3GPP2 C.P0048-B v0.05

November 2013

Mobile Equipment (ME) Conformance Testing with R-UIM for cdma2000 Spread Spectrum Standards

1

1 Changes Accepted for Inclusion in C.S0048-B v1.0

Contribution #	Title
AC10-20130311-013	Adding test requirements for MEs supporting SSPR_P_REV ≥ '1' to TC 6.1.2 "MS Displaying the Roaming Indicator"
AC10-20130311-014	Correction of default settings for $EF_{3GPDOPM}$ in test case 6.32.1 to run Simple IP Authentication
AC10-20130311-015	Removing of unneeded steps from the test procedure of TC 6.3.3 "Unique Challenge While the Mobile Station is in Idle State"
AC10-20130311-016	Update Initial Conditions to comply with C.S0023-D v2.0
AC10-20130311-017	Correct Initial Conditions
AC10-20130311-018	Correct some Spelling Issues
AC10-20130409-008	Adding a default EF_{EPRL} (requirement for MEs supporting SSPR_P_REV ≥ '3') to be used in TC 6.1.2 and 6.5.3
AC10-20130709-005r1	Clarification of the TC 6.2.1 + Correction of some Spelling Issues
AC10-20130709-007	Update Initial Conditions to run TC 6.32.1
AC10-20130711-003r1	Adding a specific SSPR Download Request Message to test case 6.5.3
AC10-20131007-013	Comprion_C.S0048-B_V&V Comments
AC10-20131105-006	C.S0048-B v1.0: Fix error in section 6.5.1.4
AC10-20131112-0xx	Comprion_C.S0048-B_Editorial Corrections

2 Revision History

Revision	Description of Changes	Date
Rev 0 v1.0	Publication	July 2008
Rev A v1.0	Publication	October 2010
Rev A v2.0	Publication	December 2012
Rev A v2.0	This document was republished to add a trademark acknowledgment	March 2013
Rev B v0.04	V&V version	September 2013
Rev B v1.0	Publication	<month> 2013

Table of Contents

Table of Figures

₁ Table of Tables

₁ FOREWORD

₂ This foreword is not part of this specification.

₃ This specification was prepared by the Third Generation Partnership Project 2 (3GPP2).

1   This page intentionally left blank

1   This page intentionally left blank

1 Introduction

1.1 Scope

The present document provides the ME (Mobile Equipment) conformance test specification related to R-UIM (Removable User Identity Module), in order to ensure interoperability between an ME and an R-UIM as defined in [1], [2], [8] and [9] independently of the terminal and card manufacturers, card issuer or operator.

This document does not specify which test cases are mandatory or optional. However, to successfully execute a particular test case, its corresponding test requirements and procedures as defined in this document shall be followed.

1.2 Document Conventions

1.2.1 Requirements Language

"Shall" and "shall not" identify requirements to be followed strictly to conform to this document 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 document. "Can" and "cannot" are used for statements of possibility and capability, whether material, physical or causal.

1.2.2 Numbers

The following table describes the conventions used for non-decimal numbers.

Table 1.1 – Convention for Numbers and Strings

Convention	Description
'1' or '0'	A single binary bit
'bbbbbbbb'	An 8-bit binary number
'xx'	A single octet hexadecimal number
'xx xx xx…xx xx'	A multi-octet hexadecimal number
'hh hh hh…hh hh'	A multi-octet hexadecimal number or string
Note: If an 'x' is present in a binary or hexadecimal number, then that digit is "don't care".	

"Bn" represents Byte n of the coding starting from left to right, i.e. MSB to LSB. "bn" represents Bit n of the byte starting from right to left, i.e. LSB to MSB

1.3   Terminology

1.3.1   Acronyms

For the purposes of the present document, the following acronyms apply:

3GPP2   3rd Generation Partnership Project 2

CHV1   Card Holder Verification 1

CHV2   Card Holder Verification 2

EF   Elementary File

EPRL   Extended Preferred Roaming List

DF   Directory File

CS   Card Simulator (which simulates R-UIM for ME testing)

ME   Mobile Equipment

MEID   Mobile Equipment Identifier

MF   Master File

MO   Mobile-Originated

MS   Mobile Station. A mobile station comprises all user equipment and software needed for communication with a mobile network

MT   Mobile-Terminated

OTAPA   Over-the-Air Parameter Administration

OTASP   Over-the-Air Service Provisioning

NS   Network Simulator

PRL   Preferred Roaming List

R-UIM   Removable User Identity Module

SIM   Subscriber Identity Module

SO   Service Option

SSD   Shared Secret Data

UUT   Unit Under Test

1.4 References

1.4.1 Normative References

[1] 3GPP2 C.S0023-D v1.0 (June 2009): "Removable User Identity Module (R-UIM) for cdma2000 Spread Spectrum Systems".

[2] 3GPP 51.011: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[3] ISO/IEC 7816-1: "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[4] ISO/IEC 7816-2: "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[5] ISO/IEC 7816-3: "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols."

[6] ISO/IEC 7811-1: "Identification cards - Recording technique - Part 1: Embossing"

[7] ISO/IEC 7811-3: "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"

[8] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP 31.101: "Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] 3GPP 51.010: "Mobile Station (MS) conformance specification; Part 1: Conformance specification".

[11] Reserved.

[12] 3GPP2 C.S0043-A v1.0 (September 2010): "Signaling Conformance Test Specification for cdma2000 Spread Spectrum Systems".

[13] 3GPP2 C.S0060-0 v1.0 (December 2005): "Signaling Conformance Test Specification for Over-the-Air Service Provisioning".

[14] 3GPP2 C.S0073-B v1.0 (August 2009): "Signaling Test Specification for Mobile Station Equipment Identifier (MEID) Support for cdma2000 Spread Spectrum Systems".

[15] ITU X.509 (1 August 2005): "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[16] 3GPP2 C.S0005-E v2.0 (June 2010): "Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems".

[17] 3GPP2 C.S0004-E v2.0 (June 2010): "Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems".

1   [18] 3GPP2 C.S0016-D v1.0 (January 2010): "Over-the-Air Service Provisioning of
2   Mobile Stations in Spread Spectrum Standards".

3   [19] ETSI TS 102 221: "UICC-Terminal Interface; Physical and Logical Characteristics".

1   # 2   Reserved

3   Reserved

4   ME Test Environment

The test environment shall comply with the requirements specified in section 4 "Physical Characteristics" and section 5 "Electronic Signals and Transmission Protocols" of [2].

The following diagram illustrates the test environment involving a Card Simulator (CS), the Unit Under Test (UUT) and Network Simulator (NS). The UUT in this document is the Mobile Equipment (ME). CS simulates R-UIM or CSIM for the purpose of ME conformance testing. NS simulates the network, which is primarily a "base station" and may include other network components and servers as needed.

In this document, the CS simulates an R-UIM. Alternatively, to perform the logical tests, R-UIMs programmed with specific data may be used. Chapter 5 defines the default R-UIM data for use in all test cases. Some test cases use certain R-UIM data that are different from the default R-UIM data.
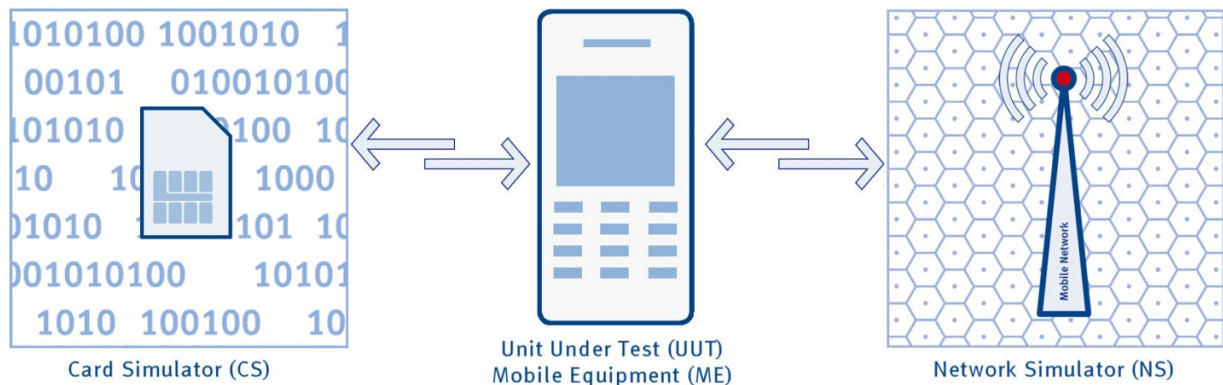
Figure 1. ME Test Environment

1   This page intentionally left blank

5 Testing of the ME

The test cases defined in chapter 6 confirm:

1. the correct interpretation of data read from the R-UIM (Removable-User Identification Module) by the ME;
2. the correct writing of data to the R-UIM by the ME;
3. the initiation of appropriate procedures by the ME;
4. exchange protocols;
5. electrical characteristics;
6. physical characteristics.

All tests apply to MEs conforming to [1].

The following sections define the default R-UIM parameters for use by all test cases.

5.1 Definition of Default Values for R-UIM/ME Interface Testing

A CS containing the following default values is used for all tests in this document unless otherwise stated.

For all data items, the logical default values and the coding within the elementary files (EFs) and other parameters of the CS follow.

In case a logical description and a hex coding are both available for an EF the logical description takes precedence over the hex coding.

5.1.1 EF$_{CST}$ (CDMA Service Table)

The common CDMA Service Table will allow the use of most of the functionality described in [1]. If specific settings for a test case have to be used, an appropriate modification for EF$_{CST}$ in the initial conditions of the test case will be needed. (In the following table, "Y" indicates "Yes" which means allocated or activated. "N" indicates "No" which means not allocated or not activated.)

Table 2. Default Values for EF$_{CST}$

Services	Description	Allocated	Activated
1	CHV Disable Function	Y	Y
2	Abbreviated Dialing Numbers (ADN)	Y	Y
3	Fixed Dialing Numbers (FDN)	Y	N
4	Short Message Storage (SMS)	Y	Y
5	HRPD	Y	Y
6	Enhanced Phone Book	N	N
7	Multi Media Domain (MMD)	N	N
8	SF_EUIMID-based EUIMID	Y	Y
9	MEID Support	Y	Y
10	Extension1	Y	Y

Services	Description	Allocated	Activated
11	Extension2	Y	N
12	SMS Parameters	Y	Y
13	Last Number Dialled (LND)	N	N
14	Service Category Program for BC-SMS	Y	Y
15	Messaging and 3GPD Extensions	Y	Y
16	Root Certificates	Y	Y
17	CDMA Home Service Provider Name	Y	Y
18	Service Dialing Numbers (SDN)	N	N
19	Extension3	N	N
20	3GPD-SIP	Y	Y
21	WAP Browser	Y	Y
22	Java™ [1]	Y	Y
23	Reserved for CDG	N	N
24	Reserved for CDG	N	N
25	Data Download via SMS Broadcast	N	N
26	Data Download via SMS-PP	N	N
27	Menu Selection	N	N
28	Call Control	N	N
29	Proactive R-UIM	N	N
30	AKA	N	N
31	IPv6	N	N
32	RFU	N	N
33	RFU	N	N
34	RFU	N	N
35	RFU	N	N
36	RFU	N	N
37	RFU	N	N
38	3GPD-MIP	Y	Y
39	BCMCS	N	N
40	Multimedia Messaging Service (MMS)	Y	Y
41	Extension 8	Y	Y
42	MMS User Connectivity Parameters	N	N
43	Application Authentication	N	N
44	Group Identifier Level 1	N	N
45	Group Identifier Level 2	N	N
46	De-Personalization Control Keys	N	N
47	Cooperative Network List	N	N

---

[1]   Java is a registered trademark of Oracle and/or its affiliates.

Coding in Hex:

| DF | C3 | DF | FC | C3 | 0F | 00 | 00 | 00 | CC | 03 | 00 |

5.1.2 EF$_{USGIND}$ (UIMID/SF_EUMID Usage Indicator)

Logically:

ESN value for CAVE authentication and MS identification: UIMID

ME identification: MEID_ME

Coding in Hex:

| 01 |

5.1.3 EF$_{IMSI\_M}$ (IMSI_M)

Logically:

IMSI_M_CLASS:	Class 0
IMSI_M_ADDR_NUM:	IMSI_M has been programmed, Address 000
MCC_M:	404 (India)
IMSI_M_11_12:	0
IMSI_M_S_1:	000 9520
IMSI_M_S_2:	000

Coding in Hex:

| 00 | E7 | 03 | A3 | E5 | F9 | 63 | 80 | 89 | 01 |

5.1.4 EF$_{ESNME}$ (ESN_ME)

Logically:

Number of bytes: 0

ESN_ME: 0 (not set)

Coding in Hex:

| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

5.1.5 EF$_{CDMAHOME}$ (CDMA Home SID, NID)

Logically:

Record 1:

CDMA Home SID (SIDp):   1000

CDMA Home NID (NIDp):   2222

Band Class: 0 (800 MHz cellular band)

1 Coding in Hex:

E8	03	AE	08	00

2 Record 2:

3   CDMA Home SID (SIDp):   1000

4   CDMA Home NID (NIDp):   2222

5   Band Class: 1 (1.8 to 2.0 GHz PCS band)

6 Coding in Hex:

E8	03	AE	08	01

7 Record 3:

8   CDMA Home SID (SIDp):   1000

9   CDMA Home NID (NIDp):   2222

10   Band Class: 3 (832 to 925 MHz JTACS band)

11 Coding in Hex:

E8	03	AE	08	03

12 Record 4:

13   CDMA Home SID (SIDp):   1000

14   CDMA Home NID (NIDp):   2222

15   Band Class: 4 (1.75 to 1.87 GHz Korean PCS band)

16 Coding in Hex:

E8	03	AE	08	04

17 Record 5:

18   CDMA Home SID (SIDp):   1000

19   CDMA Home NID (NIDp):   2222

20   Band Class: 5 (450 MHz NMT band)

21 Coding in Hex:

E8	03	AE	08	05

22 Record 6:

23   CDMA Home SID (SIDp):   1000

24   CDMA Home NID (NIDp):   2222

25   Band Class: 6 (2 GHz IMT-2000 band)

26 Coding in Hex:

E8	03	AE	08	06

1 ## 5.1.6   CHV1

2 Logically: 2468

3 Coding in Hex:

32	34	36	38	FF	FF	FF	FF

4 ## 5.1.7   CHV2

5 Logically: 3579

6 Coding in Hex:

33	35	37	39	FF	FF	FF	FF

7 ## 5.1.8   UNBLOCK CHV1

8 Logically: 13243546

9 Coding in Hex:

31	33	32	34	33	35	34	36

10 ## 5.1.9   UNBLOCK CHV2

11 Logically: 08978675

12 Coding in Hex:

30	38	39	37	38	36	37	35

13 ## 5.1.10   EF$_{ADN}$ (Abbreviated Dialing Number)

14 At least 10 records.

15 Record 1:

16   Length of alpha identifier: 32 characters

17   Alpha identifier: "ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF"

18   Length of BCD number: 3

19   TON and NPI: Telephony and Unknown

20   Dialed number: 123

21   CCI: None

22   Ext1:   None

23 Coding in Hex:

Byte:	B1	B2	B3	...	B32	B33	B34	B35	B36	B37	B38	B39	...	B46
Hex:	41	42	43	...	46	03	81	21	F3	FF	FF	FF	...	FF

5.1.11 EF_{FDN} (Fixed Dialing Numbers)

Multiple records:

Record 1:

    Length of alpha identifier: 6 characters

    Alpha identifier: "FDN111"

    Length of BCD number: 6

    TON and NPI: Telephony and Unknown

    Dialed number: 1357924680

    CCI: None

    Ext2:   None

Coding in Hex:

46	44	4E	31	31	31	06	81	31	75	29	64	08	FF	FF	FF
FF	FF	FF	FF												

Record 2:

    Length of alpha identifier: 6 characters

    Alpha identifier: "FDN222"

    Length of BCD number: 4

    TON and NPI: Telephony and Unknown

    Dialed number: 24680

    CCI: None

    Ext2:   None

Coding in Hex:

46	44	4E	32	32	32	04	81	42	86	F0	FF	FF	FF	FF	FF
FF	FF	FF	FF												

Record 3:

    Length of alpha identifier: 6 characters

    Alpha identifier: "FDN333"

    Length of BCD number: 10

    TON and NPI: Telephony and Unknown

    Dialed number: 12345678901234567890

    CCI: None

    Ext3:   None

Coding in Hex:

46	44	4E	33	33	33	0B	81	21	43	65	87	09	21	43	65
87	09	FF	FF												

5.1.12 EF_{SMSCAP} (SMS Capabilities)

Logically:

SMS Retry Period:	30 seconds
SMS Retry Interval:	5 seconds
SMS Flags:	
Send On Access:	True
Send on Traffic:	True
Send as Standard EMS:	True
SMS Preferred Service Option:	Device default

Coding in Hex:

1E	05	07	00

5.1.13 EF_{SMSP} (SMS Parameters)

Record 1:

Teleservice Identifier:	CDMA Cellular Messaging Teleservice [CMT-95]
Parameter Indicators:	MSG_ENCODING, Validity Period, Bearer Data
Message Encoding:	7-bit ASCII
Validity Period:	Indefinite
Bearer Data:	
Priority Indicator:	Urgent

Coding in Hex:

00	02	10	02	E7	FD	FF	FF	02	F5	08	03	08	01	80	FF
FF	FF	FF	FF	FF	FF	FF									

5.1.14 EF_{SIPUPP} (Simple IP User Profile Parameters)

Logically:

NAI Entry Index:	0
NAI:	"abc0@xyz.com"
Authentication Algorithm:	CHAP to PAP fallback

Coding in Hex:

0F	10	0C	61	62	63	30	40	78	79	7A	2E	63	6F	6D	30

5.1.15 EF$_{3GPDUPPExt}$ (3GPD User Profile Parameters Extension)

Logically:

NAI Entry Index:	0
Applications:	Unspecified, WAP, MMS
Priority:	100
Data Rate Mode:	High Speed
Data Bearer:	Hybrid 1xEV-DO/1x

Coding in Hex:

10	00	00	00	07	64	20

5.1.16 EF$_{SIPPAPSS}$ (Simple IP PAP SS)

Logically:

NAI Entry Index:	0
PAP SS:	"PAP SS 0"

Coding in Hex:

0A	10	42	82	0A	81	02	9A	99	01	80

5.1.17 Simple IP CHAP SS

Logically:

NAI Entry Index:	0
CHAP SS:	"CHAP SS 0"

5.1.18 EF$_{DGC}$ (Data Generic Configurations)

Logically:

Data dormant timer:	30 seconds
EPZID Type:	Packet Zone ID
Hysteresis Activation Time:	30 seconds

