



## **WiMAX Forum<sup>®</sup> Network Architecture**

Architecture, detailed Protocols and Procedures

WiMAX<sup>®</sup> Over-The-Air Provisioning & Activation Protocol  
based on OMA DM Specifications

**WMF-T33-104-R015v03**

WiMAX Forum<sup>®</sup> Approved  
(2010-11-30)

**WiMAX Forum Proprietary**

Copyright © 2010 WiMAX Forum. All Rights Reserved.

1 **Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability**

2  
3 Copyright 2010 WiMAX Forum. All rights reserved.

4  
5 The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for  
6 download from the WiMAX Forum and may be duplicated for internal use, provided that all copies contain all proprietary notices  
7 and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or  
8 distributed without the express written authorization of the WiMAX Forum.  
9

10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance  
11 of the following terms and conditions:  
12

13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**  
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND**  
15 **STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**  
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**  
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**  
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**  
19

20 Any products or services provided using technology described in or implemented in connection with this document may be  
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely  
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all  
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable  
24 jurisdiction.  
25

26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**  
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**  
29

30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**  
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**  
33

34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any  
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any  
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual  
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,  
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,  
39 technologies, standards, and specifications, including through the payment of any required license fees.  
40

41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**  
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**  
43 **INTO THIS DOCUMENT.**  
44

45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**  
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**  
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**  
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**  
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**  
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**  
51

52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is  
53 solely responsible for determining whether this document has been superseded by a later version or a different document.  
54

55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the  
56 WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks of the WiMAX  
57 Forum. All other trademarks are the property of their respective owners. Wi-Fi® is a registered trademark of the Wi-Fi  
58 Alliance.  
59

1	<b>TABLE OF CONTENTS</b>	
2	<b>1. DOCUMENT SCOPE.....</b>	<b>7</b>
3	<b>2. ABBREVIATIONS AND DEFINITIONS .....</b>	<b>8</b>
4	2.1 Abbreviations .....	8
5	2.2 Terms & Definitions .....	8
6	2.3 Conventions .....	9
7	<b>3. REFERENCES.....</b>	<b>10</b>
8	<b>4. OMA DM PROTOCOL OVERVIEW .....</b>	<b>12</b>
9	4.1 Introduction to OMA DM Protocol .....	12
10	4.1.1 Management Tree.....	12
11	4.1.2 Device Description.....	12
12	4.1.3 Bootstrap Mechanism.....	12
13	4.1.4 OMA DM Packages and Messages .....	12
14	4.1.5 OMA DM Commands.....	13
15	4.1.6 Notification Message.....	13
16	<b>5. WIMAX® OVER-THE-AIR PROVISIONING AND ACTIVATION OVERVIEW BASED ON OMA</b>	
17	<b>DM 14</b>	
18	5.1 Server-initiated Bootstrapping & WIB Methods .....	14
19	5.2 Requirements.....	15
20	5.2.1 General Requirements.....	15
21	5.2.2 OMA DM Protocol Requirements .....	16
22	5.2.3 Bootstrap and Notification Requirements .....	16
23	5.3 Bootstrap Message Format and Encoding .....	17
24	5.4 OMA Bootstrap Reliability and Retransmission .....	17
25	5.5 Subscription & Provisioning.....	18
26	5.5.1 In-band Subscription Order with In-band Provisioning.....	18
27	5.5.2 Out of band subscription order with in-band provision .....	19
28	5.6 Continuous Management.....	21
29	5.7 Device Capabilities.....	21
30	<b>6. SECURITY CONSIDERATIONS.....</b>	<b>22</b>
31	<b>APPENDIX A. OMA DM WIMAX® MO [NORMATIVE] .....</b>	<b>23</b>
32	A.1 Introduction .....	23
33	A.2 Graphical Representation.....	23
34	A.3 Status and Occurrence Guidance .....	24
35	A.4 DevInfo MO .....	24
36	A.4.1 Introduction.....	24
37	A.4.2 Graphical Representation .....	24
38	A.4.3 Node Descriptions .....	24
39	A.4.3.1 DevInfo .....	24
40	A.4.3.2 DevInfo/Ext .....	24
41	A.4.3.3 DevInfo/Bearer .....	24
42	A.4.3.4 DevInfo/DevId.....	24
43	A.4.3.5 DevInfo/Man.....	25
44	A.4.3.6 DevInfo/Mod .....	25
45	A.4.3.7 DevInfo/DmV .....	25
46	A.4.3.8 DevInfo/Lang.....	25

1	A.5	DM Account MO.....	25
2	A.5.1	Introduction.....	25
3	A.5.2	Graphical Representation.....	25
4	A.5.3	Node Descriptions.....	26
5	A.5.3.1	DMAcc/<X>/ServerID.....	26
6	A.6	DevDetail MO.....	26
7	A.6.1	Introduction.....	26
8	A.6.2	Graphical Representation.....	26
9	A.6.3	Node Descriptions.....	26
10	A.6.3.1	DevDetail/Ext.....	26
11	A.6.3.2	DevDetail/Bearer.....	26
12	A.6.3.3	DevDetail/URI.....	27
13	A.6.3.4	DevDetail/DevTyp.....	27
14	A.6.3.5	DevDetail/OEM.....	28
15	A.6.3.6	DevDetail/FwV.....	28
16	A.6.3.7	DevDetail/SwV.....	28
17	A.6.3.8	DevDetail/HwV.....	28
18	A.6.3.9	DevDetail/LrgObj.....	28
19	A.7	WiMAX® MO.....	28
20	A.7.1	Introduction.....	28
21	A.7.2	Graphical Representation.....	28
22	A.7.3	Node Descriptions.....	29
23	A.7.3.1	WiMAX®.....	29
24	A.7.3.2	WiMAX®/WiMAXRadioModule.....	29
25	A.7.3.3	WiMAX®/TerminalEquipment.....	29
26	A.7.3.4	WiMAX®/TO-WiMAX-REF.....	29
27	A.7.3.5	WiMAX®/DevCap.....	29
28	A.7.3.6	WiMAX/Ext.....	30
29	A.7.4	WiMAX® Radio Module.....	30
30	A.7.4.1	WiMAX/WiMAXRadioModule/<X>.....	30
31	A.7.4.2	WiMAX/WiMAXRadioModule/<X>/Man.....	30
32	A.7.4.3	WiMAX/WiMAXRadioModule/<X>/Mod.....	30
33	A.7.4.4	WiMAX/WiMAXRadioModule/<X>/FwV.....	31
34	A.7.4.5	WiMAX/WiMAXRadioModule/<X>/HwV.....	31
35	A.7.4.6	WiMAX/WiMAXRadioModule/<X>/SwV.....	31
36	A.7.4.7	WiMAX/WiMAXRadioModule/<X>/MACAddress.....	31
37	A.7.4.8	WiMAX/WiMAXRadioModule/<X>/CRN.....	31
38	A.7.5	WiMAX® Terminal Equipment.....	31
39	A.7.5.1	WiMAX/TerminalEquipment/Ext.....	32
40	A.7.5.2	WiMAX/TerminalEquipment/Bearer.....	32
41	A.7.5.3	WiMAX/TerminalEquipment/DevID.....	32
42	A.7.5.4	WiMAX/TerminalEquipment/DevTyp.....	32
43	A.7.5.5	WiMAX/TerminalEquipment/Man.....	33
44	A.7.5.6	WiMAX/TerminalEquipment/Mod.....	33
45	A.7.5.7	WiMAX/TerminalEquipment/FwV.....	33
46	A.7.5.8	WiMAX/TerminalEquipment/HwV.....	33
47	A.7.5.9	WiMAX/TerminalEquipment/SwV.....	33
48	A.7.5.10	WiMAX/TerminalEquipment/EmbeddingPlatformCertificationID.....	34
49	A.7.6	WiMAX® Device Capabilities.....	34
50	A.7.6.1	WiMAX/DevCap/IPCcap.....	34
51	A.7.6.2	WiMAX/DevCap/IPCcap/IPv4.....	35
52	A.7.6.3	WiMAX/DevCap/IPCcap/IPv6.....	35
53	A.7.6.4	WiMAX/DevCap/IPCcap/CMIPv4.....	35
54	A.7.6.5	WiMAX/DevCap/IPCcap/CMIPv6.....	35
55	A.7.6.6	WiMAX/DevCap/UAProfURL.....	35
56	A.7.6.7	WiMAX/DevCap/UpdateMethods.....	35

