

Document: C.S0016-0

Version:

Date: December 1999



3RD GENERATION  
PARTNERSHIP  
PROJECT 2  
"3GPP2"

---

## **Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems**

### ***COPYRIGHT***

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



1  
2  
3  
4  
5  
6  
7

***TIA/EIA/IS-683-A:***

***Over-the-Air Service Provisioning of Mobile Stations in Spread  
Spectrum Systems.***

May, 1998

***Publication Version***

1 TIA/EIA/IS-683-A TITLE PAGE

2

3 File name: IS-683-A;PV

4

5 Over-the-Air Service Provisioning of  
6 Mobile Stations in Spread Spectrum  
7 Systems

8

1 COPYRIGHT PAGE

2

## **PREFACE**

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 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, provisioning of System Selection for Preferred Roaming parameters, and provisioning of Service Programming Lock.

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.

**REFERENCES**

The following standards contain provisions which, 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.

1. TIA/EIA-95-B, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum System*.
2. Common Cryptographic Algorithms, Rev.C. Information disclosed in this document is subject to the export jurisdiction of the US Department of Commerce as specified in Export Administration Regulations (title 15 CFR parts 730 through 774 inclusive). A license issued by the Department of Commerce is required for the export of such technical data. Contact the Telecommunications Industry Association, Arlington, VA.
3. Interface Specification for Common Cryptographic Algorithms, Rev.C. Contact the Telecommunications Industry Association, Arlington, VA.
4. TSB58, *Administration of Parameter Value Assignments for TIA/EIA Spread Spectrum Standards*, Revision A or later.

# CONTENTS

|    |                                                                                |      |
|----|--------------------------------------------------------------------------------|------|
| 1  |                                                                                |      |
| 2  | 1 INTRODUCTION.....                                                            | 1-1  |
| 3  | 1.1 General Description .....                                                  | 1-1  |
| 4  | 1.2 Terms and Numeric Information .....                                        | 1-1  |
| 5  | 1.2.1 Terms .....                                                              | 1-1  |
| 6  | 1.2.2 Numeric Information .....                                                | 1-5  |
| 7  | 2 MESSAGE TRANSPORT PROTOCOL.....                                              | 2-1  |
| 8  | 2.1 General .....                                                              | 2-1  |
| 9  | 2.2 Analog Transport Protocol.....                                             | 2-1  |
| 10 | 2.2.1 <i>OTASP Data Message</i> Encapsulation .....                            | 2-1  |
| 11 | 2.2.2 <i>OTASP Data Message</i> Segmentation .....                             | 2-2  |
| 12 | 2.2.3 Mobile Station Procedures .....                                          | 2-4  |
| 13 | 2.2.3.1 <i>OTASP Transport Message</i> Acknowledgment and Re-transmission..... | 2-4  |
| 14 | 2.2.3.2 Message Transmission .....                                             | 2-5  |
| 15 | 2.2.3.3 Message Reception .....                                                | 2-5  |
| 16 | 2.2.3.4 Reverse Voice Channel Message Format .....                             | 2-8  |
| 17 | 2.2.3.4.1 <i>OTASP Transport Message</i> .....                                 | 2-8  |
| 18 | 2.2.3.4.2 <i>OTASP Transport Confirmation Message</i> .....                    | 2-10 |
| 19 | 2.2.4 Base Station Procedures .....                                            | 2-11 |
| 20 | 2.2.4.1 Message Transmission .....                                             | 2-11 |
| 21 | 2.2.4.2 Message Reception .....                                                | 2-12 |
| 22 | 2.2.4.3 Forward Voice Channel Message Format .....                             | 2-13 |
| 23 | 2.2.4.3.1 <i>OTASP Transport Message</i> .....                                 | 2-13 |
| 24 | 2.2.4.3.2 <i>OTASP Transport Confirmation Message</i> .....                    | 2-16 |
| 25 | 2.3 CDMA Transport Protocol .....                                              | 2-17 |
| 26 | 3 MOBILE STATION PROCEDURES .....                                              | 3-1  |
| 27 | 3.1 Initial Values and NAM Parameters .....                                    | 3-1  |
| 28 | 3.2 Initiation of the Programming Procedures.....                              | 3-2  |
| 29 | 3.2.1 User-Initiated Procedure .....                                           | 3-2  |
| 30 | 3.2.2 Network-Initiated Procedure .....                                        | 3-4  |
| 31 | 3.2.2.1 Initiation of OTAPA in the CDMA Mobile Station Idle State .....        | 3-5  |

|    |                                                                   |      |
|----|-------------------------------------------------------------------|------|
| 1  | 3.2.2.2 Connection of the OTAPA Service Option .....              | 3-5  |
| 2  | 3.2.2.3 Starting the OTAPA session .....                          | 3-7  |
| 3  | 3.3 Programming Procedure .....                                   | 3-7  |
| 4  | 3.3.1 OTASP Data Message Processing .....                         | 3-7  |
| 5  | 3.3.2 Mobile Station SSD Update and Re-authentication .....       | 3-15 |
| 6  | 3.3.3 Activation of Message Encryption .....                      | 3-17 |
| 7  | 3.3.4 Activation of Voice Privacy .....                           | 3-17 |
| 8  | 3.3.5 System Selection for Preferred Roaming.....                 | 3-17 |
| 9  | 3.3.6 Service Programming Lock .....                              | 3-17 |
| 10 | 3.3.7 Subscriber Parameter Administration Security Mechanism..... | 3-18 |
| 11 | 3.4 Termination of the Programming Procedure.....                 | 3-18 |
| 12 | 3.5 Reverse Link Message Formats .....                            | 3-20 |
| 13 | 3.5.1 Message Contents .....                                      | 3-21 |
| 14 | 3.5.1.1 Configuration Response Message.....                       | 3-21 |
| 15 | 3.5.1.2 Download Response Message.....                            | 3-22 |
| 16 | 3.5.1.3 MS Key Response Message.....                              | 3-23 |
| 17 | 3.5.1.4 Key Generation Response Message .....                     | 3-24 |
| 18 | 3.5.1.5 Re-Authenticate Response Message .....                    | 3-24 |
| 19 | 3.5.1.6 Commit Response Message .....                             | 3-25 |
| 20 | 3.5.1.7 Protocol Capability Response Message.....                 | 3-25 |
| 21 | 3.5.1.8 SSPR Configuration Response Message .....                 | 3-28 |
| 22 | 3.5.1.9 SSPR Download Response Message .....                      | 3-29 |
| 23 | 3.5.1.10 Validation Response Message .....                        | 3-29 |
| 24 | 3.5.1.11 OTAPA Response Message.....                              | 3-30 |
| 25 | 3.5.2 NAM Parameter Blocks.....                                   | 3-31 |
| 26 | 3.5.2.1 CDMA/Analog NAM Parameter Block .....                     | 3-32 |
| 27 | 3.5.2.2 Mobile Directory Number .....                             | 3-35 |
| 28 | 3.5.2.3 CDMA NAM Parameter Block .....                            | 3-36 |
| 29 | 3.5.2.4 IMSI_T Parameter Block .....                              | 3-38 |
| 30 | 3.5.3 SSPR Parameter Blocks.....                                  | 3-39 |
| 31 | 3.5.3.1 Preferred Roaming List Dimensions Parameter Block .....   | 3-40 |
| 32 | 3.5.3.2 Preferred Roaming List Parameter Block .....              | 3-41 |

|    |                                                                            |      |
|----|----------------------------------------------------------------------------|------|
| 1  | 3.5.4 Reserved .....                                                       | 3-42 |
| 2  | 3.5.5 Preferred Roaming List .....                                         | 3-42 |
| 3  | 3.5.5.1 Preferred Roaming List CRC Calculation .....                       | 3-43 |
| 4  | 3.5.5.2 Acquisition Records.....                                           | 3-44 |
| 5  | 3.5.5.2.1 Acquisition Record Formats .....                                 | 3-44 |
| 6  | 3.5.5.2.1.1 Cellular Analog System Acquisition Record.....                 | 3-44 |
| 7  | 3.5.5.2.1.2 Cellular CDMA System Acquisition (Standard Channels) Record .. | 3-45 |
| 8  | 3.5.5.2.1.3 Cellular CDMA System Acquisition (Custom Channels) Record..... | 3-46 |
| 9  | 3.5.5.2.1.4 Cellular CDMA Preferred System Acquisition Record .....        | 3-46 |
| 10 | 3.5.5.2.1.5 PCS CDMA System Acquisition (Using Blocks) Record .....        | 3-47 |
| 11 | 3.5.5.2.1.6 PCS CDMA System Acquisition (Using Channels) Record .....      | 3-48 |
| 12 | 3.5.5.3 System Record Format .....                                         | 3-49 |
| 13 | 4 BASE STATION PROCEDURES .....                                            | 4-1  |
| 14 | 4.1 Reserved.....                                                          | 4-1  |
| 15 | 4.2 Initiation of the Programming Procedures.....                          | 4-1  |
| 16 | 4.2.1 User-Initiated Procedure .....                                       | 4-1  |
| 17 | 4.2.2 Network-Initiated Procedure. ....                                    | 4-2  |
| 18 | 4.3 Programming Data Download .....                                        | 4-2  |
| 19 | 4.3.1 OTA Data Message Processing .....                                    | 4-2  |
| 20 | 4.3.2 SSD Update and re-authentication .....                               | 4-4  |
| 21 | 4.3.3 Activation of Message Encryption .....                               | 4-4  |
| 22 | 4.3.4 Activation of Voice Privacy Mode.....                                | 4-5  |
| 23 | 4.4 Termination of the Programming Procedure.....                          | 4-5  |
| 24 | 4.5 Forward Link Message Formats .....                                     | 4-6  |
| 25 | 4.5.1 Message Contents .....                                               | 4-7  |
| 26 | 4.5.1.1 Configuration Request Message .....                                | 4-7  |
| 27 | 4.5.1.2 Download Request Message .....                                     | 4-7  |
| 28 | 4.5.1.3 MS Key Request Message .....                                       | 4-8  |
| 29 | 4.5.1.4 Key Generation Request Message.....                                | 4-9  |
| 30 | 4.5.1.5 Re-Authenticate Request Message .....                              | 4-9  |
| 31 | 4.5.1.6 Commit Request Message.....                                        | 4-10 |
| 32 | 4.5.1.7 Protocol Capability Request Message .....                          | 4-10 |

|    |                                                       |      |
|----|-------------------------------------------------------|------|
| 1  | 4.5.1.8 SSPR Configuration Request Message.....       | 4-10 |
| 2  | 4.5.1.9 SSPR Download Request Message.....            | 4-11 |
| 3  | 4.5.1.10 Validation Request Message.....              | 4-12 |
| 4  | 4.5.1.11 OTAPA Request Message .....                  | 4-12 |
| 5  | 4.5.2 NAM Parameter Blocks.....                       | 4-13 |
| 6  | 4.5.2.1 CDMA/Analog NAM Download.....                 | 4-13 |
| 7  | 4.5.2.2 Mobile Directory Number .....                 | 4-16 |
| 8  | 4.5.2.3 CDMA NAM Download .....                       | 4-17 |
| 9  | 4.5.2.4 IMSI_T Parameter Block .....                  | 4-19 |
| 10 | 4.5.3 SSPR Parameter Blocks.....                      | 4-20 |
| 11 | 4.5.3.1 Preferred Roaming List Parameter Block .....  | 4-20 |
| 12 | 4.5.4 Validation Parameter Blocks .....               | 4-21 |
| 13 | 4.5.4.1 Verify SPC .....                              | 4-21 |
| 14 | 4.5.4.2 Change SPC.....                               | 4-22 |
| 15 | 4.5.4.3 Validate SPASM.....                           | 4-22 |
| 16 | 5 KEY EXCHANGE PROCEDURES .....                       | 5-1  |
| 17 | 5.1 Mobile Station Requirements .....                 | 5-1  |
| 18 | 5.1.1 Random Number Generation.....                   | 5-1  |
| 19 | 5.1.2 Mobile Station Result.....                      | 5-1  |
| 20 | 5.1.3 A-key Computation .....                         | 5-1  |
| 21 | 5.2 Base Station Requirements .....                   | 5-1  |
| 22 | 5.2.1 Generation of the Key Exchange Parameters ..... | 5-1  |
| 23 | 5.2.2 Base Station Result.....                        | 5-2  |
| 24 | 5.2.3 A-key Computation .....                         | 5-2  |
| 25 | ANNEX A MESSAGE ENCRYPTION AND VOICE PRIVACY .....    | A-1  |
| 26 | ANNEX B BIBLIOGRAPHY .....                            | B-1  |
| 27 | ANNEX C SYSTEM SELECTION AND ACQUISITION.....         | C-1  |
| 28 | C.1 Introduction.....                                 | C-1  |
| 29 | C.2 Accelerated System Selection .....                | C-2  |
| 30 | C.2.1 Using Positive and Negative Systems.....        | C-2  |
| 31 | C.2.2 PCS Block Mode System Selection.....            | C-3  |
| 32 | C.2.3 Special Cases and Considerations .....          | C-3  |

|   |                                              |     |
|---|----------------------------------------------|-----|
| 1 | C.3 Preferred Roaming List Maintenance ..... | C-4 |
|---|----------------------------------------------|-----|

2

3

## FIGURES

|   |                                                                                           |     |
|---|-------------------------------------------------------------------------------------------|-----|
| 4 | Figure 2.2.1-1 <i>OTASP Data Message</i> Encapsulation .....                              | 2-1 |
| 5 | Figure 2.2.1-2 <i>OTASP Data Message</i> CRC .....                                        | 2-2 |
| 6 | Figure 2.2.2-1 <i>OTASP Data Message</i> Capsule Segmentation on the Forward Analog Voice |     |
| 7 | Channel.....                                                                              | 2-3 |
| 8 | Figure 2.2.2-2 <i>OTASP Data Message</i> Capsule Segmentation on the Reverse Analog Voice |     |
| 9 | Channel.....                                                                              | 2-4 |

10

11

## TABLES

|    |                                                                                   |                                |
|----|-----------------------------------------------------------------------------------|--------------------------------|
| 12 | Table 3.2-1 System Selection Code.....                                            | 3-2                            |
| 13 | Table 3.2.2.2-1 Valid Service Configuration Attributes for Service Option 18..... | 3-6                            |
| 14 | Table 3.2.2.2-2 Valid Service Configuration Attributes for Service Option 19..... | 3-6                            |
| 15 | Table 3.3.2-1 Auth_Signature Input Parameters.....                                | 3-Error! Bookmark not defined. |
| 16 | Table 3.3.6-1 Service Programming Code Values .....                               | 3-19                           |
| 17 | Table 3.5-1 Reverse Link Messages .....                                           | 3-21                           |
| 18 | Table 3.5.1.2-1 Result Codes .....                                                | 3-24                           |
| 19 | Table 3.5.1.7-1 Feature Identifier.....                                           | 3-28                           |
| 20 | Table 3.5.1.7-2 Band/mode Capability Information .....                            | 3-29                           |
| 21 | Table 3.5.2-1 NAM Parameter Block Types.....                                      | 3-33                           |
| 22 | Table 3.5.3-1 SSPR Parameter Block Types.....                                     | 3-41                           |
| 23 | Table 3.5.5.2-1 Acquisition Record Type Values .....                              | 3-45                           |
| 24 | Table 3.5.5.2.1.1-1 Cellular System A/B Selection Type Values .....               | 3-46                           |
| 25 | Table 3.5.5.2.1.2-1 Cellular CDMA Standard Channel Selection Type Values .....    | 3-47                           |
| 26 | Table 3.5.5.2.1.5-1 PCS CDMA Frequency Blocks .....                               | 3-49                           |
| 27 | Table 3.5.5.3-1 NID_INCL Values.....                                              | 3-51                           |
| 28 | Table 4.5-1 Forward Link Messages .....                                           | 4-6                            |
| 29 | Table 4.5.2-1 NAM Parameter Block Types.....                                      | 4-13                           |
| 30 | Table 4.5.3-1 SSPR Parameter Block Types.....                                     | 4-20                           |
| 31 | Table 4.5.4-1 Validation Parameter Block Types.....                               | 4-21                           |

|   |                                         |      |
|---|-----------------------------------------|------|
| 1 | Table 4.5.4.1-1. BCD Mapping.....       | 4-22 |
| 2 | Table C.1-1 Preferred Roaming List..... | C-1  |
| 3 | Table C.1-2 Acquisition Table .....     | C-1  |
| 4 | Table C.1-3 System Table .....          | C-2  |

## 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.
- System Selection for Preferred Roaming (SSPR) for providing mobile stations with information allowing acquisition of the preferred system in an area.

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

**AC.** See Authentication Center.

**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 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.)

**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.

- 1   **ESN.** See Electronic Serial Number.
- 2   **Forward CDMA Channel.** A CDMA Channel from a base station to mobile stations. The  
3   Forward CDMA Channel contains one or more code channels that are transmitted on a CDMA  
4   frequency assignment using a particular pilot PN offset.
- 5   **Forward Analog Voice Channel (FVC).** An analog voice channel used from a base station to a  
6   mobile station.
- 7   **Forward Traffic Channel.** A code channel used to transport user and signaling traffic from  
8   the base station to the mobile station.
- 9   **HLR.** See Home Location Register.
- 10   **Home Location Register (HLR).** The location register to which a MIN/IMSI is assigned for  
11   record purposes such as subscriber information.
- 12   **Home System.** The cellular system in which the mobile station subscribes for service.
- 13   **IMSI.** See International Mobile Station Identity.
- 14   **IMSI\_M.** MIN based IMSI using the lower 10-digits to store the MIN.
- 15   **IMSI\_T.** IMSI not associated with MIN. 15-digits or fewer.
- 16   **International Mobile Station Identity (IMSI).** A method of identifying stations in the land  
17   mobile service as specified in ITU-T Recommendation E.212.
- 18   **Long Code Mask.** A 42-bit binary number that creates the unique identity of the long code.  
19   See also Public Long Code, Private Long Code, Public Long Code Mask, and Private Long Code  
20   Mask.
- 21   **LSB.** Least significant bit.
- 22   **MCC.** See Mobile Country Code.
- 23   **Mobile Country Code (MCC).** A part of the E.212 IMSI identifying the home country. See  
24   ITU-T Recommendation E.212.
- 25   **Mobile Directory Number.** A dialable directory number which is not necessarily the same as  
26   the mobile station's air interface identification, i.e., MIN, IMSI\_M or IMSI\_T.
- 27   **MIN.** See Mobile Identification Number.
- 28   **MNC.** See Mobile Network Code.
- 29   **Mobile Identification Number (MIN).** The 34-bit number that is a digital representation of the  
30   10-digit number assigned to a mobile station.
- 31   **Mobile Network Code (MNC).** A part of the E.212 IMSI identifying the home network within  
32   the home country. See ITU-T Recommendation E.212.
- 33   **Mobile Station.** A station, fixed or mobile, which serves as the end user's wireless  
34   communication link with the base station. Mobile stations include portable units (e.g., hand-  
35   held personal units) and units installed in vehicles.
- 36   **Mobile Station Originated Call.** A call originating from a mobile station.