Coding in Hex:

1E	00	1E

5.1.19 EF$_{MIPUPP}$ (Mobile IP User Profiles)

Logically:

MIP Registration Max Retries:	2
MIP Registration First Retry Timeout:	2000ms
MIP Re-registration Threshold:	3 minutes
NAI Entry Index:	0

1 NAI: "abc@xyz.com"

2 T_BIT: True

3 Home Address: "11.22.33.44"

4 Primary Home Agent: "22.33.44.55"

5 Secondary Home Agent: "33.44.55.66"

6 MN-AAA Auth Algorithm: MD5

7 MN-AAA SPI: '00 00 00 00'

8 MN-HA Auth Algorithm: MD5

9 MN-HA SPI: '00 00 00 00'

10 Coding in Hex:

24	DC	31	00	B6	16	26	34	07	87	97	A2	E6	36	F6	D8
58	B1	09	60	B1	09	61	B9	09	61	BA	10	C0	00	00	00
06	00	00	00	00											

11 5.1.20 Void

12 5.1.21 Mobile IP SS

13 MN-AAA SS: "MN-AAA SS"

14 MN-HA SS: "MN-HA SS"

15 5.1.22 EF$_{MIPFlags}$ (Mobile IP Flags)

16 Logically:

17   Mobile IP 2002bis MN HA Authentication: False

18   Mobile IP Pre Rev 6 handoff optimization: False

19   Mobile IP PPP Re-sync during hand-down from 1xEV-DO Rev 0 to 1x: False

20   Mobile IP Re-registration only if data has been transferred since last registration in order to
21   extend Mobile IP address lifetime: False

22 Coding in Hex:

00

23 5.1.23 EF$_{3GPDOPM}$ (3GPD Operation Mode)

24 Logically:

25   Operation Mode: Mobile IP with Simple IP fallback

26 Coding in Hex:

01

5.1.24 EF$_{SPN}$ (CDMA Home Service Provider Name)

Logically:

Display Condition:	Display of registered system is required
Character Encoding:	7-bit ASCII
Language Indicator:	1 (English)
Service Provider Name:	"Default Service Provider Name"

Coding in Hex:

01	02	01	44	65	66	61	75	6C	74	20	53	65	72	76	69
63	65	20	50	72	6F	76	69	64	65	72	20	4E	61	6D	65
FF	FF	FF													

5.1.25 EF$_{AppLabels}$ (Application Labels)

Logically:

Character Encoding:	7-bit ASCII
Language Indicator:	1 (English)
Application Labels Present:	MMS, WAP Browser
Application Label Field 1:	"ABCD"
Application Label Field 2:	"EFG"

Coding in Hex:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	…	B36	B37
Hex:	02	01	00	03	41	42	43	44	FF	FF	FF	45

Byte:	B38	B39	B40	…	B132
Hex:	46	47	FF	FF	FF

5.1.26 EF$_{Model}$ (Device Model Information)

Logically:

Character Encoding:	not specified = 0x FF
Language Indicator:	not specified = 0x FF
Model Information:	Default coding, 32 byte 0x FF
Manufacturer Name:	Default coding, 32 byte 0x FF
Software Version:	Default coding, 60 byte 0x FF

Coding in Hex:

Byte:	B1	…	B126
Hex:	FF	…	FF

5.1.27 EF_{ECC} (Emergency Call Codes)

Logically:

Character Encoding:	BCD format
Emergency Call Code 1:	111
Emergency Call Code 2:	222
Emergency Call Code 3:	333
Emergency Call Code 4:	444
Emergency Call Code 5:	555

Coding in Hex:

11	F1	FF	22	F2	FF	33	F3	FF	44	F4	FF	55	F5	FF

5.1.28 EF_{HRPDCAP} (HRPD Capabilities)

Logically:

Maximum NAI Length:	32
Maximum Length of Shared Secret:	31
Authentication Algorithms:	PPP CHAP

Coding in Hex:

20	F8	80

5.1.29 EF_{HRPDUPP} (HRPD Access Authentication User Profile Parameters)

Logically:

HRPD Profile NAI:	"abc@xyz.com"
HRPD Profile Authentication Algorithm:	CHAP

Coding in Hex:

0D	0B	61	62	63	40	78	79	7A	2E	63	6F	6D	10

5.1.30 HRPD Access Authentication CHAP SS

Shared Secret: "HRPD SS"

5.1.31 EF_{WAPBrowserCP} (WAP Browser Connectivity Parameters)

Logically:

Gateway Information:

Address:	"170.187.51.3"
Type of address:	"IPV4"
Port:	"9201"

1   Service: "CO-WSP", WAP session service

2   Authentication type: "HTTP BASIC"

3   Authentication id: "gateway_user1"

4   Authentication pw: "gateway_password1"

5   Gateway: http://gateway.test1.invalid

6   HomeURL: http://www.test1.invalid

7   Coding in Hex:

AC	58	83	3C	20	31	37	30	2E	31	38	37	2E	35	31	2E
33	00	21	85	23	39	32	30	31	00	24	CB	19	9C	1A	67
61	74	65	77	61	79	5F	75	73	65	72	31	00	1B	67	61
74	65	77	61	79	5F	70	61	73	73	77	6F	72	64	31	00
80	18	68	74	74	70	3A	2F	2F	77	77	77	2E	74	65	73
74	31	2E	69	6E	76	61	6C	69	64						

8 ## 5.1.32 EF_{WAPBrowserBM} (WAP Browser Bookmarks)

9   Logically:

10   URL 1:   http://test1.bookmark1.invalid

11   URL Information 1:   "Test 1 Bookmark 1 Homepage"

12   URL 2:   http://test1.bookmark2.invalid

13   URL Information 2:   "Test 1 Bookmark 2 Homepage"

14   URL 3:   http://test1.bookmark3.invalid

15   URL Information 3:   "Test 1 Bookmark 3 Homepage"

16   Coding in Hex:

AD	3C	80	1E	68	74	74	70	3A	2F	2F	74	65	73	74	31
2E	62	6F	6F	6B	6D	61	72	6B	31	2E	69	6E	76	61	6C
69	64	81	1A	54	65	73	74	20	31	20	42	6F	6F	6B	6D
61	72	6B	20	31	20	48	6F	6D	65	70	61	67	65	AD	3C
80	1E	68	74	74	70	3A	2F	2F	74	65	73	74	31	2E	62
6F	6F	6B	6D	61	72	6B	32	2E	69	6E	76	61	6C	69	64
81	1A	54	65	73	74	20	31	20	42	6F	6F	6B	6D	61	72
6B	20	32	20	48	6F	6D	65	70	61	67	65	AD	3C	80	1E
68	74	74	70	3A	2F	2F	74	65	73	74	31	2E	62	6F	6F
6B	6D	61	72	6B	33	2E	69	6E	76	61	6C	69	64	81	1A
54	65	73	74	20	31	20	42	6F	6F	6B	6D	61	72	6B	20
33	20	48	6F	6D	65	70	61	67	65	FF					

5.1.33 EF$_{MMSN}$ (MMS Notification)

Logically:

For all records:

MMS Status: Free space

MMS Implementation Information: No implementation supported

MMS Notification: 'FF FF ... FF' (251 bytes)

Extension File Record Number: 'FF'

Coding in Hex:

Byte:	B1	B2	B3	B4	…	B255
Hex:	'0000XXX0' (Binary)	00	00	FF	FF	FF

5.1.34 EF$_{MMSICP}$ (MMS Issuer Connectivity Parameters)

Logically:

MMS Implementation Information: WAP

MMS Relay/Server Address: "http://mms-operator1.invalid"

Gateway Information:

    Address: "170.187.51.3"

    Type of address: "IPV4"

    Port: "9201"

    Service: "CO-WSP", WAP session service

    Authentication type: "HTTP BASIC"

    Authentication id: "gateway_user1"

    Authentication pw: "gateway_password1"

Coding in Hex:

AB	5F	80	01	01	81	1C	68	74	74	70	3A	2F	2F	6D	6D
73	2D	6F	70	65	72	61	74	6F	72	31	2E	69	6E	76	61
6C	69	64	83	3C	20	31	37	30	2E	31	38	37	2E	35	31
2E	33	0	21	85	23	39	32	30	31	00	24	CB	19	9C	1A
67	61	74	65	77	61	79	5F	75	73	65	72	31	00	1B	67
61	74	65	77	61	79	5F	70	61	73	73	77	6F	72	64	31
00															

1 ## 5.1.35 EF~MMSUP~ (MMS User Preferences)

2 Logically:

3 Record 1:

4   MMS Implementation Information: WAP

5   MMS User Preference Profile Name: "Test MMS User Preferences"

6   MMS User Preference Information:

7   X-Mms-Delivery-Report: "No"

8   X-Mms-Read-Report: "No"

9   X-Mms-Sender-visibility: "Yes"

10   X-Mms-Priority: "High"

11   X-Mms-Expiry (relative):   1104537600 seconds

12   X-Mms-Delivery-Time (absolute):   "1-Jan-2010, 12:00:00 AM UTC"

13 Coding in Hex:

80	01	01	81	19	54	65	73	74	20	4D	4D	53	20	55	73
65	72	20	50	72	65	66	65	72	65	6E	63	65	73	82	16
6	81	10	81	14	80	0F	82	8	81	04	41	D5	E8	00	07
80	04	4B	3D	3B	00										

14 ## 5.1.36 EF~MMSConfig~ (MMS Configuration)

15 Logically:

16   Max Message Size Value: 60000 bytes

17   Retry Times Value: 3

18   Retry Interval Value: 20 seconds

19   MMSC Timeout Value: 30 seconds

20 Coding in Hex:

00	00	EA	60	03	14	00	1E

21 ## 5.1.37 EF~JDL~ (Java Download URL)

22 Logically:

23   Java Download URL: "http://java.xyz.invalid"

24 Coding in Hex:

68	74	74	70	3A	2F	2F	6A	61	76	61	2E	78	79	7A	2E
69	6E	76	61	6C	69	64	00								

5.1.38 EF_{RC} (Root Certificates)

Logically:

Certificate Type:	DER Encoded Binary X.509
Applications:	Java
Certificate information:	Coding is depending on the implementation of the CS and NS.

The format of this field is defined in [15].

5.1.39 EF_{SP} (Service Preferences)

Logically:

System A/B preference:	No preference
Analog/CDMA preference:	No preference

Coding in Hex:

00

5.1.40 EF_{PRL} (Preferred Roaming List)

Logically:

PR_LIST_ID:	0
PREF_ONLY:	true
DEF_ROAM_IND:	Roaming Indicator On
NUM_ACQ_RECS:	2
NUM_SYS_RECS:	3
Acquisition Record 0:	
ACQ_TYPE:	Cellular CDMA (Standard)
System:	A
Channel:	Primary
Acquisition Record 1:	
ACQ_TYPE:	PCS CDMA (Channels)
System:	238
Channel:	283, 450
System record 0:	
SID:	1000
NID_INCL:	'01'
NID:	2222
PREF_NEG:	Preferred
GEO:	'0'

1	PRI:	'1'
2	ACQ_INDEX:	0
3	ROAM_IND:	Roaming Indicator Off
4	System record 1:	
5	SID:	1
6	NID_INCL:	'10'
7	NID:	0
8	PREF_NEG:	Preferred
9	GEO:	'1'
10	PRI:	'0'
11	ACQ_INDEX:	0
12	ROAM_IND:	Roaming Indicator On
13	System record 2:	
14	SID:	1000
15	NID_INCL:	'01'
16	NID:	2222
17	PREF_NEG:	Preferred
18	GEO:	'1'
19	PRI:	'0'
20	ACQ_INDEX:	1
21	ROAM_IND:	Roaming Indicator Off

22 Coding in Hex:

00	23	00	00	80	00	80	03	21	61	8E	E2	36	70	81	F4
21	15	D4	00	02	00	06	C0	00	00	7D	08	45	76	00	80
80	AC	E0													

23 5.1.41 EF$_{MAXPRL}$ (Max Preferred Roaming List)

24 Logically:

25 MAX_PR_LIST_SIZE for EF$_{PRL}$:   1024

26 MAX_PR_LIST_SIZE for EF$_{EPRL}$:   1024

27 Coding in Hex:

04	00	04	00

5.1.42 EF_{OTA} (OTASP/OTAPA Features)

Logically:

Number of features:	5
DATA_P_REV:	'02'
A_KEY_P_REV:	'03'
SSPR_P_REV:	'01'
SPL_P_REV:	'01'
OTASP_P_REV:	'01'

Coding in Hex:

05	00	02	01	03	02	01	03	01	04	01

5.1.43 EF_{NAMLOCK} (NAM_LOCK)

Logically:

NAM_LOCK_STATE:	NAM is unlocked
NAM_LOCK:	SPASM protection is not required
OTA_MODE:	User initiated

Coding in Hex:

00

5.1.44 EF_{OTAPASPC} (OTAPA/SPC_Enable)

Logically:

OTAPA_Enable:	User consents to the performance of OTAPA for the NAM.
SPC_Change_Enable:	User consents to allow the service provider to change the value of SPC.

Coding in Hex:

00

5.1.45 EF_{EPRL} (Extended Preferred Roaming List)

Logically:

PR_LIST_SIZE:	41
PR_LIST_ID:	666
CUR_SSPR_P_REV:	3
PREF_ONLY:	'1'
DEF_ROAM_IND:	'1' - Off
NUM_ACQ_RECS:	2
NUM_COMMON_SUBNET_RECS:	0

1   NUM_SYS_RECS: 2

2   Reserved bits 7-1:   0000000

3   EXT_ACQ_TABLE:

4   Acquisition Record 0:

5   ACQ_TYPE: Cellular CDMA (Custom Channel 3)

6   LENGTH: 2

7   NUM_CHANS: 1

8   CHAN 1:   283

9   Acquisition Record 1:

10   ACQ_TYPE: PCS CDMA (Channel 6)

11   LENGTH: 2

12   NUM_CHANS: 1

13   CHAN 1:   238

14   COMMON_SUBNET_TABLE:

15   EXT_SYS_TABLE:

16   System Record 0:

17   SYS_RECORD_LENGTH: 10

18   SYS_RECORD_TYPE: IS-2000 and IS-95 Systems

19   PREF_NEG: The ME is allowed to operate on the system associated
20   with this record Acquisition Record 0

21   GEO: First record or same geographical region as previous
22   record

23   PRI: Relative priority indicator not set

24   ACQ_INDEX: 0

25   IS-2000 and IS-95 Systems:

26   Reserved bit 1:   '0'

27   NID_INCL: NID included

28   SID: 1000

29   NID: 2222

30   ROAM_IND: Roaming Indicator Flashing '2'

31   ASSOCIATED_INC: Association tag included

32   ASSOCIATED_TAG: not supported

33   DATA_ASSOCIATION: not supported

34   Reserved bits 6-1:   000000

35   System Record 1:

36   SYS_RECORD_LENGTH: 10

1	SYS_RECORD_TYPE:	IS-2000 and IS-95 Systems
2	PREF_NEG:	The ME is allowed to operate on the system associated
3		with this record Acquisition Record 0:
4	GEO:	First record or same geographical region as previous
5		record
6	PRI:	Relative priority indicator not set
7	ACQ_INDEX:	1
8	IS-2000 and IS-95 Systems:	
9	Reserved bit 1:	'0'
10	NID_INCL:	NID included
11	SID:	1000
12	NID:	2222
13	ROAM_IND:	Roaming Indicator Flashing '2'
14	ASSOCIATED_INC:	Association tag included
15	ASSOCIATED_TAG:	not supported
16	DATA_ASSOCIATION:	not supported
17	Reserved bits 6-1:	000000
18	PR_LIST_CRC:	11539

19 Coding in Hex:

00	29	02	9A	03	80	80	80	00	01	00	03	02	09	1B	06
02	08	EE	50	40	01	07	D0	11	5C	05	00	00	50	60	09
07	D0	11	5C	05	05	00	00	2D	13	00	…	00			

5.2   Common Initial Conditions

2   The following initial conditions are common to and used by many test cases in this document:

3   • The ME is connected to the NS.

4   • The ME is connected to the CS.

5   • The CS is configured with default values given in 5.1.

6   ME Test Procedures

For each test procedure the following subsections are included:

1.   Definition

2.   Traceability

3.   Initial Conditions

4.   Procedure

5.   Minimum Standard

Unless otherwise specified, each test case is applicable to all MEs.

6.1   MS Identification

6.1.1   Mobile Station Identifier

6.1.1.1   Definition

The ME sends the MSID for registration to the base station. The content of this MSID depends on the base station's PREF_MSID_TYPE and MCC and IMSI_11_12 values. The ME uses the IMSI_S, IMSI_11_12 and MCC stored in EF_{IMSI_M} and UIMID stored in EF_{RUIMID} to create the MSID.

6.1.1.2   Traceability

The ME shall conform to the requirements referenced in section 2.6.1.2 of [12].

EF_{IMSI_M} is defined in section 3.4.2 of [1].

EF_{RUIMID} is defined in section 3.4.17 of [1].

6.1.1.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.1.1.4   Procedure

1.   The tests shall be conducted in accordance with the procedures and requirements defined in section 2.6.1.4 "MSID, MCC, and IMSI" of [12].

2.   Verify that the fields in EF_{IMSI_M} in the CS are used instead of the fields in IMSI_M (IMSI_S, IMSI_11_12, MCC, etc.) stored on the ME.

3.   Verify that EF_{RUIMID} in the CS is used instead of ESN.

6.1.1.5   Minimum Standard

The ME shall comply with the requirements in steps 2 and 3 of the procedure.

6.1.2 MS Displaying the Roaming Indicator

This test case is only applicable to an ME that displays roaming status.

6.1.2.1 Definition

The ME reads the appropriate home SID and NID stored in EF$_{CDMAHOME}$ from the R-UIM, compares that stored information to that received by the ME in the *Sync Channel Message*, and displays the appropriate roaming indication to the user.

6.1.2.2 Traceability

The ME shall conform to the requirements specified in section 2.6.2.2.1.4 of [16].

The Home SID and NID information is stored in EF$_{CDMAHOME}$ as defined in section 3.4.8 of [1].

6.1.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

The values of the SID and NID fields of the *Sync Channel Message* transmitted by the NS are set to equal to those stored in EF$_{CDMAHOME}$ of the CS.