1	A.7.6.8	WiMAX/DevCap/UpdateMethods/ServerInitiated.....	35
2	A.7.6.9	WiMAX/DevCap/UpdateMethods/ClientInitiated .....	35
3	A.7.6.10	WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingSupported.....	36
4	A.7.6.11	WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingInterval.....	36
5	A.7.6.12	WiMAX/DevCap/UpdateMethodes/ClientInitiated/PollingAttempts.....	36
6	A.7.6.13	WiMAX/Ext .....	36
7	A.8	WiMAX® Supplementary MO .....	36
8	A.8.1	Introduction.....	36
9	A.8.2	Graphical Representation .....	36
10	A.8.3	Node Descriptions .....	38
11	A.8.3.1	WiMAXSupp/Operator.....	38
12	A.8.4	Operator Node.....	38
13	A.8.4.1	WiMAXSupp/Operator/<X> .....	38
14	A.8.4.2	WiMAXSupp/Operator/<X>/NetworkParameters.....	38
15	A.8.4.3	WiMAXSupp/Operator/<X>/SubscriptionParameters .....	38
16	A.8.4.4	WiMAXSupp/Operator/<X>/RootCA .....	38
17	A.8.4.5	WiMAXSupp/Operator/<X>/Contacts .....	38
18	A.8.4.6	WiMAXSupp/Operator/<X>/TO-IP-REF .....	38
19	A.8.4.7	Network Parameters Node .....	38
20	A.8.4.7.1	WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP.....	38
21	A.8.4.7.2	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL .....	39
22	A.8.4.7.3	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL .....	39
23	A.8.4.7.4	WiMAXSupp/Operator/<X>/NetworkParameters/OperatorName.....	39
24	A.8.4.7.5	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan .....	39
25	A.8.4.7.6	WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval.....	39
26	A.8.4.7.7	WiMAXSupp/Operator/<X>/NetworkParameters/PollingAttempts .....	40
27	A.8.4.7.8	H-NSP Node.....	40
28	A.8.4.7.8.1	WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X> .....	40
29	A.8.4.7.8.2	WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X>/H-NSP-ID .....	40
30	A.8.4.7.9	CAPL Node .....	40
31	A.8.4.7.9.1	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/SelectPolicy .....	40
32	A.8.4.7.9.2	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries.....	41
33	A.8.4.7.9.3	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X> .....	41
34	A.8.4.7.9.4	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/NAP-ID .....	41
35	A.8.4.7.9.5	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/Priority .....	41
36	A.8.4.7.9.6	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds .....	41
37	A.8.4.7.9.7	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds/<X>	41
38			
39	A.8.4.7.9.8	WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanRefIds/<X>/	41
40	RefId		
41			
42	A.8.4.7.10	RAPL Node .....	42
43	A.8.4.7.10.1	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/SelectPolicy .....	42
44	A.8.4.7.10.2	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries .....	42
45	A.8.4.7.10.3	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X> .....	42
46	A.8.4.7.10.4	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/V-NSP-ID .....	42
47	A.8.4.7.10.5	WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/Priority .....	42
48	A.8.4.7.11	Channel Plan Node .....	43
49	A.8.4.7.11.1	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries.....	43
50	A.8.4.7.11.2	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/BW.....	43
51	A.8.4.7.11.3	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/FFTSize .....	43
52	A.8.4.7.11.4	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/DuplexMode .....	43
53	A.8.4.7.11.5	Channel Plan Entries.....	43
54	A.8.4.7.11.5.1	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X> .....	43
55	A.8.4.7.11.5.2	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Id.....	43

1	A.8.4.7.11.5.3		
2		WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FirstFre	
3	q	44	
4	A.8.4.7.11.5.4		
5		WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/LastFre	
6	q	44	
7	A.8.4.7.11.5.5		
8		WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/NextFre	
9	qStep	44	
10	A.8.4.7.11.5.6		
11		WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Preamb	
12	les	44	
13	A.8.4.7.11.5.7	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/BW ..44	
14	A.8.4.7.11.5.8		
15		WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FFTSiz	
16	e	44	
17	A.8.4.7.11.5.9	WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries	
18	<X>/DuplexMode.....		45
19	A.8.4.8	Subscription Parameters Node.....	45
20	A.8.4.8.1	WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary .....	45
21	A.8.4.8.2	WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions.....	45
22	A.8.4.8.3	Primary Subscription parameters.....	45
23	A.8.4.8.3.1	WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Name.....	45
24	A.8.4.8.3.2	WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated.....	46
25	A.8.4.8.3.3	WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/EAP.....	46
26	A.8.4.8.4	Other Subscription Parameters .....	46
27	A.8.4.8.4.1	WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X> .....	46
28	A.8.4.8.4.2	WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Name....	46
29	A.8.4.8.4.3	WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Activated	
30		46	
31	A.8.4.8.4.4	WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/EAP.....	47
32	A.8.4.9	RootCA Node .....	47
33	A.8.4.9.1	WiMAXSupp/Operator/<X>/RootCA/<X> .....	47
34	A.8.4.9.2	WiMAXSupp/Operator/<X>/RootCA/<X>/Certificate .....	47
35	A.8.4.10	Contacts Node.....	48
36	A.8.4.10.1	WiMAXSupp/Operator/<X>/Contacts/<X>.....	48
37	A.8.4.10.2	WiMAXSupp/Operator/<X>/Contacts/<X>/Type .....	48
38	A.8.4.10.3	WiMAXSupp/Operator/<X>/Contacts/<X>/Trigger.....	48
39	A.8.4.10.4	WiMAXSupp/Operator/<X>/Contacts/<X>/URI.....	48
40	A.8.4.10.5	WiMAXSupp/Operator/<X>/Contacts/<X>/Text .....	49
41	<b>APPENDIX B. OMA CONNECTIVITY MANAGEMENT OBJECTS [NORMATIVE] .....</b>		<b>50</b>
42	B.1	OMA EAP Management Object.....	50
43	B.1.1	Method Related Parameters.....	52
44	B.1.2	Example: EAP-TLSv0 and Plain-MSCHAPv2 .....	53
45	B.1.3	Example: EAP-AKA in Stand alone Mode .....	53
46	B.1.4	Example: EAP-AKA with EAP-TTLS Encapsulation .....	54
47	B.2	OMA IP Management Object.....	54
48	B.3	OMA NAP Management Object .....	55
49	B.3.1	Definitions for OMA Network Access Point (NAP) Management Object.....	55
50	B.3.1.1	../BearerType .....	55
51	B.3.1.2	../AddrType.....	55
52	B.3.1.3	../Addr .....	55
53	B.3.1.4	../BearerParams/WIMAX .....	56
54	B.3.1.5	../BearerParams/WIMAX/TO-WIMAXSUPP-REF .....	56