- 1 **Mobile Station Terminated Call.** A call received by a mobile station (not to be confused with  
2 a disconnect or call release).
- 3 **Mobile Switching Center (MSC).** A configuration of equipment that provides wireless  
4 radiotelephone service. Also called the Mobile Telephone Switching Office (MTSO).
- 5 **MSB.** Most significant bit.
- 6 **MSC.** See Mobile Switching Center.
- 7 **NAM.** See Number Assignment Module.
- 8 **Network.** A network is a subset of a wireless system, such as an area-wide wireless network,  
9 a private group of base stations, or a group of base stations set up to handle a special  
10 requirement. A network can be as small or as large as needed, as long as it is fully contained  
11 within a system. See also System.
- 12 **Network Identification (NID).** A number that uniquely identifies a network within a wireless  
13 system. See also System Identification.
- 14 **NID.** See Network Identification.
- 15 **Number Assignment Module (NAM).** A set of MIN/IMSI-related parameters stored in the  
16 mobile station.
- 17 **OTAF.** See Over-the-Air Service Provisioning Function.
- 18 **Over-the-Air Service Provisioning Function (OTAF).** A configuration of network equipment  
19 that controls OTASP functionality and messaging protocol.
- 20 **OTAPA.** See Over-the-Air Parameter Administration.
- 21 **OTASP.** See Over-the-Air Service Provisioning.
- 22 **Over-the-Air Parameter Administration (OTAPA).** Network initiated OTASP process of  
23 provisioning mobile station operational parameters over the air interface.
- 24 **Over-the-Air Service Provisioning (OTASP).** A process of provisioning mobile station  
25 operational parameters over the air interface.
- 26 **Parity Check Bits.** Bits added to a sequence of information bits to provide error detection,  
27 correction, or both.
- 28 **Private Long Code.** The long code characterized by the private long code mask.
- 29 **Private Long Code Mask.** The long code mask used to form the private long code.
- 30 **Public Long Code.** The long code characterized by the public long code mask.
- 31 **Public Long Code Mask.** The long code mask used to form the public long code. The mask  
32 contains the ESN of the mobile station. See also Private Long Code Mask.
- 33 **Release.** A process that the mobile station and base station use to inform each other of call  
34 disconnect.
- 35 **Reverse CDMA Channel.** The CDMA Channel from the mobile station to the base station.  
36 From the base station's perspective, the Reverse CDMA Channel is the sum of all mobile  
37 station transmissions on a CDMA frequency assignment.

- 1    **Roamer.** A mobile station operating in a wireless system (or network) other than the one from  
2    which service was subscribed.
- 3    **Service Option.** A service capability of the system. Service options may be applications such  
4    as voice, data, or facsimile. See TSB58.
- 5    **Service Programming Code (SPC).** A secret code assigned to the mobile station and known to  
6    the authorized network entity.
- 7    **Service Programming Lock (SPL).** A protection provided for preventing the over-the-air  
8    provisioning of certain mobile station parameters by unauthorized network entity by way of  
9    verifying the Service Programming Code (SPC).
- 10   **Shared Secret Data (SSD).** A 128-bit pattern stored in the mobile station (in semi-permanent  
11   memory) and known by the base station. SSD is a concatenation of two 64-bit subsets:  
12   SSD\_A, which is used to support the authentication procedures, and SSD\_B, which serves as  
13   one of the inputs to the process generating the encryption mask and private long code.
- 14   **SID.** See System Identification.
- 15   **SPASM.** See Subscriber Parameter Administration Security Mechanism.
- 16   **SPC.** See Service Programming Code.
- 17   **SPL.** See Service Programming Lock.
- 18   **SSD.** See Shared Secret Data.
- 19   **SSPR.** See System Selection for Preferred Roaming.
- 20   **Subscriber Parameter Administration Security Mechanism (SPASM).** Security mechanism  
21   protecting parameters and indicators of active NAM from programming by an unauthorized  
22   network entity during the OTAPA session.
- 23   **System.** A system is a wireless telephone service that covers a geographic area such as a city,  
24   metropolitan region, county, or group of counties. See also Network.
- 25   **System Identification (SID).** A number uniquely identifying a wireless system.
- 26   **System Selection Code.** A part of the Activation Code that specifies the user selection of a  
27   Band and a Block operated by the selected service provider.
- 28   **System Selection for Preferred Roaming (SSPR).** A feature that enhances the mobile station  
29   system acquisition process based on the set of additional parameters stored in the mobile  
30   station in the form of a Preferred Roaming List (PR\_LIST<sub>s-p</sub>).
- 31   **Traffic Channel.** A communication path between a mobile station and a base station used for  
32   user and signaling traffic. The term Traffic Channel implies a Forward Traffic Channel and  
33   Reverse Traffic Channel pair. See also Forward Traffic Channel and Reverse Traffic Channel.
- 34   **Voice Channel.** See Analog Voice Channel.
- 35   **Voice Privacy.** The process by which user voice transmitted over a CDMA Traffic Channel is  
36   afforded a modest degree of protection against eavesdropping over the air.

## 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<sub>p</sub>** - Protocol revision of the mobile station Key Exchange procedure.

**A\_KEY\_TEMP<sub>s</sub>** - A secret 64-bit pattern temporarily stored in the mobile station.

**AUTH\_OTAPA<sub>s</sub>** - The computed 18-bit result AUTH\_SIGNATURE used for validating SPASM.

**DATA\_P\_REV<sub>p</sub>** - Protocol revision of the mobile station NAM Download procedure.

**NAM\_LOCK<sub>p</sub>** - 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.

**NAM\_LOCK<sub>s</sub>** - 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<sub>s</sub>** - Key exchange parameter G.

**PARAM\_P<sub>s</sub>** - Key exchange parameter P.

**PR\_LIST<sub>s-p</sub>** - 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.

**SPC<sub>p</sub>** - 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<sub>p</sub> for unlocking the mobile station parameters for programming or reprogramming.

**SPC<sub>s</sub>** - Service Programming Code temporarily stored in the mobile station.

**SPL\_P\_REV<sub>p</sub>** - 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<sub>p</sub>** - Protocol revision of the mobile station SSPR Download procedure.

## 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.

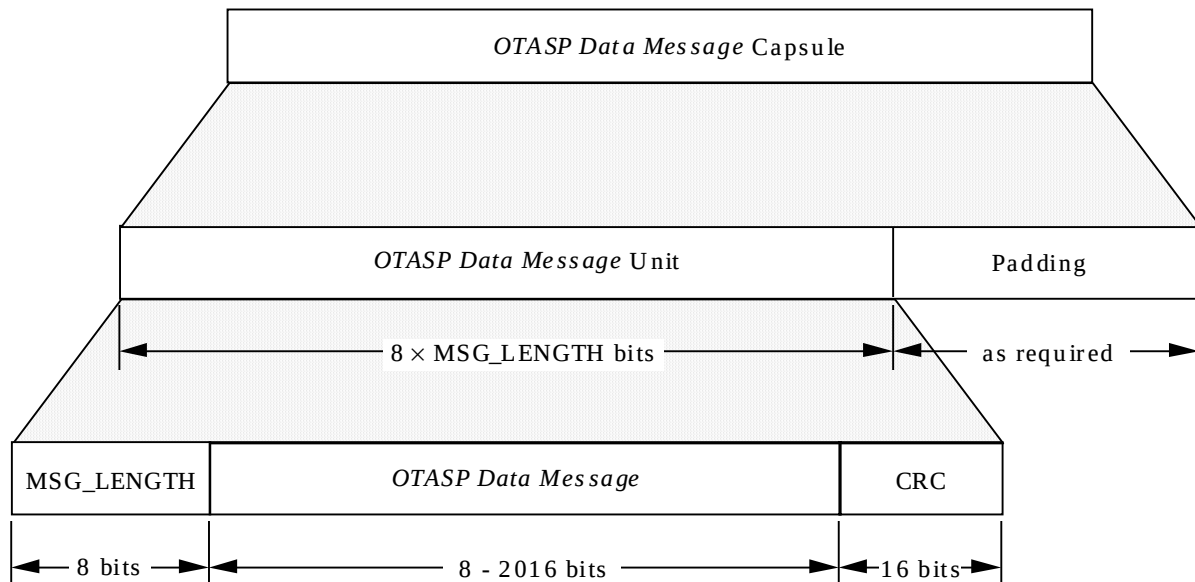
During the analog mode of operation, *OTASP Data Messages* are sent using the analog transport protocol (see 2.2). During the CDMA mode of operation, *OTASP Data Messages* are sent using the CDMA transport protocol (see 2.3).

### 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 TIA/EIA-95-B. 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**

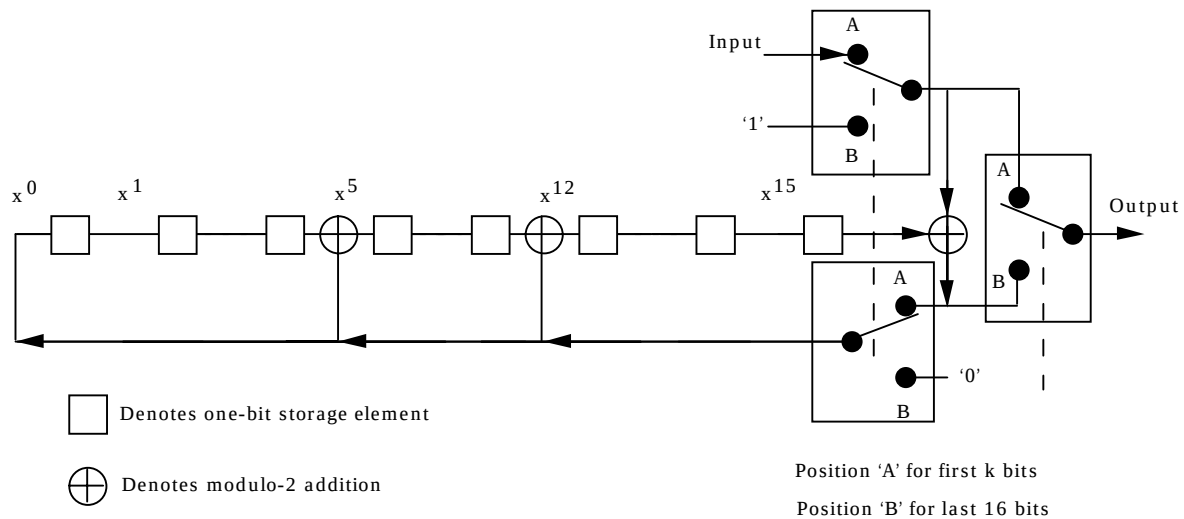
The MSG\_LENGTH field shall be set to the number of octets in the *OTASP Data Message* plus three.

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.

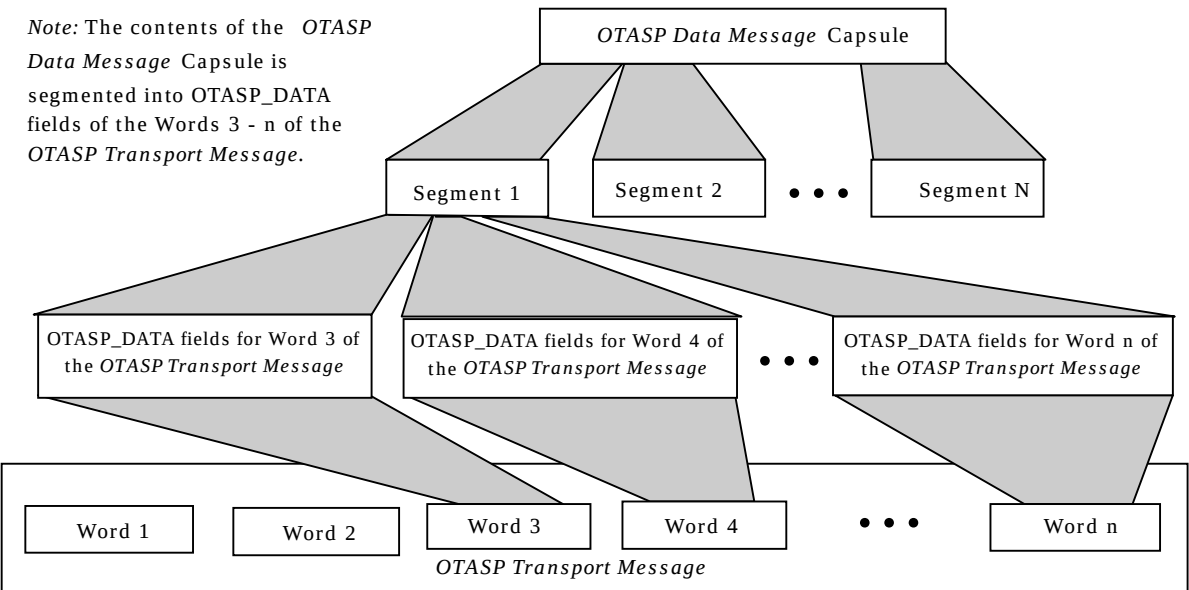


**Figure 2.2.1-2 OTASP Data Message CRC**

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

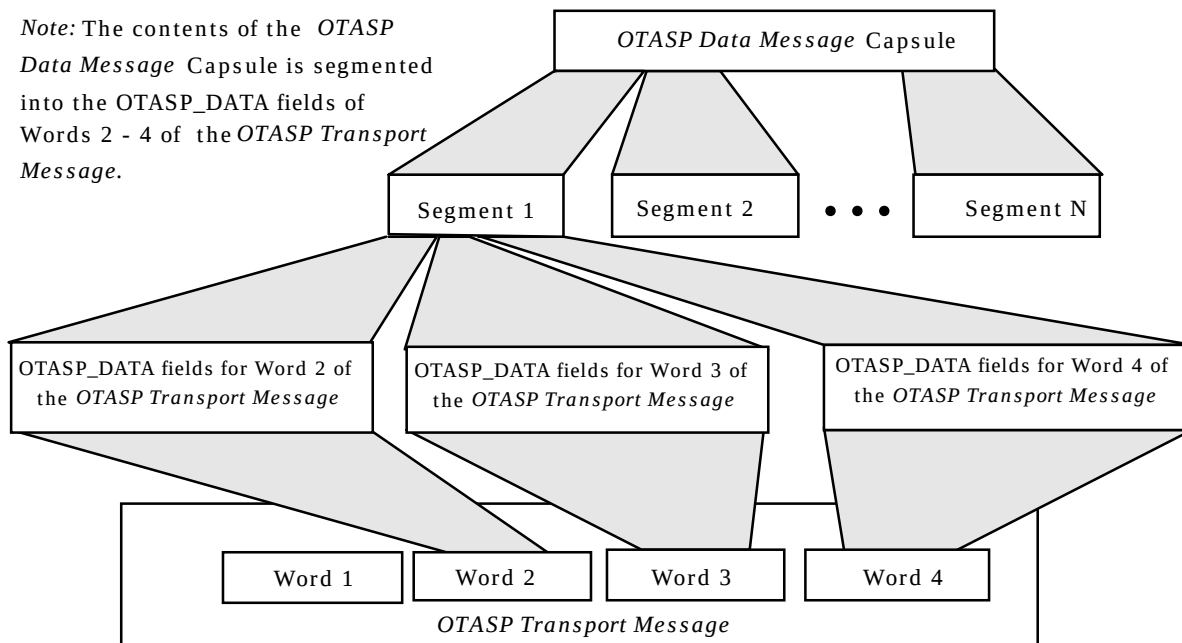
Each *OTASP Data Message Capsule* (see 2.2.1) sent on an analog voice channel shall be segmented and transmitted in one or more *OTASP Transport Messages*, as defined in 2.2.3.4 and 2.2.4.3. Figures 2.2.2-1 and 2.2.2-2 illustrate the segmentation process for the forward and reverse analog voice channels,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



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

1

Note: The contents of the *OTASP Data Message Capsule* is segmented into the *OTASP\_DATA* fields of Words 2 - 4 of the *OTASP Transport Message*.



2

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

3

### 2.2.3 Mobile Station Procedures

5

*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 TIA/EIA-95-B). The mobile station shall transmit *OTASP Transport Messages* in accordance with the procedures in 2.7.2 of TIA/EIA-95-B. 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 TIA/EIA-95-B.

10

#### 2.2.3.1 OTASP Transport Message Acknowledgment and Re-transmission

11

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.

14

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.

17

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 TIA/EIA-95-B).