For MEs supporting SSPR_P_REV ≥ '2' the EF$_{EPRL}$ shall be set as follows:

EF$_{EPRL}$ (Extended Preferred Roaming List)

Logically:

Size:	59 bytes	
PRL ID:	0	
Current Protocol Revision:	3	
Preferred only:	1	
Default roaming indication:	0	
Number of acquisition records:	3	
0:	HDR Generic:	800 MHz Cellular, Channel ID 660
1:	CDMA Cellular (custom):	Channel ID 777
2:	CDMA PCS (channels):	Channel ID 281
Number of records in the Common Subnet Table:	0	
Number of extended system records:	5	
0:		
SYS_RECORD_TYPE:	HRPD System (IS-859)	
SID/NID:	/0	
PREF_NEG:	1	
GEO:	0	
PRI:	0	

6-2

1	ACQ_INDEX:	0
2	ROAM_IND:	0
3	ASSOCIATION_INC:	0
4	PN_ASSOCIATION:	0
5	DATA_ASSOCIATION:	0
6	1:	
7	SYS_RECORD_TYPE:	1x and IS-95
8	SID/NID:	1/2
9	PREF_NEG:	1
10	GEO:	0
11	PRI:	1 (indication off)
12	ACQ_INDEX:	1
13	ROAM_IND:	1
14	ASSOCIATION_INC:	0
15	PN_ASSOCIATION:	0
16	DATA_ASSOCIATION:	0
17	2:	
18	SYS_RECORD_TYPE:	1x and IS-95
19	SID/NID:	1/0
20	PREF_NEG:	1
21	GEO:	0
22	PRI:	0
23	ACQ_INDEX:	1
24	ROAM_IND:	0 (indication on)
25	ASSOCIATION_INC:	0
26	PN_ASSOCIATION:	0
27	DATA_ASSOCIATION:	0
28	3:	
29	SYS_RECORD_TYPE:	1x and IS-95
30	SID/NID:	1/2
31	PREF_NEG:	1
32	GEO:	0
33	PRI:	1 (indication off)
34	ACQ_INDEX:	2
35	ROAM_IND:	1
36	ASSOCIATION_INC:	0

6-3

1   PN_ASSOCIATION: 0

2   DATA_ASSOCIATION: 0

3   4:

4   SYS_RECORD_TYPE: 1x and IS-95

5   SID/NID: 1/0

6   PREF_NEG: 1

7   GEO: 0

8   PRI: 0

9   ACQ_INDEX: 2

10   ROAM_IND: 0 (indication on)

11   ASSOCIATION_INC: 0

12   PN_ASSOCIATION: 0

13   DATA_ASSOCIATION: 0

14   Coding in Hex:

00	3B	00	00	03	80	00	C0	00	02	80	0B	02	02	94	03
02	0B	09	06	02	09	19	30	C0	00	00	00	00	40	60	09
00	02	00	04	02	30	60	0A	00	02	00	40	60	11	00	02
00	04	02	30	60	12	00	02	00	67	7A					

6.1.2.4 Procedure

16   1. Power on the ME.

17   2. Observe the status of any roaming indicator icon or display element on the ME.

18   3. Verify that the roaming indicator icon or display element of the ME indicates the ME
19   is operating within its home system.

20   4. Set the values of the SID and NID fields of the *Sync Channel Message* transmitted
21   by the NS to values other than those stored in the CS (EF$_{CDMAHOME}$).

22   5. Power cycle (power-off then power-on) the ME.

23   6. Observe the status of any roaming indicator icon or display element on the ME.

24   7. Verify that the roaming indicator icon or display element of the ME indicates the ME
25   is operating in a roaming status.

26   8. Power down the ME.

6.1.2.5 Minimum Standard

28   The ME shall comply with the requirements in steps 3 and 7 of the procedure.

6.2   UIMID/ESN_ME Selection

6.2.1   Removable UIMID Usage Indicator

6.2.1.1   Definition

Removable UIMID Usage Indicator indicates whether the 32 bits of the UIMID or ESN_ME is used in the MS identification procedure. The ME uses the Removable UIMID Usage Indicator stored in EF$_{USGIND}$ of the R-UIM.

6.2.1.2   Traceability

The ME shall conform to the requirements specified in sections 3.4.32 of [1] and 2.3.2.3 of [16].

6.2.1.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial conditions A:

In addition, the NS shall select ESN as PREF_MSID_TYPE.

Initial conditions B:

In addition, the UIMID Usage Indicator shall be set to '0' on the CS. The NS shall select ESN as PREF_MSID_TYPE.

EF$_{USGIND}$ (UIMID/SF_EUMID Usage Indicator)

Logically:

UIMID usage indicator:	ESN_ME is used for CAVE authentication and MS identification
SF_EUMID usage indicator:	MEID is used for MS identification

Coding in Hex:

00

6.2.1.4   Procedure

1.   Power on the ME.

2.   Initiate a ~~mobile station originated~~ MO call.

3.   Perform the following for different initial conditions:

   A.   Verify that the ME uses the UIMID stored in EF$_{RUIMID}$ to identify itself in the *Origination Message*.

   B.   Verify that the ME uses the ESN_ME stored in EF$_{ESNME}$ to identify itself in the *Origination Message*.

4.   End the call.

5.   Power down the ME

6.2.1.5   Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.2.2   ESN Management

This test is only applicable to an ME that is not assigned an MEID.

6.2.2.1   Definition

ESN_ME is the electronic serial number of the Mobile Equipment (ME) to which the R-UIM is attached. ―This number is transferred to the R-UIM when the ME determines that the R-UIM has been inserted.

6.2.2.2   Traceability

The ME shall conform to the requirements for ESN_ME specified in section 4.6 of [1] and section 2.3.2 of [16].

6.2.2.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.2.2.4   Procedure

1. Power on the ME.

2. During the ME and R-UIM initialization process, verify that

    - T̶t̶he ME invokes the "Store ESN_MEID_ME" command to store its ESN_ME in EF_{ESNME}.

    - T̶t̶he new ESN_ME stored in the EF_{ESNME} matches ESN of the ME being tested.

3. Power down the ME.

6.2.2.5   Minimum Standard

The ME shall comply with the requirements in step 2 of the procedure.

6.2.3   MEID Management

This test is only applicable to an ME that is assigned an MEID.

6.2.3.1   Definition

The ME can be assigned an MEID. If an R-UIM that has service n9 "MEID support" not activated is inserted into an ME assigned an MEID, the ME transfers its Pseudo-ESN to the R-UIM. Otherwise, the ME transfers its MEID to the R-UIM. The MEID or Pseudo-ESN is transferred to the R-UIM when the ME determines that the R-UIM has been inserted.

6.2.3.2   Traceability

The ME shall conform to the requirements for MEID specified in section 4.6 of [1] and section 2.3.2 of [16].

6.2.3.3   Initial Conditions

Initial Conditions A:

Refer to section 5.2 for the common initial conditions.

Initial Conditions B:

Refer to section 5.2 for the common initial conditions.

In addition, service n9 stored in EF_{CST} is set to "not allocated" and "not activated".

6.2.3.4   Procedure

1.   Power on the ME.

2.   Perform the following for different initial conditions:

   A.   During the ME and R-UIM initialization process, verify that the ME sends the "Store ESN_MEID_ME" command (P1 = '01') to store its MEID in EF_{ESNME} which shall match the MEID of the ME.

   B.   During the ME and R-UIM initialization process, verify that the ME sends the "Store ESN_MEID_ME" command (P1 = '00') to store its Pseudo-ESN in EF_{ESNME} which shall match the Pseudo-ESN of the ME.

3.   Power down the ME.

6.2.3.5   Minimum Standard

The ME shall comply with the requirements in step 2 of the procedure.

6.2.4   EUIMID and MEID

Refer to section 2.2 "MEID, EXT_UIMID, MEID_ME, ESN_ME Information Records" of [14] for the testing for EUIMID and MEID.

6.3 Security-related commands

6.3.1 SSD Update

6.3.1.1 Definition

SSD is derived from the "A-key" stored in the CS. SSD updates are initiated when the NS issues the command UPDATE SSD, containing the parameter RANDSSD, to the ME. The ME passes RANDSSD, RANDSeed and AUTHBS correctly to CS when the NS initiates an SSD Update process.

6.3.1.2 Traceability

The ME shall conform to the requirements specified in sections 4.4.1, 4.4.2 and 4.4.3 of [1] and 2.3.12.1.5 of [16].

6.3.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Ensure that the A-key, ESN and IMSI are aligned between the ME and the NS.

6.3.1.4 Procedure

1. Power on the ME.

2. At the NS, initiate an SSD Update on the paging channel.

3. Verify that the ME sends a Base Station Challenge Command to CS with a RANDSeed.

4. Verify that upon receipt of a Base Station Challenge Response from the CS, the ME sends a *Base Station Challenge Order* to the NS with RANDBS set to the same value as that received from CS.

5. Verify that the ME sends an Update SSD Command to the CS, containing the parameter RANDSSD received from the *SSD Update Message*.

6. Verify that upon receipt of a *Base Station Challenge Confirmation Order* from the NS, the ME sends a Confirm SSD Command to the CS with AUTHBS set to the same value as that received from the *Base Station Challenge Confirmation Order*.

7. Verify that the ME sends an *SSD Update Confirmation Order* upon receipt of a response from CS with '90 00', SW1= '90' and SW2='00'.

8. Modify the IMSI in the NS to a different value.

9. Repeat steps 2) through 6).

10. Verify that the ME sends an *SSD Update Rejection Order* upon receipt of response from CS with '98 04', SW1= '98' and SW2='04'.

11. Power down the ME.

6.3.1.5   Minimum Standard

The ME shall comply with the requirements in steps 3, 4, 5, 6, 7 and 10 of the procedure.

6.3.2   Authentication Calculation for Global Challenge

6.3.2.1   Definition

The ME initiates the start of the CAVE algorithm in the R-UIM and passes AUTHR from the R-UIM to the NS when the NS enables or initiates authentication.

6.3.2.2   Traceability

The ME shall conform to the requirements specified in sections 4.2.2 and 4.4.4 of [1] and 2.1.1.1.2.1 of [17].

6.3.2.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.3.2.4   Procedure

1. Power on the ME.

2. At the NS, enable global challenge.

3. Originate a voice call from the ME.

4. Verify that the ME sends a "Run CAVE" Command with RANDTYPE set to '00000000' and RAND to CS.

5. Upon receipt of SW '9F 03', verify that the ME sends a "Get Response" Command.

6. Upon receipt of the AUTHR, verify that AUTHR is included in the *Origination Message*.

7. Verify the audio traffic in both directions.

8. Power off the ME.

6.3.2.5   Minimum Standard

The ME shall comply with the requirements in steps 4, 5, 6 and 7 of the procedure.

6.3.3   Unique Challenge While the Mobile Station is in Idle State

6.3.3.1   Definition

The CAVE function is run in the R-UIM to calculate AUTHU when the ME sends Run CAVE Command.

6.3.3.2   Traceability

The ME shall conform to the requirements specified in sections 4.2.2 and 4.4.4 of [1] and 2.3.12.1.4 of [16].

6.3.3.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.3.3.4   Procedure

1. Power on the ME.

2. Enable authentication within the NS.

3. Instruct the NS to send an *Authentication Challenge Message*.

4. Verify that the ME sends a "Run CAVE" Command with RANDTYPE set to '00000001' and RANDU to CS.

5. Upon receipt of SW '9F 03', verify that ME sends a "Get Response" Command.

6. Upon receiving the AUTHU, verify that AUTHU is included in the *Authentication Challenge Response Message* with AUTHU same as sent from CS.

7. Power off the ME.

6.3.3.5   Minimum Standard

The ME shall comply with the requirements in steps 4, 5 and 6 of the procedure.

6.3.4   Unique Challenge While the Mobile Station is in Mobile Station Control on the Traffic Channel State

6.3.4.1   Definition

The CAVE function is executed within the R-UIM to calculate AUTHU when the ME sends the "Run CAVE" Command with RANDU when the ~~mobile station~~MS is in the *Mobile Station Control on the Traffic Channel State*.

6.3.4.2   Traceability

The ME shall conform to the requirements specified in sections 4.2.2 and 4.4.4 of [1] and 2.3.12.1.4 of [16].

6.3.4.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.3.4.4   Procedure

1. Power on the ME

2. At the NS, enable authentication.

3. Originate a voice call from the ME.

4. Verify the audio traffic in both directions.

5. While the call is in progress, instruct the NS to send an *Authentication Challenge Message*.

6. Verify that the ME sends a "Run CAVE" Command with RANDTYPE set to '00000001' and RANDU to CS.

7. Upon receipt of SW '9F 03', verify that ME sends a Get Response Command.

8. Upon receipt of AUTHU from CS, verify that the ME sends an *Authentication Challenge Response Message* with AUTHU same as sent from CS.

9. Power off the ME.

6.3.4.5   Minimum Standard

The ME shall comply with the requirements in steps 4, 6, 7 and 8 of the procedure.

6.3.5   Generate Key/VPM

6.3.5.1   Definition

The CAVE function is run in the R-UIM to generate the encryption key/VPM when the ME sends a "Generate Key/VPM" command.

6.3.5.2   Traceability

The ME shall conform to the requirements specified in sections 4.2.2 and 4.4.5 of [1] and 2.3.12 of [16].

6.3.5.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.3.5.4   Procedure

1. Power on the ME.

2. At the NS, enable authentication. On the ME, enable voice privacy.

3. Originate a voice call from the ME.

4. Verify that the ME sends a "Run CAVE" Command with the following: RANDTYPE is set to '00000000', Bit 4 of Process_Control is set to '1' and a RAND.

5. Upon receipt of SW '9F 03', verify that the ME sends a "Get Response" Command.

6. Upon receiving the AUTHR, verify that AUTHR is included in the *Origination Message*.

7. Verify that the ME sends a "Generate Key/VPM" command to the CS.

8. Power off the ME.

6.3.5.5   Minimum Standard

The ME shall comply with the requirements in steps 4, 5, 6 and 7 of the procedure.

6.3.6 Authentication

2 The ME shall conform to the test requirements for ~~mobile station~~MSs defined in section 7
3 "Authentication" of [12].

4 Refer to section 5.2 for the common initial conditions.

5 The test procedures defined in section 7 "Authentication" of [12] are used.

6 The minimum standard defined in section 7.1.1.5 of [12] is used.

1 ## 6.4   Reserved

2

6.5 OTASP/OTAPA Functionality

The tests in this section are only applicable to an ME that supports OTASP/OTAPA.

6.5.1 PRL Download

This test is only applicable to an ME that supports SSPR_P_REV=1.

6.5.1.1 Definition

The ME initiates an OTASP call, downloads a PRL, and correctly stores PRL in EF_{PRL} of the R-UIM.

6.5.1.2 Traceability

The ME shall conform to the requirements specified in sections 4.5.8 of [1] and 3.5.1.9 of [18].

6.5.1.3 Initial Conditions

Refer to the section 5.2 for the common initial conditions.

The NS is configured to send the following SSPR Download Request Message to the ME.

SSPR Download Request Message:

Field	Value	Length (bits)
OTASP_MSG_TYPE	'08'	8
BLOCK_ID	'00'	8
BLOCK_LEN	'16'	8
RESERVED	'0000000'	7
LAST_SEGMENT	'1'	1
SEGMENT_OFFSET	'00 00'	16
SEGMENT_SIZE	'12'	8
SEGMENT_DATA	See Preferred Roaming below	$8 \times$ SEGMENT_SIZE
FRESH_INCL	'0'	1
RESERVED	'0000000'	7

Command data:

Size: 18 bytes

PRL ID: 0

Preferred only: true

Default roaming indication: off

Number of Acquisition Records: 1

Number of System Records: 1

6-14

Coding in Hex:

00	12	00	00	80	00	40	01	21	00	02	80	00	50	00	00
6E	DB														

The NS is configured to send the following Commit Request Message to the ME.

Commit Request Message:

Field	Value	Length (bits)
OTASP_MSG_TYPE	'05'	8

6.5.1.4   Procedure

1. The test shall be conducted in accordance with the procedures defined in section 2.6.5 "SSPR Download Processing – Operation Successful" of [13] and the parameters defined above.

2. Verify that the ME sends a SELECT command to the R-UIM to select $EF_{NAMLOCK}$.

3. Verify that the ME sends an UPDATE BINARY command to the R-UIM with '00' (OTA_MODE is set to '0' indicating a user-initiated OTASP session).

4. After step c (see Sec. 2.6.5.1.4 of [13]), verify that the ME sends a single or multiple SSPR DOWNLOAD REQUEST command(s) to the CS with the following command data: '00 16 01 00 00 12 00 12 00 00 80 00 40 01 21 00 02 80 00 50 00 00 6E DB'. This data may be segmented if multiple commands are used.

5. After step e (see Sec. 2.6.5.1.4 of [13]), verify that the ME sends a COMMIT command to the CS

6.5.1.5   Minimum Standard

The ME shall comply with the requirements in steps 4 and 5 of the procedure.

6.5.2   OTASP/OTAPA Commands

6.5.2.1   Definition

The ME maps OTASP/OTAPA messages sent from the NS correctly to the OTASP/OTAPA commands to R-UIM and maps responses from R-UIM to OTASP/OTAPA messages (except for the PRL and EPRL download tests which are specified in sections 6.5.1 and 6.5.3).

6.5.2.2   Traceability

The ME shall conform to the requirements specified in sections 4.3.2 and 4.5 of [1] and 3.5.1 of [18].

6.5.2.3   Initial Conditions

Refer to the section 5.2 for the common initial conditions.

6.5.2.4 Procedure

1. The test shall be conducted in accordance with the procedures defined in [13].

2. Verify that the ME correctly maps the OTASP/OTAPA messages to corresponding commands and maps responses from R-UIM to OTASP/OTAPA messages.

6.5.2.5 Minimum Standard

The ME shall comply with the requirements in step 2 of the procedure.

6.5.3 EPRL Download

This test is only applicable to an ME that supports SSPR_P_REV=3.

6.5.3.1 Definition

The ME initiates an OTASP call, downloads an EPRL, and correctly stores the EPRL in EF_{EPRL} of the R-UIM.

6.5.3.2 Traceability

The ME shall conform to the requirements specified in sections 4.5.8 of [1] and 3.5.1.9 of [18].

6.5.3.3 Initial Conditions

Refer to the section 5.2 for the common initial conditions.

The NS is configured to send the following SSPR Download Request Message to the ME.