1        *B.3.2 Example: Linkage Between the OMA Network Access Point (NAP) MO WiMAX Supplementary MO56*

2    **APPENDIX C. CAPL, RAPL AND CHANNEL PLAN EXAMPLES ..... 58**

3        C.1 Parameters used in CAPL and RAPL nodes.....58

4        *C.1.1 Example: Strict CAPL and RAPL with Priority – Networks Available ..... 58*

5            C.1.1.1 Non-roaming Scenario with Terminal A: .....60

6            C.1.1.2 Roaming Scenario with Terminal B: .....60

7        *C.1.2 Example: No Restrictions in CAPL and RAPL..... 61*

8            C.1.2.1 Non-roaming Scenario:.....61

9            C.1.2.2 Roaming Scenario:.....61

10        *C.1.3 Example: Flexible CAPL and RAPL with Priority..... 61*

11            C.1.3.1 Non-roaming Scenario with Terminal A: .....63

12            C.1.3.2 Roaming Scenario with Terminal B: .....63

13        *C.1.4 Example: Strict CAPL and RAPL with Priority – Networks Not Available..... 63*

14            C.1.4.1 Non-roaming Scenario with Terminal A: .....65

15            C.1.4.2 Roaming Scenario with Terminal B: .....65

16        C.2 Channel Plan Usage.....66

17        *C.2.1 Example: Network Search – Preferred NAPs Found ..... 66*

18            C.2.1.1 NAP selection based on NAP Based Channel Plan .....67

19            C.2.1.2 NAP selection based on Root Channel Plan .....67

20            C.2.1.3 NAP selection based on Root Channel Plan, if NAPs in CAPL would not have priorities .....67

21            C.2.1.4 NAP selection based on full search if channel plan configuration is not provided.....67

22        *C.2.2 Example: Network Search – Flexible CAPL ..... 67*

23            C.2.2.1 NAPs Not Found From the Channel Plan .....69

24    **APPENDIX D. ENSURING MANAGEMENT AUTHORITY CONTROL OF MOS ..... 70**

25    **APPENDIX E. MANDATORY MOS FOR SUPPORTING MODEL B DEVICES [NORMATIVE] ..... 71**

26    **APPENDIX F. MAXIMUM SIZES OF ELEMENTS IN WIMAXSUPP FOR MODEL B DEVICES**

27    **[NORMATIVE] 72**

28

29

1 **LIST OF FIGURES**

2 FIGURE 1 - OMA DM MESSAGE .....13  
3 FIGURE 2- UDP PUSH AND WIB BOOTSTRAPPING METHODS .....14  
4 FIGURE 3 - BOOTSTRAPPING & PROVISIONING MESSAGE FLOW SEQUENCE WITH IN-BAND  
5 SUBSCRIPTION ORDER (NETWORK INITIATED) .....18  
6 FIGURE 4 - BOOTSTRAPPING & PROVISIONING MESSAGE FLOW SEQUENCE WITH OUT OF BAND  
7 SUBSCRIPTION ORDER.....20  
8 FIGURE 5 - STANDARD OMA DM TREE FOR WIMAX DEVICES .....23  
9 FIGURE 6 - STANDARD DEVINFO MO .....24  
10 FIGURE 7 - DEVDETAIL MO .....26  
11 FIGURE 8 - WIMAX MANAGEMENT OBJECT .....29  
12 FIGURE 9 - WIMAX RADIO MODULE .....30  
13 FIGURE 10 - TERMINAL EQUIPMENT .....32  
14 FIGURE 11 - WIMAX® DEVICE CAPABILITIES .....34  
15 FIGURE 12 - WIMAX® SUPPLEMENTARY MO TREE STRUCTURE .....37  
16 FIGURE 13 - EXAMPLE OF EAP-TTLSV0 AND PLAIN-MSCHAPV2 PARAMETERS .....53  
17 FIGURE 14 - EXAMPLE OF EAP-AKA PARAMETERS .....53  
18 FIGURE 15 - EXAMPLE OF EAP-AKA AND EAP-TTLS PARAMETERS .....54  
19 FIGURE 16 - LINKAGE BETWEEN NAP MO AND WIMAXSUPP (PRIMARY SUBSCRIPTION) .....56  
20 FIGURE 17 - LINKAGE BETWEEN NAP MO AND WIMAXSUPP (OTHER SUBSCRIPTIONS).....57  
21 FIGURE 18 - AN EXAMPLE CONFIGURATION HOW STRICT CAPL AND RAPL ARE USED WITH  
22 PRIORITY .....59  
23 FIGURE 19 - NETWORK SETUP .....60  
24 FIGURE 20 - AN EXAMPLE CONFIGURATION OF NO RESTRICTIONS IN CAPL AND RAPL .....61  
25 FIGURE 21 - AN EXAMPLE CONFIGURATION OF FLEXIBLE CAPL AND RAPL WITH PRIORITY .....62  
26 FIGURE 22 - NETWORK SETUP .....62  
27 FIGURE 23 - AN EXAMPLE CONFIGURATION HOW STRICT CAPL AND RAPL ARE USED WITH  
28 PRIORITY .....64  
29 FIGURE 24 - NETWORK SETUP .....65  
30 FIGURE 25 - EXAMPLE CONFIGURATION .....66  
31 FIGURE 26 - NETWORK COVERAGE AND SETUP .....67  
32 FIGURE 27 - EXAMPLE CONFIGURATION .....68  
33 FIGURE 28 - NETWORK COVERAGE AND SETUP .....69  
34

35 **LIST OF TABLES**

36 TABLE 1 - VALUES FOR DEVTYP NODE .....27  
37 TABLE 2- VALUES FOR TERMINAL EQUIPMENT DEVTYP .....32  
38 TABLE 3 - VALUES FOR NAP SELECTION POLICY NODE OF CAPL .....40  
39 TABLE 4 - VALUES OF PRIORITY IN CAPL NODE.....41  
40 TABLE 5 - VALUES FOR V-NSP SELECTION POLICY NODE OF RAPL .....42  
41 TABLE 6 - VALUE OF PRIORITY IN RAPL NODE .....42  
42 TABLE 7 - VALUES OF DUPLEX MODE NODE .....45  
43 TABLE 8 - VALUES OF URI TYPE .....48  
44 TABLE 9 - EAP METHOD VERSUS USED PARAMETERS.....52  
45 TABLE 10 - NAP ADDRESS TYPES .....55  
46

---

## 1. Document Scope

2 WiMAX® technology enables many different device types, such as notebooks, ultra mobile devices (UMD),  
3 handsets, and consumer electronics. A WiMAX service provider would require a dynamic, over-the-air provisioning  
4 solution to configure, activate, enable subscription for, and manage these device types. This document provides  
5 Stage 2 and Stage 3 specifications for over-the-air (OTA) provisioning and activation based on the OMA DM  
6 protocol for Model B WiMAX enabled devices. The WiMAX Over-The-Air General Provisioning System  
7 Specification (WMF-T33-103-R016v) describes end-to-end over the air provisioning and activation.