22

### 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 TIA/EIA-95-B:

#### 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<sub>s</sub> to '00000', shall set the SEQ\_NUM field equal to TX\_SEQ\_NUM<sub>s</sub>, 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<sub>s</sub> to '00000', shall set the SEQ\_NUM field equal to TX\_SEQ\_NUM<sub>s</sub>, 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<sub>s</sub> to (TX\_SEQ\_NUM<sub>s</sub> + 1) modulo 32, shall set the SEQ\_NUM field equal to TX\_SEQ\_NUM<sub>s</sub>, 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<sub>s</sub> to (TX\_SEQ\_NUM<sub>s</sub> + 1) modulo 32, shall set the SEQ\_NUM field equal to TX\_SEQ\_NUM<sub>s</sub>, 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 TIA/EIA-95-B. When any message is received, the mobile station shall perform all actions specified in 2.6.4.4 of TIA/EIA-95-B that apply to a message reception. The mobile station shall take the actions specified below for each message:

#### 1. *OTASP Transport Message:*

- 1        If the value of  $ESN_r$  received in the *OTASP Transport Message* does not match the  $ESN_p$   
2        that identifies the mobile station, the mobile station shall turn off the transmitter and  
3        then enter the Serving-System Determination Task (see 2.6.3.12 of TIA/EIA-95-B).
- 4        If the value of  $ESN_r$  received in the *OTASP Transport Message* matches the  $ESN_p$ , the  
5        mobile station shall do the following:
- 6        • The mobile station shall send an *OTASP Transport Confirmation Message* within 750  
7        ms after receiving the last bit of the *OTASP Transport Message*. The mobile station  
8        shall set the SEQ\_ACK field equal to SEQ\_NUM<sub>r</sub> received in the *OTASP Transport*  
9        *Message*. The mobile station shall set the DMU\_CRC\_OK field as specified below.
  - 10       • If the value of the B/F field of the received message is '11', the OTASP\_DATA field of  
11       the received message contains an *OTASP Data Message Capsule* in its entirety (i.e.,  
12       contains an unsegmented *OTASP Data Message Capsule*). The mobile station shall  
13       discard any incomplete *OTASP Data Message Capsule* being reassembled. If the  
14       CRC of the *OTASP Data Message Unit* checks (see 2.2.1), the mobile station shall  
15       set the DMU\_CRC\_OK field of the *OTASP Transport Confirmation Message* to '1', and  
16       shall process the *OTASP Data Message* as specified in Section 3; otherwise, the  
17       mobile station shall set the DMU\_CRC\_OK field of the *OTASP Transport*  
18       *Confirmation Message* to '0', and shall discard the *OTASP Data Message Capsule*.
  - 19       • If the value of the B/F field of the received message is '10', the mobile station shall  
20       discard any incomplete *OTASP Data Message Capsule* being reassembled, and shall  
21       store the OTASP\_DATA field of the received message as the first segment of an  
22       *OTASP Data Message Capsule* to be reassembled. The mobile station shall set  
23       RX\_SEQ\_NUM<sub>s</sub> to the value of the SEQ\_NUM field of the received message. The  
24       mobile station shall set the DMU\_CRC\_OK field of the *OTASP Transport*  
25       *Confirmation Message* to '0'.
  - 26       • If the value of the B/F field of the received message is '00' and a segmented *OTASP*  
27       *Data Message Capsule* is being reassembled, the mobile station shall perform the  
28       following:
    - 29       - If  $(RX\_SEQ\_NUM_s + 1)$  modulo 32 is equal to the value of the SEQ\_NUM field of  
30       the received message, the mobile station shall store the OTASP\_DATA field of  
31       the received message as the next segment of the *OTASP Data Message Capsule*  
32       being reassembled, and shall increment RX\_SEQ\_NUM<sub>s</sub>, modulo 32.
    - 33       - If RX\_SEQ\_NUM<sub>s</sub> is equal to the value of the SEQ\_NUM field of the received  
34       message, the mobile station shall discard the OTASP\_DATA field of the received  
35       message.
    - 36       - If neither RX\_SEQ\_NUM<sub>s</sub> nor  $(RX\_SEQ\_NUM_s + 1)$  modulo 32 is equal to the  
37       value of the SEQ\_NUM field of the received message, the mobile station shall  
38       discard the OTASP\_DATA field of the received message and shall discard the  
39       incomplete *OTASP Data Message Capsule* being reassembled.
    - 40       - The mobile station shall set the DMU\_CRC\_OK field of the *OTASP Transport*  
41       *Confirmation Message* to '0'.

- 1       • If the value of the B/F field of the received message is '00', and no segmented  
2       *OTASP Data Message Capsule* is being reassembled, the mobile station shall  
3       discard the OTASP\_DATA field of the received message. The mobile station shall set  
4       the DMU\_CRC\_OK field of the *OTASP Transport Confirmation Message* to '0'.
- 5       • If the value of the B/F field of the received message is '01' and a segmented *OTASP*  
6       *Data Message Capsule* is being reassembled, the mobile station shall perform the  
7       following:
  - 8       - If  $(RX\_SEQ\_NUM_s + 1)$  modulo 32 is equal to the value of the SEQ\_NUM field of  
9       the received message, the mobile station shall store the OTASP\_DATA field of  
10       the received message as the last segment of the *OTASP Data Message Capsule*  
11       being reassembled and shall increment RX\_SEQ\_NUM<sub>s</sub>, modulo 32. If the CRC  
12       of the *OTASP Data Message Unit* checks (see 2.2.1), the mobile station shall set  
13       the DMU\_CRC\_OK field of the *OTASP Transport Confirmation Message* to '1',  
14       and shall process the *OTASP Data Message* as specified in Section 3; otherwise,  
15       the mobile station shall set the DMU\_CRC\_OK field of the *OTASP Transport*  
16       *Confirmation Message* to '0', and shall discard the *OTASP Data Message*  
17       *Capsule*.
  - 18       - If RX\_SEQ\_NUM<sub>s</sub> is equal to the value of the SEQ\_NUM field of the received  
19       message, the mobile station shall discard the OTASP\_DATA field of the received  
20       message. If the CRC of the *OTASP Data Message Unit* checks (see 2.2.1), the  
21       mobile station shall set the DMU\_CRC\_OK field of the *OTASP Transport*  
22       *Confirmation Message* to '1'; otherwise, the mobile station shall set the  
23       DMU\_CRC\_OK field to '0'.
  - 24       - If neither RX\_SEQ\_NUM<sub>s</sub> nor  $(RX\_SEQ\_NUM_s + 1)$  modulo 32 is equal to the  
25       value of the SEQ\_NUM field of the received message, the mobile station shall  
26       discard the OTASP\_DATA field of the received message and shall discard the  
27       incomplete *OTASP Data Message Capsule* being reassembled. The mobile  
28       station shall set the DMU\_CRC\_OK field of the *OTASP Transport Confirmation*  
29       *Message* to '0'.
- 30       • If the value of the B/F field of the received message is '01', and no segmented  
31       *OTASP Data Message Capsule* is being reassembled, the mobile station shall  
32       discard the OTASP\_DATA field of the received message. The mobile station shall set  
33       the DMU\_CRC\_OK field of the *OTASP Transport Confirmation Message* to '0'.

34       The mobile station shall remain in the Conversation Task.

## 35       2. *OTASP Transport Confirmation Message:*

36       If the SEQ\_ACK field is equal to TX\_SEQ\_NUM<sub>s</sub>, the mobile station shall disable the  
37       OTASP acknowledgment timer; otherwise, the mobile station shall ignore the message.  
38       The mobile station shall remain in the Conversation Task.

1    2.2.3.4 Reverse Voice Channel Message Format

2    2.2.3.4.1 OTASP Transport Message

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

- 5    • 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            |

6

- 7    • 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            |

8

- 9    • 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            |

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

- 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.

- |   |            |   |                                                                             |
|---|------------|---|-----------------------------------------------------------------------------|
| 1 | OTASP_DATA | - | The mobile station shall set these fields to the corresponding octets of    |
| 2 |            |   | the <i>OTASP Data Message Capsule</i> .                                     |
| 3 | P          | - | Parity field. The mobile station shall set this field as specified in 2.7.2 |
| 4 |            |   | of TIA/EIA-95-B.                                                            |

#### 5 2.2.3.4.2 OTASP Transport Confirmation Message

6 The mobile station Reverse Voice Channel (RVC) *OTASP Transport Confirmation Message* has  
7 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=00000000000000 | 13            |
| P                   | 12            |

- |    |            |   |                                                                                |
|----|------------|---|--------------------------------------------------------------------------------|
| 8  | F          | - | First word field. The mobile station shall set this field to '1'.              |
| 9  | NAWC       | - | Number of additional words coming field. The mobile station shall set          |
| 10 |            |   | this field to '00'.                                                            |
| 11 | T          | - | T field. The mobile station shall set this field to '1'.                       |
| 12 | MSG_TYPE   | - | Message Type field. The mobile station shall set this field to '00001'.        |
| 13 | ORDQ       | - | Order qualifier field. The mobile station shall set this field to '000'.       |
| 14 | ORDER      | - | Order field. The mobile station shall set this field to '11010'.               |
| 15 | SEQ_ACK    | - | Sequence Number for Acknowledgment by the <i>OTASP Transport</i>               |
| 16 |            |   | <i>Confirmation Message</i> . The mobile station shall set this field to the   |
| 17 |            |   | value of SEQ_NUM in the <i>OTASP Transport Message</i> being                   |
| 18 |            |   | acknowledged.                                                                  |
| 19 | DMU_CRC_OK | - | <i>OTASP Data Message</i> Unit CRC status flag. The mobile station shall set   |
| 20 |            |   | this field as specified in 2.2.3.2 to indicate whether or not the <i>OTASP</i> |
| 21 |            |   | <i>Data Message</i> Unit CRC checks.                                           |
| 22 | RSVD       | - | Reserved for future use; the mobile station shall set all bits as indicated.   |
| 23 | P          | - | Parity field. The mobile station shall set this field as specified in 2.7.2    |
| 24 |            |   | of TIA/EIA-95-B.                                                               |

## 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 TIA/EIA-95-B). The base station shall transmit *OTASP Transport Messages* as specified in 3.7.2 of TIA/EIA-95-B. 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 TIA/EIA-95-B.

### 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 TIA/EIA-95-B:

#### 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 TIA/EIA-95-B. When any message is received, the base station should perform all actions specified in 3.6.4.4 of TIA/EIA-95-B 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  $(RX\_SEQ\_NUM + 1) \text{ modulo } 32$  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  $(RX\_SEQ\_NUM + 1) \text{ modulo } 32$  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.

- 1       • If the value of the B/F field of the received message is '01' and a segmented *OTASP*
- 2       *Data Message Capsule* is being reassembled, the base station should perform the
- 3       following:
- 4       - If  $(RX\_SEQ\_NUM + 1)$  modulo 32 is equal to the value of the *SEQ\_NUM* field of
- 5       the received message, the base station should store the *OTASP\_DATA* field of
- 6       the received message as the last segment of the *OTASP Data Message Capsule*
- 7       being reassembled, should increment *RX\_SEQ\_NUM* modulo 32, and should
- 8       process the *OTASP Data Message* as specified in Section 4.
- 9       - If *RX\_SEQ\_NUM* is equal to the value of the *SEQ\_NUM* field of the received
- 10      message, the base station may discard the *OTASP\_DATA* field of the received
- 11      message.
- 12      - If neither *RX\_SEQ\_NUM* nor  $(RX\_SEQ\_NUM + 1)$  modulo 32 is equal to the
- 13      value of the *SEQ\_NUM* field of the received message, the base station may
- 14      discard the *OTASP\_DATA* field of the received message and may discard the
- 15      incomplete *OTASP Data Message Capsule* being reassembled.
- 16      • If the value of the B/F field of the received message is '01', and no segmented
- 17      *OTASP Data Message Capsule* is being reassembled, the base station may discard
- 18      the *OTASP\_DATA* field of the received message.

19      The base station should remain in the Conversation Task.

## 20      2. *OTASP Transport Confirmation Message:*

21      If *SEQ\_ACK* is equal to the sequence number of the last *OTASP Transport Message*

22      sent, the base station may transmit the next *OTASP Transport Message*; otherwise, the

23      base station should ignore the message. If the *DMU\_CRC\_OK* field indicates that the

24      CRC of the *OTASP Data Message Unit* did not check at the mobile station (see 2.2.3.3),

25      the base station should resend the *OTASP Data Message*. The base station should

26      remain in the Conversation Task.

## 27      2.2.4.3 Forward Voice Channel Message Format

### 28      2.2.4.3.1 *OTASP Transport Message*

29      When the base station sends an *OTASP Transport Message* on the Forward Voice Channel

30      (FVC), it shall use the following variable-length message format:

- 1 • 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            |

2

- 3 • 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            |

4

- 5 • 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            |

6

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

| Information Element                | Length (bits) |
|------------------------------------|---------------|
| T <sub>1</sub> T <sub>2</sub> = 01 | 2             |
| RSVD=00                            | 2             |
| OTASP_DATA                         | 24            |
| P                                  | 12            |

1

2           T<sub>1</sub>T<sub>2</sub>    -   Type field. The base station shall set this field to '10' in the first word  
3                   of the message, and to '01' in all other words.

4           SCC     -   SAT color code for new channel. The base station shall set this field to  
5                   '11'.

6           PSCC    -   Present SAT color code. The base station shall set this field to indicate  
7                   the SAT color code associated with the present channel as specified in  
8                   the Table 3.7.1.1-2 of TIA/EIA-95-B.

9           EF       -   Extended Protocol Forward Channel Indicator. The base station shall  
10                  set this field to '0'.

11          SEQ\_NUM -   Message Sequence Number. The base station shall set this field to the  
12                  message sequence number of this *OTASP Transport Message*.

13          DATA\_WORDS - The number of words in the *OTASP Transport Message* containing the  
14                  OTASP\_DATA field. The base station shall set this field to the number  
15                  of words in the *OTASP Transport Message*, not including Word 1 and  
16                  Word 2.

17          MSG\_TYPE -   Message Type field. The base station shall set this field to '00000'.

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

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

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

28          ESN\_4    -   The base station shall set this field to the most significant octet (bits  
29                  d31-d24) of the mobile station ESN.

30          ESN\_3    -   The base station shall set this field to the next to the most significant  
31                  octet (bits d23-d16) of the mobile station ESN.

32          ESN\_2    -   The base station shall set this field to the next to the least significant  
33                  octet (bits d15-d8) of the mobile station ESN.

- 1           ESN\_1    -   The base station shall set this field to the least significant octet (bits d7-  
2                            d0) of the mobile station ESN.
- 3           OTASP\_DATA   -   The base station shall set these fields to the corresponding octets of the  
4                            *OTASP Data Message Capsule*.
- 5           RSVD       -   Reserved for future use; the base station shall set all bits as indicated.
- 6           P         -   Parity field. The base station shall set this field as specified in 3.7.2 of  
7                            TIA/EIA-95-B.

#### 8   2.2.4.3.2 *OTASP Transport Confirmation Message*

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

11

| Information Element                | Length (bits) |
|------------------------------------|---------------|
| T <sub>1</sub> T <sub>2</sub> = 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            |

- 12           T<sub>1</sub>T<sub>2</sub>    -   Type field. The base station shall set this field to '10'.
- 13           SCC       -   SAT color code for new channel. The base station shall set this field to  
14                            '11'.
- 15           PSCC       -   Present SAT color code. The base station shall set this field to indicate  
16                            the SAT color code associated with the present channel as specified in  
17                            the Table 3.7.1.1-2 of TIA/EIA-95-B.
- 18           EF         -   Extended Protocol Forward Channel Indicator. The base station shall  
19                            set this field to '0'.
- 20           SEQ\_ACK   -   Sequence Number for Acknowledgment by the *OTASP Transport*  
21                            *Confirmation Message*. The base station shall set this field to the value  
22                            of SEQ\_NUM in the *OTASP Transport Message* being acknowledged.
- 23           MSG\_TYPE   -   Message Type field. The base station shall set this field to '00001'.
- 24           ORDQ       -   Order qualifier field. The base station shall set this field to '000'.

- 1           ORDER    -   Order field. The base station shall set this field to '11010'.
- 2           RSVD    -   Reserved for future use; the base station shall set all bits as indicated.
- 3           P       -   Parity field. The base station shall set this field as specified in 3.7.2 of
- 4                    TIA/EIA-95-B.

### 5   **2.3 CDMA Transport Protocol**

6   The messages defined in 3.5 and 4.5 shall be sent in the CHARi fields of *Data Burst Messages*

7   (see 6.7.2.3.2.4 and 7.7.3.3.2.4 of TIA/EIA-95-B). The BURST\_TYPE field of *Data Burst*

8   *Messages* carrying *OTASP Data Messages* shall be set to '000100' (as assigned in TSB58). The

9   MSG\_NUMBER and NUM\_MSGS fields shall be set to 1 and the NUM\_FIELDS field shall be set

10   to the number of octets in the *OTASP Data Message*.

11   The base station should send *Data Burst Messages* carrying *OTASP Data Messages* only on

12   CDMA Traffic Channels. Mobile stations shall ignore *Data Burst Messages* with the

13   BURST\_TYPE field equal to '000100' that are received on CDMA channels other than CDMA

14   Traffic Channels. *Data Burst Messages* carrying *OTASP Data Messages* shall be sent as

15   messages requiring layer 2 acknowledgment (see 6.6.4.1.3.1 and 7.6.4.1.3.1 of TIA/EIA-95-B).

- 1 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 TIA/EIA-95-B. The standard NAM indicators, stored in the mobile station's permanent and semi-permanent memory, are defined in F.3 of TIA/EIA-95-B. 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<sub>p</sub> (see 3.3.6).

Mobile stations supporting the Over-the-Air Parameter Administration (OTAPA) shall maintain an additional indicator for each NAM, NAM\_LOCK<sub>p</sub> (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, and 4.5.4.

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<sub>p</sub> shall be set to 0.
- MCC\_M<sub>p</sub>, IMSI\_M\_11\_12<sub>p</sub>, and IMSI\_M\_S<sub>p</sub> shall be set to the coded value of the IMSI\_M with the four least-significant digits set to ESN<sub>p</sub>, converted directly from binary to decimal, modulo 10000. The other digits shall be set to 0.
- IMSI\_M\_ADDR\_NUM<sub>p</sub> shall be set to '000'.
- IMSI\_T\_CLASS<sub>p</sub> shall be set to 0.
- MCC\_T<sub>p</sub>, IMSI\_T\_11\_12<sub>p</sub>, and IMSI\_T\_S<sub>p</sub> shall be set to the coded value of the IMSI\_T with the four least-significant digits set to ESN<sub>p</sub>, converted directly from binary to decimal, modulo 10000. The other digits shall be set to 0.
- IMSI\_T\_ADDR\_NUM<sub>p</sub> shall be set to '000'.
- ACCOLC<sub>p</sub> shall be set as specified in 6.3.5 of TIA/EIA-95-B.
- HOME\_SID<sub>p</sub>, 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 TIA/EIA-95-B).

