay/Server, encoded in ASCII string, refer to [16], [17] and [18].

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

3.5.12.2 MMS URI Capability Parameters

The PARAM_DATA field of the MMS URI Capability Parameters Block consists of the following fields:

Field	**Length (bits)**
MAX_NUM_MMS_URI	4
MAX_MMS_URI_LENGTH	8
RESERVED	7

MAX_NUM_MMS_URI - Maximum MMS URI Entries.

The mobile station shall set this field to the maximum number of MMS URI entries supported by the mobile station.

MAX_MMS_URI_LENGTH - Maximum MMS URI length.

The mobile station shall set this field to the maximum length, in units of octets, of the MMS URI supported by the mobile station.

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

4 BASE STATION PROCEDURES

4.1 Reserved

4.2 Initiation of the Programming Procedures

4.2.1 User-Initiated Procedure

If the base station sends a message to the mobile station on the CDMA Paging Channel or Forward Common Control Channel, and if the active NAM of this mobile station has not been provisioned, the base station should address the message using the ESN or MEID of the mobile station.

After receiving an activation origination, the base station should assign the mobile station to a CDMA Traffic Channel or analog voice channel and perform appropriate procedures as specified in 6.6.4 of [1] or 2.6.4 of [7].

The base station should not process an activation origination as an implicit registration (see 6.6.5.1 of [1] or 2.6.5.1 of [7]). The base station should not send the *Mobile Station Registered Message* (see 7.7.3.3.2.15 of [1] or 3.7.3.3.2.15 of [7]) during the programming session.

If the mobile station includes authentication information when sending an activation origination, the base station should process the authentication data as required in 7.3.1 of [1] or 3.3.1 of [7]. During the programming session, the base station should invoke signaling message encryption and voice privacy (CDMA only) whenever available.

If the base station sets the AUTH field of the *Access Parameters Message* to ‘01’ or sets SENDING RAND field of the MC-RR Parameters Message to ‘1’, and if the mobile station does not include authentication information when sending an activation origination, the base station shall not activate voice privacy or message encryption.

If the base station sets the AUTH field of the *Access Parameters Message* to ‘01’ or sets SENDING RAND field of the MC-RR Parameters Message to ‘1’, and if the mobile station includes authentication information when sending an activation origination, but authentication fails, the base station may perform the following to provide signaling message encryption and voice privacy prior to performing full mobile station activation:

- The base station should complete the exchange of the A-key information and, optionally, set a non-default mobile station identifier. The base station should store the information in its database so that authentication and key calculation can be performed.
- Following the exchange of A-key information, the base station should perform SSD update (see 3.3.2) procedures of 6.3.12.1.9 of [1] or 2.3.12.1.5 of [7]. The base station may confirm the SSD update by performing the Unique Challenge-Response Procedure defined in 6.3.12.1.5 of [1] or 2.3.12.1.4 of [7].
- When the SSD update has been completed, the base station may send the *Re-Authenticate Message* (see 4.3.2).

- The base station may activate message encryption (see 4.3.3) and voice privacy (see 4.3.4).

4.2.2 Network-Initiated Procedure.

If the network initiates OTAPA for the mobile station that is already in a CDMA *Conversation Substate* or the analog Conversation Task (i.e. the base station is communicating with the mobile station on the CDMA Traffic Channel or on the Analog Voice Channel), the base station shall send the *OTAPA Request Message* with the START_STOP field set to '1' to the mobile station in order to start the OTAPA session in the mobile station.

If the network initiates OTAPA for the mobile station that is in the CDMA *Mobile Station Idle State*, the base station shall do the following:

- The base station shall page the mobile station and establish a Traffic Channel using the procedures defined in 7.6 of [1] or 3.6 of [7]. The base station shall request Service Option 18 or 19, and perform service negotiation.
- If the base station establishes a service configuration, as specified in a *Service Connect Message*, that includes a service option connection using Service Option 18 or 19, then the service option connection shall become part of the current service configuration at the action time associated with the *Service Connect Message*. Service Option 18 or 19 is considered connected when the current service configuration includes a service option connection for it.
- When the Service Option 18 or 19 is connected, the Service Option shall discard all primary traffic data bits received from the multiplex sublayer, and the base station should transmit null traffic channel data.
- The base station shall send the *OTAPA Request Message* with the START_STOP field set to '1' to the mobile station in order to start the OTAPA session in the mobile station.

4.3 Programming Data Download

4.3.1 OTA Data Message Processing

While in the CDMA *Conversation Substate* or the analog Conversation Task, the base station may send the messages prescribed below. If the base station sends a message requiring a response, the base station should wait for receipt of the appropriate response before sending further Over-the-Air Service Provisioning messages. If the base station does not receive a response to the message, it may retransmit the message.

If the base station receives any *OTASP Data Message* containing the RESULT_CODE = '00001010', "Rejected - Mobile station locked", or '00001011', "Rejected - Invalid SPC" or '00001101', "Rejected - Invalid SPASM", indicating that the mobile station parameters are locked (see 3.3.6 and 3.3.7), the base station may attempt to unlock the mobile station before continuing the programming procedure.

If the base station receives any message containing a RESULT_CODE indicating any other error condition, the base station may terminate the programming session, or select appropriate action to correct the error condition.

1. *Configuration Request Message**:* The base station should wait for a *Configuration Response Message*.
2. *Download Request Message:* The base station should wait for a *Download Response Message*.
3. *Commit Request Message:* The base station should wait for a *Commit Response Message*. Upon receipt of the *Commit Response Message* with the RESULT_CODE set to ‘00000000’, “Accepted - Operation successful,” the base station should update its stored database to include the activation information.
4. *Re-Authenticate Request Message:* The base station should wait for a *Re-Authenticate Response Message*.
5. *MS Key Request Message:* The base station should wait for an *MS Key Response Message*.
6. *Key Generation Request Message:* The base station should receive an *MS Key Response Message* with RESULT_CODE equal to ‘00000000’, “Accepted - Operation successful,” prior to sending this message. The base station should wait for a *Key Generation Response Message*.
7. *Protocol Capability Request Message:* The base station should wait for a *Protocol Capability Response Message* or an *Extended Protocol Capability Response Message*. The base station shall not send the *Protocol Capability Request Message* with additional fields to the mobile stations which don’t support the additional fields defined in Section 4.5.1.7[5].
8. *SSPR Configuration Request Message:* The base station should wait for an *SSPR Configuration Response Message*.
9. *SSPR Download Request Message:* The base station should wait for *an SSPR Download Response Message*.
10. *Validation Request Message:* The base station should wait for a *Validation Response Message*. The following procedures may be used:
    - In order to unlock the mobile station, the base station may send the Verify SPC Parameter Block with the SPC field set to the value of the Service Programming Code assigned to the mobile station.

~~[5] The base station may use the first 8 bits of the received value in the ESN field to determine if the mobile station is MEID-capable (i.e. MEID-capable mobile stations will have ‘10000000’ to indicate a pseudo ESN.).~~

- If the base station elects to change the value of the SPC assigned to the mobile station, the base station may send the Change SPC Parameter Block with the SPC field set to the value of the new Service Programming Code assigned to the mobile station. If the base station elects to permanently unlock the mobile station, the base station shall set the SPC field to the default value (see Table 3.3.6-1).

- In order to unlock the active mobile station NAM secured by SPASM, the base station may send the Validate SPASM Parameter Block.

  - If the programming session was initiated by the user as described in 3.2.1, the base station should not send this Parameter Block.

  - If the base station received the RAND_OTAPA value from the mobile station in the *OTAPA Response Message*, the base station should set the AUTH_OTAPA_INCL field to '1' and the AUTH_OTAPA field to the value computed by the base station as specified in 3.3.7.

  - If the base station did not receive the RAND_OTAPA value from the mobile station in the *OTAPA Response Message*, the base station may not send this Parameter Block. If the base station sends this Parameter Block, the base station should set the AUTH_OTAPA_INCL field to '0' and omit the AUTH_OTAPA field.

  - The base station should set the NAM_LOCK field to '1' to activate SPASM protection of programmable parameters and indicators of the active NAM for subsequent OTAPA session, otherwise the base station should set this field to '0'. SPASM protection specified by the value of the NAM_LOCK field will take effect for the subsequent OTAPA session if it is committed into the permanent mobile station memory during the current OTAPA session.

11. *OTAPA Request Message:* The base station should wait for *an OTAPA Response Message*. The following procedures may be used:

    - If the programming session was initiated by the user as described in 3.2.1, the base station should not send this message.

    - In order to invoke the OTAPA session in the mobile station, the base station shall set the START_STOP field to '1' in the message.

    - In order to terminate the OTAPA session in the mobile station, the base station shall set the START_STOP field to '0' in the message.

12. *PUZL Configuration Request Message*: The base station should wait for a *PUZL Configuration Response Message*.

13. *PUZL Download Request Message*: The base station should wait for a *PUZL Download Response Message*.

14. *3GPD Configuration Request Message*: The base station should wait for a *3GPD Configuration Response Message*.

15. *3GPD Download Request Message*: The base station should wait for a *3GPD Download Response Message*.

16. *Secure Mode Request Message:* The base station should wait for a *Secure Mode Response Message*. The following procedures may be used:
    - The base station shall generate the Secure Mode Ciphering Key (SMCK) as specified in 4.3.5. If SMCK generation is unsuccessful, the base station shall not send the message.
    - In order to invoke the Secure Mode in the mobile station, the base station shall set the START_STOP field to '1' and the RAND_SM field to a randomly selected 64-bit value used for generating the Secure Mode Ciphering Key SMCK (see 4.3.5). Upon receipt of the *Secure Mode Response Message* with the RESULT_CODE set to '00000000', "Accepted - Operation successful," the base station should activate the Secure Mode as specified in 4.3.5.
    - In order to terminate the Secure Mode in the mobile station, the base station shall set the START_STOP field to '0' in the message.

17. *MMD Configuration Request Message*: The base station should wait for a *MMD Configuration Response Message*.

18. *MMD Download Request Message*: The base station should wait for a *MMD Download Response Message*.

19. *System Tag Configuration Request Message:* The base station should wait for a *System Tag Configuration Response Message*.

20. *System Tag Download Request Message:* The base station should wait for a *System Tag Download Response Message*.

21. *Service Key Generation Request Message:* The base station should wait for a *Service Key Generation Response Message*.

22. *MMS Configuration Request Message*: The base station should wait for a *MMS Configuration Response Message*.

23. *MMS Download Request Message*: The base station should wait for a *MMS Download Response Message*.

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

4.3.2 SSD Update and re-authentication

Re-authentication is the process by which the base station instructs the mobile station to perform authentication and generate the Private Long Code Mask and Message Encryption parameters while on the CDMA Traffic channel or analog voice channel. The authentication key, A-key, should be generated in the mobile station during the present programming session.

The base station shall disable voice privacy and message encryption prior to performing re-authentication.

The Shared Secret Data, SSD, shall be generated prior to performing re-authentication. The procedure for setting the interface values and for generating the authentication signature, voice privacy and message encryption parameters, is described in 3.3.2.

4.3.3 Activation of Message Encryption

To enhance the security of the programming session and to protect sensitive subscriber information, the base station should enable message encryption (see 7.3.2 of [1] or 3.3.2 of [7]).

If message encryption was enabled or transition to the Private Long Code Mask was made (see 7.3.3 of [1] or 3.3.3 of [7]) before the re-authentication operation, message encryption parameters active at that time shall remain unchanged for the duration of the call.

Otherwise, message encryption parameters are re-calculated during the re-authentication operation. In this case, the data used to initialize the algorithm for calculating message encryption parameters is computed based on parameters in effect at the time the *Re-Authenticate Request Message* was sent.

Messages shall not be encrypted following an unsuccessful re-authentication.