## 2. Abbreviations and Definitions

### 2.1 Abbreviations

Refer to section 3.1 of [23] for other abbreviations which are not mentioned in this section.

### 2.2 Terms & Definitions

Term	Definition
<b>Channel Plan</b>	A Channel Plan is used by the device to speed up Network Access Provider (NAP) discover process. It contains physical information such as channel bandwidth (BW), center frequency, and PHY profile.
<b>Contractual Agreement Preference List (CAPL)</b>	A list consisting of Network Access Providers (NAP) preferred to be connected to the home network directly.
<b>Device Management System</b>	A background system capable to interact with a (set of) Device(s) for the purpose of Device Management.
<b>DM System</b>	A background system capable of interacting with a (set of) Devices for the purpose of DM.
<b>Host Device</b>	Refers to a standalone device or a submodule in which WiMAX modem (chipset) is embedded. This is the device that is to be managed, associated with MSID, and SHOULD appear in DevInfo or DevDetail Management Object (MO). Examples of the Host Devices are: <ul style="list-style-type: none"> <li>1) Removable Modem (e.g., Personal Computer (PC) Card, USB Modem, etc.) with an embedded WiMAX chipset;</li> <li>2) WiMAX submodule physically attached to a Customer Premises Equipment (CPE);</li> <li>3) WiMAX submodule temporarily or permanently built into a laptop;</li> <li>4) WiMAX enabled CE (e.g., Digital Camera, PMP, etc.) that has an embedded WiMAX chipset;</li> <li>5) Embedded laptop which has WiMAX submodule permanently built in.</li> </ul>
<b>NAP Based Channel Plan</b>	A Channel Plan which is a subset of Root Channel Plan and is associated with a NAP.
<b>Prior Connect Info</b>	Specified in [21]
<b>Roaming Agreement Preference List (RAPL)</b>	A list consisting of Network Service Providers preferred to be connected when roaming.
<b>Root Channel Plan</b>	A Channel Plan which contains all Channel Plan Entries.
<b>WiMAX<sup>®</sup> Radio Module</b>	Refers to WiMAX <sup>®</sup> radio chipset and subsystem present in the host device and that enables WiMAX radio connectivity for the Host Device.
<b>Terminal Equipment</b>	Refers to the device in which host device is temporarily (through PC card slot, USB port etc.) or permanently (for example, embedded laptop) inserted to get WiMAX connectivity. Examples of terminal equipment are: 1) PC which has a PC card slot for peripheral devices, and PC Card (host device) is inserted in PC to get WiMAX connectivity; 2) WiMAX CPE Gateway which has a WiMAX submodule; 3) Embedded laptop which has WiMAX sub-module permanently built in; 4) Consumer electronics that has a WiMAX submodule

Refer to section 3.2 of [23] for other Terms & Definitions which are not mentioned in this section.

1 See the OMA DM Tree and Description [12] document as well for definitions of terms related to the management  
2 tree.

### 3 **2.3 Conventions**

4 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD  
5 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in  
6 [33].

---

## 1 3. References

- [1] "White Paper on Provisioning Objects". Open Mobile Alliance. OMA-WP-AC-MO. URL:<http://www.openmobilealliance.org>
- [2] "OMA DM Bootstrap, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_Bootstrap-V1\_2. URL:<http://www.openmobilealliance.org>
- [3] "Standardized Connectivity Management Objects, Version 1.0". Open Mobile Alliance. OMA-DDS-DM\_ConnMO-V1\_0. URL:<http://www.openmobilealliance.org>
- [4] "OMA DM Device Description Framework Version 1.2 Document Type Definition". Open Mobile Alliance. OMA-SUP-dtd\_dm\_ddf-v1\_2. URL:<http://www.openmobilealliance.org>
- [5] "OMA DM Notification Initiated Session, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_Notification-V1\_2. URL:<http://www.openmobilealliance.org>
- [6] "OMA DM Protocol, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_Protocol-V1\_2. URL:<http://www.openmobilealliance.org>
- [7] "DM Requirements Document, Version 1.2". Open Mobile Alliance. OMA-RD-DM-V1\_2. URL:<http://www.openmobilealliance.org>
- [8] "OMA DM Representation Protocol, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_RepPro-V1\_2. URL:<http://www.openmobilealliance.org>
- [9] "OMA DM Security, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_Security-V1\_2. URL:<http://www.openmobilealliance.org>
- [10] "SyncML HTTP Bidding, Version 1.2.1". Open Mobile Alliance. OMA-TS-SyncMLBinding-V1\_2\_1. URL: <http://www.openmobilealliance.org>
- [11] "OMA DM Standardized Objects, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_StdObj-V1\_2. URL:<http://www.openmobilealliance.org>
- [12] "OMA DM Tree and Description, Version 1.2". Open Mobile Alliance. OMA-TS-DM\_TND-V1\_2. URL:<http://www.openmobilealliance.org>
- [13] "Standard Connectivity MOs, Version 1.0". Open Mobile Alliance. OMA-DDS-DM\_ConnMO -V1\_0. URL:<http://www.openmobilealliance.org>
- [14] "Standard Connectivity Management Objects EAP Paramets, Version 1.0". Open Mobile Alliance. OMA-DDS-DM\_ConnMO\_EAP-V1\_0-20071017-D.doc. URL:<http://www.openmobilealliance.org>
- [15] "Standard Connectivity MOs Internet Protocol (IP) Paramets, Version 1.0". Open Mobile Alliance. OMA-DDS-DM\_ConnMO\_IP-V1\_0. URL:<http://www.openmobilealliance.org>
- [16] "Enabler Release Definition for Client Provisioning, Version 1.1". Open Mobile Alliance. OMA-ERELED-ClientProvisioning-V1\_1. URL:<http://www.openmobilealliance.org>
- [17] "Enabler Release Definition for OMA Device Management, Approved Version 1.2". Open Mobile Alliance. OMA-ERELED-DM-V1\_2. URL:<http://www.openmobilealliance.org>