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 which 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. 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            |
| 1.8 GHz, A Block | 02            |
| 1.8 GHz, B Block | 03            |
| 1.8 GHz, C Block | 04            |
| 1.8 GHz, D Block | 05            |
| 1.8 GHz, E Block | 06            |
| 1.8 GHz, F Block | 07            |
| Reserved         | 08 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 which 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:

- 1       • Set #1:
  - 2           - The mobile station supports the Service Programming Lock feature, and
  - 3           - The SPC<sub>P</sub> is set to any value other than the default value (see 3.3.6), and
  - 4           - The mobile station supports SSPR and the PR\_LIST\_SIZE is greater than zero (see
  - 5               3.5.5).
- 6       • Set #2:
  - 7           - The user has entered the feature code (\*FC) only (no system selection code or any
  - 8               additional digits have been entered), and
  - 9           - The mobile station supports SSPR and the PR\_LIST\_SIZE is greater than zero (see
  - 10               3.5.5).

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

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

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

- 18       • If an 800 MHz system is selected for provisioning, the mobile station shall perform the  
19       following:
  - 20           - The mobile station shall set CDMABAND<sub>S</sub> to '00000'.
  - 21           - If the user selects System A, the mobile station shall set SERVSYS<sub>S</sub> to SYS\_A. If the
  - 22               user selects System B, the mobile station shall set SERVSYS<sub>S</sub> to SYS\_B.
  - 23           - The mobile station shall set CDMACH<sub>S</sub> either to the Primary or Secondary CDMA
  - 24               Channel number (see 6.1.1.1.1 of TIA/EIA-95-B) for the selected system (A or B),
  - 25               and shall attempt to acquire the system as specified in 6.6.1.1.3 of TIA/EIA-95-B. If
  - 26               the mobile station fails to acquire a CDMA system on the first CDMA Channel it
  - 27               tries, the mobile station should attempt to acquire on the alternate CDMA Channel
  - 28               (Primary or Secondary) before attempting other alternatives.
  - 29           - If the mobile station fails to acquire a CDMA system on either the Primary or
  - 30               Secondary CDMA Channel, the mobile station may attempt to acquire an analog
  - 31               system as specified in 6.6.1.1.3 of TIA/EIA-95-B, using the current setting of
  - 32               SERVSYS<sub>S</sub>.
- 33       • If a 1.8 GHz system is selected for provisioning, the mobile station shall perform the  
34       following:
  - 35           - The mobile station shall set CDMABAND<sub>S</sub> = '00001'.
  - 36           - The mobile station shall set CDMACH<sub>S</sub> to a preferred CDMA Channel number (see
  - 37               Table 6.1.1.1-4 of TIA/EIA-95-B) within the selected frequency block, and shall
  - 38               attempt to acquire a CDMA system as specified in 6.6.1.1.3 of TIA/EIA-95-B.

- 1           - If the mobile station fails to acquire a CDMA system on the preferred CDMA channel  
2           it tries, the mobile station should set CDMACH<sub>s</sub> to an alternate preferred CDMA  
3           Channel number within the selected frequency block, and should attempt to acquire  
4           a CDMA system. The mobile station should continue attempting to acquire different  
5           preferred CDMA Channels until it acquires a CDMA system or until it exhausts all  
6           preferred CDMA Channels within the selected frequency block.
- 7           • If the mobile station fails to acquire a system, or the selected band is not supported by  
8           the mobile station, the mobile station shall terminate the programming procedure, and  
9           shall retain the NAM indicator values and parameters, specified in 3.1, in effect prior to  
10          the initiation of the programming procedure.

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

- 12          • If the mobile station is in the CDMA mode, the mobile station shall perform the *Mobile*  
13          *Station Origination Operation*, as defined in 6.6.2.5 of TIA/EIA-95-B, using the activation  
14          code as the dialed digits. The mobile station should request a voice service option in the  
15          *Origination Message*. The mobile station shall format each message sent on the CDMA  
16          Access Channel using an MSID field format that contains the mobile station's ESN.<sup>1</sup>
- 17          • If the mobile station is in the analog mode, the mobile station shall enter the System  
18          Access Task with an "origination" indication, using the activation code as the dialed  
19          digits. Regardless of the value of the S<sub>s</sub> bit, the mobile station shall send Serial Number  
20          Word C in all Reverse Analog Control Channel messages.

21   If the mobile station responds to a page, the mobile station shall terminate the programming  
22   procedure and shall retain the NAM indicator values and parameters, specified in 3.1, in effect  
23   prior to the initiation of the programming procedure.

24   If the mobile station does not support Service Programming Lock, the mobile station shall set  
25   mobile station locking state SP\_LOCK\_STATE to '0'.

26   If the mobile station supports Service Programming Lock and SPC<sub>p</sub> is equal to '0' (the default  
27   value), the mobile station shall set SP\_LOCK\_STATE to '0'; otherwise, the mobile station shall  
28   set SP\_LOCK\_STATE to '1'.

29   The mobile station shall set SPC<sub>s</sub> = SPC<sub>p</sub>.

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

### 33   3.2.2 Network-Initiated Procedure

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

37   OTAPA procedures can be conducted when the mobile station is in the CDMA *Conversation*  
38   *Substate* or the analog Conversation Task (see 3.2.2.3). All *OTASP Data Messages* during the

---

<sup>1</sup>For TIA/EIA-95-B, this means the MSID\_TYPE field must be set to '000' or '011'.

1 OTAPA session are exchanged between the base station and the mobile station using signaling  
2 traffic.

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

#### 6 3.2.2.1 Initiation of OTAPA in the CDMA Mobile Station Idle State

7 The network can initiate OTAPA by placing a mobile terminated call to the mobile station  
8 indicating the OTAPA service option in the *General Page Message*. The OTAPA Service Option  
9 when using Multiplex Option 1 is called Service Option 18. The OTAPA Service Option when  
10 using Multiplex Option 2 is called Service Option 19. The mobile station shall respond to  
11 paging as defined in 6.6 of TIA/EIA-95-B and perform service negotiation.

#### 12 3.2.2.2 Connection of the OTAPA Service Option

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

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

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

| <b>Service Configuration Attribute</b> | <b>Valid Selections</b>                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------|
| 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. |

2

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

| <b>Service Configuration Attribute</b> | <b>Valid Selections</b>                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------|
| 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. |

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

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

14     When Service Option 18 or 19 is connected, the Service Option shall discard all primary traffic  
15     data bits received from the multiplex sublayer, and the mobile station shall transmit null traffic  
16     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<sub>r</sub>* equal to '1', while in the *CDMA Conversation Substate* or the analog *Conversation Task*.

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<sub>s</sub>* = *NAM\_LOCK<sub>p</sub>* and *NAM\_LOCK\_STATE* = *NAM\_LOCK<sub>p</sub>*. The *NAM\_LOCK\_STATE* set to '0' indicates that SPASM protection of the mobile station's active NAM is disabled. The *NAM\_LOCK\_STATE* 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 *SPC<sub>p</sub>* 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<sub>s</sub>* = *SPC<sub>p</sub>*.

## 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:

- 1           - If the mobile station does not support a requested parameter block, the mobile  
2           station shall set RESULT\_CODE in the corresponding returned confirmation  
3           block to '00000111', "Rejected - BLOCK\_ID value not supported." The mobile  
4           station shall include the parameter block with the BLOCK\_LEN field set to  
5           '00000000'.
- 6           - If the requested data blocks exceed the allowable message length, the mobile  
7           station shall set RESULT\_CODE in the corresponding returned confirmation  
8           block to '00000000', "Accepted - Operation successful" for each Parameter  
9           Block included in the message. The mobile station shall include data blocks, in  
10          the order requested, up to the maximum number of blocks that fit into the  
11          message.
- 12          - Otherwise, the mobile station shall set RESULT\_CODE to '00000000', "Accepted  
13          - Operation successful" for each Parameter Block included in the corresponding  
14          confirmation block. The mobile station shall include complete data blocks, in  
15          the order requested, in the *Configuration Response Message*.
- 16      2. *Download Request Message*: The mobile station shall respond to the message with a  
17      *Download Response Message* within 750 ms.
  - 18          • If the *Download Request Message* contains an OTASP Parameter Block with a  
19          BLOCK\_ID that is not supported by the mobile station, the mobile station shall set  
20          BLOCK\_ID to the received parameter block identifier and RESULT\_CODE to  
21          '00000111', "Rejected - BLOCK\_ID value not supported;"
  - 22          • If the *Download Request Message* contains an OTASP Parameter Block having a  
23          size different from that supported by the mobile station, the mobile station shall set  
24          BLOCK\_ID to the received parameter block identifier and RESULT\_CODE to  
25          '00000010', "Rejected - Data size mismatch;"
  - 26          • If the *Download Request Message* contains an OTASP Parameter Block with a  
27          parameter value that is out-of-range, the mobile station shall set BLOCK\_ID to the  
28          received parameter block identifier and RESULT\_CODE to '00000100', "Rejected -  
29          Invalid parameter;"
  - 30          • If the *Download Request Message* contains an OTASP Parameter Block with  
31          MAX\_SID\_NID larger than that supported by the mobile station, the mobile station  
32          shall set BLOCK\_ID to the received parameter block identifier and RESULT\_CODE  
33          to '00000101', "Rejected - SID/NID length mismatch;"
  - 34          • If the *Download Request Message* is not accepted for any other reason, the mobile  
35          station shall set BLOCK\_ID to the received parameter block identifier and  
36          RESULT\_CODE to '00000001', "Rejected - Unknown reason;"

- 1       • Otherwise, the mobile station shall store the message data in temporary memory,  
2       set BLOCK\_ID to the received parameter block identifier, and set RESULT\_CODE to  
3       '00000000', "Accepted - Operation successful." Then, if the mobile station supports  
4       the optional NAM indicators (see F.3 of TIA/EIA-95-B), the mobile station should  
5       also store values for CDMA\_PREF\_SERV<sub>p</sub> and ANALOG\_PREF\_SERV<sub>p</sub> equal to the  
6       serving system selected for activation in temporary memory. If more than one  
7       *Download Request Message* or parameter block is received containing values for the  
8       same indicators, the mobile station shall retain only the most recently received  
9       values. If the received data includes SID/NID pairs, the mobile station shall retain  
10      only the SID/NID pairs from the most recently received message.
- 11    3. *Commit Request Message:* The mobile station shall send a *Commit Response Message*  
12      within 10 seconds after receiving the message.
- 13      • If either SP\_LOCK\_STATE, or NAM\_LOCK\_STATE, or both are set to '1', the mobile  
14      station shall not move data from temporary memory to permanent memory. The  
15      mobile station shall set RESULT\_CODE to '00001010', "Rejected - Mobile station  
16      locked;" otherwise,
  - 17       - If the mobile station is able to move data from temporary memory to permanent  
18       memory successfully, the mobile station shall set the RESULT\_CODE to  
19       '00000000', "Accepted - Operation successful."
  - 20       - If the mobile station is not able to move data from temporary memory to  
21       permanent memory for any other reason, the mobile station shall set the  
22       RESULT\_CODE to '00000001', "Rejected - Unknown reason."
  - 23       - If the mobile station has received configuration parameters in one or more  
24       *Download Request Messages*, it shall set the NAM indicators to the values  
25       contained in the received configuration parameters data. The mobile station  
26       shall not change the value of any NAM indicator for which no data has been  
27       received.
  - 28       - If the mobile station has received Preferred Roaming List parameters in one or  
29       more *SSPR Download Request Messages*, it shall set the permanent Preferred  
30       Roaming List parameters to the values contained in the received data.
  - 31       - If the received data includes SID/NID pairs, the mobile station shall set the  
32       NAM indicators to include only the SID/NID pairs received.
  - 33       - If the mobile station has stored A\_KEY\_TEMP<sub>s</sub> after receiving a *Key Generation*  
34       *Request Message*, it shall set the value of the A\_KEY<sub>p</sub> NAM indicator equal to  
35       A\_KEY\_TEMP<sub>s</sub>.
  - 36       - If the mobile station has generated the SSD<sub>s</sub> as a result of an SSD update  
37       procedure based on the A\_KEY\_TEMP<sub>s</sub>, the mobile station shall store the SSD<sub>s</sub>  
38       in SSD<sub>s-p</sub>.
  - 39       - If the mobile station has stored the SPC<sub>s</sub> after receiving a *Validation Request*  
40       *Message*, it shall set the value of the SPC<sub>p</sub> parameter equal to SPC<sub>s</sub>.

- 1                   - If the mobile station has stored the  $NAM\_LOCK_S$  after receiving a *Validation*  
2                   *Request Message*, it shall set the value of the  $NAM\_LOCK_P$  parameter equal to  
3                    $NAM\_LOCK_S$ .
- 4   4. *Re-Authenticate Request Message:* The mobile station shall send a *Re-Authenticate*  
5                   *Response Message* within 750 ms after receiving the message. The mobile station shall  
6                   set  $RAND_S = RAND_R$ . The mobile station shall perform the re-authentication procedures  
7                   specified in 3.3.2.
- 8   5. *MS Key Request Message:* The mobile station shall set  $PARAM\_P_S = PARAM\_P_R$  and  
9                    $PARAM\_G_S = PARAM\_G_R$ .
- 10                   • If the value of  $A\_KEY\_P\_REV$  in the *MS Key Request Message* is not supported by  
11                   the mobile station, the mobile station shall indicate the error condition by setting  
12                    $RESULT\_CODE$  to '00000011', "Rejected - Protocol version mismatch." The mobile  
13                   station shall send an *MS Key Response Message* within 750 ms after receiving this  
14                   message.
- 15                   • If the value of  $A\_KEY\_P\_REV$  in the *MS Key Request Message* is supported by the  
16                   mobile station, the mobile station shall set  $RESULT\_CODE$  to '00000000', "Accepted  
17                   - Operation successful." The mobile station shall compute the  $MS\_RESULT$  value in  
18                   accordance with 5.1.2 and send an *MS Key Response Message* within 30 seconds  
19                   after receiving this message.
- 20                   • If the mobile station is unable to compute the  $MS\_RESULT$  value in accordance  
21                   with 5.1.2, the mobile station shall set  $RESULT\_CODE$  to '00000001', "Rejected -  
22                   Unknown reason." The mobile station shall send an *MS Key Response Message*  
23                   within 30 seconds after receiving this message.
- 24   6. *Key Generation Request Message:*
- 25                   • If the mobile station has not received an *MS Key Request Message*, the mobile  
26                   station shall indicate the error condition by setting  $RESULT\_CODE$  to '00000110',  
27                   "Rejected - Message not expected in this mode." The mobile station shall send a *Key*  
28                   *Generation Response Message* within 750 ms after receiving this message.
- 29                   • If the mobile station has received an *MS Key Request Message* and returned  
30                    $RESULT\_CODE$  other than '00000000', "Accepted - Operation successful," the  
31                   mobile station shall indicate the error condition by setting  $RESULT\_CODE$  to  
32                   '00000110', "Rejected - Message not expected in this mode." The mobile station  
33                   shall send a *Key Generation Response Message* within 750 ms after receiving this  
34                   message.
- 35                   • Otherwise, the mobile station shall compute the value of the A-key in accordance  
36                   with 5.1.3.
- 37                   • If the mobile station has not successfully calculated the A-key in accordance with  
38                   5.1.3, the mobile station shall set  $RESULT\_CODE$  to '00000001', "Rejected -  
39                   Unknown reason." The mobile station shall then send a *Key Generation Response*  
40                   *Message* within 30 seconds after receiving this message.

- If the mobile station has successfully calculated the A-key in accordance with 5.1.3, the mobile station shall set RESULT\_CODE to '00000000', "Accepted - Operation successful." The mobile station shall then send a *Key Generation Response Message* within 30 seconds after receiving this message.

7. *Protocol Capability Request Message*: The 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 REQUEST\_OFFSET<sub>r</sub> 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<sub>r</sub>, set the SEGMENT\_SIZE to '00000000', and 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 the REQUEST\_OFFSET<sub>r</sub> 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<sub>s-p</sub>) starting at the offset corresponding to the REQUEST\_OFFSET<sub>r</sub> and not exceeding a maximum number of octets corresponding to the REQUEST\_MAX\_SIZE<sub>r</sub> received in the message.

The mobile station shall set the SEGMENT\_OFFSET in the returned Parameter Block to the value of the REQUEST\_OFFSET<sub>r</sub> 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 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 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 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.

- Otherwise, if the *SSPR Download Request Message* contains a Preferred Roaming List Parameter Block, the mobile station shall perform the following:
  - 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 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.
    - + If LAST\_SEGMENT is equal to '0', the mobile station shall set the RESULT\_CODE to '00000000', "Accepted - Operation successful" and the BLOCK\_ID to the received parameter block identifier.

- + 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 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 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 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 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 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 the BLOCK\_ID to the received parameter block identifier.