SSPR Download Request Message:

Field	Value	Length (bits)
OTASP_MSG_TYPE	'08'	8
BLOCK_ID	'01'	8
BLOCK_LEN	'2D'	8
RESERVED	'0000000'	7
LAST_SEGMENT	'1'	1
SEGMENT_OFFSET	'00 00'	16
SEGMENT_SIZE	'29'	8
SEGMENT_DATA	See Extended Preferred Roaming below	8 x SEGMENT_SIZE
FRESH_INCL	'0'	1
RESERVED	'0000000'	7

1 Command data:

2   Size: 41 bytes

3   PRL ID: 0

4   Preferred only: true

5   Default roaming indication: off

6   Number of Acquisition Records: 1

7   Number of System Records: 1

8 Coding in Hex:

00	29	02	9A	03	80	80	80	00	01	00	03	02	09	1B	06
02	09	1B	50	40	01	07	D0	11	5C	05	00	00	50	60	09
07	D0	11	5C	05	00	00	5C	6A							

9 The NS is configured to send the following Commit Request Message to the ME.

10 Commit Request Message:

Field	Value	Length (bits)
OTASP_MSG_TYPE	'05'	8

11 ## 6.5.3.4   Procedure

12   1. The test shall be conducted in accordance with the procedures defined in section
13   2.6.5 "SSPR Download Processing – Operation Successful" of [13] and the parameters
14   defined above.

15   2. Verify that the ME sends a SELECT command to the R-UIM to select EF$_{NAMLOCK}$.

16   3. Verify that the ME sends an UPDATE BINARY command to the R-UIM with '00'
17   (OTA_MODE is set to '0' indicating a user-initiated OTASP session).

18   4. After step c (see Sec. 2.6.5.1.4 of [13]), verify that the ME sends a single or multiple
19   SSPR DOWNLOAD REQUEST command(s) to the CS with the following command
20   data: : '01 00 00 29 00 29 02 9A 03 80 80 80 00 01 00 03 02 09 1B 06 02 09 1B 50
21   40 01 07 D0 11 5C 05 00 00 50 60 09 07 D0 11 5C 05 00 00 5C 6A'. This data may
22   be segmented if multiple commands are used.

23   5. After step e (see Sec. 2.6.5.1.4 of [13]), verify that the ME sends a COMMIT
24   command to the CS.

25 ## 6.5.3.5   Minimum Standard

26 The ME shall comply with the requirements in step 4 and 5 of the procedure.

1 ## 6.6 Reserved

2 ## 6.7 Reserved

3 ## 6.8 Reserved

4 ## 6.9 Reserved

5 ## 6.10 Reserved

6

6.11 Exchange Protocol Tests

The ME shall conform to the test requirements and procedures specified in section 27.11 of [10].

6.12 Evaluation of Directory Characteristics

6.12.1 Operating Speed in Authentication Procedure

6.12.1.1 Definition

Authentication is performed in a cdma2000®[1] network on an R-UIM enabled ~~mobile station~~MS by the ME sending a random number received from the network to the R-UIM. The R-UIM then performs a calculation on the random number, and sends the result to the network for verification.

6.12.1.2 Traceability

If bit b2 of the file characteristics is set to 1, the ME shall provide a clock frequency of at least 13/4 MHz to enable the R-UIM to run the authentication process in the required time. See section 5.4 of [2].

6.12.1.3 Initial Conditions

The ME is powered on and connected to the CS with bit b2 of the file characteristics set to '1'.

6.12.1.4   Procedure

1. The test shall be conducted in accordance with the procedures defined in section 7.9 "Authentication Upon Originations" of [12].

2. Verify that the frequency of the clock is at least 13/4 MHz during the authentication procedure if bit b2 of the file characteristics is set to 1.

6.12.1.5 Minimum Standard

The ME shall comply with the requirements in step 2 of the procedure.

6.12.2 Clock Stop

6.12.2.1 Definition

The ME may switch off the clock signal to the R-UIM if the R-UIM indicates that it supports this feature.

---

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

6.12.2.2 Traceability

The ME shall not stop the clock, unless the requirements indicated in byte 1 of the file characteristics are met. See section 5.2 of [2].

The ME shall wait at least 860 clock cycles after having received the last character including the minimum guard time (2 elementary time units [etu]) of the response before switching off the clock. The ME shall wait at least 744 clock cycles before it sends the first command after having restarted the clock. See section 6.6 of [19].

6.12.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions. CHV1 is enabled.

6.12.2.4   Procedure

1. The CS is used with the file characteristics bits set as follows:

Bit b1	Bit b3	Bit b4
0	0	0

2. The ME is powered on. When the ME is in mode CHV1 check, 10 seconds shall elapse before the CHV1 is entered.

3. Verify that the ME does not switch off the clock.

4. The ME is powered off, and the CS is used with the file characteristics bits set as follows:

Bit b1	Bit b3	Bit b4
0	1	0

5. The ME is powered on. When the ME is in mode CHV1 check, 10 seconds shall elapse before the CHV1 is entered.

6. Verify that the ME

    - Does not switch off the clock, unless at high level.

    - Does not switch off the clock until at least 1,860 clock cycles after having received the last character of the response including the minimum guard time (2 etu).

    - Waits at least 744 clock cycles before it sends the first command after having restarted the clock.

7. The ME is powered off, and the CS is used with the file characteristics bits set as follows:

Bit b1	Bit b3	Bit b4
0	0	1

8. The ME is powered on. When the ME is in mode CHV1 check, 10 seconds shall elapse before the CHV1 is entered.

9. Verify that the ME

6-21

- Does not switch off the clock, unless at low level.

- Does not switch off the clock until at least 1,860 clock cycles after having received the last character of the response including the minimum guard time (2 etu).

- Waits at least 744 clock cycles before it sends the first command after having restarted the clock.

10. The ME is powered off, and the CS is used with the file characteristics bits set as follows:

Bit b1	Bit b3	Bit b4
1	0	0

11. The ME is powered on. When the ME is in mode CHV1 check, 10 seconds shall elapse before the CHV1 is entered.

12. Verify that the ME

- Does not switch off the clock until at least 1,860 clock cycles after having received the last character of the response including the minimum guard time (2 etu).

- Waits at least 744 clock cycles before it sends the first command after having restarted the clock.

6.12.2.5 Minimum Standard

The ME shall comply with the requirements in steps 2, 3, 5, 6, 8, 9, 11 and 12 of the procedure.

6.12.3 Reserved

1   # 6.13 Mechanical Tests

2   The ME shall conform to the requirements specified in section 27.13 of [10].

3

6.14 Secret Code Usage

For the test cases in this section, refer to section 5.2 for the common initial conditions.

In addition, the CS shall be configured with the following:

EF_{CST} (CDMA Service Table)

(Different from the default CDMA Service Table Service defined in section 5.1):

n1-: CHV disable function is not activated to enforce authentication via CHV entry.

6.14.1 Entry of CHV1

The ME shall conform to the requirements specified in section 27.14.1 of [10].

6.14.2 Change of CHV1

The ME shall conform to the requirements specified in section 27.14.2 of [10].

6.14.3 Disabling the CHV1

6.14.3.1 Definition

Entry of the CHV1 may be disabled by the user, depending on the service table of the R-UIM.- It is the responsibility of the ME to check the CDMA Service Table.

6.14.3.2 Traceability

Disabling CHV1 is achieved through the DISABLE CHV command. If the CHV1 disable function in the R-UIM service table is not allocated or activated, the ME shall not attempt to disable the CHV1. See sections 2.5 and 3.4.18 of [1].

6.14.3.3 Initial Conditions

The ME is powered on and a correct CHV1 entered.

6.14.3.4 Procedure

1. Using the ME's user interface procedure, attempt to disable the CHV1.

2. Verify that the ME does not send a DISABLE CHV command across the R-UIM/ME interface.

6.14.3.5 Minimum Standard

The ME shall comply with the requirements in step 2 of the procedure.

6.14.4 UNBLOCK CHV1 Entry

The ME shall conform to the requirements specified in section 27.14.4 of [10].

6.14.5 Entry of CHV2

The ME shall conform to the requirements specified in section 27.14.5 of [10].

6.14.6 Change of CHV2

The ME shall conform to the requirements specified in section 27.14.6 of [10].

6.14.7 UNBLOCK CHV2 Entry

The ME shall conform to the requirements specified in section 27.14.7 of [10].

6.14.8 Reserved

6.15 Abbreviated Dialing Number (ADN)

6.15.1 Definition

Abbreviated Dialing Numbers contain subscriber number and supplementary service control strings. They may also contain alpha identifiers.

6.15.2 Traceability

The ME shall be able to update and retrieve ADNs from the R-UIM and set up calls to these numbers. See section 2.7 of [1].

6.15.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the following EF values shall be configured:

EF$_{ADN}$ (Abbreviated Dialing Number)

At least 101 records.

Record 1:

Length of alpha identifier:	32 characters
Alpha identifier:	"ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF"
Length of BCD number:	"03"
TON and NPI:	Telephony and Unknown
Dialed number:	123
CCI:	None
Ext1:	None

Coding for record 1:

Byte:	B1	B2	B3	...	B32	B33	B34	B35	B36	B37	B38	B39	...	B46
Hex:	41	42	43	...	46	03	81	21	F3	FF	FF	FF	...	FF

6.15.4 Procedure

1. The code "1234567890123456" is stored (entered) in the MS as abbreviated dialing entry number 7 on the R-UIM.

2. The code "00112233" is stored (entered) in the MS as abbreviated dialing entry number 6 on the R-UIM.

3. The code "**21*44556677#" is stored (entered) in the MS as abbreviated dialing entry number 101 on the R-UIM.

4. Retrieve data from R-UIM entry number 7 using the procedure N(N)(N)#.

5. Verify that the number "1234567890123456" is displayed.

6.   Retrieve data from R-UIM entry number 6 using the procedure N(N)(N)#.

7.   Verify that the number "00112233" is displayed.

8.   Retrieve data from R-UIM entry number 101 using the procedure N(N)(N)#.

9.   Verify that the number "**21*44556677#" (or an equivalent representation) is displayed.

10.   Retrieve data from R-UIM entry number 1 using the procedure N(N)(N)#, and display the alpha identifier.

11.   Verify that the ME displays at least part of the alpha identifier, and sustains normal operation.

12.   Verify that EF_{ADN} in the CS is updated with the new codes for R-UIM entries 1, 6, 7 and 101.

6.15.5 Minimum Standard

The ME shall comply with the requirements in steps 5, 7, 9, 11 and 12 of the procedure.

6.16 UI Reaction to R-UIM Status Encoding

The ME shall conform to the requirements specified in section 27.16 of [10].

6.17 Electrical Tests

The ME shall conform to the requirements specified in section 27.17 of [10] with the following exception: ~~T~~the command "SELECT CDMA" shall be used in place of "SELECT GSM".

6.18 Fixed Dialing Number (FDN)

The ME shall conform to the requirements specified in section 27.18 of [10] with the following exceptions:

1. Appropriate cdma2000 NS settings shall be used in place of the GSM-specific settings identified in [10].

2. Rehabilitation of EF_{LOCI} is not applicable.

3. EF_{CST} shall be set as the following which is different from the default CDMA Service Table Service defined in section 5.1:

   n3: Fixed Dialing Numbers (FDN) – is activated and allocated

6.19 Version Identification

6.19.1 Definition

The version of the R-UIM is indicated in the Elementary File $EF_{Revision}$. This allows the ME to identify the version of the R-UIM and adapt its functionality accordingly.

6.19.2 Traceability

The version of the card shall be determined as part of the initialization procedure. See sections 3.4.25 and 4.11.5 of [1].

6.19.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.19.4 Procedure

1. Power on the ME.

2. Monitor the R-UIM initialization procedure using the CS.

3. Verify that the ME requests the version ($EF_{Revision}$) of the CS as part of the initialization procedure.

4. Power off the ME.

6.19.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.20 R-UIM Presence Detection

2   The ME shall conform to the requirements specified in section 27.20 of [10].

3

6.21 Reserved

6.22 Suggested Slot Cycle Index

6.22.1 Definition

The file EF_{SSCI} suggests a value for the ME's preferred Slot Cycle Index for CDMA operation. Since the ME may not support all the slot cycle indexes, the ME shall select the minimum, as the preferred Slot Cycle Index, between the Slot Cycle Index supported by the ME and the suggested Slot Cycle Index contained in EF_{SSCI}.

6.22.2 Traceability

The ME shall read the contents of EF_{SSCI} (Suggested Slot Cycle Index) and apply it to ~~mobile station~~ MS processing. See section 3.4.14 of [1].

6.22.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, EF_{SSCI} shall be set to the value '00000010'. The NS is configured such that the value of MAX_SLOT_CYCLE_INDEX within the *System Parameters Message* is set to '011'.

Initial Conditions B:

In addition, EF_{SSCI} shall be set to the value '00000010'.

The NS is configured such that the value of MAX_SLOT_CYCLE_INDEX within the *System Parameters Message* is set to '001'.

6.22.4 Procedure

1. Power on the ME.

2. Allow a sufficient time for the ME to complete power-up registration with the NS. Determine the value of the Slot Cycle Index used by the ME. Also note the value of the preferred Slot Cycle Index (SLOT_CYCLE_INDEX) reported by the ME in the *Registration Message*.

3. Perform the following for different initial conditions:

   A. Verify that ME sends a *Registration Message* to the NS with a preferred Slot Cycle Index (SLOT_CYCLE_INDEX) value of '010'. Similarly, the ME shall be operating using a value of '010' for the Slot Cycle Index.

   B. Verify that ME sends a *Registration Message* to the NS with a preferred Slot Cycle Index (SLOT_CYCLE_INDEX) value of '010'. The ME shall also, however, be operating using a value of '001' for the Slot Cycle Index.

4. Power down the ME.

6.22.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.23 Service Provider Name

This test is only applicable to an ME that supports the display of service provider name.

6.23.1 Definition

During the ME and R-UIM initialization procedure, the ME reads the contents of EF_{SPN} and displays the corresponding information to the ~~mobile station~~ user.

6.23.2 Traceability

If present, the device should display the operator name provisioned in EF_{SPN} on the idle screen. See section 3.4.31 of [1].

6.23.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.23.4 Procedure

1. Power on the ME.

2. Wait for the ME to register with the NS.

3. Verify that the ME reads and displays the contents of EF_{SPN} on the CS.

4. Power down the ME.

6.23.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.24 CDMA Service Table

6.24.1 Definition

The CDMA Service Table in the R-UIM indicates which services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the R-UIM, the ME shall not select this service.

6.24.2 Traceability

The ME shall read the contents of EF_{CST} from the CS and shall provide user access and/or service to the functions and services allocated and activated within EF_{CST}. See section 3.4.18 of [1].

6.24.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, the settings of EF_{CST} shall indicate "service allocated" and "service not activated" for the following services: SMS (n4), FDN (n3), ADN (n2), and CHV disable (n1).

Coding in Hex:

55	FF	C3	FF	CF	0F	FF	3C	00	CC	3F	00

In addition, the NS is configured to accept SMS messages from the MS.

Initial Conditions B:

In addition, the settings of EF_{CST} shall indicate "service allocated" and "service activated" for the following services: SMS (n4), FDN (n3), ADN (n2), and CHV disable (n1).

Coding in Hex:

FF	FF	C3	FF	CF	0F	FF	3C	00	CC	3F	00

In addition, the NS is configured to accept SMS messages from the MS.

6.24.4 Procedure

1. Power on the ME.

2. Use a UI dependent method to check if:

   - SMS services can be used

   - FDNs are available

   - ADNs are available

   - The card holder verification (CHV) can be disabled

3. Perform the following for different initial conditions:

6-36

1   A.   Verify that the listed services and functions are not operational.

2   B.   Verify that the listed services and functions are operational.

3   4.   Power off the ME.

6.24.5 Minimum Standard

The ME shall comply with the requirements in step 2.

6.25 Application Labels

6.25.1 Application Labels Present on R-UIM

6.25.1.1 Definition

Application Labels stored in R-UIM allow the operators to customize the UI display of the text labels for the applications, such as MMS and WAP.

6.25.1.2 Traceability

If an application label has been provisioned for a particular application in $EF_{AppLabels}$, the device's user interface shall display this text label with the associated icon or menu item used to launch that application. See section 3.4.84 of [1].

6.25.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.25.1.4 Procedure

1. Power on the ME.

2. Navigate to the application menus or icons using the ME's UI.

3. Observe the application labels displayed.

4. Verify that the ME displays the Application Labels as configured in $EF_{AppLabels}$. The application label for MMS shall be "ABCD" and the application label for WAP Browser shall be "EFG".

5. Power down the ME.

6.25.1.5 Minimum Standard

The ME shall comply with the requirements in step 4 of the procedure.

6.25.2 Application Labels Not Present on R-UIM

6.25.2.1 Definition

Application Labels on the R-UIM might not be present so that the ME needs to display the default labels stored in the ME. The ME displays the handset vendor-defined labels when the R-UIM does not contain the application labels.

6.25.2.2 Traceability

If an application label has not been provisioned for a particular application in $EF_{AppLabels}$, the ME shall display the handset vendor-defined labels. See section 3.4.84 of [1].

6.25.2.3   Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

EF$_{AppLabels}$ (Application Labels)

Logically:

| File ID: | 3F00/7F25/6F92 |

| Character Encoding: | 7-bit ASCII |

| Language Indicator: | 1 (English) |

| Application Labels Present: | None |

Coding in Hex:

Byte:	B1	B2	B3	B4	B5	…	B132
Hex:	00	01	00	00	FF	FF	FF

Initial Conditions B:

EF$_{AppLabels}$ is not present on the CS.

6.25.2.4   Procedure

The following process applies to all initial conditions:

1. Power on the ME.

2. Navigate to the application menus or icons using the ME's UI.

3. Observe the display of the application labels on the ME.

4. Verify that ME displays the handset vendor-defined labels.

5. Power down the ME.

6.25.2.5   Minimum Standard

The ME shall comply with the requirements in step 4 of the procedure.

6.26 Device Model Information

6.26.1 Definition

The ME writes the ME's model information to the R-UIM so that the applications residing in the R-UIM can use that information for various purposes.

6.26.2 Traceability

The ME shall be capable of writing the ME's model information to EF_{Model} in the R-UIM during power-up initialization. See section 3.4.85 of [1].

6.26.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.26.4 Procedure

1. Power on the ME.

2. Wait until the ME has finished intialization.

3. Verify that EF_{Model} on the R-UIM has these fields filled correctly based on ME's model information using the coding definitions in [1]:

   - Character Encoding

   - Language Indicator

   - Model Information

   - Manufacturer Name

   - Software Version Information

4. Power down the ME.

6.26.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.27 Emergency Numbers

6.27.1 Definition

The R-UIM contains emergency call numbers so that the user can make emergency calls using the emergency numbers stored in the R-UIM.

6.27.2 Traceability

The ME shall allow the user to dial the emergency call codes stored in the R-UIM. See section 3.4.37 of [1].

6.27.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured to accept emergency voice calls.