- [18] “Firmware Update Management Object (FUMO), Version 1.0”. Open Mobile Alliance. OMA-TS-DM-FUMO-V1\_0. URL:<http://www.openmobilealliance.org>
- [19] <http://www.iana.org/assignments/eap-numbers>
- [20] WMF-T32-004-R010, WiMAX Forum® Network Architecture- Architecture Tenets, Reference Model and Reference Points
- [21] WMF-T33-001-R015, WiMAX Forum® Network Architecture- Detailed Protocols and Procedures, Base Specification
- [22] WiMAX Forum® Mobile System Profile
- [23] WMF-T33-103-R015, WiMAX Forum® Network Architecture- Architecture, detailed Protocols and Procedures, WiMAX Over-The-Air General Provisioning System Specification
- [24] “Push OTA Protocol”, Open Mobile Alliance, WAP-235-PushOTA-20010425-a, URL:<http://www.openmobilealliance.org>
- [25] “Push Message”, Open Mobile Alliance, WAP-251-PushMessage-20010322-a, URL:<http://www.openmobilealliance.org>
- [26] “Tag for the Identification of Language”, H Alvestrand, March 1995, URL:<http://www.ietf.org/rfc/rfc1766.txt>
- [27] “URN Syntax”, R. Moats, MAY 1997, URL:<http://www.ietf.org/rfc/rfc2141.txt>
- [28] “The Network Access Identifier,” URL: <http://www.ietf.org/rfc/rfc4282.txt>
- [29] “User Agent Profile - Approved Version 2.0 – 06 Feb 2006,” Open Mobile Alliance URL: [http://www.openmobilealliance.org/release\\_program/uap\\_v2\\_0.html](http://www.openmobilealliance.org/release_program/uap_v2_0.html)
- [30] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Version 6-October-2000.
- [31] IEEE Std 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
- [32] WMF-T33-001-R015, “Network Stage3 Base”, WiMAX Forum®, section 4.1.3 (Configuration Information)
- [33] RFC2119 – Key words for use in RFCs to Indicate Requirement Levels, S. Bradley, March 1997, Best Current Practice
- [34] “Hypertext Transfer Protocol – HTTP/1.1”, R. Fielding et al, June 1999, <http://www.ietf.org/rfc/rfc2616.txt>
- [35] IANA, <http://www.iana.org/>

1 Refer to section 4 of [23] for other references which are not mentioned in this section.

---

## 1 4. OMA DM Protocol Overview

### 2 4.1 Introduction to OMA DM Protocol

3 The OMA DM Protocol [6] defines a management framework and a protocol for various management procedures.  
4 This section describes briefly the core components of OMA DM architecture.

#### 5 4.1.1 Management Tree

6 Every device that supports OMA DM SHALL contain a management tree. All available MOs are logically grouped  
7 in the MS as a hierarchical tree structure called the management tree. Thus, the management of a service or  
8 application in the DM framework requires accessing nodes in the management tree corresponding to the service or  
9 application.

10 The management tree is structured on the basis of services, and applications. Each node in the management tree is  
11 addressed with a URI as described in the OMA DM Tree and Descriptions specification [12].

12 Using the Device Description Framework (DDF) [4] of the management tree, and the tree exchange mechanism  
13 [12], the management server knows the URI [6] of the location to be referred to for a specific management action.

14 In the management tree, WiMAX<sup>®</sup> objects would be specific sub-trees. Similarly application objects from other sub-  
15 trees of the management tree. Annex A describes the WiMAX management tree.

#### 16 4.1.2 Device Description

17 The MOs in the management tree are made known to the management server through the DDF of the MS. The DDF  
18 document is an XML document [30], which is made available to the management server. The DDF Document Type  
19 Definition (DTD) specified in [4] is used to describe the management syntax and semantics for a particular MS.

20 The DDF description gives the properties, such as type, format, description etc of each object, and their relative  
21 location in the management tree. The server learns the MOs and how to manage the objects from the DDF  
22 description.

23 The DDF mechanism provides management of new and customized features in the device.

24 Features common to a class of devices can be grouped and standardized for interoperability and can coexist as a  
25 standardized MOs in the management tree of such a device along with non-standardized MOs. The elements, or  
26 nodes, that describe the common features of all WiMAX devices described in Annex A of this document, SHALL  
27 be grouped into a single standardized WiMAX MO that can be represented using the DDF DTD.

#### 28 4.1.3 Bootstrap Mechanism

29 In order for the DM client of a device to initiate a management session, a bootstrap process MUST be performed to  
30 provision the device with the required settings to initiate a session with a specific DM server. OMA DM supports  
31 three possible methods for the bootstrap process: factory bootstrap, bootstrap from smartcard, or secure server-  
32 initiated bootstrap for initial provisioning. The bootstrap mechanism is defined in the OMA DM Bootstrap  
33 specification [2].

34 If the network operator desires to ensure interoperability with all devices the bootstrap file interchange SHALL  
35 conform to [12].

36 This document specifies how the server-initiated and WiMAX specific client-initiated bootstrap (WIB) are  
37 implemented in WiMAX. The other bootstrap methods are fully implemented in WiMAX as defined in [2] except as  
38 stated otherwise in this specification.

#### 39 4.1.4 OMA DM Packages and Messages

40 In OMA DM, a set of messages exchanged between the DM client and the management server, is conceptually  
41 combined into a package. In most situations a package corresponds to a single message, but when large objects are  
42 involved in the transfer, each package is sent over multiple DM messages. A DM message is a well-formed XML

- 1 document with header and body. The XML specification for OMA DM is described in the protocol specifications  
2 [8].  
3 Limitations on package size, message boundaries etc., are defined in OMA DM representation protocol [8]. An  
4 example of a DM message is shown below.

```
<SyncML xmlns='SYNCML:SYNCML1.1'>  
  <SyncHdr>  
    <!--header information, credentials>  
  </SyncHdr>  
  <SyncBody>  
    <!-- Message body - commands, alerts>  
    <Final/>  
  </SyncBody>  
</SyncML>
```

5

6

**Figure 1 - OMA DM Message**

- 7 The SyncBody container element carries one or more OMA DM commands.

#### 8 **4.1.5 OMA DM Commands**

- 9 OMA DM protocol allows commands to be executed on a node in the management tree, resulting in a specific  
10 management action. The management action can be get, replace, add, delete, execute etc., OMA DM management  
11 commands are used to represent the management actions and associated data elements that are transferred between  
12 the DM client and the DM server

- 13 OMA DM commands are transferred in the XML format defined in [8].

#### 14 **4.1.6 Notification Message**

- 15 The OMA DM notification message causes the client to initiate a connection to the management server and begin a  
16 management session. The notification is a signed message, which the client can authenticate. There are several fields  
17 in the notification message, for example the UI-mode field is used for specifying user interaction when the client  
18 receives the notification.

- 19 Notification message can also originate within the device, thus triggering the establishment of a session, for example  
20 when a timer expires.

- 21 The format and security mechanism for OMA DM notification message are described in the OMA DM Notification  
22 Initiated Session specification [5].

## 5. WiMAX<sup>®</sup> Over-the-Air Provisioning and Activation Overview based on OMA DM

### 5.1 Server-initiated Bootstrapping & WIB Methods

This section describes the OMA DM server-initiated bootstrap (case #1) and the DM client-initiated bootstrap (case #2) methods.

The first step of the subscription and provisioning phase is bootstrapping. This step is required to establish a security association between the device and the provisioning server in order to initiate the first management session.

Bootstrapping process may take place whenever the device does not have the required information to establish a security association with the server or when it fails to establish it based on the information it has (the definition of fail is not in scope of this document). With the successful execution of the bootstrapping process, a secure path between the device DM client and the DM server can be established and the provisioning process for the device can begin. See [9] for information concerning the existing OMA DM security mechanisms.