- 1                   - If SP\_LOCK\_STATE = '0' and SPC<sub>S</sub> is set to the default value, the mobile station  
2                   shall do the following:
    - 3                   + If the mobile station is programmed by the user to accept SPC change (see  
4                   3.3.6), the mobile station shall set the RESULT\_CODE to '00000000',  
5                   "Accepted - Operation successful" and the BLOCK\_ID to the received  
6                   parameter block identifier. The mobile station shall set SPC<sub>S</sub> to SPC<sub>R</sub>  
7                   received in the message.
    - 8                   + If the mobile station is programmed by the user to deny SPC change, the  
9                   mobile station shall set the RESULT\_CODE to '00001100', "Rejected - SPC  
10                  change denied by the user" and the BLOCK\_ID to the received parameter  
11                  block identifier.
  - 12               - Otherwise, if SP\_LOCK\_STATE = '0' and the SPC<sub>S</sub> is not set to the default value,  
13               the mobile station shall set SPC<sub>S</sub> = SPC<sub>R</sub> received in the message, and set the  
14               RESULT\_CODE to '00000000', "Accepted - Operation successful" and the  
15               BLOCK\_ID to the received parameter block identifier.
  - 16               • If the *Validation Request Message* contains both the Verify SPC Parameter Block  
17               and the Change SPC Parameter Block, the mobile station shall process the Verify  
18               SPC Parameter Block first.
  - 19               • If the *Validation Request Message* contains the Validate SPASM Parameter Block,  
20               the mobile station shall do the following:
    - 21               - If the programming session was initiated by the user as described in 3.2.1, the  
22               mobile station shall set the RESULT\_CODE to '00001110', "Rejected -  
23               BLOCK\_ID not expected in this mode" and the BLOCK\_ID to the received  
24               parameter block identifier.
    - 25               - If the NAM\_LOCK\_STATE = '0', the mobile station shall set the RESULT\_CODE  
26               to '00000000', "Accepted - Operation successful" and the BLOCK\_ID to the  
27               received parameter block identifier. The mobile station shall set NAM\_LOCK<sub>S</sub> =  
28               NAM\_LOCK<sub>R</sub> received in the message.
    - 29               - If the NAM\_LOCK\_STATE = '1', the mobile station shall compare the  
30               AUTH\_OTAPAR received in the message with the AUTH\_OTAPAS calculated using  
31               SPASM Validation Procedure defined in 3.3.7.
      - 32               + If the comparison results in a mismatch, the mobile station shall set the  
33               RESULT\_CODE to '00001101', "Rejected - Invalid SPASM" and the  
34               BLOCK\_ID to the received parameter block identifier.
      - 35               + If the comparison results in a match, the mobile station shall set the  
36               RESULT\_CODE to '00000000', "Accepted - Operation successful" and the  
37               BLOCK\_ID to the received parameter block identifier. The mobile station  
38               shall set the NAM\_LOCK\_STATE to '0' and the NAM\_LOCK<sub>S</sub> = NAM\_LOCK<sub>R</sub>.
- 39   11. OTAPA Request Message: The mobile station shall send the *OTAPA Response Message*  
40       within 750 ms after receiving the message.

- 1       • If the programming session was initiated by the user as described in 3.2.1, the  
2       mobile station shall indicate the error condition by setting RESULT\_CODE to  
3       '00000110', "Rejected - Message not expected in this mode." The mobile station  
4       shall set the NAM\_LOCK\_IND field to '0' and omit the RAND\_OTAPA field in the  
5       OTAPA Response Message.
- 6       • If the mobile station does not support OTAPA, or if the OTAPA was disabled by the  
7       user as described in 3.2.2, the mobile station shall indicate the error condition by  
8       setting RESULT\_CODE to '00000110', "Rejected - Message not expected in this  
9       mode." The mobile station shall set the NAM\_LOCK\_IND field to '0' and omit the  
10      RAND\_OTAPA field in the OTAPA Response Message.
- 11      • If the START\_STOP<sub>r</sub> field received in the message is equal to '1', the mobile station  
12      shall do the following:
  - 13      - If the NAM\_LOCK\_STATE = '1', the mobile station shall set the  
14      NAM\_LOCK\_IND field to '1', RAND\_OTAPA field to a randomly generated 32-bit  
15      value, and the RESULT\_CODE to the '00000000', "Accepted - Operation  
16      successful" in the OTAPA Response Message. The mobile station shall generate  
17      the AUTH\_OTAPA<sub>s</sub> as specified in 3.3.7.
  - 18      - If the NAM\_LOCK\_STATE = '0', the mobile station shall set the  
19      NAM\_LOCK\_IND field to '0', the RESULT\_CODE to the '00000000', "Accepted -  
20      Operation successful", and omit the RAND\_OTAPA field in the OTAPA Response  
21      Message.
  - 22      - The mobile station shall start the OTAPA session (see 3.2.2.3).
- 23      • If the START\_STOP<sub>r</sub> field received in the message is equal to '0', the mobile station  
24      shall set the NAM\_LOCK\_IND field to '0', the RESULT\_CODE to the '00000000',  
25      "Accepted - Operation successful", and omit the RAND\_OTAPA field in the OTAPA  
26      Response Message. The mobile station shall terminate the OTAPA session. (see 3.4)

27   If the mobile station receives an OTASP Data Message that it does not recognize or which  
28   requires a capability that is not supported, the mobile station shall discard the message and  
29   send a Mobile Station Reject Order with ORDQ set to '00000110' within T<sub>56m</sub> seconds.

### 30   3.3.2 Mobile Station SSD Update and Re-authentication

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

36   If the mobile station has not generated an A-key during the present programming session via  
37   the Key Generation Request Message, the mobile station shall follow the procedures specified in  
38   6.3.12 of TIA/EIA-95-B when performing an SSD update.

39   If the mobile station has correctly generated an A-key during the present programming session  
40   , the mobile station shall follow the procedures specified in 6.3.12 of TIA/EIA-95-B when  
41   performing an SSD update with the following exceptions:

- 1       • The mobile station shall use A\_KEY\_TEMP<sub>s</sub> as the A-key input.
- 2       • The mobile station shall store the SSD\_A\_NEW and SSD\_B\_NEW outputs in SSD\_A<sub>s</sub> and
- 3       SSD\_B<sub>s</sub>, respectively, rather than in SSD\_A<sub>s-p</sub> and SSD\_B<sub>s-p</sub>.

4       Once SSD has been generated from A\_KEY\_TEMP<sub>s</sub>, the mobile station shall use SSD<sub>s</sub> instead

5       of SSD<sub>s-p</sub> until SSD<sub>s</sub> is stored into SSD<sub>s-p</sub> after receiving a *Commit Request Message*.

6       The authentication algorithms are described in “Common Cryptographic Algorithms.” The

7       interface for the algorithms is described in “Interface Specification for Common Cryptographic

8       Algorithms.”

9       Re-authentication shall be performed as follows:

10       In the mobile station,

- 11       • Set the input parameters of the Auth\_Signature procedure (see 2.3 of “Interface
- 12       Specification for Common Cryptographic Algorithms”) as follows:
  - 13       - If the programming session was initiated by the network as described in 3.2.2,
  - 14       the input parameters shall be set as defined in 6.3.12.1.7 of TIA/EIA-95-B.
  - 15       - If the programming session was initiated by the user as described in 3.2.1, the
  - 16       input parameters shall be set as defined in 6.3.12.1.6 of TIA/EIA-95-B.
- 17       • Execute the Auth\_Signature procedure;
- 18       • Set AUTHR<sub>s</sub> equal to the 18-bit output AUTH\_SIGNATURE;
- 19       • Send AUTHR<sub>s</sub>, RANDC (eight most significant bits of RAND<sub>s</sub>), AUTH\_DATA<sub>s</sub>, and
- 20       COUNT<sub>s-p</sub> to the base station in the *Re-Authenticate Response Message*.

21       At the base station,

- 22       • Compare the received values for RANDC, and optionally COUNT, with the internally
- 23       stored values associated with the mobile station being activated;
- 24       • Compute AUTHR as described above, except use the internally stored value of
- 25       SSD\_A;
- 26       • Compare the value for AUTHR computed internally with the value of AUTHR
- 27       received from the mobile station.

28       If the comparisons executed at the base station are successful, the base station may activate

29       Message Encryption (see 3.3.3) and may also activate Voice Privacy (see 3.3.4). The base

30       station may issue a *Parameter Update Order* to the mobile station on the Forward Voice

31       Channel or on the Forward Traffic Channel, updating the value of COUNT<sub>s-p</sub> in the mobile

32       station.

33       If any of the comparisons fail, the base station may deny activation, initiate the Unique

34       Challenge-Response Procedure (see 6.3.12.1.5 of TIA/EIA-95-B ) or commence the process of

35       updating SSD (see 6.3.12.1.9 of TIA/EIA-95-B ).

### 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 Annex A).

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 TIA/EIA-95-B) or transition to the Private Long Code Mask was made (see 6.3.12.3 of TIA/EIA-95-B) 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 TIA/EIA-95-B) by means of the Private Long Code Mask used for PN spreading.

The generation of the Private Long Code Mask is specified in Annex A of TIA/EIA-95-B.

If transition to the Private Long Code Mask was made (see 6.3.12.3 of TIA/EIA-95-B) or signaling message encryption was activated (see 2.3.12.2.1 and 6.3.12.2 of TIA/EIA-95-B) 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 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<sub>s-p</sub>) 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-95-B, the SSD\_AUTH input parameter to the exclusive OR of SSD\_A<sub>S-p</sub> and A\_KEY, the ESN input parameter to the mobile station ESN, and the SAVE\_REGISTERS input parameter to FALSE.

The mobile station shall execute the Auth\_Signature procedure. The AUTH\_OTAPA<sub>S</sub> 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 computes AUTH\_OTAPA as described above with the exception of using the SSD\_AUTH input parameter set to the exclusive OR of the internally stored values 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 AUTH\_OTAPA<sub>r</sub> received in the message to its locally-computed value of the AUTH\_OTAPA<sub>S</sub>.

## 3.4 Termination of the Programming Procedure

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.

- 1 Following a CDMA-to-analog handoff, the mobile station may terminate the programming  
2 session; however, the mobile station shall not autonomously release the call.
- 3 If the mobile station receives more than five *Validation Request Messages* during the same  
4 programming session with the  $SPC_R$  value not equal to the  $SPC_P$ , the mobile station should  
5 terminate the programming session and should not begin another session until after the mobile  
6 station power is cycled.
- 7 If more than five validations of SPASM (see 3.3.7) result in a mismatch during the same  
8 programming session, the mobile station should terminate the programming session and  
9 should not begin another session until after the mobile station power is cycled.
- 10 The mobile station shall provide a means for the user to end the programming session. If the  
11 user directs the mobile station to end the programming process, the mobile station shall  
12 release the call and shall terminate the programming session.
- 13 If the programming session was initiated by the network as described in 3.2.2, and the mobile  
14 station is directed by the user to initiate a call during the OTAPA session, the mobile station  
15 shall terminate the OTAPA session and release the OTAPA call prior to proceeding with the  
16 origination procedure.
- 17 If the mobile station receives the *OTAPA Request Message* with the  $START\_STOP_R$  equal to '0', it  
18 shall terminate the OTAPA session.
- 19 If the programming session is terminated, the mobile station shall discard all the NAM  
20 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 |
|--------------------------------------------------------------------------|-------------------------------|-----------|
| <i>Configuration Response Message</i>                                    | '00000000'                    | 3.5.1.1   |
| <i>Download Response Message</i>                                         | '00000001'                    | 3.5.1.2   |
| <i>MS Key Response Message</i>                                           | '00000010'                    | 3.5.1.3   |
| <i>Key Generation Response Message</i>                                   | '00000011'                    | 3.5.1.4   |
| <i>Re-Authenticate Response Message</i>                                  | '00000100'                    | 3.5.1.5   |
| <i>Commit Response Message</i>                                           | '00000101'                    | 3.5.1.6   |
| <i>Protocol Capability Response Message</i>                              | '00000110'                    | 3.5.1.7   |
| <i>SSPR Configuration Response Message</i>                               | '00000111'                    | 3.5.1.8   |
| <i>SSPR Download Response Message</i>                                    | '00001000'                    | 3.5.1.9   |
| <i>Validation Response Message</i>                                       | '00001001'                    | 3.5.1.10  |
| <i>OTAPA Response Message</i>                                            | '00001010'                    | 3.5.1.11  |
| Reserved for future standardization                                      | '00001011' through '10111111' |           |
| Available for manufacturer-specific <i>OTASP Data Message</i> definition | '11000000' through '11111110' | See TSB58 |
| 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 |
|-------------|---|

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.

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.

1

## 2 3.5.1.2 Download Response Message

3 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 |

4 OTASP\_MSG\_TYPE - OTASP Data Message type.

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

6 NUM\_BLOCKS - Number of parameter blocks.

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

10 BLOCK\_ID - Parameter block identifier.

11 The mobile station shall set this field to the value of the  
 12 BLOCK\_ID field of the corresponding parameter block in the  
 13 *Download Request Message* that is being confirmed (see Table  
 14 4.5.2-1).

15 RESULT\_CODE - Download result code.

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

**Table 3.5.1.2-1 Result Codes**

| <b>RESULT_CODE</b>         | <b>Message Parameter Description</b>                                    |
|----------------------------|-------------------------------------------------------------------------|
| '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' -<br>'01111111' | Reserved for future standardization                                     |
| '10000000' -<br>'11111110' | Available for manufacturer-specific Result Code definitions. See TSB58. |
| '11111111'                 | Reserved                                                                |

### 3.5.1.3 MS Key Response Message

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

| <b>Field</b>                | <b>Length (bits)</b> |
|-----------------------------|----------------------|
| 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                   | $8 \times \text{MS\_RESULT\_LEN}$ |

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.

The mobile station shall set this field equal to the value of MS\_RESULT as described in 5.1.2.

## 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.

- 1                   RANDC    -   Random challenge value.  
 2                                The mobile station shall set this field as specified in 3.3.2.  
 3                   COUNT   -   Call history parameter.  
 4                                The mobile station shall set this field as specified in 3.3.2.  
 5                   AUTH\_DATA   -   Authentication Data input parameter.  
 6                                The mobile station shall set this field as specified in 3.3.2.

7

## 8   3.5.1.6 Commit Response Message

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

| Field                       | Length (bits) |
|-----------------------------|---------------|
| OTASP_MSG_TYPE ('00000101') | 8             |
| RESULT_CODE                 | 8             |

10

- 11           OTASP\_MSG\_TYPE   -   *OTASP Data Message* type.  
 12                                The mobile station shall set this field to '00000101'.  
 13           RESULT\_CODE       -   Data commit result code.  
 14                                The mobile station shall set this field to indicate acceptance or  
 15                                rejection status of the *Commit Request Message*, using values  
 16                                defined in Table 3.5.1.2-1.

17

## 18   3.5.1.7 Protocol Capability Response Message

19   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 | $8 \times \text{ADD\_LENGTH}$ |

1

2 OTASP\_MSG\_TYPE - OTASP Data Message type.

3 The mobile station shall set this field to '00000110'.

4 MOB\_FIRM\_REV - Mobile station firmware revision number.

5 The mobile station shall set this field to the value of the  
6 MOB\_FIRM\_REV<sub>p</sub> permanent mobile station indicator (see F.2.1  
7 of TIA/EIA-95-B).

8 MOB\_MODEL - Mobile station manufacturer's model number.

9 The mobile station shall set this field to the value of the  
10 MOB\_MODEL<sub>p</sub> permanent mobile station indicator (see F.2.1 of  
11 TIA/EIA-95-B).

12 NUM\_FEATURES - Number of Features.

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

15 FEATURE\_ID - Feature Identifier.

16 The mobile station shall set this field according to Table 3.5.1.7-  
17 1 to indicate the feature supported by the mobile station.

18 FEATURE\_P\_REV - Feature protocol version.

19 The mobile station shall set this field according to Table 3.5.1.7-  
20 1 to indicate the protocol version of the feature supported by the  
21 mobile station.

22

**Table 3.5.1.7-1 Feature Identifier**

| <b>Features</b>                                     | <b>FEATURE_ID</b>                   | <b>FEATURE_P_REV</b> |
|-----------------------------------------------------|-------------------------------------|----------------------|
| NAM Download (DATA_P_REV)                           | '00000000'                          | '00000010'           |
| Key Exchange (A_KEY_P_REV)                          | '00000001'                          | '00000010'           |
| System Selection for Preferred Roaming (SSPR_P_REV) | '00000010'                          | '00000001'           |
| Service Programming Lock (SPL_P_REV)                | '00000011'                          | '00000001'           |
| Over-The-Air Parameter Administration (OTAPA_P_REV) | '00000100'                          | '00000001'           |
| Reserved for future standardization                 | '00000101'<br>through<br>'10111111' |                      |
| Available for manufacturer-specific features        | '11000000'<br>through<br>'11111110' | See TSB58            |
| 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.

| <b>Field</b>  | <b>Length (bits)</b> |
|---------------|----------------------|
| 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**

| <b>Description</b>  | <b>Length (bits)</b> |
|---------------------|----------------------|
| Band Class 0 Analog | 1                    |
| Band Class 0 CDMA   | 1                    |
| Band Class 1 CDMA   | 1                    |
| RESERVED            | 5                    |

### 3.5.1.8 SSPR Configuration Response Message

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

| <b>Field</b>                | <b>Length (bits)</b>         |
|-----------------------------|------------------------------|
| OTASP_MSG_TYPE ('00000111') | 8                            |
| BLOCK_ID                    | 8                            |
| RESULT_CODE                 | 8                            |
| BLOCK_LEN                   | 8                            |
| PARAM_DATA                  | $8 \times \text{BLOCK\_LEN}$ |

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.

### 3.5.1.9 SSPR Download Response Message

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

| Field                       | Length (bits) |
|-----------------------------|---------------|
| OTASP_MSG_TYPE ('00001000') | 8             |
| BLOCK_ID                    | 8             |
| RESULT_CODE                 | 8             |
| 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.

The mobile station shall set this field to the value of SEGMENT\_OFFSET from the *SSPR Download Request Message* that is being confirmed.

SEGMENT\_SIZE - Segment size.

The mobile station shall set this field to the number of octets of the preferred roaming list (PR\_LIST<sub>s-p</sub>) included in SEGMENT\_DATA of the *SSPR Download Request Message* that is being confirmed.

### 3.5.1.10 Validation Response Message

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

1

| 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 |

2

3 OTASP\_MSG\_TYPE - OTASP Data Message type.

4 The mobile station shall set this field to '00001001'.

5 NUM\_BLOCKS - Number of parameter blocks.

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

9 BLOCK\_ID - Parameter block identifier.

10 The mobile station shall set this field to the value of the  
11 BLOCK\_ID field of the corresponding parameter block in the  
12 *Validation Request Message* that is being confirmed (see Table  
13 4.5.4-1).