6.27.4 Procedure

1. Power on the ME.

2. Verify that the ME reads the emergency numbers stored in EF_{ECC}.

3. Select the emergency number "111" using the ME's UI.

4. Dial "111".

5. Verify that the ME displays that it is making an emergency call using "111" from EF_{ECC} in the CS.

6. Wait until call is connected.

7. Verify that the ME has successfully established an emergency voice call.

8. End call.

9. Select the emergency number "222" using the ME's UI.

10. Dial "222".

11. Verify that the ME displays that it is making an emergency call using "222" from EF_{ECC} in the CS.

12. Wait until call is connected.

13. Verify that the ME has successfully established an emergency voice call.

14. End call.

15. Power down the ME.

6.27.5 Minimum Standard

The ME shall comply with the requirements in steps 2, 5, 7, 11 and 13 of the procedure.

6.28 SMS Capabilities

The tests in this section are only applicable to an ME supporting the SMS feature.

6.28.1   SMS Retries

6.28.1.1 Definition

The R-UIM contains SMS retry configurations for the ME to use for retrying MO SMS messages.

6.28.1.2 Traceability

The ME shall be capable of performing MO SMS retry using the SMS retry period and SMS retry interval parameters in EF_{SMSCAP} of the R-UIM. See section 3.4.87 of [1].

6.28.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured so that it will respond with an SMS Acknowledgement Message (Error Class = 2 "temporary error" and Cause Code = 0 "unspecified") to MO SMS messages from the ME.

Coding of elementary files in the CS is defined in 5.1, with the addition of:

EF_{SMSCAP} (SMS Capabilities):

Logically:

SMS Retry Period:	60 seconds
SMS Retry Interval:	8 seconds
SMS Flags:	
Send On Access:	True
Send on Traffic:	True
Send as Standard EMS:	True
SMS Preferred Service Option:	SO 6

Coding in Hex:

3C	08	07	01

EF_{SMS} (Short Messages):

Record 1 - Logically (Main parameters only):

Status:	MS originating message; message to be sent, Message protection disabled
MSG_LEN:	35 bytes
SMS Transport Layer Message:	
SMS_MSG_TYPE:	SMS Point-to-Point

6-42

1   Destination Address: +0123456789

2   Message Type: SMS-Submit

3   User Data: "Retry"

4   Coding in Hex:

07	23	00	00	02	10	02	04	07	02	A8	48	D1	59	E2	40
08	13	00	03	20	00	00	01	06	10	2D	2C	BD	39	79	07
01	05	08	01	80	00	..	..	00							

5   All other records are empty.

6.28.1.4 Procedure

7   1.   Power on the ME.

8   2.   Send the SMS message stored on the R-UIM from the ME.

9   3.   Wait for 65 seconds.

10   4.   Verify that the ME retries to send the SMS for up to 60 to 62 seconds after the first
11   Temporary Network Error was been sent by the NS with an interval of 8 to 10
12   seconds between the retries as configured in EF$_{SMSCAP}$.

13   5.   Power down the ME.

6.28.1.5 Minimum Standard

15   The ME shall comply with the requirements in steps 4 of the procedure.

6.28.2   Sending SMS on Access Channel

6.28.2.1 Definition

18   The R-UIM contains SMS access channel configuration for the ME to use when the ME
19   sends SMS messages.

6.28.2.2 Traceability

21   The ME shall send MO SMS over access channel if the access channel flag in EF$_{SMSCAP}$ is
22   enabled and the message size fits in the access channel. See section 3.4.87 of [1].

6.28.2.3 Initial Conditions

24   Refer to section 5.2 for the common initial conditions.

25   In addition, the following values are used:

26   **EF$_{SMSCAP}$ (SMS Capabilities):**

27   Logically:

28   SMS Retry Period: 60 seconds

29   SMS Retry Interval: 7 seconds

1 SMS Flags:

2   Send On Access: True

3   Send on Traffic: True

4   Send as Standard EMS: True

5 SMS Preferred Service Option: Service Option 6

6 Coding in Hex:

3C	07	07	01

7 **EF_SMS (Short Messages):**

8 Record 1 - Logically (Main parameters only):

9 Status: MS originating message; message to be sent, Message
10 protection disabled

11 MSG_LEN: 36 bytes

12 SMS Transport Layer Message:

13   SMS_MSG_TYPE: SMS Point-to-Point

14   Destination Address: +0123456789

15   Message Type: SMS-Submit

16   User Data: "Access"

17 Coding in Hex:

07	24	00	00	02	10	02	04	07	02	A8	48	D1	59	E2	40
08	14	00	03	20	00	00	01	07	10	34	1C	78	F2	F3	E6
07	01	05	08	01	80	00	..	..	00						

18 All other records are empty.

19 The NS is configured so that it will accept MO SMS over access channel.

6.28.2.4 Procedure

21 1. Power on the ME.

22 2. Wait until the ME has initialized.

23 3. Verify that the ME reads EF_SMSCAP.

24 4. Send the SMS message stored on the R-UIM.

25 5. Verify that the NS receives an SMS with character string "Access" over the access
26 channel.

27 6. Power down the ME.

6.28.2.5 Minimum Standard

29 The ME shall comply with the requirements in steps 3 and 5 of the procedure.

6.28.3 Sending SMS on Traffic Channel

6.28.3.1 Definition

The R-UIM contains SMS traffic channel configuration for the ME to use when sending MO SMS messages.

6.28.3.2 Traceability

The ME shall support MO SMS over traffic channel based on the SMS traffic channel configuration in EF_{SMSCAP} of the R-UIM. See section 3.4.87 of [1].

6.28.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the following values are used:

Initial Conditions A:

EF$_{SMSCAP}$ (SMS Capabilities):

Logically:

SMS Retry Period:	60 seconds
SMS Retry Interval:	6 seconds
SMS Flags:	
Send On Access:	False
Send on Traffic:	True
Send as Standard EMS:	True
SMS Preferred Service Option:	Service Option 6

Coding in Hex:

3C	06	06	01

EF$_{SMS}$ (Short Messages):

Record 1 - Logically (Main parameters only):

Status:	MS originating message; message to be sent, Message protection disabled
MSG_LEN:	33 bytes
SMS Transport Layer Message:	
SMS_MSG_TYPE:	SMS Point-to-Point
Destination Address:	+0123456789
Message Type:	SMS-Submit
User Data:	"T6"

1 Coding in Hex:

07	21	00	00	02	10	02	04	07	02	A8	48	D1	59	E2	40
08	11	00	03	20	00	00	01	04	10	15	46	C0	07	01	05
08	01	80	00	..	..	00

2 All other records are empty.

3 The NS is configured so that it will accept traffic channel requests with SO 6 and SO 14.

4 Initial Conditions B:

5 **EF$_{SMSCAP}$ (SMS Capabilities):**

6 Logically:

7   SMS Retry Period: 60 seconds

8   SMS Retry Interval: 6 seconds

9   SMS Flags:

10   Send On Access: False

11   Send on Traffic: True

12   Send as Standard EMS: True

13   SMS Preferred Service Option: Service Option 14

14 Coding in Hex:

3C	06	06	02

15 **EF$_{SMS}$ (Short Messages):**

16 Record 1 - Logically (Main parameters only):

17   Status: MS originating message; message to be sent, Message
18   protection disabled

19   MSG_LEN: 34 bytes

20   SMS Transport Layer Message:

21   SMS_MSG_TYPE: SMS Point-to-Point

22   Destination Address: +0123456789

23   Message Type: SMS-Submit

24   User Data: "T14"

25 Coding in Hex:

07	22	00	00	02	10	02	04	07	02	A8	48	D1	59	E2	40
08	12	00	03	20	00	00	01	05	10	1D	46	2D	00	07	01
05	08	01	80	00	..	..	00

26 All other records shall be empty.

6.28.3.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

1. Power on the ME.

2. Wait until the ME has initialized.

3. Send the SMS message stored on the R-UIM.

4. Perform the following for different initial conditions:

   A. Verify that the NS receives an SMS with the character string "T6" over traffic channel with SO 6.

   B. Verify that the NS receives an SMS with the character string "T14" over traffic channel with SO 14.

5. Power down the ME.

6.28.3.5 Minimum Standard

The ME shall comply with the requirements in step 4 of the procedure.

6.28.4 Sending EMS messages

This test is only applicable to an ME supporting the SMS and EMS features.

6.28.4.1 Definition

The R-UIM contains EMS configuration for the ME to use when sending MO EMS messages.

6.28.4.2 Traceability

The ME shall be capable of sending EMS messages per configuration in EF_{SMSCAP} of the R-UIM. See section 3.4.87 of [1].

6.28.4.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, the file EF_{SMSCAP} is configured as follows:

EF_{SMSCAP} (SMS Capabilities):

Logically:

SMS Retry Period:	60 seconds
SMS Retry Interval:	6 seconds
SMS Flags:	
Send On Access:	True
Send on Traffic:	True

1   Send as Standard EMS: True

2   SMS Preferred Service Option: Service Option 6

3 Coding in Hex:

3C	06	07	01

4 The NS is configured so that it will accept EMS messages from the ME.

5 <u>Initial Conditions B:</u>

6 In addition, the file EF$_{SMSCAP}$ is configured as follows:

7 **EF$_{SMSCAP}$ (SMS Capabilities):**

8 Logically:

9   SMS Retry Period: 60 seconds

10   SMS Retry Interval: 6 seconds

11   SMS Flags:

12   Send On Access: True

13   Send on Traffic: True

14   Send as Standard EMS: False

15   SMS Preferred Service Option: Service Option 06

16 Coding in Hex:

3C	06	03	01

17 The NS is configured so that it will not accept EMS messages from the ME.

6.28.4.4 Procedure

19 This procedure shall be performed for each set of Initial Conditions.

20   1.   Power on the ME.

21   2.   Send a long SMS message which is longer than 160 bytes from the ME.

22   3.   Perform the following for different initial conditions:

23   A.   Verify that the NS receives long SMS segments using the standard EMS
24   (enabled in EF$_{SMSCAP}$ of the R-UIM).

25   B.   Verify that the NS does not receive long SMS segments using the standard EMS
26   (disabled in EF$_{SMSCAP}$ of the R-UIM).

27   4.   Power down the ME.

6.28.4.5 Minimum Standard

29 The ME shall comply with the requirements in step 3 of the procedure.

30

6.29 SMS Messages on R-UIM

The tests in this section are only applicable to an ME supporting the SMS feature.

If the ME supports both automatic storing and manual storing of SMS on the R-UIM, either test case 6.29.1 or 6.29.2 can be executed for verifying that the ME is capable of writing SMS messages to the R-UIM.

6.29.1 Automatically Storing Received SMS in R-UIM

6.29.1.1 Definition

The R-UIM provides storage space for the ~~mobile station~~MS to store received SMS messages on the R-UIM.

6.29.1.2 Traceability

The ME shall be capable of automatically storing SMS messages received from the network into EF_{SMS} in the R-UIM. See 3.4.27 section of [1].

6.29.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions. In addition, EF_{SMS} is empty. The NS is configured with the following SMS to be sent to the ME:

SMS_MSG_LEN:	103
SMS_MSG_TYPE:	SMS Point-to-Point
Teleservice Identifier:	CDMA Cellular Messaging Teleservice [CMT-95]
Service Category:	Unknown or unspecified
Originating Address:	+0123456789
Bearer Reply Option:	Reply Seq 0
Bearer Data:	
Message Identifier:	Deliver
MESSAGE_ID:	0
Message Center Time Stamp:	2010/01/01, 12:00:00am
Validity Period (Absolute):	2020/01/01, 12:00:00am
Priority:	Normal
Privacy:	Restricted
Number of Messages:	0
Language Indicator:	English
User Data:	
MSG_ENCODING:	7-bit ASCII
User Data:	"This message shall be stored on the R-UIM."

6.29.1.4 Procedure

1. Power on the ME.

2. Send the SMS message from the NS to the ME.

3. Wait until the ME has received the SMS.

4. Verify that EF_{SMS} contains one record with an unread SMS.

5. Use a UI dependent procedure to select the SMS and display it.

6. Verify that the ME displays the text "This message shall be stored on the R-UIM." from originating address "+0123456789".

7. Power down the ME.

6.29.1.5 Minimum Standard

The ME shall comply with the requirements in step 4 and 6 of the procedure.

6.29.2 Saving SMS in R-UIM

6.29.2.1 Definition

The R-UIM provides storage space for the ~~mobile station~~MS to save SMS messages on the R-UIM.

6.29.2.2 Traceability

The ME shall be capable of saving SMS messages into EF_{SMS} in the R-UIM. See 3.4.27 section of [1].

6.29.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, EF_{SMS} is empty.

The NS is configured with the SMS defined in 6.28.1.4. This SMS is to be sent to the ME.

6.29.2.4 Procedure

1. Power on the ME.

2. Send the SMS message from the NS to the ME.

3. Wait until the ME has received the SMS.

4. Verify that EF_{SMS} contains one record with an unread SMS.

5. Use a UI dependent procedure to copy the received message from the ME to the CS.

6. Use a UI dependent procedure to display the message saved in the CS.

7. Verify that the ME displays the text "This message shall be stored on the R-UIM." from originating address "+0123456789".

1   8.   Power down the ME.

6.29.2.5 Minimum Standard

The ME shall comply with the requirements in steps 4 and 7 of the procedure.

6.29.3 Reading SMS from R-UIM

6.29.3.1 Definition

The R-UIM provides storage space for the ME to store SMS messages. The ME shall be capable of allowing the user to read the SMS messages stored in the R-UIM.

6.29.3.2 Traceability

The ME shall be capable of allowing the user to read all SMS messages stored in EF_{SMS} from the R-UIM. See 3.4.27 section of [1].

6.29.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, EF_{SMS} contains the following record:

Status:	Message received by ME from network, message to be read, message protection disabled
MS_MSG_LEN:	103
MS_MSG_TYPE:	SMS Point-to-Point
PARAMETER_ID:	Teleservice Identifier
Teleservice:	CDMA Cellular Messaging Teleservice [CMT-95]
Service Category:	Unknown or unspecified
Originating Address:	+0123456789
Bearer Reply Option:	Reply Seq: 0
Bearer data:	
MESSAGE_TYPE:	Deliver
MESSAGE_ID:	0
Message Center Time Stamp:	2010/01/01, 12:00:00 am
Validity Period- Absolute:	2020/01/01, 12:00:00 am
Priority:	Normal
Privacy:	Restricted
Number of Messages:	0
Language Indicator:	English
User Data:	
MSG_ENCODING:	7-bit ASCII

1   User-Data: "This message shall be read from the R-UIM."

2   Coding in Hex:

03	67	00	00	02	10	02	01	02	00	00	02	0D	88	85	18
18	99	19	9A	1A	9B	1B	9C	1C	80	06	01	00	08	4A	00
03	10	00	00	01	27	11	55	4D	1A	79	A0	DB	97	9F	3C
39	F2	A0	E7	A3	0E	CD	88	31	65	41	CB	2E	1C	88	33
72	DF	B5	07	4D	19	50	52	5B	56	4C	D5	C0	03	06	10
01	01	00	00	00	04	06	20	01	01	00	00	00	08	01	00
09	01	40	0B	01	00	0D	01	01	00	00	..	00			

6.29.3.4 Procedure

4   1. Power on the ME.

5   2. Use UI dependent procedure to read the stored message from the R-UIM.

6   3. Verify that the ME displays the text message "This message shall be read from the
7   R-UIM."

8   4. Read the SMS messages.

9   5. Power down the ME.

6.29.3.5 Minimum Standard

11   The ME shall comply with the requirements in step 3 of the procedure.

6.29.4   Deleting SMS in R-UIM

6.29.4.1 Definition

14   The R-UIM provides storage space for the ~~mobile station~~MS to store SMS messages on the
15   R-UIM. The ME shall be capable of allowing the user to delete the SMS messages stored in
16   the R-UIM.

6.29.4.2 Traceability

18   The ME shall be capable of allowing the user to delete selected SMS messages stored in
19   EF_{SMS} in the R-UIM. See 3.4.27 section of [1].

6.29.4.3 Initial Conditions

21   Refer to section 5.2 for the common initial conditions.

22   In addition, EF_{SMS} contains the following record 1:

23   Status: Message received by ME from network, message read,
24   message protection disabled

25   MS_MSG_LEN: 105

26   MS_MSG_TYPE: SMS Point-to-Point

1	PARAMETER_ID:	Teleservice Identifier
2	Teleservice:	CDMA Cellular Messaging Teleservice [CMT-95]
3	Service Category:	Unknown or unspecified
4	Originating Address:	+0123456789
5	Bearer Reply Option:	Reply Seq: 0
6	Bearer data:	
7	MESSAGE_TYPE:	Deliver
8	MESSAGE_ID:	0
9	Message Center Time Stamp:	2010/01/01, 12:00:00 am
10	Validity Period- Absolute:	2020/01/01, 12:00:00 am
11	Priority:	Normal
12	Privacy:	Restricted
13	Number of Messages:	0
14	Language Indicator:	English
15	User Data:	
16	MSG_ENCODING:	7-bit ASCII
17	User-Data:	"This message shall be deleted from the R-UIM."

18   Coding in Hex:

03	69	00	00	02	10	02	01	02	00	00	02	0D	88	85	18
18	99	19	9A	1A	9B	1B	9C	1C	80	06	01	00	08	4C	00
03	10	00	00	01	29	11	6D	4D	1A	79	A0	DB	97	9F	3C
39	F2	A0	E7	A3	0E	CD	88	31	65	41	93	2E	CC	BD	32
E4	41	9B	96	FD	A8	3A	68	CA	82	92	DA	B2	66	AE	03
06	10	01	01	00	00	00	04	06	20	01	01	00	00	00	08
01	00	09	01	40	0B	01	00	0D	01	01	00	..	00		

6.29.4.4 Procedure

20   1.   Power on the ME.

21   2.   Use UI dependent procedure to select the stored message from the R-UIM.

22   3.   Delete the SMS message with content "This message shall be deleted from the
23   R-UIM."

24   4.   Verify that the first byte of record 1 in EF$_{SMS}$ is '00'.

25   5.   Power down the ME.

6.29.4.5 Minimum Standard

27   The ME shall comply with the requirements in step 4 of the procedure.

6.30 SMS Parameters on R-UIM

The tests in this section are only applicable to an ME supporting the SMS feature.

6.30.1 Saving SMS Parameters in R-UIM

6.30.1.1 Definition

The R-UIM provides storage space for the ~~mobile station~~MS to save SMS parameters on the R-UIM.

6.30.1.2 Traceability

The ME shall be capable of saving SMS parameters into EF_{SMSP} in the R-UIM. See 3.4.28 section of [1].

6.30.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addtion, EF_{SMSP} in the CS does not have any records.

6.30.1.4 Procedure

1. Power on the ME.

2. Go to the menu on the ME to enter new SMS parameters.

3. Create a new record of SMS Parameters with priority set to "low".

4. Save the new SMS parameters into the CS.

5. Verify that the ME allows the user to save new SMS parameters into record 1 in EF_{SMSP}.

6. Verify that the ME sets at least the following Parameter Indicator bits to '1': MSG_ENCODING, Validity Period, Bearer Data.