4.3.4 Activation of Voice Privacy Mode

To enhance the security of the programming session and to protect sensitive subscriber information, the base station should enable voice privacy (see 7.3.3 of [1] or 3.3.3 of [7]).

If a transition to the Private Long Code Mask was made or signaling message encryption was activated (see 2.3.12.2.1 and 6.3.12.2 of [1] or 2.3.12.2 of [7]) before the re-authentication operation, the Private Long Code Mask active at that time shall remain unchanged for the duration of the call.

Otherwise, the Private Long Code Mask is recalculated during the re-authentication operation. In this case, the data used to initialize the algorithm for calculating the Private Long Code Mask is computed based on parameters in effect at the time the *Re-Authenticate Request Message* was sent.

Voice privacy shall not be enabled following an unsuccessful re-authentication.

4.3.5 Secure Mode

To enhance security of the programming session and to protect sensitive subscriber information, a method is provided to encrypt PARAM_DATA fields of Parameter Blocks in OTASP messages irrespective of the air interface message encryption described in 4.3.3. This method allows setting up a secure "tunnel" between the network based Over-The-Air Service Provisioning entity and the mobile station.

If the mobile station indicates its support for Secure Mode by setting appropriate feature-related fields in the *Protocol Capability Response Message*, the base station may activate the Secure Mode by sending the *Secure Mode Request Message* to the mobile station with the START_STOP field set to '1'.

Prior to initiating the Secure Mode, the base station should generate the Secure Mode Ciphering Key SMCK as specified in 4.3.5.1. The base station should not initiate the Secure Mode if generation of the SMCK is unsuccessful.

The base station shall use the SMCK as a key for encryption and decryption, as specified in 4.3.5.2, of all PARAM_DATA of all Parameter Blocks sent and received by the base station in the OTASP Data Messages while the Secure mode is active.

When encrypting the message, the base station should select a value of FRESH associated with this message and unique for the duration of Secure Mode session. The value of FRESH can be selected at random, or can be set to a monotonically increasing counter.

When decrypting the message, the base station should use the value of FRESH received in the message.

The base station can terminate the Secure Mode by sending the *Secure Mode Request Message* to the mobile station with the START_STOP field set to '0'. When Secure Mode session is terminated, the base station should reset the SMCK to NULL.

4.3.5.1 Generation of Secure Mode Ciphering Key

The Secure Mode Ciphering Key Generation SMCK is generated by the algorithmic function specified in Section 2.2.2.6 of [8].

If KEY_IN_USE = '0000', the input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to SSD-A|SSD-B.
- The fi parameter shall be set to 0x45.
- The RAND parameter shall be set to RAND_SM|RAND_SM.
- The Fmk parameter shall be set to 0x41484147.

If KEY_IN_USE = '0001',the input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to the 128-bit Root Key K.
- The fi parameter shall be set to 0x45.
- The RAND parameter shall be set to RAND_SM|RAND_SM.
- The Fmk parameter shall be set to 0x41484147.

The base station shall execute the Ciphering Key Generation Procedure as specified in 2.2.2.6 of [8]. The base station shall set SMCK to the computed 128-bit output of f3.

The base station shall set input parameter to the *ESP_privacykey Procedure* as follows:

- The *key* parameter shall be set to SMCK.

The base station shall execute the *ESP_privacykey Procedure*.

4.3.5.2 Encryption and Decryption of Messages in Secure Mode

Encryption and decryption of PARAM_DATA information is performed by the Enhanced Privacy Algorithm specified in 2.3.2.2 of [8].

The base station shall set input parameters to the Enhanced Privacy Algorithm as follows:

- If the base station presents the data for encryption, the base station shall set the *fresh* parameter to FRESH|’ 1’|BLOCK_ID; otherwise, if the base station presents the data for decryption, the base station shall set the *fresh* parameter to FRESH_r|’ 0’|BLOCK_ID;
- The *freshsize* parameter shall be set to 3;
- The *buf* parameter shall be set to the address of the octet containing the first bit of the buffer that contains the data to be encrypted or decrypted.
- The *bit_offset* parameter shall be set to the offset between the bit position of the most significant bit of the data to be encrypted/decrypted and the bit position of the most significant bit of the buffer (e.g., if the bit position of the most significant bit of the data to be encrypted/decrypted and the bit position of the most significant bit of the buffer are equal, *bit_offset* shall be set to 0).
- The *bit_count* parameter shall be set to the number of bits of the data to be encrypted/decrypted.

The base station shall execute the *ESP_maskbits Procedure*.

4.3.6 Generation of Service Keys

Generation of service keys consists of generating an intermediate key and using the intermediate key to generate service keys.

4.3.6.1 Generation of Intermediate Key

The Intermediate value ITM_RAND is generated by the algorithmic function specified in Section 2.2.2.2 of [8].

The input parameters to the algorithmic function *f0* shall be set as follows:

- The K parameter shall be set to RK_P.
- The fi parameter shall be set to 0x41.
- The Fmk parameter shall be set to 0x534B474B.

The base station shall execute f0 twice. ITM_RAND is set to the 128-bit output of f0.

4.3.6.2 Generation of Service Keys

For each bit in the bitmap as illustrated in Table 4.5.1.17-1 that is turned on, the base station shall generate the service key by invoking key generation function as specified in Section 2.2.2.6 of [8].

The input parameters to the algorithmic function *f3* shall be set as follows:

- The K parameter shall be set to ITM_RAND.
- The fi parameter shall be set to 0x45.
- The RAND parameter shall be set according to table 4.3.6.2-1, with remaining least significant bits padded with ‘0’, for each service requested.
- The Fmk parameter shall be set to 0x534B474B.

The base station shall execute f3 to produce 128-bit service root key.

Table 4.3.6.2-1 Key Identifier Table

Service Key Requested	**RAND Value**
IMS ROOT KEY	0x494D53
BCMCS ROOT KEY	0x42434D4353
WLAN ROOT KEY	0x574C414E

4.4 Termination of the Programming Procedure

The programming session ends when the OTAPA service option is disconnected.

If the programming session was initiated by the network as described in 3.2.2, and if the base station processes the incoming call directed to the mobile station during the OTAPA process, the base station shall perform the following:

1. If either the mobile station or the base station does not support concurrent services the base station shall disconnect the OTAPA session and may release the traffic channel prior to connecting the incoming call.
2. If both the mobile station and base station supports concurrent service then the base station may disconnect the OTAPA session and may release the traffic channel prior to connecting the incoming call.

If the programming session was initiated by the network as described in 3.2.2, the base station may terminate the OTAPA session by sending the *OTAPA Request Message* to the mobile station with the START_STOP field set to ‘0’.

4.5 Forward Link Message Formats

The forward link *OTASP Data Messages* are summarized in Table 4.5-1.

Table 4.5-1 Forward Link Messages

Message Name	OTASP_MSG_TYPE	Reference
Configuration Request Message	‘00000000’	4.5.1.1
Download Request Message	‘00000001’	4.5.1.2
MS Key Request Message	‘00000010’	4.5.1.3
Key Generation Request Message	‘00000011’	4.5.1.4
Re-Authenticate Request Message	‘00000100’	4.5.1.5
Commit Request Message	‘00000101’	4.5.1.6
Protocol Capability Request Message	‘00000110’	4.5.1.7
SSPR Configuration Request Message	‘00000111’	4.5.1.8
SSPR Download Request Message	‘00001000’	4.5.1.9
Validation Request Message	‘00001001’	4.5.1.10
OTAPA Request Message	‘00001010’	4.5.1.11
PUZL Configuration Request Message	‘00001011’	4.5.1.12
PUZL Download Request Message	‘00001100’	4.5.1.13
3GPD Configuration Request Message	'00001101'	4.5.1.14
3GPD Downloaded Request Message	'00001110'	4.5.1.15
Secure Mode Request Message	‘00001111’	4.5.1.16
Reserved	‘00010000’	
MMD Configuration Request Message	‘00010001’	4.5.1.18
MMD Download Request Message	‘00010010’	4.5.1.19
System Tag Configuration Request Message	‘00010011’	4.5.1.20
System Tag Download Request Message	‘00010100’	4.5.1.21

Service Key Generation Request Message	‘00010101’	4.5.1.22
MMS Configuration Request Message	‘00010110’	4.5.1.23
MMS Download Request Message	‘00010111’	4.5.1.24
Reserved for future standardization	‘00011000’ through ‘10111111’	
Available for manufacturer-specific *OTASP Data Message* definition	‘11000000’ through ‘11111110’	See [4]
Reserved	‘11111111’	

4.5.1 Message Contents

4.5.1.1 Configuration Request Message

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

Field	Length (bits)
OTASP_MSG_TYPE (‘00000000’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following field:	
BLOCK_ID	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000000’.

NUM_BLOCKS - Number of parameter blocks requested.

The base station shall set this field to the number of parameter blocks requested.

BLOCK_ID - Parameter block identifier.

The base station shall include NUM_BLOCKS occurrences of this field. The base station shall set each field to the value of the parameter block type requested (see Table 3.5.2-1).

4.5.1.2 Download Request Message

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

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00000001’)	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following parameter block:

BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000001’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *Download Request Message*.

BLOCK_ID - Parameter block identifier.

The base station shall include NUM_BLOCKS occurrences of this field. The base station shall set each field to the value of the parameter block type requested (see Table 4.5.2-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block (see 4.5.2) specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA fields shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall include this field and set it to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1’, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.1.3 MS Key Request Message

The *MS Key Request Message* has the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00000010’)	8
A_KEY_P_REV	8
PARAM_P_LEN	0 or 8
PARAM_P	0 or 8 × PARAM_P_LEN
PARAM_G_LEN	0 or 8
PARAM_G	0 or 8 × PARAM_G_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000010’.

A_KEY_P_REV - Key exchange protocol version.

The base station shall set this field to ‘00000010’ for 2G A-key generation, ‘00000011’ for combination 2G A-key and 3G Root Key generation, ‘00000100’ for 3G Root Key generation, or ‘00000101’ for Enhanced 3G Root Key generation.

PARAM_P_LEN - Length of PARAM_P field.

If A_KEY_P_REV = ‘00000010’, the base station shall set this field to the number of octets in the PARAM_P field, and the base station shall set this field to ‘01000000’. If A_KEY_P_REV > ‘00000010’, the base station shall omit this field.

PARAM_P - Key exchange parameter P.

If A_KEY_P_REV = ‘00000010’, the base station shall set this field as described in 5.2.1. If A_KEY_P_REV > ‘00000010’, the base station shall omit this field.

PARAM_G_LEN - Length of PARAM_G field.

If A_KEY_P_REV = ‘00000010’, the base station shall set this field to the number of octets in the PARAM_G field, and the base station shall set this field to ‘00010100’. If A_KEY_P_REV > ‘00000010’, the base station shall omit this field.

PARAM_G - Key exchange parameter G.

If A_KEY_P_REV = ‘00000010’, the base station shall set this field as described in 5.2.1. If A_KEY_P_REV > ‘00000010’, the base station shall omit this field.

4.5.1.4 Key Generation Request Message

The *Key Generation Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000011’)	8
BS_RESULT_LEN	8
BS_RESULT	8 × BS_RESULT_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000011’.

BS_RESULT_LEN - Length of BS_RESULT field.

The base station shall set this field to the number of octets in the BS_RESULT field.

BS_RESULT - Base station calculation result.

If A_KEY_P_REV = ‘00000010’, the base station shall set this field equal to the value of BS_RESULT as described in 5.2.2. If A_KEY_P_REV = ‘00000011’ or ‘00000100’, the base station shall set this field equal to the value of BS_RESULT as described in 5.4.2. If A_KEY_P_REV = ‘00000101’, the base station shall set this field equal to the value of BS_RESULT as described in 5.6.2.