14 RESULT\_CODE - Service programming lock result code.

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

19

#### 20 3.5.1.11 OTAPA Response Message

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

22

| Field                       | Length (bits) |
|-----------------------------|---------------|
| OTASP_MSG_TYPE ('00001010') | 8             |
| RESULT_CODE                 | 8             |
| RESERVED                    | 7             |
| NAM_LOCK_IND                | 1             |
| RAND_OTAPA                  | 0 or 32       |

23

24 OTASP\_MSG\_TYPE - OTASP Data Message type.

|    |              |   |                                                                          |
|----|--------------|---|--------------------------------------------------------------------------|
| 1  |              |   | The mobile station shall set this field to '00001010'.                   |
| 2  | RESULT_CODE  | - | OTAPA result code.                                                       |
| 3  |              |   | The mobile station shall set this field using the values defined in      |
| 4  |              |   | Table 3.5.1.2.-1.                                                        |
| 5  | RESERVED     | - | Reserved field.                                                          |
| 6  |              |   | The mobile station shall set this field to '0000000'                     |
| 7  | NAM_LOCK_IND | - | NAM_LOCK indicator.                                                      |
| 8  |              |   | If the mobile station is sending this message in response to the         |
| 9  |              |   | <i>OTAPA Request Message</i> containing the START_STOP field equal       |
| 10 |              |   | to '1', the mobile station shall set this field to '1' if the indicators |
| 11 |              |   | and parameters of the active NAM are secured by SPASM (see               |
| 12 |              |   | 3.3.7); otherwise, the mobile station shall set this field to '0'.       |
| 13 |              |   | If the mobile station is sending this message in response to the         |
| 14 |              |   | <i>OTAPA Request Message</i> containing the START_STOP field equal       |
| 15 |              |   | to '0', the mobile station shall set this field to '0'.                  |
| 16 | RAND_OTAPA   | - | SPASM random challenge.                                                  |
| 17 |              |   | If the NAM_LOCK_IND is equal to '1', the mobile station shall set        |
| 18 |              |   | this field as specified in 3.3.7; otherwise, the mobile station shall    |
| 19 |              |   | omit this field.                                                         |

20

### 21 3.5.2 NAM Parameter Blocks

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

24

1

**Table 3.5.2-1 NAM Parameter Block Types**

| <b>Parameter Block Type</b>                                        | <b>BLOCK_ID</b>                     | <b>Reference</b> |
|--------------------------------------------------------------------|-------------------------------------|------------------|
| 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'<br>through<br>'01111111' |                  |
| Available for manufacturer-specific<br>parameter block definitions | '10000000'<br>through<br>'11111110' | See TSB58        |
| Reserved                                                           | '11111111'                          |                  |

2

## 3 3.5.2.1 CDMA/Analog NAM Parameter Block

4 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 |
|----------|--------|

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13

- FIRSTCHP - First paging channel used in the home system.  
The mobile station shall set this field to the value of the FIRSTCHP<sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).
- HOME\_SID - Home system identification.  
The mobile station shall set this field to the value of the HOME\_SID<sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).
- EX - Extended address indicator.  
The mobile station shall set this field to the value of the EX<sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).
- SCM - Station class mark.  
The mobile station shall set this field to the value of the SCM<sub>p</sub> permanent mobile station indicator (see F.2.1 of TIA/EIA-95-B).

|    |                  |   |                                                                           |
|----|------------------|---|---------------------------------------------------------------------------|
| 1  | MOB_P_REV        | - | Mobile station protocol revision number.                                  |
| 2  |                  |   | The mobile station shall set this field to the value of the               |
| 3  |                  |   | MOB_P_REV <sub>p</sub> permanent mobile station indicator (see F.2.1 of   |
| 4  |                  |   | TIA/EIA-95-B).                                                            |
| 5  | IMSI_M_CLASS     | - | IMSI_M Class assignment of the mobile station.                            |
| 6  |                  |   | If the mobile station's IMSI_M is a class 0 IMSI, the mobile              |
| 7  |                  |   | station shall set this field to '0'; otherwise, the mobile station        |
| 8  |                  |   | shall set this field to '1'.                                              |
| 9  | IMSI_M_ADDR_NUM  | - | Number of IMSI_M address digits.                                          |
| 10 |                  |   | If the mobile station has been assigned a class 1 IMSI_M (see             |
| 11 |                  |   | F.3 and 6.3.1 of TIA/EIA-95-B), the mobile station shall set this         |
| 12 |                  |   | field to four less than the number of digits in the NMSI;                 |
| 13 |                  |   | otherwise, the mobile station shall set this field to '000'.              |
| 14 | MCC_M            | - | Mobile country code.                                                      |
| 15 |                  |   | The mobile station shall set this field to the value of the               |
| 16 |                  |   | MCC_M <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).     |
| 17 | IMSI_M_11_12     | - | 11th and 12th digits of the IMSI_M.                                       |
| 18 |                  |   | The mobile station shall set this field to the value of the               |
| 19 |                  |   | IMSI_M_11_12 <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95- |
| 20 |                  |   | B).                                                                       |
| 21 | IMSI_M_S         | - | The least significant 10 digits of the IMSI_M.                            |
| 22 |                  |   | The mobile station shall set this field to the value of the               |
| 23 |                  |   | IMSI_M_S <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).  |
| 24 | ACCOLC           | - | Access overload class.                                                    |
| 25 |                  |   | The mobile station shall set this field to the value of the               |
| 26 |                  |   | ACCOLC <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).              |
| 27 | LOCAL_CONTROL    | - | Local control status.                                                     |
| 28 |                  |   | If the local control status is enabled (see 2.6.1.2.2 of TIA/EIA-         |
| 29 |                  |   | 95-B), the mobile station shall set this field to '1'; otherwise, the     |
| 30 |                  |   | mobile station shall set this field to '0'.                               |
| 31 | MOB_TERM_HOME    | - | Termination indicator for the home system.                                |
| 32 |                  |   | The mobile station shall set this field to the value of the               |
| 33 |                  |   | MOB_TERM_HOME <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).       |
| 34 | MOB_TERM_FOR_SID | - | Termination indicator for SID roaming.                                    |
| 35 |                  |   | The mobile station shall set this field to the value of the               |
| 36 |                  |   | MOB_TERM_FOR_SID <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-       |
| 37 |                  |   | B).                                                                       |
| 38 | MOB_TERM_FOR_NID | - | Termination indicator for NID roaming.                                    |
| 39 |                  |   | The mobile station shall set this field to the value of the               |
| 40 |                  |   | MOB_TERM_FOR_NID <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-       |
| 41 |                  |   | B).                                                                       |
| 42 | MAX_SID_NID      | - | Maximum stored SID/NID pairs.                                             |

- 1 The mobile station shall set this field to the maximum number of  
2 SID/NID pairs that it can store in the NAM.
- 3 **STORED\_SID\_NID** - Number of stored SID/NID pairs.
- 4 The mobile station shall set this field to the number of SID/NID  
5 pairs stored in the NAM. All SID/NID pairs stored in the NAM  
6 shall be included in the parameter block.
- 7 **SID** - System identification.
- 8 The mobile station shall include one occurrence of this field for  
9 each SID/NID pair stored in the NAM. The mobile station shall  
10 set this field to the value of the SID<sub>p</sub> NAM indicator (see F.3 of  
11 TIA/EIA-95-B).
- 12 **NID** - Network identification.
- 13 The mobile station shall include one occurrence of this field for  
14 each SID/NID pair stored in the NAM. The mobile station shall  
15 set this field to the value of the NID<sub>p</sub> NAM indicator (see F.3 of  
16 TIA/EIA-95-B).
- 17 **RESERVED** - Reserved bits.
- 18 The mobile station shall add reserved bits as needed in order to  
19 make the length of the entire parameter block equal to an  
20 integer number of octets. The mobile station shall set these bits  
21 to '0'.

22

### 23 3.5.2.2 Mobile Directory Number

24 The PARAM\_DATA field of the Mobile Directory Number Parameter Block consists of the  
25 following fields:

| Field    | Length (bits) |
|----------|---------------|
| N_DIGITS | 4             |

N\_DIGITS occurrences of the following field:

|                    |   |
|--------------------|---|
| DIGIT <sub>n</sub> | 4 |
|--------------------|---|

The parameter block ends with the following field:

|          |                    |
|----------|--------------------|
| RESERVED | 0 or 4 (as needed) |
|----------|--------------------|

26

- 27 **N\_DIGITS** - Number of digits.
- 28 The mobile station shall set this field to the number of digits  
29 included in the parameter block.
- 30 **DIGIT<sub>n</sub>** - Digit.
- 31 The mobile station shall set these fields to the digits of the  
32 mobile station directory number. Each digit shall be encoded  
33 according to Table 6.7.1.3.2.4-4 of TIA/EIA-95-B.

1                    RESERVED    -    Reserved bits.

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

6

### 7    3.5.2.3 CDMA NAM Parameter Block

8    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 |
|----------|--------|

9

10                    RESERVED    -    Reserved bits.

11                                    The mobile station shall set this field to '00'.

12                    SLOTTED\_MODE    -    Slotted mode.

|    |                  |                                                                           |
|----|------------------|---------------------------------------------------------------------------|
| 1  |                  | If the mobile station is operating in the slotted mode, the mobile        |
| 2  |                  | station shall set this field to '1'; otherwise, the mobile station        |
| 3  |                  | shall set this field to '0'.                                              |
| 4  | RESERVED         | - Reserved bits.                                                          |
| 5  |                  | The mobile station shall set this field to '00000'.                       |
| 6  | MOB_P_REV        | - Mobile station protocol revision number.                                |
| 7  |                  | The mobile station shall set this field to the value of the               |
| 8  |                  | MOB_P_REV <sub>p</sub> permanent mobile station indicator (see F.2.1 of   |
| 9  |                  | TIA/EIA-95-B).                                                            |
| 10 | IMSI_M_CLASS     | - IMSI_M Class assignment of the mobile station.                          |
| 11 |                  | If the mobile station's IMSI_M is a class 0 IMSI, the mobile              |
| 12 |                  | station shall set this field to '0'; otherwise, the mobile station        |
| 13 |                  | shall set this field to '1'.                                              |
| 14 | IMSI_M_ADDR_NUM  | - Number of IMSI_M address digits.                                        |
| 15 |                  | If the mobile station has been assigned a class 1 IMSI_M (see             |
| 16 |                  | F.3 TIA/EIA-95-B), the mobile station shall set this field to four        |
| 17 |                  | less than the number of digits in the NMSI; otherwise, the                |
| 18 |                  | mobile station shall set this field to '000'.                             |
| 19 | MCC_M            | - Mobile country code.                                                    |
| 20 |                  | The mobile station shall set this field to the value of the               |
| 21 |                  | MCC_M <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).     |
| 22 | IMSI_M_11_12     | - 11th and 12th digits of the IMSI.                                       |
| 23 |                  | The mobile station shall set this field to the value of the               |
| 24 |                  | IMSI_M_11_12 <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95- |
| 25 |                  | B).                                                                       |
| 26 | IMSI_M_S         | - The least significant 10 digits of the IMSI.                            |
| 27 |                  | The mobile station shall set this field to the value of the               |
| 28 |                  | IMSI_M_S <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).  |
| 29 | ACCOLC           | - Access overload class.                                                  |
| 30 |                  | The mobile station shall set this field to the value of the               |
| 31 |                  | ACCOLC <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).              |
| 32 | LOCAL CONTROL    | - Local control status.                                                   |
| 33 |                  | If the local control status is enabled (see 6.3.9 of TIA/EIA-95-B),       |
| 34 |                  | the mobile station shall set this field to '1'; otherwise, the mobile     |
| 35 |                  | station shall set this field to '0'.                                      |
| 36 | MOB_TERM_HOME    | - Termination indicator for the home system.                              |
| 37 |                  | The mobile station shall set this field to the value of the               |
| 38 |                  | MOB_TERM_HOME <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-B).       |
| 39 | MOB_TERM_FOR_SID | - Termination indicator for SID roaming.                                  |
| 40 |                  | The mobile station shall set this field to the value of the               |
| 41 |                  | MOB_TERM_FOR_SID <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-       |
| 42 |                  | B).                                                                       |

- |    |                  |   |                                                                               |
|----|------------------|---|-------------------------------------------------------------------------------|
| 1  | MOB_TERM_FOR_NID | - | Termination indicator for NID roaming.                                        |
| 2  |                  |   | The mobile station shall set this field to the value of the                   |
| 3  |                  |   | MOB_TERM_FOR_NID <sub>p</sub> NAM indicator (see F.3 of TIA/EIA-95-           |
| 4  |                  |   | B).                                                                           |
| 5  | MAX_SID_NID      | - | Maximum stored SID/NID pairs.                                                 |
| 6  |                  |   | The mobile station shall set this field to the maximum number of              |
| 7  |                  |   | SID/NID pairs that it can store in the NAM.                                   |
| 8  | STORED_SID_NID   | - | Number of stored SID/NID pairs.                                               |
| 9  |                  |   | The mobile station shall set this field to the number of SID/NID              |
| 10 |                  |   | pairs stored in the NAM. All SID/NID pairs stored in the NAM                  |
| 11 |                  |   | shall be included in the parameter block.                                     |
| 12 | SID              | - | System identification.                                                        |
| 13 |                  |   | The mobile station shall include one occurrence of this field for             |
| 14 |                  |   | each SID/NID pair stored in the NAM. The mobile station shall                 |
| 15 |                  |   | set this field to the value of the SID <sub>p</sub> NAM indicator (see F.3 of |
| 16 |                  |   | TIA/EIA-95-B).                                                                |
| 17 | NID              | - | Network identification.                                                       |
| 18 |                  |   | The mobile station shall include one occurrence of this field for             |
| 19 |                  |   | each SID/NID pair stored in the NAM. The mobile station shall                 |
| 20 |                  |   | set this field to the value of the NID <sub>p</sub> NAM indicator (see F.3 of |
| 21 |                  |   | TIA/EIA-95-B).                                                                |
| 22 | RESERVED         | - | Reserved bits.                                                                |
| 23 |                  |   | The mobile station shall add reserved bits as needed in order to              |
| 24 |                  |   | make the length of the entire parameter block equal to an                     |
| 25 |                  |   | integer number of octets. The mobile station shall set these bits             |
| 26 |                  |   | to '0'.                                                                       |

### 28 3.5.2.4 IMSI\_T Parameter Block

29 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             |

- 31 IMSI\_T\_CLASS - IMSI\_T Class assignment of the mobile station.

|    |                 |   |                                                                                |
|----|-----------------|---|--------------------------------------------------------------------------------|
| 1  |                 |   | If the mobile station's IMSI_T is a class 0 IMSI, the mobile                   |
| 2  |                 |   | station shall set this field to '0'; otherwise, the mobile station             |
| 3  |                 |   | shall set this field to '1'.                                                   |
| 4  | IMSI_T_ADDR_NUM | - | Number of IMSI_T address digits.                                               |
| 5  |                 |   | If the mobile station has been assigned a class 1 IMSI_T (see                  |
| 6  |                 |   | 6.3.1 of TIA/EIA-95-B), the mobile station shall set this field to             |
| 7  |                 |   | four less than the number of digits in the NMSI; otherwise, the                |
| 8  |                 |   | mobile station shall set this field to '000'.                                  |
| 9  | MCC_T           | - | Mobile country code.                                                           |
| 10 |                 |   | The mobile station shall set this field to the value of the MCC_T <sub>p</sub> |
| 11 |                 |   | NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).                             |
| 12 | IMSI_T_11_12    | - | 11th and 12th digits of the IMSI_T.                                            |
| 13 |                 |   | The mobile station shall set this field to the value of the                    |
| 14 |                 |   | IMSI_T_11_12 <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-      |
| 15 |                 |   | B).                                                                            |
| 16 | IMSI_T_S        | - | The least significant 10 digits of the IMSI_T.                                 |
| 17 |                 |   | The mobile station shall set this field to the value of the                    |
| 18 |                 |   | IMSI_T_S <sub>p</sub> NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).       |
| 19 | RESERVED        | - | Reserved bits.                                                                 |
| 20 |                 |   | The mobile station shall set this field to '0'.                                |

21

### 22 3.5.3 SSPR Parameter Blocks

23 Table 3.5.3-1 lists the types of parameter blocks used in the *SSPR Configuration Request*  
 24 *Message* and the *SSPR Configuration Response Message*.

25

**Table 3.5.3-1 SSPR Parameter Block Types**

| <b>SSPR Parameter Block Type</b>                                | <b>BLOCK_ID</b>            | <b>Reference</b> |
|-----------------------------------------------------------------|----------------------------|------------------|
| Preferred Roaming List Dimensions                               | '00000000'                 | 3.5.3.1          |
| Preferred Roaming List                                          | '00000001'                 | 3.5.3.2          |
| Reserved for future standardization                             | '00000010' -<br>'01111111' |                  |
| Available for manufacturer-specific parameter block definitions | '10000000'-<br>'11111110'  | See TSB58        |
| 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:

| <b>Field</b>     | <b>Length (bits)</b> |
|------------------|----------------------|
| 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<sub>s-p</sub>).
- 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<sub>s-p</sub>) by the base station.
- RESERVED** - Reserved bit.
- The mobile station shall set this field to '0'.
- NUM\_ACQ\_RECS** - Number of acquisition records.

1                   The mobile station shall set this field to the number of  
2                   acquisition records contained in the ACQ\_TABLE field of the  
3                   current preferred roaming list.

4           NUM\_SYS\_RECS   -   Number of system records.

5                   The mobile station shall set this field to the number of system  
6                   records contained in the SYS\_TABLE field of the current  
7                   preferred roaming list.