This section describes the OMA DM server-initiated bootstrap (case #1) and the DM client-initiated WIB (case #2) methods.

In the case of #1, the server-initiated bootstrap method is based on the UDP Push method as defined by OMA, where the DM server sends an encrypted OMA DM bootstrap document to the DM client.

In the case of #2, the client-initiated bootstrap method is based on WIB [23], where the device gets the bootstrap document from the server using the WIB procedure, i.e., Domain Name Server (DNS) and HTTP GET. The client-initiated bootstrap method is used if the device does not support the server-initiated bootstrap method, e.g., laptops with firewall/NAT that prevent the reception of UDP Push messages.

The Figure 2 illustrates case #1 and case #2 of the UDP Push and WIB bootstrapping methods.

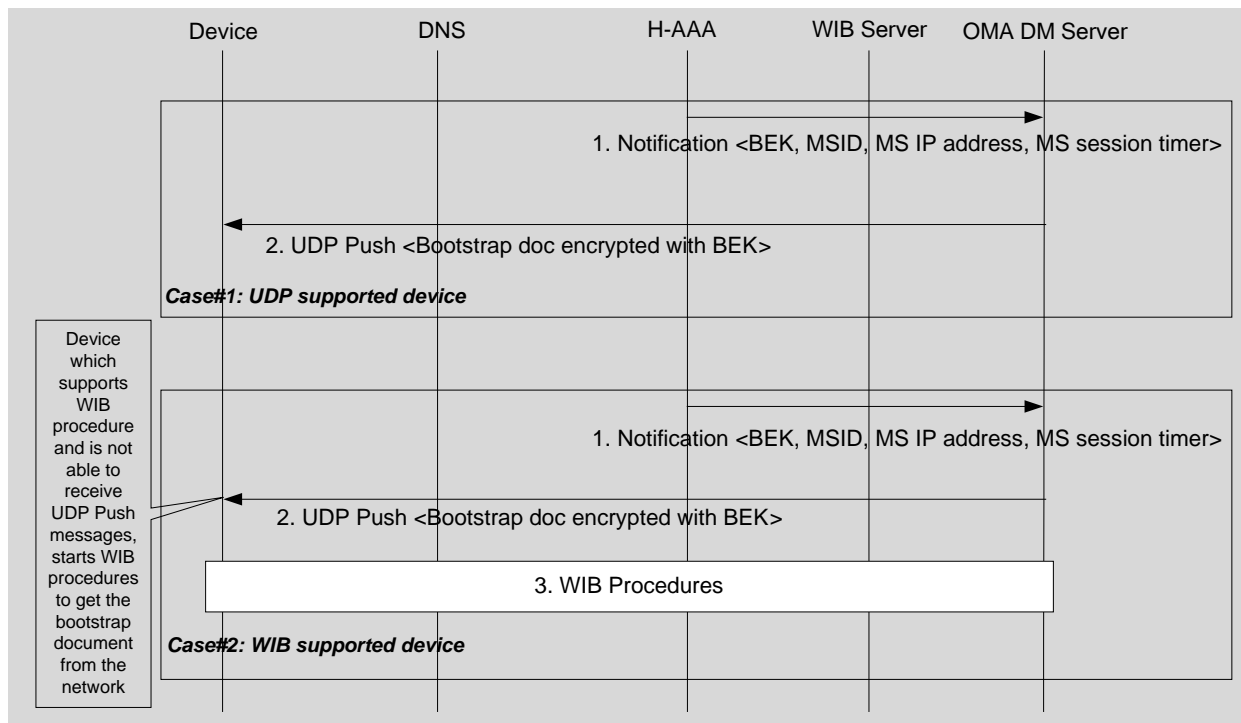


Figure 2- UDP Push and WIB Bootstrapping Methods

## 5.2 Requirements

### 5.2.1 General Requirements

- 1) The device and network MUST successfully complete the Pre-Provisioning Phase, as specified in [23].
- 2) Default bootstrapping and device capabilities policy SHALL be installed by the operator at OMA DM server.
- 3) The device and the OMA DM server SHALL use the OMA DM Protocol [6] to establish a management session and interaction between each other.
- 4) The OMA DM bootstrap procedures as described in [2] SHALL be applied for bootstrapping an unprovisioned WiMAX<sup>®</sup> device.
- 5) The OMA DM server MUST support both the server-initiated bootstrapping procedure, as specified in section 6.1, and the WIB procedure, as specified in [23].
- 6) The device SHALL support either the server-initiated bootstrapping procedures as specified in section 6.1 or the WIB bootstrapping procedures as specified in [23], or both.
- 7) The client-initiated bootstrap method, i.e., WIB, MUST be used on devices that cannot support the server-initiated bootstrap method.
- 8) Delivery of the bootstrap data from OMA DM server to the device SHALL be done in a secure manner. The bootstrap data SHALL be protected as defined in [23] Chapter 9 (Security Considerations).
- 9) Device SHALL process the bootstrap data, as specified in Section 7, Security Consideration.
- 10) The bootstrap data SHALL be mappable to the OMA DM WiMAX MO, as specified in ANNEX A.
- 11) Service provider locked devices SHALL include minimal pre-provisioning information such as.
  - a. The network selection parameters
  - b. Initial NAP/ Network Service Provider (NSP) connection rule/limitation, as specified in ANNEX A, CAPL and RAPL nodes,  
and MAY include
  - c. OMA DM server bootstrap information  
to be able to select, connect and get activated to the network.If the device does not include OMA DM server bootstrap information, the device SHALL be bootstrapped through WIB or UDP Push bootstrap procedure.
- 12) The unlocked devices MAY be factory bootstrapped with the operator network specific parameters.
- 13) The device capabilities query procedure MAY be performed after the device is bootstrapped.
- 14) The OMA DM OTA Provisioning protocol service SHALL be provisioned in the home DNS server as described in [23].
- 15) The device SHALL decrypt and authenticate the bootstrap message as described in [23] Chapter 9 (Security Considerations). If the bootstrap message is successfully decrypted and authenticated, the device SHALL process the bootstrap document as described in [2]. If the authentication of the bootstrap message fails, the device SHALL discard the bootstrap message. The message MAY be displayed to the user to allow the user to accept or reject the initiation of provisioning manually. If the bootstrap message is not discarded, the OMA DM bootstrap information SHALL be persistently stored in the device for later use in communication with the OMA DM server.
- 16) Error cases in WIB procedures are defined in [23].
- 17) The OMA DM server SHALL support assignment of different DDF files to every combination of values of Man (in DevInfo MO), Mod (in DevInfo MO) and SwV (in DevDetail MO) nodes in order to support all devices from all OEMs with all possible software versions.

- 1 18) The bootstrapping process (either server initiated or client initiated) should be performed whenever the  
2 device is not provisioned with the information (DM\_Account) required to establish the secure association  
3 with the OMA DM server.
- 4 19) The bootstrapping process (either server initiated or client initiated) should be performed whenever the  
5 client fails (the decision of fail is out of scope of this specification) to establish the secure association with  
6 the OMA DM server based on its provisioned information.
- 7 20) In case of client initiated bootstrap i.e. WIB – the server must respond with a bootstrap file as described in  
8 [23] regardless of the device state in the operator network.  
9

## 10 5.2.2 OMA DM Protocol Requirements

11 Additional requirements beyond [6] and [8]:

### 12 1. Source element

13 When used in SyncHdr element, the LocURI element in the Source element SHALL contain the device identifier  
14 (DevInfo/DevId) as specified in Annex A.