4.5.1.5 Re-Authenticate Request Message

The *Re-Authenticate Request Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000100’)	8
RAND	32

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000100’.

RAND - Random Challenge value.

The base station shall set this field to the value used as an input to the Auth_Signature procedure for performing re-authentication. See 3.3.2.

4.5.1.6 Commit Request Message

The *Commit Request Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00000101’)	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000101’.

4.5.1.7 Protocol Capability Request Message

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

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

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000110’.

OTASP_P_REV - OTASP protocol revision.

If the ~~mobile~~*base* station *does not request new capability information records as defined in Table 3.5.1.17.1-1*~~is not MEID capable (See footnote 3)~~, the base station shall omit this field; otherwise, the base station shall set this field to ‘00000100’.

NUM_CAP_RECORDS - Number of Capability Records.

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

CAP_RECORD_TYPE - Capability Record Type.

If *OTASP_P_REV field is not included*~~the mobile station is not~~

~~MEID capable (See footnote 3)~~, the base station shall omit this field; otherwise, the base station shall set this field to the record type value shown in Table 3.5.1.17.1-1 corresponding to the information record requested.

4.5.1.8 SSPR Configuration Request Message

The *SSPR Configuration Request Message* has the following variable-length format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00000111’)	8
BLOCK_ID	8

If BLOCK_ID = ‘00000001’ (Preferred Roaming List Parameter Block), the message also includes the following fields:

REQUEST_OFFSET	16
REQUEST_MAX_SIZE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00000111’.

BLOCK_ID Parameter block identifier.

The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message (see Table 3.5.3-1).

If the BLOCK_ID field is set to ‘00000001’ (Preferred Roaming List Parameter Block), the base station shall include the following fields in the message:

REQUEST_OFFSET - Segment offset.

The base station shall set this field to the starting offset within the preferred roaming list (PR_LIST_{S-P}) of the octets being requested.

REQUEST_MAX_SIZE - Maximum segment size.

The base station shall set this field to the maximum number of preferred roaming list octets that the mobile station is to return.

4.5.1.9 SSPR Download Request Message

The *SSPR Download Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001000’)	8
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001000’.

BLOCK_ID Parameter block identifier.

The base station shall set this field to the value of the parameter block type being downloaded (see Table 4.5.3-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data.

The base station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA field shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall set this field to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA field of the message.

If FRESH_INCL = ‘1’, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA field of the Parameter Data block included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.1.10 Validation Request Message

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

Field	Length (bits)
OTASP_MSG_TYPE (‘00001001’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001001’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *Validation Request Message*.

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the parameter block type being included in the message (see Table 4.5.4-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block specified by the BLOCK_ID field.

4.5.1.11 OTAPA Request Message

The *OTAPA Request Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001010’)	8
START_STOP	1
RESERVED	7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001010’.

START_STOP - OTAPA session start-stop indicator.

The base station shall set this field to ‘1’ to invoke the OTAPA session in the mobile station. The base station shall set this field to ‘0’ to terminate the OTAPA session in the mobile station.

RESERVED - Reserved bits.

The base station shall set this field to ‘0000000’.

4.5.1.12 PUZL Configuration Request Message

The *PUZL Configuration Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001011’)	8
BLOCK_ID	8

If BLOCK_ID = ‘00000001’ (PUZL Priorities Parameter Block), the message also includes the following fields:

REQUEST_INDEX	12
REQUEST_MAX_ENTRIES	8
RESERVED	4

If BLOCK_ID = ‘00000010’ (User Zone Parameter Block), the message also includes the following fields:

UZ_ID	16
UZ_SID	15
REQUEST_OFFSET	12
REQUEST_MAX_SIZE	8
RESERVED	5

If BLOCK_ID = ‘00000011’ (Preferred User Zone List Parameter Block), the message also includes the following fields:

REQUEST_INDEX	12
REQUEST_OFFSET	12
REQUEST_MAX_SIZE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001011’.

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message [see Table 3.5.6-1].

If the BLOCK_ID field is set to '00000001' (PUZL Priorities Parameter Block), the base station shall include the following fields in the message:

REQUEST_INDEX - Starting index.

The base station shall set this field to the index value of the starting user zone entry in the preferred user zone list. The starting value of this index shall be set to '000000000001'

REQUEST_MAX_ENTRIES- Maximum number of entries.

The base station shall set this field to the maximum number of user zone entries to be returned by the mobile station.

RESERVED - Reserved bits.

The base station shall set this field to '0000'.

If the BLOCK_ID field is set to '00000010' (User Zone Parameter Block), the base station shall include the following fields in the message:

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

REQUEST_OFFSET - Segment offset.

The base station shall set this field to the starting offset, in octets, within the requested user zone entry of the preferred user zone list ($PUZL_{s-p}$).

REQUEST_MAX_SIZE - Maximum segment size.

The base station shall set this field to the maximum number of user zone entry octets that the mobile station is to return.

RESERVED - Reserved bits.

The base station shall set this field to '00000'.

If the BLOCK_ID field is set to '00000011' (Preferred User Zone List Parameter Block), the base station shall include the following fields in the message:

REQUEST_INDEX - Starting index

The base station shall set this field to the index value of the starting user zone entry in the preferred user zone list. The starting value of this index shall be set to '000000000001'

REQUEST_OFFSET - Segment offset.

The base station shall set this field to the starting offset, in octets, within the requested user zone entry (identified by REQUEST_INDEX) of the preferred user zone list ($PUZL_{s-p}$).

REQUEST_MAX_SIZE - Maximum segment size.

The base station shall set this field to the maximum number of user zone entry octets that the mobile station is to return.

4.5.1.13 PUZL Download Request Message

The *PUZL Download Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001100’)	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following parameter block:

BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001100’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *PUZL Download Request Message*.

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the parameter block type being included in the message (see Table 4.5.6-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA fields shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall set this field to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL= ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.1.14 3GPD Configuration Request Message

The *3GPD Configuration Request Message* has the following format:

Field	**Length (bits)**
OTASP_MSG_TYPE (‘00001101’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following fields:	
BLOCK_ID	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001101’.

NUM_BLOCKS - Number of parameter blocks requested.

The base station shall set this field to the number of parameter blocks requested.

The base station shall include NUM_BLOCKS occurrences of the following field:

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message (see Table 3.5.8-1).

4.5.1.15 3GPD Download Request Message

The *3GPD Download Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001110’)	8
NUM_BLOCKS	8

NUM_BLOCKS occurrences of the following parameter block:

BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001110’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *3GPD Download Request Message*.

The base station shall include NUM_BLOCKS occurrences of the following fields:

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the parameter block type being included in the message (see Table 4.5.7-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA fields shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall include this field and set it to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1’, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL = ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.1.16 Secure Mode Request Message

The *Secure Mode Request Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00001111’)	8
START_STOP	1
KEY_IN_USE	4
RESERVED	3
RAND_SM	0 or 64

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00001111’.

START_STOP - Secure Mode start-stop indicator.

The base station shall set this field to ‘1’ to invoke the Secure Mode in the mobile station. The base station shall set this field to ‘0’ to terminate the Secure Mode in the mobile station.

KEY_IN_USE - Key in use indicator.

If the START_STOP is set to ‘1’, the base station shall set this field to ‘0000’ to indicate SMCK generation using SSD_A and SSD_B, or ‘0001’ to indicate SMCK generation using 3G Root Key, otherwise, this field shall be set to ‘0000’.

RESERVED - Reserved bits.

The base station shall set all the bits of this field to ‘0’.

RAND_SM - Random Number used for SMCK generation.

If the START_STOP is set to ‘1’, the base station shall set this field to a randomly selected 64-bit value used for generation of the SMCK. If the START_STOP is set to ‘0’, the base station shall omit this field.

4.5.1.17 Reserved

4.5.1.18 MMD Configuration Request Message

The *MMD Configuration Request Message* has the following format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010001’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following fields:	
BLOCK_ID	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010001’.

NUM_BLOCKS - Number of parameter blocks requested.

The base station shall set this field to the number of parameter blocks requested.

The base station shall include NUM_BLOCKS occurrences of the following field:

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message (see Table 3.5.9-1).

4.5.1.19 MMD Download Request Message

The *MMD Download Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010010’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010010’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *MMD Download Request Message*.

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the parameter block type being included in the message (see Table 4.5.8-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA fields shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall set this field to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL= ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.1.20 System Tag Configuration Request Message

The *System Tag Configuration Request Message* shall have the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010011’)	8
BLOCK_ID	8
If BLOCK_ID = ‘00000001’ (System Tag List Parameter Block), the message also includes the following fields:	
REQUEST_OFFSET	16
REQUEST_MAX_SIZE	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010011’.

BLOCK_ID Parameter block identifier.

The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message (see Table 3.5.10-1).

If the BLOCK_ID field is set to ‘00000001’ (System Tag List Parameter Block), the base station shall include the following fields in the message:

REQUEST_OFFSET - Segment offset.

The base station shall set this field to the starting offset within the group tag list (GROUP_TAG_ LIST$_{s\text{-}p}$), specific tag list (SPEC_TAG_ LIST$_{s\text{-}p}$), or call prompt list (CALL_PRMPT_ LIST$_{s\text{-}p}$) of the octets being requested.

REQUEST_MAX_SIZE - Maximum segment size.

The base station shall set this field to the maximum number of system tag list octets that the mobile station is to return.

4.5.1.21 System Tag Download Request Message

The *System Tag Download Request Message* shall have the following format

Field	Length (bits)
OTASP_MSG_TYPE (‘00010100’)	8
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010100’.

BLOCK_ID Parameter block identifier.

The base station shall set this field to the value of the parameter block type being downloaded (see Table 4.5.9-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data.

The base station shall include the parameter block specified by the BLOCK_ID field.

4.5.1.22 Service Key Generation Request Message

The *Service Key Generation Request Message* has the following fixed-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010101’)	8
KEY_ID	12
RESERVED	4

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010101’.

KEY_ID - Key exchange identifier.

The base station shall set this field corresponding to the key requested as shown in Table 4.5.1.17-1 in the form of a bitmap; otherwise, the base station shall omit this field.

Table 4.5.1.22-1 Key Identifier Table

Subfield	Length (bits)
IMS Root Key	1
BCMCS Root Key	1
WLAN Root Key	1
RESERVED	9

RESERVED - Reserved bits.

The base station shall set all bits of this field ‘0’.

4.5.1.23 MMS Configuration Request Message

The *MMS Configuration Request Message* has the following format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010110’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following fields:	
BLOCK_ID	8

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010110’.

NUM_BLOCKS - Number of parameter blocks requested.

The base station shall set this field to the number of parameter blocks requested.

The base station shall include NUM_BLOCKS occurrences of the following field:

BLOCK_ID - Parameter block identifier.
The base station shall set this field to the value of the BLOCK_ID of the parameter block being requested in this message (see Table 3.5.12-1).

4.5.1.24 MMS Download Request Message

The *MMS Download Request Message* has the following variable-length format:

Field	Length (bits)
OTASP_MSG_TYPE (‘00010111’)	8
NUM_BLOCKS	8
NUM_BLOCKS occurrences of the following parameter block:	
BLOCK_ID	8
BLOCK_LEN	8
PARAM_DATA	8 × BLOCK_LEN
FRESH_INCL	1
FRESH	0 or 15
RESERVED	0 or 7

OTASP_MSG_TYPE - *OTASP Data Message* type.

The base station shall set this field to ‘00010111’.

NUM_BLOCKS - Number of parameter blocks.

The base station shall set this field to the number of parameter blocks contained in the *MMS Download Request Message*.

BLOCK_ID - Parameter block identifier.

The base station shall set this field to the value of the parameter block type being included in the message (see Table 4.5.10-1).

BLOCK_LEN - Parameter block length.

The base station shall set this field to the number of octets in the parameter block, not including the BLOCK_ID and BLOCK_LEN fields.