7. Verify that the ME sets the Priority parameter in the SMS parameters of record 1 to "normal".

8. Power down the ME.

6.30.1.5 Minimum Standard

The ME shall comply with the requirements in steps 5, 6 and 7 of the procedure.

6.30.2 Reading SMS Parameters in R-UIM

6.30.2.1 Definition

The R-UIM provides storage space for the ~~mobile station~~MS to save SMS parameters on the R-UIM.

6.30.2.2 Traceability

The ME shall be capable of allowing the user to read SMS parameters in EF_{SMSP} in the R-UIM. See 3.4.28 section of [1].

6.30.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.30.2.4 Procedure

1. Power on the ME.

2. Open the SMS parameter record on the CS using a UI dependent procedure.

3. Verify that the ME displays the SMS Priority parameter set to "Urgent".

4. Power down the ME.

6.30.2.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.30.3 Deleting SMS Parameters in R-UIM

6.30.3.1 Definition

The R-UIM provides storage space for the ~~mobile station~~ MS to save SMS parameters on the R-UIM.

6.30.3.2 Traceability

The ME shall be capable of allowing the user to delete SMS parameters in EF_{SMSP} in the R-UIM. See 3.4.28 section of [1].

6.30.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.30.3.4 Procedure

1. Power on the ME.

2. Open the SMS Parameter record on the CS using a UI dependent procedure.

3. Delete the SMS Parameter record.

4. Verify that the ME allows the user to delete the record in the CS.

5. Verify that the Parameter Indicators field of record 1 in EF_{SMSP} is 'FF'.

6. Power down the ME.

6.30.3.5 Minimum Standard

The ME shall comply with the requirements in steps 4 and 5 of the procedure.

6.31 SMS Status on R-UIM

This test is only applicable to an ME supporting SMS.

6.31.1 Definition

The R-UIM provides storage space for the ~~mobile station~~MS to record the last used SMS Message ID number on the R-UIM.

6.31.2 Traceability

The ME shall be capable of recording the last used SMS Message ID number into EF_{SMSS} in the R-UIM. See 3.4.29 section of [1].

6.31.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition the MESSAGE_ID in EF_{SMSS} (SMS Status) shall be set to:

~~EF_{SMSS} (SMS Status):~~

   MESSAGE_ID: 1000

6.31.4 Procedure

   1.   Power on the ME.

   2.   Use a UI dependent procedure to send a message from the ME to the NS.

   3.   Wait until the ME has successfully sent the SMS.

   4.   Verify that the ME sends a message to the network using the Message ID value as stored in R-UIM.

   5.   Verfiy that the Message ID value in EF_{SMSS} is incremented by 1.

   6.   Power down the ME.

6.31.5 Minimum Standard

The ME shall comply with the requirements in step 5 of the procedure.

6.32 Simple IP

The tests in this section are only applicable to an ME supporting the Simple IP feature.

6.32.1 PAP and CHAP Authentication

6.32.1.1 Definition

The R-UIM contains Simple IP PAP and CHAP configurations that the ME shall use to set up PPP sessions.

6.32.1.2 Traceability

The ME shall be capable of setting up data sessions using PAP and CHAP authentication feature in the R-UIM. See sections 3.4.42, 3.4.46, 3.5.1, 4.7, and 4.8.1 of [1].

6.32.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Different to what is defined for EF$_{3GPDOPM}$ in section 5.2 the following setting shall be used:

EF$_{3GPDOPM}$ (3GP Operation Mode):

Logically:

   Operation Mode: Simple IP only

Coding in Hex:

00

Initial Conditions A:

Configure the NS so that it will have the same PAP and CHAP parameters as in the R-UIM and will propose CHAP authentication to the ME when establishing a data session.

Initial Conditions B:

Configure the NS so that it will have the same PAP and CHAP parameters as in the R-UIM and will propose PAP authentication to the ME when establishing a data session.

6.32.1.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

   1.   Power on the ME.

   2.   Wait for the ME to be registered by the NS.

   3.   Set up a data session from the ME using one of applications WAP Browser or MMS.

   4.   Perform the following for different initial conditions:

      A.   Verify that the ME performs CHAP authentication with the NS using the CHAP parameters from the R-UIM.

1 B. Verify that the ME performs PAP authentication with the NS using the PAP
2 parameters from the R-UIM.

3 5. Tear down the data session.

4 6. Power down the ME.

6.32.1.5 Minimum Standard

6 The ME shall comply with the requirements in step 4 of the procedure.

6.32.2 Multiple User Profiles

8 This test is only applicable to an ME that supports the Simple IP feature and also supports
9 MMS, WAP and an application that is not MMS or WAP.

6.32.2.1 Definition

11 The R-UIM contains multiple Simple IP user profiles that the ME shall use to set up data
12 sessions with a profile that is associated with a particular application.

6.32.2.2 Traceability

14 The ME shall be capable of setting up data sessions using the correct Simple IP user
15 profiles based on what applications are requesting the data sessions. See sections 3.4.42,
16 3.4.46, 3.4.89 and 3.5.1 of [1].

6.32.2.3 Initial Conditions

18 Refer to section 5.2 for the common initial conditions.

19 In addition, the files EF_{SIPUPP}, $EF_{3GPDUPPExt}$, $EF_{SIPPAPSS}$ and Simple IP CHAP SS shall be
20 configured as follows:

21 **EF_{SIPUPP} (Simple IP User Profile Parameters)**

22 Logically:

23 NAI Entry Index: 0

24 NAI: "abc0@xyz.com"

25 Authentication Algorithm: PPP CHAP to PAP fallback

26 NAI Entry Index: 1

27 NAI: "abc1@xyz.com"

28 Authentication Algorithm: PPP CHAP to PAP fallback

29 NAI Entry Index: 2

30 NAI: "abc2@xyz.com"

31 Authentication Algorithm: PPP CHAP to PAP fallback

6-58

Coding in Hex:

2B	30	0C	61	62	63	30	40	78	79	7A	2E	63	6F	6D	31
0C	61	62	63	31	40	78	79	7A	2E	63	6F	6D	32	0C	61
62	63	32	40	78	79	7A	2E	63	6F	6D	30				

EF₃GPDUPPExt (3GPD User Profile Parameters Extension)

Logically:

NAI Entry Index:	0
Applications:	Java, Terminal, Reserved for CDG, Unspecified
Priority:	100
Data Rate Mode:	High
Data Bearer:	Hybrid 1xEV-DO/1x
NAI Entry Index:	1
Applications:	MMS
Priority:	80
Data Rate Mode:	High
Data Bearer:	Hybrid 1xEV-DO/1x
NAI Entry Index:	2
Applications:	WAP Browser
Priority:	90
Data Rate Mode:	High
Data Bearer:	Hybrid 1xEV-DO/1x

Coding in Hex:

30	00	00	00	79	64	20	10	00	00	00	25	02	02	00	00
00	04	5A	20												

EF_SIPPAPSS (Simple IP PAP SS)

Logically:

NAI Entry Index:	0
PAP SS:	"PAP SS 0"
NAI Entry Index:	1
PAP SS:	"PAP SS 1"
NAI Entry Index:	2
PAP SS:	"PAP SS 2"

6-59

Coding in Hex:

1C	30	42	82	0A	81	02	9A	99	01	80	A1	41	05	40	81
4D	4C	80	C4	90	A0	82	A0	40	A6	A6	40	64			

Simple IP CHAP SS:

Logically:

NAI Entry Index:	0
CHAP SS:	"CHAP SS 0"
NAI Entry Index:	1
CHAP SS:	"CHAP SS 1"
NAI Entry Index:	2
CHAP SS:	"CHAP SS 2"

6.32.2.4 Procedure

1. Power on the ME.

2. Set up a data session from the ME using the MMS application.

3. Verify that the ME sets up a data session using the user profile in the R-UIM with the MMS application bit turned on.

4. Tear down the data session.

5. Set up a data session from the ME using the WAP Browser application.

6. Verify that the ME sets up a data session using the user profile in the R-UIM with the WAP Browser application bit turned on.

7. Tear down the data session.

8. Set up a data session from the ME using an application that is not MMS or WAP Browser.

9. Verify that the ME sets up a data session using the user profile in the R-UIM with the Unspecified application bit turned on.

10. Tear down the data session.

11. Power down the ME.

6.32.2.5 Minimum Standard

The ME shall comply with the requirements in steps 3, 6 and 9 of the procedure.

6.32.3 Prioritization among User Profiles

This test is only applicable to an ME supporting the Simple IP feature, and additionally MMS and WAP.

6.32.3.1 Definition

The R-UIM contains multiple Simple IP user profiles that the ME shall use to set up data sessions with a profile that is associated with a particular application. When a data session is requested by the second application, the priorities of the profiles for these applications stored in the R-UIM will determine how the second application and its data session are accommodated. The ME shall support MMS, WAP and an application that is not MMS or WAP, and the ME allows the user to start a new data session when an existing data session is in progress.

6.32.3.2 Traceability

When an existing data session is in progress for an application, the ME shall be capable of handling the request of the second application based on the priorities of both applications' user profiles. See sections 3.4.42, 3.4.46, 3.4.89 and 3.5.1 of [1].

6.32.3.3 Initial Conditions

Initial Conditions A:

Refer to section 5.2 for the common initial conditions.

Initial Conditions B:

Refer to section 5.2 for the common initial conditions.

In addition, the files EF_{SIPUPP}, $EF_{3GPDUPPExt}$, $EF_{SIPPAPSS}$ and Simple IP CHAP SS shall be configured as follows:

EF_{SIPUPP} (Simple IP User Profile Parameters)

Logically:

NAI Entry Index:	0
NAI:	"abc0@xyz.com"
Authentication Algorithm:	PPP CHAP to PAP fallback
NAI Entry Index:	1
NAI:	"abc1@xyz.com"
Authentication Algorithm:	PPP CHAP to PAP fallback

Coding in Hex:

1D	20	0C	61	62	63	30	40	78	79	7A	2E	63	6F	6D	31
0C	61	62	63	31	40	78	79	7A	2E	63	6F	6D	30		

$EF_{3GPDUPPExt}$ (3GPD User Profile Parameters Extension)

Logically:

NAI Entry Index:	0
Applications:	MMS
Priority:	100

6-61

1	Data Rate Mode:	High
2	Data Bearer:	Hybrid 1xEV-DO/1x
3	NAI Entry Index:	1
4	Applications:	WAP Browser
5	Priority:	90
6	Data Rate Mode:	High
7	Data Bearer:	Hybrid 1xEV-DO/1x

8 Coding in Hex:

20	00	00	00	02	64	20	10	00	00	00	45	A2	00

9 **EF$_{SIPPAPSS}$ (Simple IP PAP SS)**

10 Logically:

11	NAI Entry Index:	0
12	PAP SS:	"PAP SS 0"
13	NAI Entry Index:	1
14	PAP SS:	"PAP SS 1"

15 Coding in Hex:

14	20	42	82	0A	81	02	9A	99	01	80	A1	41	05	40	81
4D	4C	80	C4	00											

16 **Simple IP CHAP SS:**

17 Logically:

18	NAI Entry Index:	0
19	CHAP SS:	"CHAP SS 0"
20	NAI Entry Index:	1
21	CHAP SS:	"CHAP SS 1"

22 Initial Conditions C:

23 Refer to section 5.2 for the common initial conditions.

24 In addition, the files EF$_{SIPUPP}$, EF$_{3GPDUPPExt}$, EF$_{SIPPAPSS}$ and Simple IP CHAP SS shall be
25 configured as follows:

26 **EF$_{SIPUPP}$ (Simple IP User Profile Parameters)**

27 See EF$_{SIPUPP}$ given in Initial Conditions B

28 ~~NAI Entry Index:~~ ~~0~~

29 ~~NAI:~~ ~~"abc0@xyz.com"~~

30 ~~Authentication Algorithm:~~ ~~PPP CHAP to PAP fallback~~

31 ~~NAI Entry Index:~~ ~~1~~

1   ~~NAI: "abc1@xyz.com"~~

2   ~~Authentication Algorithm: PPP CHAP to PAP fallback~~

3   **EF$_{3GPDUPPExt}$ (3GPD User Profile Parameters Extension)**

4   Logically:

5   NAI Entry Index: 0

6   Applications: MMS

7   Priority: 90

8   Data Rate Mode: High

9   Data Bearer: Hybrid 1xEV-DO/1x

10   NAI Entry Index: 1

11   Applications: WAP Browser

12   Priority: 100

13   Data Rate Mode: High

14   Data Bearer: Hybrid 1xEV-DO/1x

15   Coding in Hex:

20	00	00	00	02	5A	20	10	00	00	00	46	42	00

16   **EF$_{SIPPAPSS}$ (Simple IP PAP SS)**

17   See EF$_{SIPPAPSS}$ given in Initial Conditions B

18   ~~NAI Entry Index: 0~~

19   ~~PAP SS: "PAP SS 0"~~

20   ~~NAI Entry Index: 1~~

21   ~~PAP SS: "PAP SS 1"~~

22   **Simple IP CHAP SS:**

23   See Simple IP CHAP SS given in Initial Conditions B

24   ~~NAI Entry Index: 0~~

25   ~~CHAP SS: "CHAP SS 0"~~

26   ~~NAI Entry Index: 1~~

27   ~~CHAP SS: "CHAP SS 1"~~

28   ## 6.32.3.4 Procedure

29   This procedure shall be performed for each set of Initial Conditions.

30   1.   Power on the ME.

31   2.   Set up a data session from the ME using the WAP Browser application.

32   3.   Wait until the data session is connected.

33   4.   Set up a data session from the ME using the MMS application.

1   5.   Perform the following for different initial conditions:

2   A.   Verify that the ME launches the MMS application by sharing the current data
3   connection.

4   B.   Verify that the ME rejects the MMS application and that the ME continues the
5   current data connection for WAP Browser.

6   C.   Verify that the ME disconnects the current data connection for WAP Browser
7   and established a new data connection for MMS.

8   6.   Power down the ME.

6.32.3.5 Minimum Standard

10   The ME shall comply with the requirements in step 5 of the procedure.

11

6.33 Mobile IP

The tests in this section are only applicable to an ME supporting the Mobile IP feature.

6.33.1 Mobile IP Registration Retries

6.33.1.1 Definition

The R-UIM contains the Mobile IP Registration Max Retries value MAX_NUM_RETRY and the First Retry Timeout value FIRST_RETRY_TIMEOUT that the ME shall use to perform Mobile IP registrations.

6.33.1.2 Traceability

The ME shall be capable of making the number of Mobile IP registration retries based on the Max Retries value and the First Retry Timeout value stored in the R-UIM. See section 3.4.43 of [1] and 3.5.8.6 of [18].

6.33.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured to support Mobile IP and not to respond to Mobile IP registration requests from the ME.

6.33.1.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify the following:

   - That the ME sends Mobile IP registration after receiving home agent advertisement from the NS.

   - That the ME sends a first Mobile IP registration retry after the time period indicated by the First Retry Timeout value provisioned in the CS has passed.

   - That the ME sends a second Mobile IP registration retry after the time period indicated by the First Retry Timeout value provisioned in the CS has passed.

   - That the ME releases the data call after having performed the maximum number of Mobile IP registration retries defined by the Max Retries value provisioned in the CS.

4. Power down the ME.

6.33.1.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.33.2 Mobile IP Re-registration Threshold

6.33.2.1 Definition

The R-UIM contains the Mobile IP Re-registration Threshold value REREG_THRESHOLD that the ME shall use to perform Mobile IP re-registrations.

6.33.2.2 Traceability

The ME shall be capable of performing Mobile IP re-registration after the time period has passed as indicated in the Mobile IP Re-Registration Threshold value stored in the R-UIM. See section 3.4.43 of [1] and 3.5.8.6 of [18].

6.33.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured such that it supports Mobile IP and the Mobile IP registration lifetime value of the home agent is greater than re-registration threshold provisioned in the CS.

6.33.2.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify the following:

   - That the ME sends Mobile IP registration after receiving foreign agent advertisement from the NS.

   - That the ME completes the registration successfully.

4. Wait for at least the time of the Re-registration Threshold.

5. Verify that the ME sends Mobile IP re-registration after the time period indicated by the Re-registration Threshold has passed and before the Registration Lifetime is reached.

6. Power down the ME.

6.33.2.5 Minimum Standard

The ME shall comply with the requirements in steps 3 and 5 of the procedure.

6.33.3 Mobile IP to Simple IP Fallback

This test is only applicable to an ME supporting both the Simple IP and the Mobile IP features.

6.33.3.1 Definition

The R-UIM contains the 3GPD Operation Mode parameter that allows the ~~mobile station~~MS to perform Mobile IP to Simple IP fallback.

6.33.3.2 Traceability

The ME shall be capable of performing Mobile IP to Simple IP fallback as provisioned in the R-UIM. See section 3.4.39 of [1] and 3.5.8.2 of [18].

6.33.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions. The NS is configured to reject a Mobile IP data call and accept a Simple IP data call.

6.33.3.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify that the ME tries to set up a data session using Mobile IP.

4. Verify that the ME falls back to Simple IP upon network rejection and successfully set up a Simple IP data session.

5. Power down the ME.

6.33.3.5 Minimum Standard

The ME shall comply with the requirements in steps 3 and 4 of the procedure.

6.33.4   Mobile IP MN-HA 2002bis Authentication

6.33.4.1 Definition

The R-UIM contains the Mobile IP configuration regarding the use of Mobile IP 2002bis MN-HA Authentication.

6.33.4.2 Traceability

The ME shall be capable of performing Mobile IP MN-HA authentication per the 2002bis configuration on the R-UIM. See section 3.4.88 of [1].

6.33.4.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the file $EF_{MIPFlags}$ is set as follows:

$EF_{MIPFlags}$ (Mobile IP Flags):

Logically:

Mobile IP 2002bis MN HA Authentication: True

Mobile IP Pre Rev 6 handoff optimization: False

Mobile IP PPP Re-sync during hand-down from 1xEV-DO Rev 0 to 1x: False

Mobile IP Re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime: False

Coding in Hex:

01

The NS is configured to support Mobile IP with MN-HA 2002bis authentication.

6.33.4.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify that the ME successfully completes Mobile IP registration with the NS using the 2002bis authentication.

4. Power down the ME.

6.33.4.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.33.5 Mobile IP Pre Rev 6 Handoff Optimization

6.33.5.1 Definition

The R-UIM contains the Mobile IP configuration regarding Mobile IP Pre Rev 6 handoff optimization.

6.33.5.2 Traceability

The ME shall be capable of performing Mobile IP Pre Rev 6 handoff optimization per configuration on the R-UIM. See section 3.4.88 of [1].