15 The device and the OMA DM server MAY use FUMO to update the device firmware. The WiMAX<sup>®</sup> DM client and  
16 OMA DM server MAY support OMA DM download procedure, as specified in [18].

17 The OMA DM client may commit all non atomic OMA commands at the successful end of the OMA DM session.

## 18 5.2.3 Bootstrap and Notification Requirements

19 This section provides the bootstrap and notification requirements.

- 20 • For Case #1 (server initiated method using the UDP push):
  - 21 1. The OMA DM server SHALL use the non-secure connectionless WSP session service (UDP port  
22 2948) [24] to deliver the encrypted server initiated bootstrap document and the OMA DM notifications  
23 [5] to the OMA DM client.
  - 24 2. The X-WAP-Application-ID header [25] SHALL contain the application-id associated with the  
25 SyncML Device Management user agent. The application-id code 0x07 MUST be used instead of the  
26 textual representation of the application-id.
  - 27 3. The Content-Type header [25] SHALL contain the MIME media type for WiMAX bootstrap  
28 (application/vnd.wmf.bootstrap) as defined in [23] for the bootstrap message. The Content-Type code  
29 (0x0318) MUST be used instead of the textual representation.
  - 30 4. The Content-Type header [25] SHALL contain the MIME media type for OMA DM Package #0  
31 (application/vnd.syncml.notification) as defined in [35] for OMA DM notifications. The Content-Type  
32 code 0x44 MUST be used instead of the textual representation.
- 33 • For Case #2 (client-initiated method using the WIB):
  - 34 1. The WIB Server SHALL respond with an HTTP Response message as specified in [23], when WIB  
35 Server receives the HTTP Get message.
  - 36 2. The Content-Type header of the HTTP Response [34] SHALL contain the MIME media type for  
37 WiMAX bootstrap (application/vnd.wmf.bootstrap) as defined in [23] and the WiMAX bootstrap  
38 message SHALL be delivered in the HTTP body.
  - 39 3. The WiMAX bootstrap message SHALL include the bootstrap content only and SHALL NOT include  
40 and OMA-DM defined headers such as WSP header.
  - 41 4. The Bootstrap message SHALL be encoded according to the DM profile as defined in [17]
- 42 • For Case #1 and #2:
  - 43 1. The device SHALL process the bootstrap document, as specified in [2].

- 1           2. The OMA DM Server SHALL send the bootstrap message to the OMA DM client whenever it receives  
2           the notification message from H-AAA. The OMA DM server SHALL attempt to bootstrap the OMA  
3           DM client during the period of MS IP session timer. The OMA-DM server should attempt to bootstrap  
4           the device upon each NW entry until it receives an indication that bootstrap was successful.
- 5           3. After successfully processing the bootstrap document, the OMA DM client SHALL initiate a session  
6           to OMA DM server configured in the bootstrap. OMA DM Package #1 sent by the client SHALL  
7           contain DevInfo as specified in Annex A.
- 8           4. The OMA DM server SHOULD re-send the bootstrap document until the client connects for the first  
9           time. The number of retry and duration of sending the bootstrap document are out of scope of this  
10          specification.
- 11          5. If the device detects an error during any of these phases the device MAY perform device initiated  
12          network exit procedure as described in [21] and network re-entry in order to repeat the sequence of  
13          obtaining a bootstrap message. The timer value to wait for the bootstrap message from the network to  
14          the device is out of scope of this document. The amount of attempts should be limited (the actual  
15          number is out of the scope of this spec). After completing the attempts, the device SHALL stay  
16          connected.
- 17          6. The content of notifications in both cases SHALL be the same, because if the device receives multiple  
18          notifications only one management session SHOULD be triggered as defined in [5].
- 19          7. The content of bootstrap document in both cases SHALL be the same.

### 20   **5.3 Bootstrap Message Format and Encoding**

21   The OMA DM Bootstrap specification [2] defines two formats for the inner content of the bootstrap message, called  
22   “bootstrap profiles”.

- 23   • **OMA Client Provisioning** - This profile specifies alignment of two existing enablers – OMA Client  
24    Provisioning [16] and OMA Device Management [17]. The profile defines how the information  
25    provisioned using OMA Client Provisioning can be transferred to the management tree specified in the  
26    OMA Device Management.
- 27   • **OMA Device Management** - This profile defines how the OMA Device Management [17] can be used for  
28    bootstrapping.

29  
30   WiMAX<sup>®</sup> devices MUST support the OMA Device Management profile for the bootstrap message. This means the  
31   bootstrap document MUST be formatted in accordance with [17], and then encrypted as described in [23] Security  
32   Consideration section.

33  
34   Support for OMA Client Provisioning over WiMAX is not prohibited in the UDP bootstrap case, but is not  
35   recommended either.

36  
37   The encrypted bootstrap message and the nonce value SHALL be transmitted to the client in a TLV encoded  
38   message as described in the “Bootstrap Message Encoding” section of the OTA General Specification [23].

### 39   **5.4 OMA Bootstrap Reliability and Retransmission**

40   In the case of #1, the OMA Bootstrap document is sent to the device with an unacknowledged UDP message. Due to  
41   the unreliable nature of UDP in a wireless environment like WiMAX, the bootstrap message MAY not be received  
42   by the device for any number of potential reasons. Because of this, the OMA DM server SHALL be capable of  
43   retransmitting the bootstrap document.

44   Each time the OMA DM server retransmits a bootstrap document it SHALL encrypt and authenticate the document  
45   with the same BEK and nonce as the first time it transmitted the bootstrap document for the life of the BEK as  
46   described in [23] Chapter 9 (Security Considerations). The contents of the bootstrap document MUST be  
47   unmodified when retransmission is necessary. Retransmission is performed to enhance the reliability of the delivery  
48   of the bootstrap document—not to enable the delivery of modified bootstrap documents. The device can treat any  
49   received bootstrap message as a retransmission, not as an updated copy of a bootstrap document. Once a new BEK