PARAM_DATA - Parameter data fields.

The base station shall include the parameter block specified by the BLOCK_ID field. If Secure Mode is active (see 4.3.5), PARAM_DATA fields shall be encrypted as specified in 4.3.5.

FRESH_INCL - FRESH included indicator.

If Secure Mode is active (See 4.3.5), the base station shall set this field to ‘1’; otherwise the base station shall set this field to ‘0’.

FRESH - Cryptographic Synchronizer (crypto-sync) selected for encrypting PARAM_DATA fields of the message.

If FRESH_INCL = ‘1’, the base station shall include this field and set it to a 15-bit value chosen as specified in 4.3.5 for encrypting the PARAM_DATA fields of all Parameter Data blocks included in the message; otherwise the base station shall omit this field.

RESERVED - Reserved bits.

If FRESH_INCL= ‘1’, the base station shall omit this field; otherwise, the base station shall set all the bits of this field to ‘0’.

4.5.2 NAM Parameter Blocks

Table 4.5.2-1 lists the types of parameter blocks used in the *Download Request Message* and the *Download Response Message.*

Table 4.5.2-1 NAM Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
CDMA/Analog NAM Download	'00000000'	4.5.2.1
Mobile Directory Number	'00000001'	4.5.2.2
CDMA NAM Download	'00000010'	4.5.2.3
IMSI_T	'00000011'	4.5.2.4
Reserved for future standardization	'00000100' through '01111111'	
Available for manufacturer-specific parameter block definitions	'10000000' through '11111110'	See [4]
Reserved	'11111111'	

4.5.2.1 CDMA/Analog NAM Download

The PARAM_DATA field of the CDMA/Analog NAM Download Parameter Block consists of the following fields:

Field	**Length (bits)**
FIRSTCHP	11
HOME_SID	15
EX	1
IMSI_M_CLASS	1
IMSI_M_ADDR_NUM	3
MCC_M	10
IMSI_M_11_12	7
IMSI_M_S	34
ACCOLC	4
LOCAL_CONTROL	1
MOB_TERM_HOME	1
MOB_TERM_FOR_SID	1
MOB_TERM_FOR_NID	1
N_SID_NID	8
N_SID_NID occurrences of the following SID/NID pair:	
SID	15
NID	16
The parameter block ends with the following field:	
RESERVED	0 to 7 (as needed)

FIRSTCHP - First paging channel used in the home system.

The base station shall set this field to the value for the FIRSTCHP_p mobile station NAM indicator (see F.3 of [1, 7]).

HOME_SID - Home system identification.

The base station shall set this field to the value for the HOME_SID_p mobile station NAM indicator (see F.3 of [1, 7]).

EX - Extended address indicator.

The base station shall set this field to the value for the EX_p mobile station NAM indicator (see F.3 of [1, 7]).

IMSI_M_CLASS - IMSI_M Class assignment of the mobile station.

If the base station is assigning a class 0 IMSI_M to the mobile station, the base station shall set this field to ‘0’; otherwise the base station shall set this field to ‘1’.

IMSI_M_ADDR_NUM - Number of IMSI_M address digits.

If the mobile station has been assigned a class 1 IMSI_M (see 6.3.1 of [1] or 2.3.1 of [7]), the base station shall set this field to four less than the number of digits in the NMSI; otherwise, the base station shall set this field to ‘000’.

MCC_M - Mobile country code of the IMSI_M.

The base station shall set this field to the value for the MCC_M$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_11_12 - 11th and 12th digits of the IMSI_M.

The base station shall set this field to the value for the IMSI_M_11_12$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7].

IMSI_M_S - The least significant 10 digits of the IMSI_M.

The base station shall set this field to the value for the IMSI_M_S$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

ACCOLC - Access overload class.

The base station shall set this field to the value for the ACCOLC$_p$ mobile station NAM indicator (see F.3 of [1, 7]).

LOCAL_CONTROL - Local control status.

The base station shall set this field to ‘1’ to enable local control status in the mobile station, or to ‘0’ to disable local control status (see 2.6.1.2.2 of [1]).

MOB_TERM_HOME - Termination indicator for the home system.

The base station shall set this field to the value for the MOB_TERM_HOME$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

MOB_TERM_FOR_SID - Termination indicator for SID roaming.

The base station shall set this field to the value for the MOB_TERM_FOR_SID$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

MOB_TERM_FOR_NID - Termination indicator for NID roaming.

The base station shall set this field to the value for the MOB_TERM_FOR_NID$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

N_SID_NID - Number of SID/NID pairs.

The base station shall set this field to the number of SID/NID pairs included in the parameter block. The base station shall include at least one SID/NID pair.

SID - System identification.

The base station shall set this field to the value of the SID component of the SID/NID pair (see F.3 of [1, 7]).

NID - Network identification.

The base station shall set this field to the value of the NID component of the SID/NID pair (see F.3 of [1, 7]).

RESERVED - Reserved bits.

The base station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to '0'.

4.5.2.2 Mobile Directory Number

The PARAM_DATA field of the Mobile Directory Number Parameter Block consists of the following fields:

Field	Length (bits)
N_DIGITS	4
N_DIGITS occurrences of the following field:	
DIGITn	4
The parameter block ends with the following field:	
RESERVED	0 or 4

N_DIGITS - Number of digits.

The base station shall set this field to the number of digits included in the parameter block.

DIGITn - Digit.

The base station shall set these fields to the digits of the mobile station directory number. Each digit shall be encoded according to Table 6.7.1.3.2.4-4 of [1] or Table 2.7.1.3.2.4.4 of [7].

RESERVED - Reserved bits.

The base station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to '0'.

4.5.2.3 CDMA NAM Download

The PARAM_DATA field of the CDMA NAM Download Parameter Block consists of the following fields:

Field	Length (bits)
IMSI_M_CLASS	1
IMSI_M_ADDR_NUM	3
MCC_M	10
IMSI_M_11_12	7
IMSI_M_S	34
ACCOLC	4
LOCAL CONTROL	1
MOB_TERM_HOME	1
MOB_TERM_FOR_SID	1
MOB_TERM_FOR_NID	1
N_SID_NID	8
N_SID_NID occurrences of the following SID/NID pair:	
SID	15
NID	16
The parameter block ends with the following field:	
RESERVED	0 to 7 (as needed)

IMSI_M_CLASS - IMSI_M Class assignment of the mobile station.

If the base station is assigning a class 0 IMSI_M to the mobile station, the base station shall set this field to ‘0’; otherwise the base station shall set this field to ‘1’.

IMSI_M_ADDR_NUM - Number of IMSI_M address digits.

If the mobile station has been assigned a class 1 IMSI_M (see 6.3.1 of [1] or 2.3.1 of [7]), the base station shall set this field to four less than the number of digits in the NMSI; otherwise, the base station shall set this field to ‘000’.

MCC_M - Mobile country code of the IMSI_M.

The base station shall set this field to the value for the MCC_M_p mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_11_12 - 11th and 12th digits of the IMSI_M.

The base station shall set this field to the value for the IMSI_M_11_12$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_M_S - The least significant 10 digits of the IMSI_M.

The base station shall set this field to the value for the IMSI_M_S$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

ACCOLC - Access overload class.

The base station shall set this field to the value for the ACCOLC$_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

LOCAL CONTROL - Local control status.

The base station shall set this field to '1' to enable local control status in the mobile station, or to '0' to disable local control status (see 6.3.9 of [1] or 2.3.9 of [7]).

MOB_TERM_HOME - Termination indicator for the home system.

The base station shall set this field to the value for the MOB_TERM_HOME$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

MOB_TERM_FOR_SID - Termination indicator for SID roaming.

The base station shall set this field to the value for the MOB_TERM_FOR_SID$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

MOB_TERM_FOR_NID - Termination indicator for NID roaming.

The base station shall set this field to the value for the MOB_TERM_FOR_NID$_p$ mobile station NAM indicator (see F.3 and 6.6.5.3 of [1] or F.3 and 2.6.5.3 of [7]).

N_SID_NID - Number of SID/NID pairs.

The base station shall set this field to the number of SID/NID pairs included in the parameter block. The base station shall include at least one SID/NID pair.

SID - System identification.

The base station shall set this field to the value of the SID component of the SID/NID pair (see F.3 of [1, 7]).

NID - Network identification.

The base station shall set this field to the value of the NID component of the SID/NID pair (see F.3 of [1, 7]).

RESERVED - Reserved bits.

The base station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to '0'.

4.5.2.4 IMSI_T Parameter Block

The PARAM_DATA field of the IMSI_T Parameter Block consists of the following fields:

Field	**Length (bits)**
IMSI_T_CLASS	1
IMSI_T_ADDR_NUM	3
MCC_T	10
IMSI_T_11_12	7
IMSI_T_S	34
RESERVED	1

IMSI_T_CLASS - IMSI_T Class assignment of the mobile station.

If the base station is assigning a class 0 IMSI_T to the mobile station, the base station shall set this field to ‘0’; otherwise the base station shall set this field to ‘1’.

IMSI_T_ADDR_NUM - Number of IMSI_T address digits.

If the mobile station has been assigned a class 1 IMSI_T (see 6.3.1 of [1] or 2.3.1 of [7]), the base station shall set this field to four less than the number of digits in the NMSI; otherwise, the base station shall set this field to ‘000’.

MCC_T - Mobile country code of the IMSI_T.

The base station shall set this field to the value for the MCC_T_p mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

IMSI_T_11_12 - 11th and 12th digits of the IMSI_T.

The base station shall set this field to the value for the $IMSI\_T\_11\_12_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7])).

IMSI_T_S - The least significant 10 digits of the IMSI_T.

The base station shall set this field to the value for the $IMSI\_T\_S_p$ mobile station NAM indicator (see F.3 and 6.3.1 of [1] or F.3 and 2.3.1 of [7]).

RESERVED - Reserved bits.

The base station shall set this field to ‘0’.

4.5.3 SSPR Parameter Blocks

Table 4.5.3-1 lists the type of the parameter blocks used in the *SSPR Download Request Message* and the *SSPR Download Response Message*.

Table 4.5.3-1 SSPR Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
Preferred Roaming List	‘00000000’	4.5.3.1
Extended Preferred Roaming List with SSPR_P_REV greater than ‘00000001’	‘00000001’	4.5.3.1
Reserved for future standardization	‘00000010’ through ‘01111111’	
Available for manufacturer-specific parameter block definitions	‘10000000’ through ‘11111110’	See [4]
Reserved	‘11111111’	

4.5.3.1 Preferred Roaming List Parameter Block

The PARAM_DATA field of the Preferred Roaming List and Extended Preferred Roaming List Parameter Block consists of the following fields:

Field	Length (bits)
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	8 × SEGMENT_SIZE

RESERVED - Reserved bits.

The base station shall set this field to ‘0000000’.

LAST_SEGMENT - Last segment indicator bit.

The base station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the preferred roaming list (PR_LIST_{S-P}) sent to the mobile station; otherwise, the base station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The base station shall set this field to the starting offset, within the preferred roaming list at which the mobile station is to store the octets included in SEGMENT_DATA.

SEGMENT_SIZE - Segment size.

The base station shall set this field to the number of octets of the preferred roaming list included in SEGMENT_DATA.

SEGMENT_DATA - Segment data.

The base station shall set this field to sequential octets of the preferred roaming list. The octets shall be those starting at the offset within the preferred roaming list specified by SEGMENT_OFFSET.

4.5.4 Validation Parameter Blocks

Table 4.5.4-1 lists the types of parameter blocks used in the *Validation Request Message* and the *Validation Response Message*.