6.33.5.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the file $EF_{MIPFlags}$ is set as follows:

$EF_{MIPFlags}$ (Mobile IP Flags):

Logically:

Mobile IP 2002bis MN HA Authentication: False

Mobile IP Pre Rev 6 handoff optimization: True

Mobile IP PPP Re-sync during hand-down from 1xEV-DO Rev 0 to 1x: False

Mobile IP Re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime: False

Coding in Hex:

02

The NS is configured to support Mobile IP with Pre Rev 6 handoff optimization enabled.

6.33.5.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify that the ME successfully completes Mobile IP registration with the NS.

4. Wait for the ME to go into dormancy.

5. While the ME is still in dormancy, trigger the NS to make the ME to move from the current BSC to another BSC which is connected to a different PDSN.

6. Verify that the ME initiates PPP re-negotiation with inter-PCF dormant handoff.

7. Verify that the ME successfully performes Mobile IP registration.

8. Power down the ME.

6.33.5.5 Minimum Standard

The ME shall comply with the requirements in steps 3, 6 and 7 of the procedure.

6.33.6 Mobile IP PPP Re-sync during Hand-down from 1xEV-DO Rev 0 to 1x

This test is only applicable to an ME supporting the Mobile IP feature, 1x and 1xEV-DO.

6.33.6.1 Definition

The R-UIM contains the Mobile IP configuration regarding PPP Re-sync during Hand-down from 1xEV-DO Rev 0 to 1x. See section 3.4.88 of [1].

6.33.6.2 Traceability

The ME shall be capable of performing Mobile IP PPP Re-sync during Hand-down from 1xEV-DO Rev 0 to 1x per configuration on the R-UIM.

6.33.6.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the file $EF_{MIPFlags}$ is set as follows:

$EF_{MIPFlags}$ (Mobile IP Flags):

Logically:

Mobile IP 2002bis MN HA Authentication: False

Mobile IP Pre Rev 6 handoff optimization: False

Mobile IP PPP Re-sync during hand-down from 1xEV-DO Rev 0 to 1x: True

Mobile IP Re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime: False

Coding in Hex:

04

The NS is configured to be on 1xEV-DO Rev 0 system in order to support Mobile IP with PPP Re-sync during Hand-down from 1xEV-DO Rev 0 to 1x.

6.33.6.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Wait for the ME to complete Mobile IP registration with the NS on 1xEV-DO Rev 0 system.

4. Trigger the NS to make the ME hand down to 1x system while PPP is in active state.

5. Verify that the ME performes a hand-down to the 1x system and re-synchronized PPP.

6. Power down the ME.

6.33.6.5 Minimum Standard

The ME shall comply with the requirements in step 5 of the procedure.

6.33.7 Mobile IP Re-registration for Extending Mobile IP address lifetime

6.33.7.1 Definition

The R-UIM contains the "Mobile IP re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime" flag that the ME shall use to perform Mobile IP re-registrations.

6.33.7.2 Traceability

The ME shall be capable of performing Mobile IP re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime according to the Mobile IP flags set in $EF_{MIPFlags}$ of the R-UIM. See section 3.4.88 of [1].

6.33.7.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured such that it supports Mobile IP and the Mobile IP registration lifetime value of the home agent is greater than re-registration threshold provisioned in the CS.

In addition, the file $EF_{MIPFlags}$ is set as follows:

EF_{MIPFlags} (Mobile IP Flags):

Logically:

Mobile IP 2002bis MN HA Authentication: False

Mobile IP Pre Rev 6 handoff optimization: False

Mobile IP PPP Re-sync during hand-down from 1xEV-DO Rev 0 to 1x: False

Mobile IP Re-registration only if data has been transferred since last registration in order to extend Mobile IP address lifetime: True

Coding in Hex:

08

6.33.7.4 Procedure

1. Power on the ME.

2. Set up a Mobile IP data call from the ME.

3. Verify that the ME successfully completes the registration.

4. Send data from the ME.

5. Verify that the NS receives the data from the ME.

6. Wait for at least the time of the re-registration threshold.

7. Verify that the ME successfully performes an Mobile IP re-registration.

8. Wait for at least the time of the Mobile IP registration lifetime.

9. Verify that ME does not perform Mobile IP re-registration and the NS disconnected the Mobile IP data session.

10. Power down the ME.

6.33.7.5 Minimum Standard

The ME shall comply with the requirements in steps 3, 5, 7 and 9 of the procedure.

6.34 Data Configurations

6.34.1 Data Dormant Mode Timer

This test is only applicable to an ME supporting either the Simple IP or Mobile IP feature.

6.34.1.1 Definition

The R-UIM contains the data dormant timer configuration that the ME shall use.

6.34.1.2 Traceability

The ME shall be capable of performing data dormancy procedure per configuration in the R-UIM. See section 3.4.93 of [1].

6.34.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.34.1.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME.

3. Verify that the ME goes into the data dormant state after having no data activity for a period equal to the data dormant timer defined in EF_{DGC} plus/minus 10%.

4. Power down the ME.

6.34.1.5 Minimum Standard

The ME shall comply with the requirements in step 4 of the procedure.

6.34.2 Hysteresis Activation Time

This test is only applicable to an ME supporting either the Simple IP or Mobile IP feature.

6.34.2.1 Definition

The R-UIM contains the hysteresis activation time configuration that the ME shall use.

6.34.2.2 Traceability

The ME shall be capable of performing hysteresis activation procedure per configuration in the R-UIM. See section 3.4.93 of [1].

6.34.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.34.2.4 Procedure

1. Power on the ME.

2. Set up a data call from the ME and send some data to the NS.

3. Wait for a period that is 1 second longer than the dormant timer value in the CS so that the ME goes into dormant state.

4. Trigger the NS to make the ME switch to a new packet zone.

5. Wait for a period shorter than the hysteresis activation timer in the CS.

6. Verify that the ME does not add a new packet zone to its packet zone list.

7. Continue to wait so that the total waiting period is equal to the hysteresis activation timer in the CS.

8. Verify that the ME adds a new packet zone to its packet zone list.

9. Power down the ME.

6.34.2.5 Minimum Standard

The ME shall comply with the requirements in steps 6 and 9 of the procedure.

6.34.3 EPZID

6.34.3.1 Definition

The R-UIM contains the EPZID configuration that the ME shall use.

6.34.3.2 Traceability

The ME shall be capable of handling packet zone IDs based on the EPZID configuration in the R-UIM. See section 3.4.93 of [1].

6.34.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, the file EF_{DGC} is configured as follows:

EF_{DGC} (Data Generic Configurations):

Logically:

Data dormant timer:	30 seconds
EPZID Type:	Packet Zone ID plus SID
Hysteresis Activation Time:	30 seconds

Coding in Hex:

1E	01	1E

The NS is configured to allow Simple IP data sessions from the ~~mobile station~~MS.

Initial Conditions B:

In addition, the file EF_{DGC} is configured as follows:

6-73

EF_{DGC} (Data Generic Configurations):

Logically:

    Data dormant timer: 30 seconds

    EPZID Type: Packet Zone ID plus SID and NID

    Hysteresis Activation Time: 30 seconds

Coding in Hex:

1E	02	1E

The NS is configured to allow Simple IP data sessions from the ~~mobile station~~MS.

6.34.3.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

    1.   Power on the ME.

    2.   Set up a data call from the ME and send some data to the NS

    3.   Wait until the data transmission is completed.

    4.   Wait for a period that is longer than the dormant timer value in the CS.

    5.   Trigger the NS in order to make the ME switch to a new packet zone.

    6.   Wait for a period that is longer than the hysteresis activation timer in the CS.

    7.   Perform the following for different initial conditions:

        A.   Verify that the ME adds the new packet zone to its packet zone list using the "Packet Zone ID plus SID" format.

        B.   Verify that the ME adds the new packet zone to its packet zone list using the "Packet Zone ID plus SID and NID" format.

    8.   Power down the ME.

6.34.3.5 Minimum Standard

The ME shall comply with the requirements in step 7 of the procedure.

6.35 HRPD Access Authentication

This test is only applicable to an ME supporting the HRPD feature.

6.35.1 Definition

The R-UIM contains the HRPD access authentication parameters that the ME shall use.

6.35.2 Traceability

The ME shall be capable of performing HRPD access authentication using the parameters stored in the R-UIM. See sections 3.4.53, 3.5.3 and 4.7.4 of [1].

6.35.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured to stay in HRPD system and to have the same HRPD parameters as on the R-UIM.

6.35.4 Procedure

1. Power on the ME.

2. Set up a data session.

3. Verify that the ME successfully completes the HRPD access authentication with the NS and that the ME successfully set up the data session.

4. Power down the ME.

6.35.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.36 WAP Browser Connectivity Parameters

This test is only applicable to an ME supporting the WAP Browser feature.

6.36.1 Definition

The R-UIM contains WAP Browser Connectivity Parameters that the ME shall use to set up browsing sessions. The R-UIM also contains the bookmarks that the ME can use to connect to those websites.

6.36.2 Traceability

The ME shall be capable of setting up browsing sessions using the WAP Browser connectivity parameters in the R-UIM. The ME shall be capable of connecting to the websites stored in the R-UIM. See section 3.4.94 of [1].

6.36.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, the NS is configured to provide access to the web servers defined in $EF_{WAPBrowserBM}$ through the gateway server defined in $EF_{WAPBrowserCP}$.

Initial Conditions B:

In addition, Gateway and HomeURL in $EF_{WAPBrowserCP}$ shall be set to~~is configured as follows~~:

~~$EF_{WAPBrowserCP}$ **(WAP Browser Connectivity Parameters)**~~

    Gateway: http://gateway.test2.invalid

    HomeURL: http://www.test2.invalid

The NS is configured to provide access to the web servers defined in $EF_{WAPBrowserBM}$ through a gateway server http://gateway.test2.invalid.

6.36.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

1. Power on the ME.

2. Set up a WAP browsing session from the ME.

3. Verify the that the ME uses the WAP gateway provisioned in the CS.

4. Verity that the ME uses the HomeURL provisioned in the CS for the browsing session.

5. Tear down the browsing session.

6. Power down the ME.

1   ## 6.36.5 Minimum Standard

2   The ME shall comply with the requirements in steps 3 and 4 of the procedure.

3

6.37 WAP Browser Bookmarks

This test is only applicable to an ME supporting the WAP Browser feature.

6.37.1 Definition

The R-UIM contains WAP Browser bookmarks that the ME shall allow the user to read and update even if the WAP Browser connectivity parameters are not available on the R-UIM.

6.37.2 Traceability

The ME shall be capable of allowing the user to read and update bookmarks in the R-UIM in case the R-UIM does not contain the WAP Browser connectivity parameters. See section 3.4.95 of [1].

6.37.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

The NS is configured to provide access to the web servers defined in $EF_{WAPBrowserBM}$ through the gateway server provisioned in $EF_{WAPBrowserCP}$.

6.37.4 Procedure

1. Power on the ME.

2. Switch to the menu display of the ME to the list of bookmarks stored on the CS.

3. Verify that the ME displays the available bookmarks as provisioned in the CS.

4. Change bookmark "Test 1 Bookmark 1 Homepage" - http://test1.bookmark1.invalid to "Test 1 Modified Bookmark 1 Homepage" - http://test1.modifiedbookmark1.invalid and save it.

5. Verify that the ME displays the modified bookmark in the UI and shall have stored the modified bookmark in file $EF_{WAPBrowserBM}$ of the CS.

6. Delete existing bookmark "Test 1 Bookmark 3 Homepage" - http://test1.bookmark3.invalid using a UI dependent procedure.

7. Verify that the ME no longer displays the bookmark in the UI and shall have deleted the bookmark from file $EF_{WAPBrowserBM}$ of the CS.

8. Add a new bookmark "Test 1 Bookmark 4 Homepage" - http://test1.bookmark4.invalid using a UI dependent procedure.

9. Verify that the ME displays the added bookmark in the UI and shall have added the bookmark to file $EF_{WAPBrowserBM}$ of the CS.

10. Use the newly added bookmark "Test 1 Bookmark 4 Homepage" to connect to the NS.

11. Verify that the ME connects to the CS using bookmark "Test 1 Bookmark 4 Homepage".

1   12. Power down the ME.

6.37.5 Minimum Standard

3   The ME shall comply with the requirements in steps 3, 5, 7, 9 and 11 of the procedure.

4

6.38 MMS Issuer Connectivity Parameters

This test is only applicable to an ME supporting the MMS feature.

6.38.1 Definition

The R-UIM contains MMS Issuer Connectivity Parameters that the ME shall use to connect to the MMS server.

6.38.2 Traceability

The ME shall be capable of connecting to the MMS server using the MMS Issuer Connectivity Parameters stored in the R-UIM. The gateway address can be a domain name or an IP address. See section 3.4.69 of [1].

6.38.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

<u>Initial Conditions A:</u>

In addition, the NS is configured to provide access to the MMS server defined in EF_{MMSICP} of the CS.

<u>Initial Conditions B:</u>

In addition, file EF_{MMSICP} is configured as follows:

EF_{MMSICP} (MMS Issuer Connectivity Parameters)

<u>Logically:</u>

MMS Implementation Information:	WAP
MMS Relay/Server Address:	"http://mms-operator1.invalid"
Gateway Information:	
Address FQDN:	"gateway.test1.invalid"
Port:	"9201"
Service:	"CO-WSP", WAP session service
Authentication type:	"HTTP BASIC"
Authentication id:	"gateway_user1"
Authentication pw:	"gateway_password1"

Coding in Hex:

AB	68	80	01	01	81	1C	68	74	74	70	3A	2F	2F	6D	D6
73	2D	6F	70	65	72	61	74	6F	72	31	2E	69	6E	76	61
6C	69	64	83	45	20	67	61	74	65	77	61	79	2E	74	65
73	74	31	2E	69	6E	76	61	6C	69	64	00	21	85	23	39
32	30	31	00	24	CB	19	9C	1A	67	61	74	65	77	61	79
5F	75	73	65	72	31	00	1B	67	61	74	65	77	61	79	5F
70	61	73	73	77	6F	72	64	31	00	FF	...	FF			

The NS is configured to provide access to the MMS server defined in EF_{MMSISP} of the CS.

6.38.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

1. Power on the ME.

2. Send an MMS message from the ME.

3. Perform the following for different initial conditions:

   A. Verify that the ME connects to the MMS server using the MMS Relay/Server address and the WAP Gateway address stored on the R-UIM.

   B. Verify that the ME connects to the MMS server using the MMS Relay/Server address and the WAP Gateway address stored on the R-UIM.

4. Power down the ME.

6.38.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

6.39 MMS Configurations

The tests in this section are only applicable to an ME supporting the MMS feature.

6.39.1 Maximum Message Size

6.39.1.1 Definition

The R-UIM contains MMS Maximum Message Size value that the ME shall use when sending MMS messages.

6.39.1.2 Traceability

The ME shall be capable of sending MMS messages not longer than the maximum message size value in $EF_{MMSConfig}$ of the R-UIM. See section 3.4.96 of [1].

6.39.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, $EF_{MMSConfig}$ ~~on the CS~~ is configured ~~with the following parameter values~~ as follows:

$EF_{MMSConfig}$ (MMS Configuration):

Logically:

Max Message Size Value:	6000 bytes
Retry Times Value:	3
Retry Interval Value:	20 seconds
MMSC Timeout Value:	30 seconds

Coding in Hex:

00	00	17	70	03	14	00	1E

The NS is configured to provide access to the MMS server defined in EF_{MMSICP} of the CS.

The following message is going to be sent from the ME:

X-Mms-Message-Type:	m-send-req
To:	"+0123456789"
Subject:	"Send MMS"
X-Mms-Priority:	Normal
Content-Type:	text/plain (0x03)
	"To be sent successfully"

Initial Conditions B:

In addition, $EF_{MMSConfig}$ on the CS is configured with the following parameter values:

1 **EF_{MMSConfig} (MMS Configuration):**

2 <u>Logically:</u>

3   Max Message Size Value: 10 bytes

4   Retry Times Value: 3

5   Retry Interval Value: 20 seconds

6   MMSC Timeout Value: 30 seconds

7 The NS is configured to provide access to the MMS server defined in EF_{MMSICP} of the CS.

8 The following message is going to be sent from the ME:

9   X-Mms-Message-Type: m-send-req

10   To: "+0123456789"

11   Subject: "Send MMS"

12   X-Mms-Message-Class: Personal

13   X-Mms-Priority: Normal

14   Content-Type: text/plain (0x03)

15   "Message too large"

16 6.39.1.4 Procedure

17 This procedure shall be performed for each set of Initial Conditions.

18   1.   Power on the ME.

19   2.   Send the message from the ME to the NS.

20   3.   Perform the following for different initial conditions:

21   A.   Verify that the ME successfully sends the message to the NS.

22   B.   Verify that the ME does not send the message to the NS.

23   4.   Power down the ME.

24 6.39.1.5 Minimum Standard

25 The ME shall comply with the requirements in step 3 of the procedure.

26 6.39.2 MMS Retries

27 6.39.2.1 Definition

28 The R-UIM contains Retry Times value and the Retry Interval value that the ME shall use
29 when sending MMS messages.

6.39.2.2 Traceability

The ME shall be capable of using the Retry Times value and the Retry Interval value from $EF_{MMSConfig}$ of the R-UIM when the ME retries to send MMS messages. See section 3.4.96 of [1].

6.39.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured so that the MMS Relay/Server will immediately respond with an M-Send.conf PDU (with Status "Error-transient-failure") to MMS messages from the ME.

6.39.2.4 Procedure

1. Power on the ME.

2. Send an MMS message from the ME.

3. Wait for 90 seconds.

4. Verify that the ME retries to send the MMS message exactly 3 times to the NS.

5. Verify that the ME waits for 20 to 22 seconds each time before it retries the message.

6. Power down the ME.

6.39.2.5 Minimum Standard

The ME shall comply with the requirements in step 4 and 5 of the procedure.

6.39.3 MMSC Timeout

6.39.3.1 Definition

The R-UIM contains the MMSC Timeout value that the ME shall use when sending MMS messages.

6.39.3.2 Traceability

The ME shall be capable of declaring an MMSC timeout after having waited for the number of seconds defined by the MMSC Timeout value in $EF_{MMSConfig}$ of the R-UIM. See section 3.4.96 of [1].

6.39.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured so that the MMS Relay/Server will not respond to MMS messages from the MS.

6.39.3.4 Procedure

1. Power on the ME.

2. Send an MMS message from the ME.

3. Wait for 210 seconds.

4. Verify that the ME retries to send the MMS message exactly 3 times to the network.

5. Verify that the ME waits for 50 to 52 seconds each time before it retries the message.

6. Power down the ME.

6.39.3.5 Minimum Standard

The ME shall comply with the requirements in steps 4 and 5 of the procedure.