8

### 9   3.5.3.2 Preferred Roaming List Parameter Block

10   The PARAM\_DATA field of the Preferred Roaming List Parameter Block consists of the following  
11   fields:

12

| Field          | Length (bits)                   |
|----------------|---------------------------------|
| RESERVED       | 7                               |
| LAST_SEGMENT   | 1                               |
| SEGMENT_OFFSET | 16                              |
| SEGMENT_SIZE   | 8                               |
| SEGMENT_DATA   | $8 \times \text{SEGMENT\_SIZE}$ |

13

14           RESERVED   -   Reserved bits.

15                   The mobile station shall set this field to '0000000'.

16           LAST\_SEGMENT   -   Last segment indicator bit.

17                   The mobile station shall set this field to '1' if SEGMENT\_DATA  
18                   contains the last octet of the preferred roaming list (PR\_LIST<sub>s-p</sub>);  
19                   otherwise, the mobile station shall set this field to '0'.

20           SEGMENT\_OFFSET   -   Segment offset.

21                   The mobile station shall set this field to the value of  
22                   REQUEST\_OFFSET from the corresponding *SSPR Configuration*  
23                   *Request Message*.

24           SEGMENT\_SIZE   -   Segment size.

25                   The mobile station shall set this field to the number of octets of  
26                   the preferred roaming list (PR\_LIST<sub>s-p</sub>) included in  
27                   SEGMENT\_DATA.

28           SEGMENT\_DATA   -   Segment of the preferred roaming list (PR\_LIST<sub>s-p</sub>) data.

29                   If REQUEST\_OFFSET from the corresponding *SSPR*  
30                   *Configuration Request Message* specifies an offset which is  
31                   invalid for the current preferred roaming list, the mobile station  
32                   shall include no octets in this field.

If REQUEST\_OFFSET specifies an offset which 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.

#### 3.5.4 Reserved

Reserved.

#### 3.5.5 Preferred Roaming List

The preferred roaming list (PR\_LIST<sub>s-p</sub>) 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.

The preferred roaming list 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<sub>s-p</sub>) by the base station.

|    |              |                                                                      |
|----|--------------|----------------------------------------------------------------------|
| 1  | PREF_ONLY    | - Preferred only.                                                    |
| 2  |              | This field is set to '1' if the mobile station is to operate only on |
| 3  |              | systems that are specified in SYS_TABLE with PREF_NEG set to         |
| 4  |              | '1'. This field is set to '0' if the mobile station is to operate on |
| 5  |              | systems that are specified in SYS_TABLE with PREF_NEG set to         |
| 6  |              | '1' or on systems that are not specified in SYS_TABLE <sup>2</sup> . |
| 7  | DEF_ROAM_IND | - Default roaming indication.                                        |
| 8  |              | This field is set to the roaming indication value the mobile         |
| 9  |              | station is to use when operating on systems not specified in         |
| 10 |              | SYS_TABLE (see TSB58).                                               |
| 11 | NUM_ACQ_RECS | - Number of acquisition records.                                     |
| 12 |              | This field is set to the number of acquisition records contained     |
| 13 |              | in ACQ_TABLE (see Table 3.5.5.2-1).                                  |
| 14 | NUM_SYS_RECS | - Number of system records.                                          |
| 15 |              | This field is set to the number of system records contained in       |
| 16 |              | SYS_TABLE.                                                           |
| 17 | ACQ_TABLE    | - Acquisition Table.                                                 |
| 18 |              | This field contains acquisition records. The number of               |
| 19 |              | acquisition records is specified by NUM_ACQ_RECS. The                |
| 20 |              | acquisition record formats are specified in 3.5.5.2.                 |
| 21 | SYS_TABLE    | - System Table.                                                      |
| 22 |              | This field contains system records. The number of system             |
| 23 |              | records is specified by NUM_SYS_RECS. The system record              |
| 24 |              | format is specified in 3.5.5.3.                                      |
| 25 | RESERVED     | - Reserved bits.                                                     |
| 26 |              | This field is populated with '0' bits as necessary to make the       |
| 27 |              | length of the entire preferred roaming list equal to an integer      |
| 28 |              | number of octets.                                                    |
| 29 | PR_LIST_CRC  | - CRC for preferred roaming list.                                    |
| 30 |              | This field is set to the 16-bit CRC calculated according to          |
| 31 |              | 3.5.5.1.                                                             |

32

### 33 3.5.5.1 Preferred Roaming List CRC Calculation

34 The 16-bit preferred roaming list CRC field PR\_LIST\_CRC is calculated on all bits of the  
 35 preferred roaming list excluding the bits of the PR\_LIST\_CRC field itself. The generator  
 36 polynomial for this CRC is  $g(x) = x^{16} + x^{12} + x^5 + x^0$ .

---

<sup>2</sup> For emergency access (911) the mobile station may ignore restrictions set by the PREF\_ONLY and PREF\_NEG fields and access any available system.

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. Table 3.5.5.2-1 defines the types of acquisition records. Each type of acquisition record is tailored for use in acquiring a particular kind of system.

**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'          |
| Reserved                          | '0111' - '1111' |

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 System Acquisition (Standard Channels) Record

This acquisition record type is for use in acquiring a cellular 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 Standard Channel Selection Type Values**

| <b>Standard Channel Selection Type</b> | <b>Value</b> |
|----------------------------------------|--------------|
| Reserved                               | '00'         |
| Primary CDMA Channel                   | '01'         |
| Secondary CDMA Channel                 | '10'         |
| Primary or Secondary CDMA Channel      | '11'         |

**3.5.5.2.1.3 Cellular CDMA System Acquisition (Custom Channels) Record**

This acquisition record type is for use in acquiring a cellular CDMA system using a list of CDMA channels, and has the following variable length format:

| <b>Acquisition Record Field</b>               | <b>Length (bits)</b> |
|-----------------------------------------------|----------------------|
| 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 channels included in this record.

CHAN - Cellular CDMA channel.

This field specifies a cellular CDMA channel number (see 6.1.1.1 of TIA/EIA-95-B). 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             |

1

2

ACQ\_TYPE - Acquisition record type.

3

This field is set to '0100' (see Table 3.5.5.2-1).

4

A\_B - System A/B selection type.

5

The values for this field are specified in Table 3.5.5.2.1.1-1.

6

## 7 3.5.5.2.1.5 PCS CDMA System Acquisition (Using Blocks) Record

8

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:

9

10

| Acquisition Record Field | Length (bits) |
|--------------------------|---------------|
| ACQ_TYPE ('0101')        | 4             |
| NUM_BLOCKS               | 3             |

NUM\_BLOCKS occurrences of the following field:

|       |   |
|-------|---|
| BLOCK | 3 |
|-------|---|

11

12

ACQ\_TYPE - Acquisition record type.

13

This field is set to '0101' (see Table 3.5.5.2-1).

14

NUM\_BLOCKS - Number of frequency blocks.

15

This field is set to the number of PCS frequency blocks included in this record.

16

17

BLOCK - PCS frequency block.

18

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.

19

20

21

22

**Table 3.5.5.2.1.5-1 PCS CDMA Frequency Blocks**

| <b>PCS CDMA Frequency Block</b> | <b>Value</b> |
|---------------------------------|--------------|
| 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 System Acquisition (Using Channels) Record

This acquisition record type is for use in acquiring a PCS CDMA system using a list of CDMA channels, and has the following variable length format:

| <b>Acquisition Record Field</b>               | <b>Length (bits)</b> |
|-----------------------------------------------|----------------------|
| 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 channels included in this record.

CHAN - PCS CDMA channel.

This field specifies a PCS CDMA channel number (see 6.1.1.1 of TIA/EIA-95-B). The CHAN fields should be listed in priority order (highest priority first) according to the desired mobile station system selection scanning priorities.

### 3.5.5.3 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.

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 '0000000000000000' 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                                              |

|    |           |   |                                                                          |
|----|-----------|---|--------------------------------------------------------------------------|
| 1  | NID       | - | Network identification.                                                  |
| 2  |           |   | If the NID_INCL field of this record is equal to '01', this field is     |
| 3  |           |   | included and is set to the NID of the network associated with            |
| 4  |           |   | this record; otherwise, this field is omitted.                           |
| 5  |           |   | The value '1111111111111111' denotes any NID (i.e., serves as            |
| 6  |           |   | a NID wildcard). Not including the NID field is equivalent to            |
| 7  |           |   | including it and setting it to '1111111111111111'.                       |
| 8  |           |   | The value '0000000000000000' denotes a NID of the public                 |
| 9  |           |   | system (see 6.6.5.2 of TIA/EIA-95-B)                                     |
| 10 | PREF_NEG  | - | Preferred/negative system.                                               |
| 11 |           |   | This field is set to '1' if the mobile station is allowed to operate     |
| 12 |           |   | on the system associated with this record. This field is set to '0'      |
| 13 |           |   | if the mobile station is not allowed to operate on the system            |
| 14 |           |   | associated with this record.                                             |
| 15 | GEO       | - | Geographical region indicator.                                           |
| 16 |           |   | If this is the first system record, this field is set to '0'.            |
| 17 |           |   | If this is not the first system record, then this field is set as        |
| 18 |           |   | follows: If the system associated with this record is in the same        |
| 19 |           |   | geographical region as the system associated with the previous           |
| 20 |           |   | system record, this field is set to '1'; otherwise, this field is set    |
| 21 |           |   | to '0'.                                                                  |
| 22 | PRI       | - | Relative priority indicator.                                             |
| 23 |           |   | If the PREF_NEG field of this system record is equal to '0', this        |
| 24 |           |   | field is omitted; otherwise, this field is included and is set as        |
| 25 |           |   | follows:                                                                 |
| 26 |           |   | If this is the last system record in the specific geographical           |
| 27 |           |   | region, or if the PREF_NEG field in the next system record is            |
| 28 |           |   | equal to '0', this field is set to '0' and has no meaning.               |
| 29 |           |   | If the system associated with this system record is more                 |
| 30 |           |   | desirable than the system associated with the next system                |
| 31 |           |   | record, this field is set to '1'.                                        |
| 32 |           |   | If the system associated with this system record is as desirable         |
| 33 |           |   | as the system associated with the next system record, this field         |
| 34 |           |   | is set to '0'.                                                           |
| 35 | ACQ_INDEX | - | Acquisition record index.                                                |
| 36 |           |   | This field is set to the index of the acquisition record that            |
| 37 |           |   | specifies the acquisition parameters for the system associated           |
| 38 |           |   | with this record.                                                        |
| 39 |           |   | Note: The index of the $n^{\text{th}}$ acquisition record is $n-1$ . For |
| 40 |           |   | example, the index of the first acquisition record in ACQ_TABLE          |
| 41 |           |   | is 0, and the index for the fourth acquisition record is 3.              |
| 42 | ROAM_IND  | - | If the PREF_NEG field of this record is equal to '1', this field is      |
| 43 |           |   | included and is set to the roaming indication value (see TSB58)          |
| 44 |           |   | for the system associated with this record; otherwise, this field is     |
| 45 |           |   | omitted.                                                                 |

1

2    No text.

3

## 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, and the active NAM of this mobile station has not been provisioned, the base station should address the message using the ESN 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 TIA/EIA-95-B.

The base station should not process an activation origination as an implicit registration (see 6.6.5.1 of TIA/EIA-95-B). The base station should not send the *Mobile Station Registered Message* (see 7.7.3.3.2.15 of TIA/EIA-95-B) 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 TIA/EIA-95-B. 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' and 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' and 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 TIA/EIA-95-B. The base station may confirm the SSD update by performing the Unique Challenge-Response Procedure defined in 6.3.12.1.5 of TIA/EIA-95-B.
- 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 TIA/EIA-95-B. 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 following messages. 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", '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*.
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*.
  - 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.
  - 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*.

- 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.

#### 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 TIA/EIA-95-B).

If message encryption was enabled or transition to the Private Long Code Mask was made (see 7.3.3 of TIA/EIA-95-B) 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

1 encryption parameters is computed based on parameters in effect at the time the *Re-*  
2 *Authenticate Request Message* was sent.

3 Messages shall not be encrypted following an unsuccessful re-authentication.

#### 5 4.3.4 Activation of Voice Privacy Mode

6 To enhance the security of the programming session and to protect sensitive subscriber  
7 information, the base station should enable voice privacy (see 7.3.3 of TIA/EIA-95-B).

8 If a transition to the Private Long Code Mask was made or signaling message encryption was  
9 activated (see 2.3.12.2.1 and 6.3.12.2 of TIA/EIA-95-B) before the re-authentication operation,  
10 the Private Long Code Mask active at that time shall remain unchanged for the duration of the  
11 call.

12 Otherwise, the Private Long Code Mask is recalculated during the re-authentication operation.  
13 In this case, the data used to initialize the algorithm for calculating the Private Long Code  
14 Mask is computed based on parameters in effect at the time the *Re-Authenticate Request*  
15 *Message* was sent.

16 Voice privacy shall not be enabled following an unsuccessful re-authentication.

#### 18 4.4 Termination of the Programming Procedure

19 The programming session ends when the call is released.

20 If the programming session was initiated by the network as described in 3.2.2, and the base  
21 station processes the incoming call directed to the mobile station during the OTAPA process,  
22 the base station shall terminate the OTAPA session and may release the call prior to proceeding  
23 with the call termination procedure.

24 If the programming session was initiated by the network as described in 3.2.2, the base station  
25 may terminate the OTAPA session by sending the *OTAPA Request Message* to the mobile  
26 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**

| <b>Message Name</b>                                                      | <b>OTASP_MSG_TYPE</b>         | <b>Reference</b> |
|--------------------------------------------------------------------------|-------------------------------|------------------|
| <i>Configuration Request Message</i>                                     | '00000000'                    | 4.5.1.1          |
| <i>Download Request Message</i>                                          | '00000001'                    | 4.5.1.2          |
| <i>MS Key Request Message</i>                                            | '00000010'                    | 4.5.1.3          |
| <i>Key Generation Request Message</i>                                    | '00000011'                    | 4.5.1.4          |
| <i>Re-Authenticate Request Message</i>                                   | '00000100'                    | 4.5.1.5          |
| <i>Commit Request Message</i>                                            | '00000101'                    | 4.5.1.6          |
| <i>Protocol Capability Request Message</i>                               | '00000110'                    | 4.5.1.7          |
| <i>SSPR Configuration Request Message</i>                                | '00000111'                    | 4.5.1.8          |
| <i>SSPR Download Request Message</i>                                     | '00001000'                    | 4.5.1.9          |
| <i>Validation Request Message</i>                                        | '00001001'                    | 4.5.1.10         |
| <i>OTAPA Request Message</i>                                             | '00001010'                    | 4.5.1.11         |
| Reserved for future standardization                                      | '00001011' through '10111111' |                  |
| Available for manufacturer-specific <i>OTASP Data Message</i> definition | '11000000' through '11111110' | See TSB58        |
| 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 |

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*.

- 1                   BLOCK\_ID    -   Parameter block identifier.
- 2                                   The base station shall include NUM\_BLOCKS occurrences of this
- 3                                   field. The base station shall set each field to the value of the
- 4                                   parameter block type requested (see Table 4.5.2-1).
- 5                   BLOCK\_LEN   -   Parameter block length.
- 6                                   The base station shall set this field to the number of octets in
- 7                                   the parameter block, not including the BLOCK\_ID and
- 8                                   BLOCK\_LEN fields.
- 9                   PARAM\_DATA   -   Parameter data fields.
- 10                                  The base station shall include the parameter block (see 4.5.2)
- 11                                  specified by the BLOCK\_ID field.

12

## 13   4.5.1.3 MS Key Request Message

14   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                 | 8               |
| PARAM_P                     | 8 × PARAM_P_LEN |
| PARAM_G_LEN                 | 8               |
| PARAM_G                     | 8 × PARAM_G_LEN |

15

- 16                   OTASP\_MSG\_TYPE   -   *OTASP Data Message* type.
- 17                                   The base station shall set this field to '00000010'.
- 18                   A\_KEY\_P\_REV    -   Key exchange protocol version.
- 19                                   The base station shall set this field to '00000010'.
- 20                   PARAM\_P\_LEN    -   Length of PARAM\_P field.
- 21                                   The base station shall set this field to the number of octets in
- 22                                   the PARAM\_P field. The base station shall set this field to
- 23                                   '01000000'.
- 24                   PARAM\_P        -   Key exchange parameter P.
- 25                                   The base station shall set this field as described in 5.2.1.
- 26                   PARAM\_G\_LEN    -   Length of PARAM\_G field.
- 27                                   The base station shall set this field to the number of octets in
- 28                                   the PARAM\_G field. The base station shall set this field to
- 29                                   '00010100'.
- 30                   PARAM\_G        -   Key exchange parameter G.

The base station shall set this field as described in 5.2.1.

#### 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                   | $8 \times \text{BS\_RESULT\_LEN}$ |

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.

The base station shall set this field equal to the value of BS\_RESULT as described in 5.2.2.

#### 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 fixed-length format:

| Field                       | Length (bits) |
|-----------------------------|---------------|
| OTASP_MSG_TYPE ('00000110') | 8             |

OTASP\_MSG\_TYPE - *OTASP Data Message* type.

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

## 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.

1                   The base station shall set this field to the value of the BLOCK\_ID  
2                   of the parameter block being requested in this message (see  
3                   Table 3.5.3-1).

4   If the BLOCK\_ID field is set to '00000001' (Preferred Roaming List Parameter Block), the base  
5   station shall include the following fields in the message:

6       REQUEST\_OFFSET   -   Segment offset.

7                   The base station shall set this field to the starting offset within  
8                   the preferred roaming list (PR\_LIST<sub>s-p</sub>) of the octets being  
9                   requested.

10      REQUEST\_MAX\_SIZE   -   Maximum segment size.

11                   The base station shall set this field to the maximum number of  
12                   preferred roaming list octets that the mobile station is to return.

13

#### 14   4.5.1.9 SSPR Download Request Message

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

16

| Field                       | Length (bits) |
|-----------------------------|---------------|
| OTASP_MSG_TYPE ('00001000') | 8             |
| BLOCK_ID                    | 8             |
| BLOCK_LEN                   | 8             |
| PARAM_DATA                  | 8 × BLOCK_LEN |

17

18      OTASP\_MSG\_TYPE   -   *OTASP Data Message* type.

19                   The base station shall set this field to '00001000'.

20           BLOCK\_ID    Parameter block identifier.

21                   The base station shall set this field to the value of the parameter  
22                   block type being downloaded (see Table 4.5.3-1).