Table 4.5.4-1 Validation Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
Verify SPC	'00000000'	4.5.4.1
Change SPC	'00000001'	4.5.4.2
Validate SPASM	'00000010'	4.5.4.3
Reserved for future standardization	'00000011' through '01111111'	
Available for manufacturer-specific parameter block definitions	'10000000' through '11111110'	See [4]
Reserved	'11111111'	

4.5.4.1 Verify SPC

The PARAM_DATA field of the Verify SPC Parameter Block consists of the following field:

Field	Length (bits)
SPC	24

SPC - Service programming code.

The base station shall set this field to the BCD coded value of Service Programming Code assigned for the mobile station (see Table 3.3.6-1). Each digit shall be encoded according to the Table 4.5.4.1-1.

Table 4.5.4.1-1. BCD Mapping

Decimal Digit	Binary Number
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

4.5.4.2 Change SPC

The PARAM_DATA field of the Change SPC Parameter Block consists of the following field:

Field	Length (bits)
SPC	24

SPC - Service programming code

The base station shall set this field to the BCD coded value of newly assigned Service Programming Code for the mobile station (see Table 3.3.6-1). Each digit shall be encoded according to the Table 4.5.4.1-1.

4.5.4.3 Validate SPASM

The PARAM_DATA field of the Validate SMASM Parameter Block consists of the following fields:

Field	Length (bits)
AUTH_OTAPA_INCL	1
AUTH_OTAPA	0 or 18
NAM_LOCK	1
RESERVED	4 or 6

AUTH_OTAPA_INCL - OTAPA SPASM validation signature included indicator.

The base station shall set this field to '1' to indicate that the OTAPA SPASM validation signature, AUTH_OTAPA, is included in the message; otherwise, the base station shall set this field to '0'.

AUTH_OTAPA - OTAPA SPASM validation signature.

If the AUTH_OTAPA_INCL is set to '1', the base station shall set this field as described in 3.3.7; otherwise, the base station shall omit this field.

NAM_LOCK - SPASM protection indicator for the active NAM.

The base station shall set this field to '1' to activate SPASM protection of programmable parameters and indicators of the active NAM after completion of the current OTAPA session, otherwise the base station shall set this field to '0'.

RESERVED - Reserved bits.

The base station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to '0'.

4.5.5 Reserved

Reserved.

4.5.6 PUZL Parameter Blocks

Table 4.5.6-1 lists the types of parameter blocks used in the *PUZL Download Request Message* and the *PUZL Download Response Message*.

Table 4.5.6-1 PUZL Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
User Zone Insert	‘00000000’	4.5.6.1
User Zone Update	‘00000001’	4.5.6.1
User Zone Delete	‘00000010’	4.5.6.2
User Zone Priority Change	‘00000011’	4.5.6.3
PUZL Flags	‘00000100’	4.5.6.4
Reserved for future standardization	‘00000101’ through ‘01111111’	
Available for manufacturer-specific parameter block definitions	‘10000000’ through ‘11111110’	See [4]
Reserved	‘11111111’	

4.5.6.1 User Zone Insert and User Zone Update

The PARAM_DATA field of the User Zone Insert and User Zone Update Parameter Blocks consists of the following fields:

Field	Length (bits)
UZ_ID	16
UZ_SID	15
LAST_SEGMENT	1
SEGMENT_OFFSET	12
RESERVED	4
SEGMENT_SIZE	8
SEGMENT_DATA	8 × SEGMENT_SIZE

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

LAST_SEGMENT - Last segment indicator bit.

The base station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the user zone entry; otherwise, the base station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The base station shall set this field to the starting offset, within the user zone entry at which the mobile station is to store the octets included in SEGMENT_DATA. The first octet of the user zone entry is offset zero.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘0000’.

SEGMENT_SIZE - Segment size.

The base station shall set this field to the number of octets of the user zone included in SEGMENT_DATA.

SEGMENT_DATA - Segment data.

Segment of the user zone data.

4.5.6.2 User Zone Delete

The PARAM_DATA field of the User Zone Delete Parameter Block consists of the following fields:

Field	**Length (bits)**
UZ_ID	16
UZ_SID	15
RESERVED	1

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

RESERVED - Reserved bit.

The base station shall set this field to ‘0’.

4.5.6.3 User Zone Priority Change

The PARAM_DATA field of the User Zone Priority Change Parameter Block consists of the following fields:

Field	Length (bits)
UZ_ID	16
UZ_SID	15
UZ_PRIORITY	4
RESERVED	5

UZ_ID - User Zone ID.

Identification number for the User Zone. This is used over the air interface to identify the User Zone to the network and the mobile station.

UZ_SID - User Zone System ID.

The System Identifier (SID) associated with the User Zone ID. The User Zone ID and User Zone SID values together provide a unique identifier for the user zone.

UZ_PRIORITY - User Zone priority.

The priority by which User Zones are selected by the mobile station when more than one User Zone is present. A priority of null indicates that a User Zone is for manual selection only. A mobile station will never automatically select a User Zone of priority ‘null’ unless initiated manually by the user. Note that the value of User Zone Priority is non-exclusive. Normally two User Zones of the same priority would not occupy the same geographical area. When two User Zones of the same priority overlap and they are the highest priority to be selected, the mobile station shall offer the user a choice of the user zones via the Mobile Station's user interface.

RESERVED - Reserved bits.

The base station shall set this field to ‘00000’.

4.5.6.4 PUZL Flags

The PARAM_DATA field of the PUZL Flags Parameter Block consists of the following fields:

Field	Length (bits)
UZ_TEMP_SUBSC	1
UZ_ORIG_ONLY	1
RESERVED	6

UZ_TEMP_SUBSC - User Zone Temporary Subscription flag.

The base station shall set this field accordingly to indicate whether or not the mobile station is permitted to access User Zones that offer temporary subscription. If allowed, UZ_TEMP_SUBSC = ‘1’; otherwise, UZ_TEMP_SUBSC = ‘0’.

UZ_ORIG_ONLY - User Zone Origination Only flag.

The base station shall set this field accordingly to indicate whether or not the mobile station is permitted to originate calls only when within the serving area of a currently assigned User Zone. If call origination is only allowed within an assigned user zone, UZ_ORIG_ONLY = ‘1’; otherwise, UZ_ORIG_ONLY = ‘0’.

RESERVED - Reserved bits.

The base station shall set this field to ‘000000’.

4.5.7 3GPD Parameter Blocks

Table 4.5.7-1 lists the types of parameter blocks used in the *3GPD Download Request Message* and the *3GPD Download Response Message.*

Table 4.5.7-1 3GPD Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
3GPD Operation Mode Parameters	‘00000000’	4.5.7.1
SimpleIP User Profile Parameters	‘00000001’	4.5.7.2
Mobile IP User Profile Parameters	‘00000010’	4.5.7.3
SimpleIP Status Parameters	‘00000110’	4.5.7.4
MobileIP Status Parameters	‘00000111’	4.5.7.5
SimpleIP PAP SS Parameters[1]	‘00001000’	4.5.7.6
SimpleIP CHAP SS Parameters[1]	‘00001001’	4.5.7.7
MobileIP SS Parameters[1]	‘00001010’	4.5.7.8
HRPD Access Authentication User Profile Parameters	‘00001011’	4.5.7.9
HRPD Access Authentication CHAP SS Parameters[1]	‘00001100’	4.5.7.10
Reserved	‘00001101’ through ‘11111111’	
[1] The shared secret parameters shall not be transmitted over the air unencrypted.		

4.5.7.1 3GPD Operation Mode Parameters

The PARAM_DATA field of the 3GPD Operation Mode Parameters Block consists of the following fields:

Field	Length
OP_MODE	2
RESERVED	6

OP_ MODE - The operation mode to be used by the mobile station.

The base station shall set this field to the operation mode to be used by the mobile station as specified in Table 3.5.8.2-1.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The base station shall set this field to ‘000000’.

4.5.7.2 SimpleIP User Profile Parameters

The PARAM_DATA field of the SimpleIP User Profile Parameters Block consists of the following fields:

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
AUTH_ALGORITHM	4
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The base station shall set this field to the number of SimpleIP NAI entries.

The base station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The base station shall set this field to the index in the SimpleIP NAI Table.

NAI_LENGTH - SimpleIP NAI length.

The base station shall set this field to the length of the NAI in units of octet.

NAI - Network Access Identifier.

The base station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.

AUTH_ALGORITHM - Authentication Algorithm for SimpleIP.

The base station shall set this field to the authentication algorithm used to calculate the Simple IP Authentication. The Authentication Algorithm is specified in Table 3.5.8.5-1.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to ‘0’.

4.5.7.3 Mobile IP User Profile Parameters

The PARAM_DATA field of the Mobile IP User Profile Parameters Block consists of the following fields:

Field	Length (bits)
RETRY_INFO_INCLUDED	1
MAX_NUM_RETRY	0 or 2
FIRST_RETRY_TIMEOUT	0 or 3
REREG_THRESHOLD	0 or 6
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
T_BIT	1
HOME_ADDRESS	32
PRIMARY_HOME_AGENT	32
SECONDARY_HOME_AGENT	32
MN-AAA_AUTH_ALGORITHM	4
MN-AAA-SPI_INDICATOR	1
MN-AAA_SPI	0 or 32
MN-HA_AUTH_ALGORITHM	4
MN-HA_SPI_INDICATOR	1
MN-HA_SPI	0 or 32
RESERVED	0 to 7 (as needed)

RETRY_INFO_INCLUDED - Indicate if the retry information is included or not.

If MAX_NUM_RETRY, FIRST_RETRY_TIMEOUT and REREG_THRESHOLD are included in this block, the base station shall set this field to ‘1’; otherwise, the base station shall set this field to ‘0’.

MAX_NUM_RETRY - Maximum Number of Retry for the MobileIP Registration.

If RETRY_INFO_INCLUDED is set to ‘0’, the base station shall omit this field; otherwise, the base station shall set this field as follows:

		The base station shall set this field to the maximum number of retries for MobileIP registration.
FIRST_RETRY_TIMEOUT	-	The amount of time elapsed between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply.
		If RETRY_INFO_INCLUDED is set to '0', the base station shall omit this field; otherwise, the base station shall set this field as follows:
		The base station shall set this field to one less than the number of amount of time elapsed, in units of 250ms, between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply.
REREG_THRESHOLD	-	Re-Registration Threshold.
		If RETRY_INFO_INCLUDED is set to '0', the base station shall omit this field; otherwise, the base station shall set this field as follows:
		The base station shall set this field to the time, in units of minute, before the expiration of the registration lifetime that the mobile will try to reregister.
NUM_NAI	-	Number of MobileIP NAI Entries.
		The base station shall set this field to the number of MobileIP NAI entries.

The base station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX	-	MobileIP NAI entry index.
		The base station shall set this field to the index in the MobileIP NAI Table.
NAI_LENGTH	-	MobileIP NAI length.
		The base station shall set this field to the length of the MobileIP NAI, in units of octet.
NAI	-	Network Access Identifier.
		The base station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.
T_BIT	-	Reverse Tunneling.
		The base station shall set this field to '1' to request reverse tunneling or set this field to '0' if reverse tunneling is not required, see [13].
HOME_ADDRESS	-	Home Address.
		The base station shall set this field to the IP address of the mobile node in the form of network byte code.
PRIMARY_HOME_AGENT	-	Primary Home Agent.

The base station shall set this field to the IP address of the mobile node's primary home agent in the form of network byte code.

SECONDARY_HOME_AGENT - Secondary Home Agent.

The base station shall set this field to the IP address of the mobile node's back-up/secondary home agent in the form of network byte code.

MN-AAA_AUTH_ALGORITHM - Authentication Algorithm (MN-AAA)

The base station shall set this field to the authentication algorithm used to calculate the Mobile IP MN-AAA Authentication Extension as defined in [15]. The Authentication Algorithm is specified in Table 3.5.8.6-1.

MN-AAA_SPI_INDICATOR - Indicator of SPI between MN and AAA.