6.40 MMS Notifications

The tests in this section are only applicable to an ME supporting the MMS feature.

6.40.1 Reading and Using MMS Notification in R-UIM

6.40.1.1 Definition

The R-UIM provides space for storing MMS Notifications.

6.40.1.2 Traceability

The ME shall be capable of reading and using the MMS Notifications in EF_{MMSN} of the R-UIM. See section 3.4.67 of [1].

6.40.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, EF_{MMSN} contains the following MMS notification in record 1:

MMS Status:	'00000001' (Notification not read, Notification not retrieved)
MMS Implementation:	WAP implementation of MMS
X-Mms-Message-Type:	m-notification-ind
X-Mms-Transaction-ID:	"12345678"
X-Mms-MMS-Version:	1.2
From:	"+0123456789"
Subject:	"MMS to be retrieved"
X-Mms-Message-Class:	Personal
X-Mms-Priority:	Normal
X-Mms-Message-Size:	44 bytes
X-Mms-Expiry:	10 days
X-Mms-Content-Location:	http://test.invalid/mmsc/test1.mms

The NS is configured to respond to the MMS Retrieval request from the ME using the following MMS message:

X-Mms-Message-Type:	m-retrieve-conf
X-Mms-Transaction-ID:	"12345678"
X-Mms-MMS-Version:	1.2
Message-ID:	<12345678@test.invalid>
Date:	2010/01/01, 12:00:00am
From:	"+0123456789"
To:	"+9876543210/TYPE=PLMN"

1	Subject:	"MMS to be retrieved"
2	X-Mms-Message-Class:	Personal
3	X-Mms-Priority:	Normal
4	Content-Type:	text/plain (0x03)
5		"This is the message that has been retrieved."

6.40.1.4 Procedure

1. Power on the ME.

2. Using the UI of the ME, select the MMS Notification record 1 from the CS and display it.

3. Verify that the fields in MMS Notification record 1 of EF_{MMSN} are displayed, and MMS Status is "Notification read".

4. Verify that Record 1 of EF_{MMSN} on the CS contains MMS Status '00000011' (Notification read, MM not retrieved).

5. Retrieve the MMS message from the NS using the MMS Notification that is being displayed.

6. Verify that the ME successfully retrieves the MMS message using the MMS Notification that is being displayed.

7. Verify that the MMS Status in record 1 of EF_{MMSN} in the CS is '00000111' (Notification read, MM retrieved), or '0000XXX0' (Free space)

8. Power down the ME.

6.40.1.5 Minimum Standard

The ME shall comply with the requirements in steps 3, 4, 6 and 7 of the procedure.

6.40.2 Automatically Storing MMS Notification in R-UIM

This test is only applicable to an ME supporting the MMS feature and automatically storing MMS notifications in R-UIM.

6.40.2.1 Definition

The R-UIM provides space for storing MMS Notifications.

6.40.2.2 Traceability

The ME shall be capable of automatically storing the received MMS Notifications in EF_{MMSN} of the R-UIM. See section 3.4.67 of [1].

6.40.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the ME is configured to automatically store received MMS notifications in CS.

The NS is configured to send MMS notification to the MS with the following fields:

X-Mms-Message-Type:	m-notification-ind
X-Mms-Transaction-ID:	"12345678"
X-Mms-MMS-Version:	1.2
From:	"+0123456789"
Subject:	"MMS to be retrieved"
X-Mms-Message-Class:	Personal
X-Mms-Priority:	Normal
X-Mms-Message-Size:	100 bytes
X-Mms-Expiry:	10 days
X-Mms-Content-Location:	http://test.invalid/mmsc/test1.mms

6.40.2.4 Procedure

1. Power on the ME.

2. Send an MMS Notification from the NS to the MS.

3. Wait until the MS has successfully received the MMS Notification.

4. Verify that EF_{MMSN} in the CS has a record containing MMS Notification fields with the same values as has been sent from the NS.

5. Verify that the MMS Status of the MMS Notification is '00000001' (Notification not read, MM not retrieved).

6. Power down the ME.

6.40.2.5 Minimum Standard

The ME shall comply with the requirements in steps 4 and 5 of the procedure.

6.40.3 Forwarding MMS Notifications

6.40.3.1 Definition

The R-UIM provides space for storing MMS Notifications.

6.40.3.2 Traceability

The ME shall be capable of forwarding the MMS Notifications in EF_{MMSN} of the R-UIM and updating their status on the R-UIM accordingly. See section 3.4.67 of [1].

6.40.3.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured to accept MMS forwarding request from the MS.

EF_{MMSN} contains the following MMS notification in record 1:

MMS Status:	'00000011' (Notification read, MM not retrieved)	
MMS Implementation:	WAP implementation of MMS	
X-Mms-Message-Type:	m-notification-ind	
X-Mms-Transaction-ID:	"12345678"	
X-Mms-MMS-Version:	1.2	
From:	"+0123456789"	
Subject:	"MMS Notification to be forwarded"	
X-Mms-Message-Class:	Personal	
X-Mms-Priority:	Normal	
X-Mms-Message-Size:	100 bytes	
X-Mms-Expiry:	10 days	
X-Mms-Content-Location:	http://test.invalid/mmsc/test1.mms	

6.40.3.4 Procedure

1. Power on the ME.

2. Using the UI of the ME, select the MMS Notification from the CS and display it.

3. Forward the MMS Notification stored in the CS to a recipient using address "To: 4445556666".

4. Wait until the NS accepts the forwarded notification.

5. Verify that MMS Status of record 1 in EF_{MMSN} is '00001111' (Notification read, MM forwarded).

6. Power down the ME.

6.40.3.5 Minimum Standard

The ME shall comply with the requirements in step 5 of the procedure.

6.40.4   Deleting MMS Notification from R-UIM

6.40.4.1 Definition

The R-UIM provides space for storing MMS Notifications.

6.40.4.2 Traceability

The ME shall be capable of deleting the MMS Notifications in EF_{MMSN} of the R-UIM. See section 3.4.67 of [1].

6.40.4.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, EF_{MMSN} contains the following MMS notification in record 1:

1	MMS Status:	'00000011' (Notification read, MM not retrieved)
2	MMS Implementation:	WAP implementation of MMS
3	X-Mms-Message-Type:	m-notification-ind
4	X-Mms-Transaction-ID:	"12345678"
5	X-Mms-MMS-Version:	1.2
6	From:	"+0123456789"
7	Subject:	"MMS Notification to be deleted"
8	X-Mms-Message-Class:	Personal
9	X-Mms-Priority:	Normal
10	X-Mms-Message-Size:	100 bytes
11	X-Mms-Expiry:	10 days
12	X-Mms-Content-Location:	http://test.invalid/mmsc/test1.mms

6.40.4.4 Procedure

1. Power on the ME.

2. Using the UI of the ME, select the MMS Notification from record 1 of EF_{MMSN} in the CS and display it.

3. Delete the MMS Notification from the CS.

4. Verify that the ME does not display the MMS Notification any longer.

5. Verify that MMS Status of record 1 in EF_{MMSN} is '0000XXX0' (Free space).

6. Power down the ME.

6.40.4.5 Minimum Standard

The ME shall comply with the requirements in steps 4 and 5 of the procedure.

6.41 MMS User Preferences

The tests in this section are only applicable to an ME supporting the MMS feature.

6.41.1 Reading and Using MMS User Preferences

6.41.1.1 Definition

The R-UIM contains user preference records for sending MMS. The user shall be able to use these preferences for sending MMS messages.

6.41.1.2 Traceability

The ME shall be capable of providing MMS User Preferences stored in EF_{MMSUP} of the R-UIM to the user. The ME shall provide the user the ability to send MMS using User Preferences stored in the R-UIM. See section 3.4.70 of [1].

6.41.1.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.41.1.4   Procedure

1. Power on the ME.

2. Use a UI dependent procedure to select the MMS User Preferences record 1 on the CS.

3. Verify that the ME displays the User Preference information "Priority" with value "High".

4. Compose and send an MMS message from the ME using record 1 of EF_{MMSUP} without overriding the priority field of the message.

5. Verify that the ME sends an MMS message with priority "High" to the NS.

6. Power down the ME.

6.41.1.5 Minimum Standard

The ME shall comply with the requirements in steps 3 and 5 of the procedure.

6.41.2 Updating MMS User Preferences

6.41.2.1 Definition

The R-UIM contains MMS user preference records for sending MMS. The user shall be able to modify and update these preferences.

6.41.2.2 Traceability

The ME shall be capable of updating MMS User Preferences stored in EF_{MMSUP} of the R-UIM to the user. See section 3.4.70 of [1].

6.41.2.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

6.41.2.4   Procedure

1. Power on the ME.

2. Use a UI dependent procedure to select the MMS User Preferences record 1.

3. Use a UI dependent procedure to set the priority of MMS User Preferences record 1 to "Low" on the CS.

4. Verify that the priority field in record 1 of EF_{MMSUP} on the CS has the value "Low".

5. Power down the ME.

6.41.2.5 Minimum Standard

The ME shall comply with the requirements in step 4 of the procedure.

6.42 Root Certificates

This test is only applicable to an ME supporting the Java and the Root Certificates feature.

6.42.1 Definition

The R-UIM contains the root certificates that the ME shall use for verifying signed applications.

6.42.2 Traceability

The ME shall be capable of verifying the signed Java application that is downloaded from the Java download server using the root certificate store in EF_{RC} in the R-UIM. See section 3.4.86 of [1].

6.42.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

Initial Conditions A:

In addition, the NS is configured to accept HTTP connection and allow the download of Java applications to the ME using the Java download URL as stored in the CS, and sign the Java applications using the same root certificate information as stored in the CS.

The Java application to be downloaded shall display "Hello world!" when it is executed.

Initial Conditions B:

In addition, the NS is configured to accept HTTP connection and allow the download of Java applications to the ME using the Java download URL as stored in the CS, and sign the Java applications using root certificate information different from the root certificate stored in the CS.

The Java application to be downloaded shall display "Hello world!" when it is executed.

6.42.4 Procedure

This procedure shall be performed for each set of Initial Conditions.

1. Power on the ME.

2. Using the UI dependent procedure of the ME, start the Java download program in the ME and perform application download.

3. Start the downloaded Java application.

4. Perform the following for different initial conditions:

    A. Verify that the ME successfully runs the downloaded Java application which displayed "Hello world!"

    B. Verify that ME does not run the downloaded Java application.

5. Power down the ME.

₁ 6.42.5 Minimum Standard

₂ The ME shall comply with the requirements in step 4 of the procedure.

₃

6.43 Java

This test is only applicable to an ME supporting the Java feature.

6.43.1 Definition

The R-UIM contains the Java Download URL that the ME shall use.

6.43.2 Traceability

The ME shall be capable of using the Java Download URL stored in the R-UIM to perform Java application download. See section 3.4.97 of [1].

6.43.3 Initial Conditions

Refer to section 5.2 for the common initial conditions.

In addition, the NS is configured to accept HTTP connection and allow the download of Java applications to the ME using the Java download URL as stored in CS.

6.43.4 Procedure

1. Power on the ME.

2. Using the UI dependent procedure of the ME, connect to the Java download server.

3. Verify that the ME connects to the Java download server successfully using the URL provisioned in EF$_{JDL}$ on the CS.

4. Power down the ME.

6.43.5 Minimum Standard

The ME shall comply with the requirements in step 3 of the procedure.

1 Annex A - [Informative] Applicability Matrix

2 The following table summarizes the applicability of test cases in terms of testing the ME
3 with an R-UIM having a particular C.S0023 revision.

4 "Yes" indicates that a test case applies to that R-UIM revision, and "--" indicates that a test
5 case does not apply to that R-UIM revision.

6 **Table 3. Applicability Matrix of Test Cases for the Different Revisions**

Test Case		C.S0023-0	C.S0023-A	C.S0023-B	C.S0023-C	C.S0023-D
6.1.1	Mobile Station Identifier	Yes	Yes	Yes	Yes	Yes
6.1.2	MS Displaying the Roaming Indicator	Yes	Yes	Yes	Yes	Yes
6.2.1	Removable UIMID Usage Indicator	Yes	Yes	Yes	Yes	Yes
6.2.2	ESN Management	Yes	Yes	Yes	Yes	Yes
6.2.3	MEID Management	--	--	--	Yes	Yes
6.2.4	EUIMID and MEID	--	--	--	Yes	Yes
6.3.1	SSD Update	Yes	Yes	Yes	Yes	Yes
6.3.2	Authentication Calculation for Global Challenge	Yes	Yes	Yes	Yes	Yes
6.3.3	Unique Challenge While the Mobile Station is in Idle State	Yes	Yes	Yes	Yes	Yes
6.3.4	Unique Challenge While the Mobile Station is in Mobile Station Control on the Traffic Channel State	Yes	Yes	Yes	Yes	Yes
6.3.5	Generate Key/VPM	Yes	Yes	Yes	Yes	Yes
6.3.6	Authentication	Yes	Yes	Yes	Yes	Yes
6.5.1	Preferred Roaming List	Yes	Yes	Yes	Yes	Yes
6.5.2	OTASP/OTAPA Commands	Yes	Yes	Yes	Yes	Yes
6.5.3	EPRL Download	--	--	Yes	Yes	Yes
6.11	Exchange Protocol Tests	Yes	Yes	Yes	Yes	Yes
6.12.1	Operating Speed in Authentication Procedure	Yes	Yes	Yes	Yes	Yes
6.12.2	Clock Stop	Yes	Yes	Yes	Yes	Yes
6.13	Mechanical Tests	Yes	Yes	Yes	Yes	Yes

6.14.1	Entry of CHV1	Yes	Yes	Yes	Yes	Yes
6.14.2	Change of CHV1	Yes	Yes	Yes	Yes	Yes
6.14.3	Disabling the CHV1	Yes	Yes	Yes	Yes	Yes
6.14.4	UNBLOCK CHV1 Entry	Yes	Yes	Yes	Yes	Yes
6.14.5	Entry of CHV2	Yes	Yes	Yes	Yes	Yes
6.14.6	Change of CHV2	Yes	Yes	Yes	Yes	Yes
6.14.7	UNBLOCK CHV2 Entry	Yes	Yes	Yes	Yes	Yes
6.15	Abbreviated Dialing Numbers (ADN)	Yes	Yes	Yes	Yes	Yes
6.16	UI Reaction to R-UIM Status Encoding	Yes	Yes	Yes	Yes	Yes
6.17	Electrical Tests	Yes	Yes	Yes	Yes	Yes
6.19	Version Identification	Yes	Yes	Yes	Yes	Yes
6.20	R-UIM Presence Detection	Yes	Yes	Yes	Yes	Yes
6.22	Suggested Slot Cycle Index	Yes	Yes	Yes	Yes	Yes
6.23	Service Provider Name	Yes	Yes	Yes	Yes	Yes
6.24	CDMA Service Table	Yes	Yes	Yes	Yes	Yes
6.25.1	Application Labels Present on R-UIM	--	--	--	--	Yes
6.25.2	Application Labels Not Present on R-UIM	--	--	--	--	Yes
6.26	Device Model Information	--	--	--	--	Yes
6.27	Emergency Numbers	--	--	Yes	Yes	Yes
6.28.1	SMS Retries	--	--	--	--	Yes
6.28.2	Sending SMS on Access Channel	--	--	--	--	Yes
6.28.3	Sending SMS on Traffic Channel	--	--	--	--	Yes
6.28.4	Sending EMS messages	--	--	--	--	Yes
6.29.1	Automatically Storing Received SMS in R-UIM	Yes	Yes	Yes	Yes	Yes
6.29.2	Saving SMS in R-UIM	Yes	Yes	Yes	Yes	Yes
6.29.3	Reading SMS from R-UIM	Yes	Yes	Yes	Yes	Yes
6.29.4	Deleting SMS in R-UIM	Yes	Yes	Yes	Yes	Yes

6.30.1	Saving SMS Parameters in R-UIM	Yes	Yes	Yes	Yes	Yes
6.30.2	Reading SMS Parameters in R-UIM	Yes	Yes	Yes	Yes	Yes
6.30.3	Deleting SMS Parameters in R-UIM	Yes	Yes	Yes	Yes	Yes
6.31	SMS Status on R-UIM	Yes	Yes	Yes	Yes	Yes
6.32.1	PAP and CHAP Authentication	--	Yes	Yes	Yes	Yes
6.32.2	Multiple User Profiles	--	--	--	--	Yes
6.32.3	Prioritization among User Profiles	--	--	--	--	Yes
6.33.1	Mobile IP Registration Retries	--	Yes	Yes	Yes	Yes
6.33.2	Mobile IP Re-registration Threshold	--	Yes	Yes	Yes	Yes
6.33.3	Mobile IP to Simple IP Fallback	--	Yes	Yes	Yes	Yes
6.33.4	Mobile IP MN-HA 2002bis Authentication	--	--	--	--	Yes
6.33.5	Mobile IP Pre Rev 6 Handoff Optimization	--	--	--	--	Yes
6.33.6	Mobile IP PPP Re-sync during Hand-down from 1xEV-DO Rev 0 to 1x	--	--	--	--	Yes
6.33.7	Mobile IP Re-registration for Extending Mobile IP address lifetime	--	--	--	--	Yes
6.34.1	Data Dormant Mode Timer	--	--	--	--	Yes
6.34.2	Hysteresis Activation Time	--	--	--	--	Yes
6.34.3	EPZID	--	--	--	--	Yes
6.35	HRPD Access Authentication	--	--	Yes	Yes	Yes
6.36	WAP Browser Connectivity Parameters	--	--	--	--	Yes
6.37	WAP Browser Bookmarks	--	--	--	--	Yes
6.38	MMS Issuer Connectivity Parameters	--	--	--	Yes	Yes

6.39.1 Maximum Message Size	--	--	--	--	Yes
6.39.2 MMS Retries	--	--	--	--	Yes
6.39.3 MMSC Timeout	--	--	--	--	Yes
6.40.1 Reading and Using MMS Notification in R-UIM	--	--	--	Yes	Yes
6.40.2 Automatically Storing MMS Notification in R-UIM	--	--	--	Yes	Yes
6.40.3 Forwarding MMS Notifications	--	--	--	Yes	Yes
6.40.4 Deleting MMS Notification from R-UIM	--	--	--	Yes	Yes
6.41.1 Reading and Using MMS User Preferences	--	--	--	Yes	Yes
6.41.2 Updating MMS User Preferences	--	--	--	Yes	Yes
6.42 Root Certificates	--	--	--	--	Yes
6.43 Java	--	--	--	--	Yes

1