23      BLOCK\_LEN       -   Parameter block length.

24                   The base station shall set this field to the number of octets in  
25                   the parameter block, not including the BLOCK\_ID and  
26                   BLOCK\_LEN fields.

27      PARAM\_DATA       -   Parameter data.

28                   The base station shall include the parameter block specified by  
29                   the BLOCK\_ID field.

30

## 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'.

#### 4.5.2 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'<br>through<br>'01111111' |           |
| Available for manufacturer-specific parameter block definitions | '10000000'<br>through<br>'11111110' | See TSB58 |
| 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:

| SubfieldField    | 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) |
|----------|--------------------|

- 1
- 2           FIRSTCHP   -   First paging channel used in the home system.
- 3                           The base station shall set this field to the value for the
- 4                           FIRSTCHP<sub>p</sub> mobile station NAM indicator (see F.3 of TIA/EIA-
- 5                           95-B).
- 6           HOME\_SID   -   Home system identification.
- 7                           The base station shall set this field to the value for the
- 8                           HOME\_SID<sub>p</sub> mobile station NAM indicator (see F.3 of TIA/EIA-
- 9                           95-B).
- 10                       EX   -   Extended address indicator.
- 11                           The base station shall set this field to the value for the EX<sub>p</sub>
- 12                           mobile station NAM indicator (see F.3 of TIA/EIA-95-B).
- 13           IMSI\_M\_CLASS   -   IMSI\_M Class assignment of the mobile station.
- 14                           If the base station is assigning a class 0 IMSI\_M to the mobile
- 15                           station, the base station shall set this field to '0'; otherwise the
- 16                           base station shall set this field to '1'.
- 17           IMSI\_M\_ADDR\_NUM   -   Number of IMSI\_M address digits.

|    |                  |   |                                                                                |
|----|------------------|---|--------------------------------------------------------------------------------|
| 1  |                  |   | If the mobile station has been assigned a class 1 IMSI_M (see                  |
| 2  |                  |   | 6.3.1 of TIA/EIA-95-B), the base station shall set this field to               |
| 3  |                  |   | four less than the number of digits in the NMSI; otherwise, the                |
| 4  |                  |   | base station shall set this field to '000'.                                    |
| 5  | MCC_M            | - | Mobile country code of the IMSI_M.                                             |
| 6  |                  |   | The base station shall set this field to the value for the MCC_M <sub>p</sub>  |
| 7  |                  |   | mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-                 |
| 8  |                  |   | B).                                                                            |
| 9  | IMSI_M_11_12     | - | 11th and 12th digits of the IMSI_M.                                            |
| 10 |                  |   | The base station shall set this field to the value for the                     |
| 11 |                  |   | IMSI_M_11_12 <sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1      |
| 12 |                  |   | of TIA/EIA-95-B).                                                              |
| 13 | IMSI_M_S         | - | The least significant 10 digits of the IMSI_M.                                 |
| 14 |                  |   | The base station shall set this field to the value for the                     |
| 15 |                  |   | IMSI_M_S <sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1 of       |
| 16 |                  |   | TIA/EIA-95-B).                                                                 |
| 17 | ACCOLC           | - | Access overload class.                                                         |
| 18 |                  |   | The base station shall set this field to the value for the ACCOLC <sub>p</sub> |
| 19 |                  |   | mobile station NAM indicator (see F.3 of TIA/EIA-95-B).                        |
| 20 | LOCAL_CONTROL    | - | Local control status.                                                          |
| 21 |                  |   | The base station shall set this field to '1' to enable local control           |
| 22 |                  |   | status in the mobile station, or to '0' to disable local control               |
| 23 |                  |   | status (see 2.6.1.2.2 of TIA/EIA-95-B).                                        |
| 24 | MOB_TERM_HOME    | - | Termination indicator for the home system.                                     |
| 25 |                  |   | The base station shall set this field to the value for the                     |
| 26 |                  |   | MOB_TERM_HOME <sub>p</sub> mobile station NAM indicator (see F.3 and           |
| 27 |                  |   | 6.6.5.3 of TIA/EIA-95-B).                                                      |
| 28 | MOB_TERM_FOR_SID | - | Termination indicator for SID roaming.                                         |
| 29 |                  |   | The base station shall set this field to the value for the                     |
| 30 |                  |   | MOB_TERM_FOR_SID <sub>p</sub> mobile station NAM indicator (see F.3            |
| 31 |                  |   | and 6.6.5.3 of TIA/EIA-95-B).                                                  |
| 32 | MOB_TERM_FOR_NID | - | Termination indicator for NID roaming.                                         |
| 33 |                  |   | The base station shall set this field to the value for the                     |
| 34 |                  |   | MOB_TERM_FOR_NID <sub>p</sub> mobile station NAM indicator (see F.3            |
| 35 |                  |   | and 6.6.5.3 of TIA/EIA-95-B).                                                  |

|    |           |   |                                                                    |
|----|-----------|---|--------------------------------------------------------------------|
| 1  | N_SID_NID | - | Number of SID/NID pairs.                                           |
| 2  |           |   | The base station shall set this field to the number of SID/NID     |
| 3  |           |   | pairs included in the parameter block. The base station shall      |
| 4  |           |   | include at least one SID/NID pair.                                 |
| 5  | SID       | - | System identification.                                             |
| 6  |           |   | The base station shall set this field to the value of the SID      |
| 7  |           |   | component of the SID/NID pair (see F.3 of TIA/EIA-95-B).           |
| 8  | NID       | - | Network identification.                                            |
| 9  |           |   | The base station shall set this field to the value of the NID      |
| 10 |           |   | component of the SID/NID pair (see F.3 of TIA/EIA-95-B).           |
| 11 | RESERVED  | - | Reserved bits.                                                     |
| 12 |           |   | The base station shall add reserved bits as needed in order to     |
| 13 |           |   | make the length of the entire parameter block equal to an          |
| 14 |           |   | integer number of octets. The base station shall set these bits to |
| 15 |           |   | '0'.                                                               |

16

## 17 4.5.2.2 Mobile Directory Number

18 The PARAM\_DATA field of the Mobile Directory Number Parameter Block consists of the  
 19 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 (as needed) |
|----------|--------------------|

|    |          |   |                                                                    |
|----|----------|---|--------------------------------------------------------------------|
| 20 | N_DIGITS | - | Number of digits.                                                  |
| 21 |          |   | The base station shall set this field to the number of digits      |
| 22 |          |   | included in the parameter block.                                   |
| 23 | DIGITn   | - | Digit.                                                             |
| 24 |          |   | The base station shall set these field to the digits of the mobile |
| 25 |          |   | station directory number. Each digit shall be encoded according    |
| 26 |          |   | to Table 6.7.1.3.2.4-4 of TIA/EIA-95-B.                            |
| 27 | RESERVED | - | Reserved bits.                                                     |
| 28 |          |   | The base station shall add reserved bits as needed in order to     |
| 29 |          |   | make the length of the entire parameter block equal to an          |
| 30 |          |   | integer number of octets. The base station shall set these bits to |
| 31 |          |   | '0'.                                                               |

1

## 2 4.5.2.3 CDMA NAM Download

3 The PARAM\_DATA field of the CDMA NAM Download Parameter Block consists of the  
4 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) |
|----------|--------------------|

5

6 IMSI\_M\_CLASS - IMSI\_M Class assignment of the mobile station.

7 If the base station is assigning a class 0 IMSI\_M to the mobile  
8 station, the base station shall set this field to '0'; otherwise the  
9 base station shall set this field to '1'.

10 IMSI\_M\_ADDR\_NUM - Number of IMSI\_M address digits.

11 If the mobile station has been assigned a class 1 IMSI\_M (see  
12 6.3.1 of TIA/EIA-95-B), the base station shall set this field to  
13 four less than the number of digits in the NMSI; otherwise, the  
14 base station shall set this field to '000'.

15 MCC\_M - Mobile country code of the IMSI\_M.

16 The base station shall set this field to the value for the MCC\_M<sub>p</sub>  
17 mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-  
18 B).

19 IMSI\_M\_11\_12 - 11th and 12th digits of the IMSI\_M.

|    |                  |                                                                                |
|----|------------------|--------------------------------------------------------------------------------|
| 1  |                  | The base station shall set this field to the value for the                     |
| 2  |                  | IMSI_M_11_12 <sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1      |
| 3  |                  | of TIA/EIA-95-B).                                                              |
| 4  | IMSI_M_S         | - The least significant 10 digits of the IMSI_M.                               |
| 5  |                  | The base station shall set this field to the value for the                     |
| 6  |                  | IMSI_M_S <sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1 of       |
| 7  |                  | TIA/EIA-95-B).                                                                 |
| 8  | ACCOLC           | - Access overload class.                                                       |
| 9  |                  | The base station shall set this field to the value for the ACCOLC <sub>p</sub> |
| 10 |                  | mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-                 |
| 11 |                  | B).                                                                            |
| 12 | LOCAL CONTROL    | - Local control status.                                                        |
| 13 |                  | The base station shall set this field to '1' to enable local control           |
| 14 |                  | status in the mobile station, or to '0' to disable local control               |
| 15 |                  | status (see 6.3.9 of TIA/EIA-95-B).                                            |
| 16 | MOB_TERM_HOME    | - Termination indicator for the home system.                                   |
| 17 |                  | The base station shall set this field to the value for the                     |
| 18 |                  | MOB_TERM_HOME <sub>p</sub> mobile station NAM indicator (see F.3 and           |
| 19 |                  | 6.6.5.3 of TIA/EIA-95-B).                                                      |
| 20 | MOB_TERM_FOR_SID | - Termination indicator for SID roaming.                                       |
| 21 |                  | The base station shall set this field to the value for the                     |
| 22 |                  | MOB_TERM_FOR_SID <sub>p</sub> mobile station NAM indicator (see F.3            |
| 23 |                  | and 6.6.5.3 of TIA/EIA-95-B).                                                  |
| 24 | MOB_TERM_FOR_NID | - Termination indicator for NID roaming.                                       |
| 25 |                  | The base station shall set this field to the value for the                     |
| 26 |                  | MOB_TERM_FOR_NID <sub>p</sub> mobile station NAM indicator (see F.3            |
| 27 |                  | and 6.6.5.3 of TIA/EIA-95-B).                                                  |
| 28 | N_SID_NID        | - Number of SID/NID pairs.                                                     |
| 29 |                  | The base station shall set this field to the number of SID/NID                 |
| 30 |                  | pairs included in the parameter block. The base station shall                  |
| 31 |                  | include at least one SID/NID pair.                                             |
| 32 | SID              | - System identification.                                                       |
| 33 |                  | The base station shall set this field to the value of the SID                  |
| 34 |                  | component of the SID/NID pair (see F.3 of TIA/EIA-95-B).                       |
| 35 | NID              | - Network identification.                                                      |
| 36 |                  | The base station shall set this field to the value of the NID                  |
| 37 |                  | component of the SID/NID pair (see F.3 of TIA/EIA-95-B).                       |
| 38 | RESERVED         | - Reserved bits.                                                               |
| 39 |                  | The base station shall add reserved bits as needed in order to                 |
| 40 |                  | make the length of the entire parameter block equal to an                      |
| 41 |                  | integer number of octets. The base station shall set these bits to             |
| 42 |                  | '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 TIA/EIA-95-B), 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<sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).

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<sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).

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<sub>p</sub> mobile station NAM indicator (see F.3 and 6.3.1 of TIA/EIA-95-B).

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   |
| Reserved for future standardization                             | '00000001'<br>through<br>'01111111' |           |
| Available for manufacturer-specific parameter block definitions | '10000000'<br>through<br>'11111110' | See TSB58 |
| Reserved                                                        | '11111111'                          |           |

## 4.5.3.1 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 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<sub>s-p</sub>) 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.

1            SEGMENT\_SIZE    -    Segment size.

2                                The base station shall set this field to the number of octets of the  
3                                preferred roaming list included in SEGMENT\_DATA.

4            SEGMENT\_DATA    -    Segment data.

5                                The base station shall set this field to sequential octets of the  
6                                preferred roaming list. The octets shall be those starting at the  
7                                offset within the preferred roaming list specified by  
8                                SEGMENT\_OFFSET.

#### 10    4.5.4 Validation Parameter Blocks

11    Table 4.5.4-1 lists the types of parameter blocks used in the *Validation Request Message* and  
12    the *Validation Response Message*.

14                                **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'<br>through<br>'01111111' |           |
| Available for manufacturer-specific<br>parameter block definitions | '10000000'<br>through<br>'11111110' | See TSB58 |
| Reserved                                                           | '11111111'                          |           |

##### 16    4.5.4.1 Verify SPC

17    The PARAM\_DATA field of the Verify SPC Parameter Block consists of the following field:

| Field | Length (bits) |
|-------|---------------|
| SPC   | 24            |

20            SPC            -    Service programming code.

21                                The base station shall set this field to the BCD coded value of  
22                                Service Programming Code assigned for the mobile station (see  
23                                Table 3.3.6-1). Each digit shall be encoded according to the  
24                                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.

|    |            |   |                                                                     |
|----|------------|---|---------------------------------------------------------------------|
| 1  |            |   | The base station shall set this field to '1' to indicate that the   |
| 2  |            |   | OTAPA SPASM validation signature, AUTH_OTAPA, is included           |
| 3  |            |   | in the message; otherwise, the base station shall set this field to |
| 4  |            |   | '0'.                                                                |
| 5  | AUTH_OTAPA | - | OTAPA SPASM validation signature.                                   |
| 6  |            |   | If the AUTH_OTAPA_INCL is set to '1', the base station shall set    |
| 7  |            |   | this field as described in 3.3.7; otherwise, the base station shall |
| 8  |            |   | omit this field.                                                    |
| 9  | NAM_LOCK   | - | SPASM protection indicator for the active NAM.                      |
| 10 |            |   | The base station shall set this field to '1' to activate SPASM      |
| 11 |            |   | protection of programmable parameters and indicators of the         |
| 12 |            |   | active NAM after completion of the current OTAPA session,           |
| 13 |            |   | otherwise the base station shall set this field to '0'.             |
| 14 | RESERVED   | - | Reserved bits.                                                      |
| 15 |            |   | The base station shall add reserved bits as needed in order to      |
| 16 |            |   | make the length of the entire parameter block equal to an           |
| 17 |            |   | integer number of octets. The base station shall set these bits to  |
| 18 |            |   | '0'.                                                                |
| 19 |            |   |                                                                     |

## 5 KEY EXCHANGE PROCEDURES

### 5.1 Mobile Station Requirements

#### 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  $MS\_RESULT = PARAM\_G_s^X \text{ modulo } PARAM\_P_s$ .

#### 5.1.3 A-key Computation

The mobile station shall compute the common key  $K = BS\_RESULT_s^X \text{ modulo } PARAM\_P_s$ . The mobile station shall store the least significant 64 bits of the result  $K$  as  $A\_KEY\_TEMP_s$ .

### 5.2 Base Station Requirements

#### 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  $G$ .

1 The base station shall generate a random number Y for use in calculating the base station  
2 result, BS\_RESULT. The number Y shall have the following properties:

- 3 • The number generated shall be 160-bits in length.
- 4 • The number generated shall not be less than 4.
- 5 • The number generated shall have an uniform statistical distribution over its range.
- 6 • The numbers used in formulating different *Key Generation Request Messages* sent by  
7 the same base station shall be statistically uncorrelated.
- 8 • The numbers used in formulating *Key Generation Request Message* sent by different  
9 base stations shall be statistically uncorrelated.

#### 11 5.2.2 Base Station Result

12 The base station shall calculate  $BS\_RESULT = G^Y \text{ modulo } P$ .

#### 14 5.2.3 A-key Computation

15 The base station shall compute the common key  $K = MS\_RESULT^Y \text{ modulo } P$ . The base  
16 station shall use the least significant 64 bits of the result K as the A\_KEY.

1     **ANNEX A     MESSAGE ENCRYPTION AND VOICE PRIVACY**

2     TIA/EIA/IS-683-A Annex A forms part of this Standard and is normative.   TIA/EIA/IS-683-A  
3     Annex A and any modification to it are available as a separate document whose distribution is  
4     controlled by TIA.

5     This document contains material of a sensitive nature and is protected by TIA from general  
6     distribution.   TIA is the focal point and facilitator for making such information available.  
7     Procedures for distribution of this information are in the applicable Technology Transfer  
8     Control Plan.   The Technology Transfer Control Plan is available from TIA.

9

1    **ANNEX B   BIBLIOGRAPHY**

2    This is an informative annex. The documents listed in this annex are for information only and  
3    are not essential for the completion of the requirements of this standard.

- 4    1. TIA/EIA/IS-91, *Mobile Station - Base Station Compatibility Standard for 800 MHz Analog*  
5        *Cellular*, October 1994.

6

## 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 which 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 which 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<br>(ACQ_TYPE)                  | ROAM_IND |
|-----|----------|----------|-----|-----|------------------------------------------|----------|
| 111 | 0        | 1        | 0   | 1   | 2 [Cellular CDMA -<br>Standard Channels] | Off      |
| 77  | 0        | 1        | 1   | 0   | 0 [PCS CDMA -<br>Using Channels]         | Off      |
| 34  | 0        | 1        | 1   | 0   | 2 [Cellular CDMA -<br>Standard Channels] | Flashing |
| 34  | 0        | 0        | 1   | N/A | 4 [Cellular Analog]                      | N/A      |
| 400 | 0        | 1        | 0   | 1   | 2 [Cellular CDMA -<br>Standard Channels] | Off      |
| 4   | 0        | 1        | 1   | 1   | 0 [PCS CDMA -<br>Using Channels]         | On       |
| 12  | 0        | 1        | 1   | 1   | 3 [Cellular CDMA -<br>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 -<br>Standard Channels] | Off      |
| 56  | 0        | 1        | 1   | 0   | 1 [PCS CDMA -<br>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 which is preferable. The mobile station can then use the acquisition table entry to determine the frequencies which 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

which is preferable. The mobile station can then use the acquisition table entry to determine the frequencies which 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 which 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 TIA/EIA-95-B) 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 none of 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.