The base station shall set this field to ‘1’ if the Security Parameter Index is included; otherwise, the base station shall set this field to ‘0’.

MN-AAA_SPI - SPI between MN and AAA.

If the MN-AAA_SPI_INDICATOR field is set to ‘1’, the base station shall set this field to the Security Parameter Index (MN-AAA); otherwise, the base station shall omit this field.

MN-HA_AUTH_ALGORITHM - Authentication Algorithm (MN-HA)

The base station shall set this field to the authentication algorithm used to calculate the Mobile IP MN-HA Authentication Extension as defined in [12]. The Authentication Algorithm is encoded according to Table 3.5.8.6-1.

MN-HA_SPI_INDICATOR - Indicator of SPI between MN and HA.

The base station shall set this field to ‘1’ if Security Parameter Index is included; otherwise, the base station shall set this field to ‘0’.

MN-HA_SPI - SPI between MN and HA.

If the MN-HA_SPI_INDICATOR field is set to ‘1’, the base station shall set this field to the Security Parameter Index between MN and HA; otherwise, The base station shall omit this field.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall these bits to ‘0’.

4.5.7.4 SimpleIP Status Parameters

Field	Length (bits)
ACT_NAI_ENTRY_INDEX	4
RESERVED	4

ACT_NAI_ENTRY_INDEX - The SimpleIP NAI entry index to be used by the mobile station.

The base station shall set this field to the SimpleIP NAI entry index to be used by the mobile station.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The base station shall set this field to ‘0000’.

4.5.7.5 MobileIP Status Parameters

Field	Length (bits)
ACT_NAI_ENTRY_INDEX	4
NUM_ADD_ACT_NAI	4
NUM_ADD_ACT_NAI occurrences of the following field:	
ADD_ACT_NAI_ENTRY_INDEX	4
RESERVED	0 or 4 (as needed)

ACT_NAI_ENTRY_INDEX - The MobileIP NAI entry index to be used by the mobile station.

The base station shall set this field to the MobileIP NAI entry index to be used by the mobile station in the *3GPD Download Request Message*.

NUM_ADD_ACT_NAI - Number of additional Active MobileIP NAI entries.

The base station shall set this field to the number of additional active MobileIP NAI entries.

ADD_ACT_NAI_ENTRY_INDEX - Additonal Active MobileIP NAI entry index.

The base station shall set this field to the active MobileIP NAI entry index.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets.

The base station shall set this field to ‘0000’.

4.5.7.6 SimpleIP PAP SS Parameters

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The base station shall set this field to the number of SimpleIP NAI entries.

The base station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The base station shall set this field to the index in the SimpleIP NAI Table.

SS_LENGTH - Shared Secret Data Length.

The base station shall set this field to the length, in units of octet, of the shared secret data.

SS - Shared Secret Data.

The base station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to ‘0’.

4.5.7.7 SimpleIP CHAP SS Parameters

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of SimpleIP NAI Entries.

The base station shall set this field to the number of SimpleIP NAI entries.

The base station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - SimpleIP NAI entry index.

The base station shall set this field to the index in the SimpleIP NAI Table.

SS_LENGTH - Shared Secret Data Length.

The base station shall set this field to the length, in units of octet, of the shared secret data.

SS - Shared Secret Data

The base station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to ‘0’.

4.5.7.8 MobileIP SS Parameters

Field	Length (bits)
NUM_NAI	4
NUM_NAI occurrences of the following fields:	
NAI_ENTRY_INDEX	4
MN-AAA_SS_LENGTH	5
MN-AAA_SS	8 × MN-AAA_SS_LENGTH
MN-HA_SS_LENGTH	5
MN-HA_SS	8 × MN-FA_SS_LENGTH
RESERVED	0 to 7 (as needed)

NUM_NAI - Number of MobileIP NAI Entries.

The base station shall set this field to the number of MobileIP NAI entries.

The base station shall include NUM_NAI occurrences of the following fields:

NAI_ENTRY_INDEX - MobileIP NAI entry index.

The base station shall set this field to the index in the MobileIP NAI Table.

MN-AAA_SS_LENGTH - Shared Secret Data Length between MN and AAA.

The base station shall set this field to the length, in units of octet, of the shared secret data between MN and AAA.

MN-AAA_SS - Shared Secret Data between MN and AAA.

The base station shall set this field to the Shared Secret Data between MN and AAA.

MN-HA_SS_LENGTH - Shared Secret Data Length between MN and HA.

The base station shall set this field to the length, in units of octet, of the shared secret data.

MN-HA_SS - Shared Secret Data between MN and HA.

The base station shall set this field to the Shared Secret Data between MN and HA.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The base station shall set these bits to ‘0’.

4.5.7.9 HRPD Access Authentication User Profile Parameters

The PARAM_DATA field of the HRPD Access Authentication User Profile Parameters Block consists of the following fields:

Field	**Length (bits)**
NAI_LENGTH	8
NAI	8 × NAI_LENGTH
AUTH_ALGORITHM	4
RESERVED	4

NAI_LENGTH - NAI length.

The mobile station shall set this field to the length of the NAI in units of octet.

NAI - Network Access Identifier.

The mobile station shall set this field to the Network Access Identifier (NAI), encoded in ASCII string, refer to [14]. The NAI is of the form user@realm.

AUTH_ALGORITHM - Authentication Algorithm for HRPD Access Authrntication.

The mobile station shall set this field to the authentication algorithm used to calculate the HRPD Access Authentication. The Authentication Algorithm is specified in Table 3.5.8.13-1.

RESERVED - Reserved bits.

The mobile station shall set these bits to ‘0’.

4.5.7.10 HRPD Access Authentication CHAP SS Parameters

Field	**Length (bits)**
SS_LENGTH	5
SS	8 × SS_LENGTH
RESERVED	3

SS_LENGTH - Shared Secret Data Length.

The mobile station shall set this field to the length, in units of octet, of the shared secret data. The mobile station shall support the shared secret data of at least 16 octets long.

SS - Shared Secret Data

The mobile station shall set this field to the Shared Secret Data.

RESERVED - Reserved bits.

Additional reserved bits are needed in order to make the length of the entire parameter block equal to an integer number of octets. The mobile station shall set these bits to '0'.

4.5.8 MMD Parameter Block

Table 4.5.8-1 lists the types of parameter blocks used in the *MMD Download Request Message* and the *MMD Download Response Message*.

Table 4.5.8-1 MMD Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
MMD Application Parameters	'00000000'	4.5.8.1
Reserved	'00000001' through '11111111'	

4.5.8.1 MMD Application Parameters

The PARAM_DATA field of the MMD Application Parameters Block consists of the following fields:

Field	**Length (bits)**
IMPI_LENGTH	8
IMPI	8 × IMPI_LENGTH
NUM_IMPU	4

NUM_IMPU occurrences of the following fields:

IMPU_ENTRY_IDX	4
IMPU_LENGTH	8
IMPU	8 × IMPU_LENGTH

SIP_URI_LENGTH	8
SIP_DOMAIN_URI	8 × SIP_URI_LENGTH
NUM_P-CSCF	4

NUM_P-CSCF occurrences of the following fields:

P-CSCF_ENTRY_IDX	4
P-CSCF_LENGTH	8
P-CSCF_ADDRESS	8 × P-CSCF_LENGTH

RESERVED	0 to 7

IMPI_LENGTH - IMS Private Identity length

The mobile station shall set this field to the length of the IMPI in units of octets

IMPI - IMS Private Identity.

The mobile station shall set this field to the IMS Private Identity, encoded in ASCII string, refer to [17].

NUM_IMPU - Number of IMS Public Identity entries.

The mobile station shall set this field to the number of IMS Public Identity entries.

The mobile station shall include NUM_IMPU occurrences of the following fields:

IMPU_ENTRY_IDX - IMPU entry index.

The mobile station shall set this field to the index in the IMPU Table.

IMPU_LENGTH - IMS Public Identity length.

The mobile station shall set this field to the length of the IMPU in units of octet.

IMPU - IMS Public Identity.

The mobile station shall set this field to the IMS Public Identity (IMPU), encoded in ASCII string, refer to [17].

SIP_URI_LENGTH - SIP Domain URI length.

The mobile station shall set this field to the length of the SIP Domain URI.

SIP_DOMAIN_URI - SIP Domain URI.

The mobile station shall set this field to the SIP Domain URI, encoded in ASCII string, refer to [17].

NUM_P-CSCF - Number of P-CSCF entries

The mobile station shall set this field to the number of P-CSCF entries.

The mobile station shall include NUM_P-CSCF occurrences of the following fields:

P-CSCF_ENTRY_IDX - P-CSCF entry index.

The mobile station shall set this field to the index in the P-CSCF Table.

P-CSCF_LENGTH - P-CSCF length.

The mobile station shall set this field to the length of the P-CSCF in units of octet.

P-CSCF_ADDRESS - P-CSCF address.

The mobile station shall set this field to the P-CSCF address, encoded in ASCII string, refer to [17]

RESERVED - Reserved bits.

The mobile station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

4.5.9 System Tag Parameter Blocks

Table 4.5.9-1 lists the types of parameter blocks used in the *System Tag Configuration Request Message* and the *System Tag Download Request Message*.

Table 4.5.9-1 System Tag Parameter Block Types

System Tag Parameter Block Type	BLOCK_ID	Reference
Home System Tag	‘00000000’	4.5.9.1
Group Tag List	‘00000001’	4.5.9.2
Specific Tag List	‘00000010’	4.5.9.3
Call Prompt List	‘00000011’	4.5.9.4
Reserved for future standardization	‘00000100’ - ’01111111’	4.5.9.4
Available for manufacturer-specific parameter block definitions	‘10000000’- ‘11111110’	See [4]
Reserved	‘11111111’	

4.5.9.1 Home System Tag Parameter Block

The PARAM_DATA field of the Home System Tag Parameter Block consists of the following fields:

Field	Length (bits)
RESERVED	6
TAG_ENCODING	5
TAG_LEN	5
TAG	TAG_LEN × 8

RESERVED - Reserved bits.

The mobile station shall set this field to ‘000000’.

TAG_ENCODING - Tag encoding.

See [4]. This field shall be set to indicate the character set used in the TAG field included in this parameter block.

TAG_LEN Tag length.

The mobile station shall set this field to the number of octets in the TAG field.

TAG - Tag characters.

The mobile station shall set this field to characters based on the encoding method defined in TAG_ENCODING..

4.5.9.2 Group Tag List Parameter Block

The PARAM_DATA field of the Group Tag List Parameter Block consists of the following fields:

Field	**Length (bits)**
CUR_TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘0000000’.

LAST SEGMENT Last segment indicator bit.

The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the group tag list (GROUP_TAG_LIST$_{s\text{-}p}$); otherwise, the mobile station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the group tag list (GROUP_TAG_LIST$_{s\text{-}p}$) included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the group tag list (GROUP_TAG_LIST$_{s\text{-}p}$) data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current group tag list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current group tag list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the group tag list in this field. The octets shall be equal to the octets starting at the offset within the group tag list specified by SEGMENT_OFFSET.

4.5.9.3 Specific Tag List Parameter Block

The PARAM_DATA field of the Specific Tag List Parameter Block consists of the following fields:

Field	Length (bits)
CUR_TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘0000000’.

LAST SEGMENT Last segment indicator bit.

The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the specific tag list (SPEC_TAG_LIST$_{\text{s-p}}$); otherwise, the mobile station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the specific tag list (SPEC_TAG_LIST$_{\text{s-p}}$) included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the specific tag list (SPEC_TAG_LIST$_{\text{s-p}}$) data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current specific tag list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current specific tag list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the specific tag list in this field. The octets shall be equal to the octets starting at the offset within the specific tag list specified by SEGMENT_OFFSET.

4.5.9.4 Call Prompt List Parameter Block

The PARAM_DATA field of the Call Prompt List Parameter Block consists of the following fields:

Field	**Length (bits)**
CUR_TAG_P_REV	8
RESERVED	7
LAST_SEGMENT	1
SEGMENT_OFFSET	16
SEGMENT_SIZE	8
SEGMENT_DATA	SEGMENT_SIZE × 8

CUR_TAG_P_REV - Protocol revision for the system tag.

This field is used to specify the format of the rest of the System Tag.

RESERVED - Reserved bits.

The mobile station shall set this field to ‘0000000’.

LAST SEGMENT Last segment indicator bit.

The mobile station shall set this field to ‘1’ if SEGMENT_DATA contains the last octet of the call prompt list (CALL_PRMPT_LIST$_{s\text{-}p}$); otherwise, the mobile station shall set this field to ‘0’.

SEGMENT_OFFSET - Segment offset.

The mobile station shall set this field to the value of REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message*.

SEGMENT_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the call prompt list (CALL_PRMPT_LIST$_{s\text{-}p}$) included in SEGMENT_DATA.

SEGMENT_DATA - Segment of the call prompt list (CALL_PRMPT_LIST$_{s\text{-}p}$) data.

If REQUEST_OFFSET from the corresponding *System Tag Configuration Request Message* specifies an offset that is invalid for the current call prompt list, the mobile station shall include no octets in this field.

If REQUEST_OFFSET specifies an offset that is valid for the current call prompt list, the mobile station shall include at most REQUEST_MAX_SIZE sequential octets of the call prompt list in this field. The octets shall be equal to the octets starting at the offset within the call prompt list specified by SEGMENT_OFFSET.

4.5.10 MMS Parameter Block

Table 4.5.10-1 lists the types of parameter blocks used in the *MMS Download Request Message* and the *MMS Download Response Message.*

Table 4.5.10-1 MMS Parameter Block Types

Parameter Block Type	BLOCK_ID	Reference
MMS URI Parameters	'00000000'	4.5.10.1
Reserved	'00000001' through '11111111'	

4.5.10.1 MMS URI Parameters

The PARAM_DATA field of the MMS Application URI Block consists of the following fields:

Field	Length (bits)
NUM_MMS_URI	4
NUM_MMS_URI occurrences of the following fields:	
MMS_URI_ENTRY_IDX	4
MMS_URI_LENGTH	8
MMS URI	8 x MMS_URI_LENGTH
RESERVED	0 to 7

NUM_MMS_URI - Number of MMS URIs

The base station shall set this field to the number of MMS URIs stored on the mobile, encoded in ASCII string, refer to [16], [17] and [18].

The mobile station shall include NUM_MMS_URI occurrences of the following fields:

MMS_URI_ENTRY_IDX - MMS URI entry index.

The base station shall set this field to the index in the MMS URI Table, refer to [16], [17]and [18].

MMS_URI_LENGTH - MMS URI length.

The base station shall set this field to the length of the URI associated with the MMS Relay/Server in units of octet

MMS_URI - MMS_URI

The base station shall set this field to the URI of the MMS Relay/Server, encoded in ASCII string, refer to [16], [17] and [18].

RESERVED	-	Reserved bits. The base station shall add reserved bits as needed in order to make the length of the entire parameter block equal to an integer number of octets.

No text.

5 KEY EXCHANGE PROCEDURES

5.1 Mobile Station Requirements for A_KEY_P_REV < ‘00000011’

5.1.1 Random Number Generation

The mobile station shall generate a random number X for use in calculating the mobile station result, MS_RESULT. The number X shall have the following properties:

- The number generated shall be 160-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Response Messages* sent by the same mobile station shall be statistically uncorrelated.
- The number used in formulating each *Key Generation Response Message* shall not be derivable from the previously used numbers or mobile station indicator values.
- The numbers used in formulating *Key Generation Response Messages* sent by different mobile stations shall be statistically uncorrelated.

5.1.2 Mobile Station Result

The mobile station shall calculate MS_RESULT = PARAM_G_S^X modulo PARAM_P_S.

5.1.3 A-key Computation

The mobile station shall compute the common key K = BS_RESULT_S^X modulo PARAM_P_S. The mobile station shall store the least significant 64 bits of the result K as A_KEY_TEMP_S.

5.2 Base Station Requirements for A_KEY_P_REV < ‘00000011’

5.2.1 Generation of the Key Exchange Parameters

The base station shall select and store a 512-bit prime number P based on the following criteria:

- P should be chosen randomly.
- (P - 1) should have a large prime factor.
- The most significant bit of P should be equal to ‘1’.

The base station shall set PARAM_P of the *MS Key Request Message* to P.

The base station shall select a 160-bit number G such that it is greater than 1 and less than (P-1). The base station shall set PARAM_G of the *MS Key Request Message* to G.

The base station shall generate a random number Y for use in calculating the base station result, BS_RESULT. The number Y shall have the following properties:

- The number generated shall be 160-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Request Messages* sent by the same base station shall be statistically uncorrelated.
- The numbers used in formulating *Key Generation Request Message* sent by different base stations shall be statistically uncorrelated.

5.2.2 Base Station Result

The base station shall calculate BS_RESULT = G^Y modulo P.

5.2.3 A-key Computation

The base station shall compute the common key K = MS_RESULT^Y modulo P. The base station shall use the least significant 64 bits of the result K as the A_KEY.

5.3 Mobile Station Requirements for A_KEY_P_REV = ‘00000011’ or ‘00000100’

5.3.1 Random Number Generation For Diffie-Hellman Key Exchange Procedure

The mobile station shall set PARAM_P_S for use in calculating the mobile station result, MS_RESULT, to the following 1024-bit prime number (Most Significant Bit first):

0xFFFFFFFF 0xFFFFFFFF 0xC90FDAA2 0x2168C234 0xC4C6628B 0x80DC1CD1

0x29024E08 0x8A67CC74 0x020BBEA6 0x3B139B22 0x514A0879 0x8E3404DD

0xEF9519B3 0xCD3A431B 0x302B0A6D 0xF25F1437 0x4FE1356D 0x6D51C245

0xE485B576 0x625E7EC6 0xF44C42E9 0xA637ED6B 0x0BFF5CB6 0xF406B7ED

0xEE386BFB 0x5A899FA5 0xAE9F2411 0x7C4B1FE6 0x49286651 0xECE65381

0xFFFFFFFF 0xFFFFFFFF

The mobile station shall set PARAM_G_S for use in calculating MS_RESULT to ‘00000010’.

The mobile station shall generate a random number X for use in calculating MS_RESULT. The number X shall have the following properties:

- The number generated shall be 256-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Response Messages* sent

by the same mobile station shall be statistically uncorrelated.

- The number used in formulating each *Key Generation Response Message* shall not be derivable from the previously used numbers or mobile station indicator values.
- The numbers used in formulating *Key Generation Response Messages* sent by different mobile stations shall be statistically uncorrelated.

5.3.2 Mobile Station Result

The mobile station shall calculate MS_RESULT = $\text{PARAM\_G}_\text{S}^\text{X}$ modulo PARAM_P_S.

5.3.3 A Key and Root Key Computation for A_KEY_P_REV = ‘00000011’

The mobile station shall compute one of the input to *f0,* Random Secret Seed, RAND_SEED_TEMP = $\text{BS\_RESULT}_\text{S}^\text{X}$ modulo PARAM_P_S. The mobile station shall store the least significant 128 bits of the result RAND_SEED_TEMP as RAND_SEED.

The A_KEY and 3G Root Key RK are generated by invoking the algorithmic function *f0* as specified in Section 2.2.2.2 of [8]. Since each invocation of *f0* produces 64 bits, three invocation of *f0* is need for a total of 192 bits.

The input parameters to the algorithmic function *f0* shall be set as follows:

- The K parameter shall be set to RAND_SEED.
- The fi parameter shall be set to 0x41.
- The Fmk parameter shall be set to 0x41484147.

The mobile station shall invoke *f0*.

The mobile station shall store the most significant bits of the result of invocation of *f0* as the $\text{A\_KEY\_TEMP}_\text{S}$.

The mobile station shall store the remaining 128 bits of the invocation of *f0* as RK_TEMP_S.

5.3.4 Root Key Computation for A_KEY_P_REV = ‘00000100’

The mobile station shall compute the Root Key RK = $\text{BS\_RESULT}_\text{S}^\text{X}$ modulo PARAM_P_S. The mobile station shall store the least significant 128 bits of the result RK as RK_TEMP_S.

5.4 Base Station Requirements for A_KEY_P_REV = ‘00000011’ or ‘00000100’

5.4.1 Generation of the Key Exchange Parameters Root Key

The base station shall set PARAM_P_S for use in calculating the base station result, BS_RESULT, to the following 1024-bit prime number (Most Significant Bit first):

0xFFFFFFFF 0xFFFFFFFF 0xC90FDAA2 0x2168C234 0xC4C6628B 0x80DC1CD1

0x29024E08 0x8A67CC74 0x020BBEA6 0x3B139B22 0x514A0879 0x8E3404DD
0xEF9519B3 0xCD3A431B 0x302B0A6D 0xF25F1437 0x4FE1356D 0x6D51C245
0xE485B576 0x625E7EC6 0xF44C42E9 0xA637ED6B 0x0BFF5CB6 0xF406B7ED
0xEE386BFB 0x5A899FA5 0xAE9F2411 0x7C4B1FE6 0x49286651 0xECE65381
0xFFFFFFFF 0xFFFFFFFF

The base station shall set PARAM_G_S for use in calculating BS_RESULT to ‘00000010’.

The base station shall generate a random number Y for use in calculating BS_RESULT. The number Y shall have the following properties:

- The number generated shall be 256-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Request Messages* sent by the same base station shall be statistically uncorrelated.
- The numbers used in formulating *Key Generation Request Message* sent by different base stations shall be statistically uncorrelated.

5.4.2 Base Station Result

The base station shall calculate BS_RESULT = G^Y modulo P.

5.4.3 A Key and Root Key Computation for A_KEY_P_REV = ‘00000011’

The base station shall compute the input to *f0,* Random Secret Seed, RAND_SEED_TEMP = MS_RESULT^Y modulo P. The base station shall store the least significant 128 bits of the result RAND_SEED_TEMP as RAND_SEED.

The A_KEY and 3G Root Key RK are generated by invoking the algorithmic function *f0* as specified in Section 2.2.2.2 of [8]. Since each invocation of *f0* produces 64 bits, three invocation of *f0* is need for a total of 192 bits.

The input parameters to the algorithmic function *f0* shall be set as follows:

- The K parameter shall be set to RAND_SEED.
- The fi parameter shall be set to 0x41.
- The Fmk parameter shall be set to 0x41484147.

The base station shall invoke *f0*.

The base station shall store the most significant bits of the result of invocation of *f0* as the A_KEY.

The base station shall store the remaining 128 bits of the invocation of *f0* as the Root Key K.

5.4.4 Root Key K Computation for A_KEY_P_REV = ‘00000100’

The base station shall compute the Root Key RK = MS_RESULT^{Y} modulo P. The base station shall use the least significant 128 bits of the result RK as the Root Key K.

5.5 Mobile Station Requirements for A_KEY_P_REV = ‘00000101’

5.5.1 Random Number Generation and Key Generation Parameters

The mobile station shall set $PARAM\_P_S$ for use in calculating the mobile station result, MS_RESULT, to the 1024-bit prime number as specified in 5.3.1.

The mobile station shall set $PARAM\_G_S$ for use in calculating MS_RESULT to ‘00001101’.

The mobile station shall generate a random number X for use in calculating MS_RESULT. The number X shall have the following properties:

- The number generated shall be 384-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Response Messages* sent by the same mobile station shall be statistically uncorrelated.
- The number used in formulating each *Key Generation Response Message* shall not be derivable from the previously used numbers or mobile station indicator values.
- The numbers used in formulating *Key Generation Response Messages* sent by different mobile stations shall be statistically uncorrelated.

5.5.2 Mobile Station Result

The mobile station shall calculate MS_PW_HASH as the follows:

MS_PW_HASH = SHA-1[6] (0x00000001,0x00000001, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000002, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000003, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000004, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000005, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000006, MS_PW) modulo 2^{128} |

---

[6] SHA-1 refers to the FIPS-180 hash function as specified in [9].

SHA-1 (0x00000001,0x00000007, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000008, MS_PW) modulo 2^{128} |

SHA-1 (0x00000001,0x00000009, MS_PW) modulo 2^{128}.

The mobile station shall calculate MS_RESULT = (MS_PW_HASH[7] * $\text{PARAM\_G}_S{}^X$) modulo PARAM_P_S.

5.5.3 Root Key Computation for A_KEY_P_REV = ‘00000101’

The mobile station shall compute the Root Key RK = SHA-1 (0x00000003 | 0x00000C80[8] |MS_PARAM |MS_PARAM),

where MS_PARAM =MS_PW|

$\text{PARAM\_G}_S{}^X$ modulo P|

(BS_RESULT_S/BS_PW_HASH) modulo P|

((BS_RESULT_S/BS_PW_HASH)^X) modulo P.

The mobile station shall store the least significant 128 bits of the result RK as RK_TEMP_S.

5.6 Base Station Requirements for A_KEY_P_REV = ‘00000101’

5.6.1 Random Number Generation and Key Generation Parameters

The base station shall set PARAM_P_S for use in calculating the base station result, BS_RESULT, to the following 1024-bit prime number (Most Significant Bit first) as spedified in 5.4.1.

The base station shall set PARAM_G_S for use in calculating BS_RESULT to ‘00001101’.

The base station shall generate a random number Y for use in calculating BS_RESULT. The number Y shall have the following properties:

- The number generated shall be 384-bits in length.
- The number generated shall not be less than 4.
- The number generated shall have an uniform statistical distribution over its range.
- The numbers used in formulating different *Key Generation Request Messages* sent by the same base station shall be statistically uncorrelated.
- The numbers used in formulating *Key Generation Request Message* sent by different

---

[7] MS_PW_HASH may be reduced modulo PARAM_P_S prior to multiplication to simplify implementation.

[8] This value is set to the length of MS_PARAM in bits.

base stations shall be statistically uncorrelated.

5.6.2 Base Station Result

The base station shall calculate BS_PW_HASH where

BS_PW_HASH = SHA-1 (0x00000002,0x00000001, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000002, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000003, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000004, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000005, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000006, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000007, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000008, BS_PW) modulo 2^{128} |
SHA-1 (0x00000002,0x00000009, BS_PW) modulo 2^{128}.

The base station shall calculate BS_RESULT = (BS_PW_HASH[9] * G^Y) modulo P.

5.6.3 3G Root Key K Computation

The base station shall compute the Root Key RK = SHA-1 (0x00000003 | 0x00000C80[10] | BS_PARAM | BS_PARAM),

where BS_PARAM =BS_PW|
(MS_RESULT_S/MS_PW_HASH) modulo P |
G^Y modulo P |
((MS_RESULT_S/MS_PW_HASH)^Y) modulo P.

The base station shall use the least significant 128 bits of the result RK as the Root Key K.

---

[9] BS_PW_HASH may be reduced modulo P prior to multiplication to simplify implementation.

[10] This value is set to the length of BS_PARAM in bits.

No text.

ANNEX A RESERVED

No text.

ANNEX B BIBLIOGRAPHY

This is an informative annex. The documents listed in this annex are for information only and are not essential for the completion of the requirements of this standard.

1. TIA/EIA/IS-91, Mobile Station - Base Station Compatibility Standard for 800 MHz Analog Cellular, October 1994.

No text.

ANNEX C SYSTEM SELECTION AND ACQUISITION

C.1 Introduction

This is an informative annex that describes recommended use of the preferred roaming list. The preferred roaming list indicates which systems the mobile station should use (preferred systems). It also indicates which systems should not be used by the mobile station (negative systems). In addition to indicating which systems are preferred or negative, the preferred roaming list has information that can reduce the acquisition time, however, for optimum performance of the SSPR feature appropriate structuring of the roaming list is required.

The preferred roaming list consists of two tables: the system table and the acquisition table. The system table contains records. Each record identifies a system by its SID and NID. For each record, there is an indicator of whether the system is preferred or negative, the roaming status that should be indicated by the mobile station, the relative priority of the system and its geographic region. Each record also contains an acquisition index that indicates a record in the acquisition table to be used. The acquisition record provides the band and frequencies that the mobile station is to use when attempting to acquire the system.

Table C.1-1 illustrates the basic structure of the preferred roaming list.

Table C.1-1 Preferred Roaming List

PREF_ONLY	DEF_ROAM_IND	NUM_ACQ_RECS	NUM_SYS_RECS
No	On (steady)	5	12

Table C.1-2 illustrates the acquisition table. The records in the acquisition table are in order of priority (highest priority first) according to desired mobile station system selection scan order.

Table C.1-2 Acquisition Table

ACQ_INDEX	ACQ_TYPE	Description	Acquisition Parameters
0	‘0110’	PCS CDMA - Using Channels	PCS Channels 100, 125, 150, 175, 200
1	‘0101’	PCS CDMA - Using Blocks	PCS Block C
2	‘0011’	Cellular CDMA - Custom Channels	Channel Number 1
3	‘0010’	Cellular CDMA - Standard Channels	System A, Primary and Secondary CDMA Channel
4	‘0001’	Cellular Analog	System B

Table C.1-3 illustrates the system table. In this table, region changes are denoted by a change in shading.

Table C.1-3 System Table

SID	NID_INCL	PREF_NEG	GEO	PRI	ACQ_INDEX (ACQ_TYPE)	ROAM_IND
111	0	1	0	1	2 [Cellular CDMA - Standard Channels]	Off
77	0	1	1	0	0 [PCS CDMA - Using Channels]	Off
34	0	1	1	0	2 [Cellular CDMA - Standard Channels]	Flashing
34	0	0	1	N/A	4 [Cellular Analog]	N/A
400	0	1	0	1	2 [Cellular CDMA - Standard Channels]	Off
4	0	1	1	1	0 [PCS CDMA - Using Channels]	On
12	0	1	1	1	3 [Cellular CDMA - Custom Channels]	On
0	0	1	1	0	4 (Cellular Analog)	On
776	0	0	1	N/A	4 [Cellular Analog]	N/A
61	0	1	0	1	2 [Cellular CDMA - Standard Channels]	Off
56	0	1	1	0	1 [PCS CDMA - Using Blocks]	Flashing
16	0	0	1	N/A	4 [Cellular Analog]	N/A

C.2 Accelerated System Selection

C.2.1 Using Positive and Negative Systems

An entry in SYS_TABLE having a PREF_NEG bit set to ‘1’ is a preferred system. An entry in SYS_TABLE having a PREF_NEG bit set to ‘0’ is a negative system.

Once the SID of the preferred system is determined it can be used to index into the Geographic Region of the SYS_TABLE and select a system in the same Geographic Region that is preferable. The mobile station can then use the acquisition table entry to determine the frequencies that should be used when attempting to acquire the preferred system.

Similarly, once the SID of a negative system is determined, it can be used to index into the Geographic Region of the SYS_TABLE and select a system in the same Geographic Region that is preferable. The mobile station can then use the acquisition table entry to determine the frequencies that should be used when attempting to acquire the preferred system.

For example, if the mobile station acquires the analog cellular system with SID equal to 34, the mobile station should attempt to acquire the cellular CDMA system with SID equal to 111 (see Table C.1-3). If the mobile station fails to acquire this system, the mobile station should attempt to acquire the PCS CDMA system with SID equal to 77.

C.2.2 PCS Block Mode System Selection

There are two acquisition types that can be used when acquiring a PCS CDMA system: PCS CDMA System Acquisition (Using Blocks) and PCS CDMA System Acquisition (Using Channels). These correspond to ACQ_TYPE equal to '0101' and ACQ_TYPE equal to '0110', respectively.

When using the block mode, the mobile station may need to search all of the preferred frequency assignments (see 6.1.1.1 of [1] or 2.1.1.1 of [5]) within the frequency block to determine whether it can acquire the system. For the A, B and C blocks, there are 11 preferred frequency assignments. Since the acquisition time may be proportional to the number of preferred frequency assignments, specifying the entire frequency block should be avoided when a smaller set of frequencies is sufficient, thus, it is usually preferable to use the PCS CDMA System Acquisition (Using Channels) acquisition type.

C.2.3 Special Cases and Considerations

It is possible for the mobile station to acquire a channel, decode the SID/NID and find a matching SID/NID system record where the acquired channel and the acquisition type of the matching record are different. In these cases, service is allowed. For example, if the mobile station is presently scanning one of PCS channels corresponding to ACQ_TYPE = '0110' (first entry in the Table C.1-2), discovers the system with SID 61, and finds it in the system table (see Table C.1-3), service is allowed, even though the acquisition index for the record (ACQ_INDEX = 2) does not match acquired system. This situation can occur based upon service providers changing or adding channels in a market, changing broadcast SID, or purchasing another service provider's market.

Wildcard SIDs (SID = 0) can be used to universally allow or deny service in a particular band or mode(s) of operation. In this example, assume that cellular analog system SID 504 and cellular CDMA system SID 4101 can be acquired by the mobile station and are not specifically included in the system table. Assume further that the PREF_ONLY for the preferred roaming list is set to '1' ('True'). The mobile station scans channels according to all acquisition table entries attempting to acquire a system with SID that matches records in the system table. After finding no matching SIDs, the mobile station allows service on the system with SID 504 acquired at the cellular analog System B. The mobile station does not allow service on system with SID 4101, since that system does not match the acquisition record associated with the system record containing the wildcard SID.

C.3 Preferred Roaming List Maintenance

All or any part of the preferred roaming list can be replaced using Over-the-Air Service Provisioning. Segmentation of the preferred roaming list provides access to any specific area requiring modification. An area is identified by the position offset of the first modified octet in the list and includes the number of new octets to be transmitted in one or more segments (see 3.3.1).

The end of transmission is denoted by the LAST_SEGMENT field set to ‘1’. When the end of transmission is detected, the length and CRC of the preferred roaming list must be verified to ensure the data integrity. For manageability, when replacing areas of differing sizes, it is recommended that the remaining data of the list be retransmitted and replaced as well.

When the preferred roaming list data is modified, the service provider may assign a new PR_LIST_ID to the list.

ANNEX D SYSTEM SELECTION AND THE PREFERRED USER ZONE LIST

This annex is informative. The Preferred User Zone List provides the mobile station that supports the optional User Zone feature with the specification of the User Zones to which the mobile station is subscribed. The PUZL is used after the mobile station has completed system acquisition using the preferred roaming list or other techniques. Once a mobile station has found its preferred system, the PUZL is used to select the most preferred User Zone on that system. The PUZL contains a list of all User Zones that are subscribed to and any parameters needed to locate and access these User Zones.

In the case where the network is broadcasting a Private Neighbor List Message indicating the presence of the preferred User Zone on a separate RF carrier, the mobile station will then switch to that RF carrier to obtain the services of the User Zone. For purposes of the PRL, the private system in this case can be considered to be part of the original system on which the Private Neighbor List Message was detected.

It is noted that:

- Each entry in the PUZL is uniquely identified by User Zone ID and User Zone SID.
- Each User Zone entry within the PUZL is stored contiguously in the mobile station memory.
- The PUZL may be stored in a non-contiguous fashion in the mobile station memory.
- The PUZL may have up to 4095 User Zone entries.

No text.