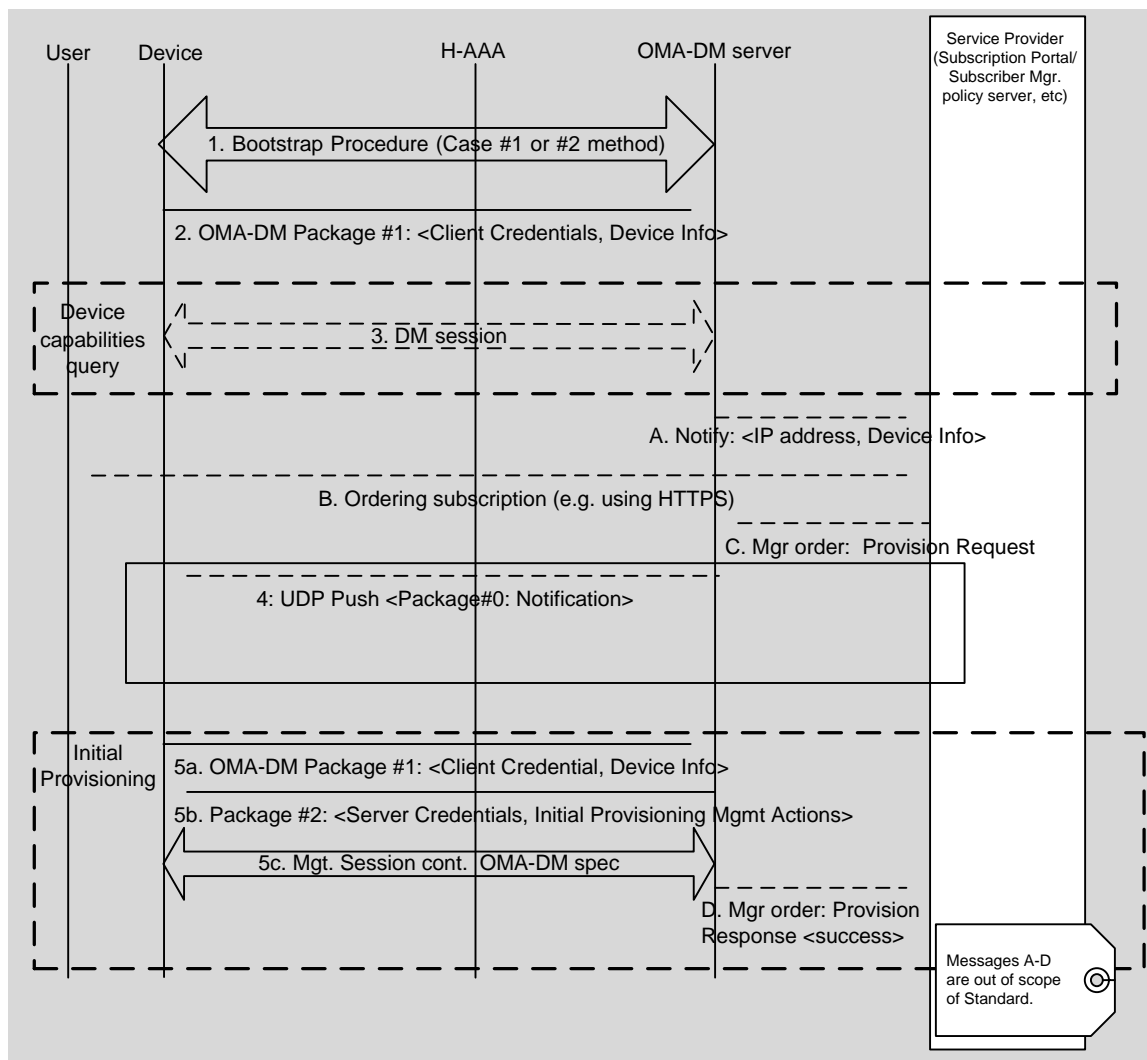
1 is available a bootstrap file can be encrypted with the new BEK and a new nonce. It is therefore possible to modify  
 2 the contents of the bootstrap document only after a new BEK is available.  
 3 The OMA server SHALL not re-transmit the bootstrap document after the first successful response, which is  
 4 package #1, is received from the device. The successful reception of a package #1 from the device indicates that the  
 5 bootstrapping process was successful and no further attempts to bootstrap the device are required. All further OMA  
 6 based notification and request retries SHALL fall under the behavior defined in OMA for notification retry behavior.

## 7 5.5 Subscription & Provisioning

### 8 5.5.1 In-band Subscription Order with In-band Provisioning

9 The following message flow sequence Figure 3 illustrates the use case where the user establishes business  
 10 relationship with the service provider by using the device to be provisioned. The ordering subscription steps MAY  
 11 occur any time prior to the step C.

12 It is a beneficial for the subscription subsystem to be aware of the device capability prior to offering the subscription  
 13 plan to the user. To achieve this, the OMA DM server MAY send a query to the device via the OMA DM protocol,  
 14 in the same OMA DM session.



15 **Figure 3 - Bootstrapping & Provisioning message flow sequence with in-band subscription order**  
 16 **(Network initiated)**  
 17

1 Message flow sequence:

- 2 1. The device and the OMA DM server SHALL perform either the case #1 or case #2 bootstrap procedure as  
3 specified in section 6.
  - 4 2. After successfully processing the bootstrap, the OMA DM client SHALL initiate a management session to  
5 the OMA DM server configured in the bootstrap. The OMA DM client sends the OMA DM package #1,  
6 which includes credentials of the client and the device information (DevInfo MO) as specified in [2], [6]  
7 and [11].
  - 8 3. Device capabilities query step:  
9 The OMA DM server MAY get the device capabilities information (e.g., WiMAX/DevCap)  
10 through the same OMA DM session which was used in step 2.
  - 11 A. Upon completion of the OMA DM session, the OMA DM server SHALL send a notification with the  
12 device information, which includes the DevInfo described in Annex A and device capabilities to the service  
13 provider subscription portal subsystem. This Notification message MAY contain other information which  
14 the OMA DM server gets through the OMA DM session from the device as described in step 3.
  - 15 B. The ordering subscription steps MAY vary depending on the implementation of the service provider  
16 subscription portal subsystem and it MAY occur any time prior to step C. Within these steps, the user uses  
17 the subscription portal to create a business relationship with the attached NSP. Based on the user input and  
18 device capability query, the subscription portal creates a user account. The user account information is  
19 stored in a database where the AAA and the OMA DM server have access to the information.
  - 20 C. Upon completion of the subscription ordering and account setup, the subscription portal sends a  
21 management provision request to the OMA DM server. The request includes the device and user  
22 credentials, and MSID. Upon receiving the subscription order from subscription portal, the OMA DM  
23 server SHALL perform step 4.
  - 24 4. Notification Step:  
25 The OMA-DM server notifies the OMA-DM client to initiate an OMA-DM session to conduct OTA  
26 provisioning. If a personal firewall in the MS blocks incoming unidentified UDP messages, this indication  
27 will not reach the OMA-DM client. In that case, the OMA-DM client should be configured (during the first  
28 session after bootstrap) to operate in polling mode so that it polls the server every specified polling interval.
  - 29 5. Upon receiving the notification message the device SHALL start an OMA DM session by sending an OMA  
30 DM Package #1 to the OMA DM server. Package #1 SHALL contain DevInfo as describer in Annex A.  
31 The OMA DM server SHALL proceed with the provisioning by managing the objects described in Annex  
32 A-C as specified in [6]. Upon successful completion of the provision phase, the OMA DM server SHALL  
33 set proper value for WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated node. Once  
34 the provisioning is completed, the OMA DM server and client SHALL terminate the DM session.
  - 35 D. The OMA DM server sends a management provision response to the subscription portal with a successful  
36 status.
- 37 The WIB procedure related error cases are defined in [23]. OMA DM session related error cases are defined in [6],  
38 [8] and [10].

## 39 **5.5.2 Out of band subscription order with in-band provision**

40 The following message flow sequence Figure 4 illustrates the following use cases:

- 41 1) Use case A: User establishes a business relationship with the service provider prior attaching an unprovisioned  
42 device to the service provider network. The user account setup is completed.
- 43 2) Use case B: User has already established account, and wishes to re-provision an existing device.

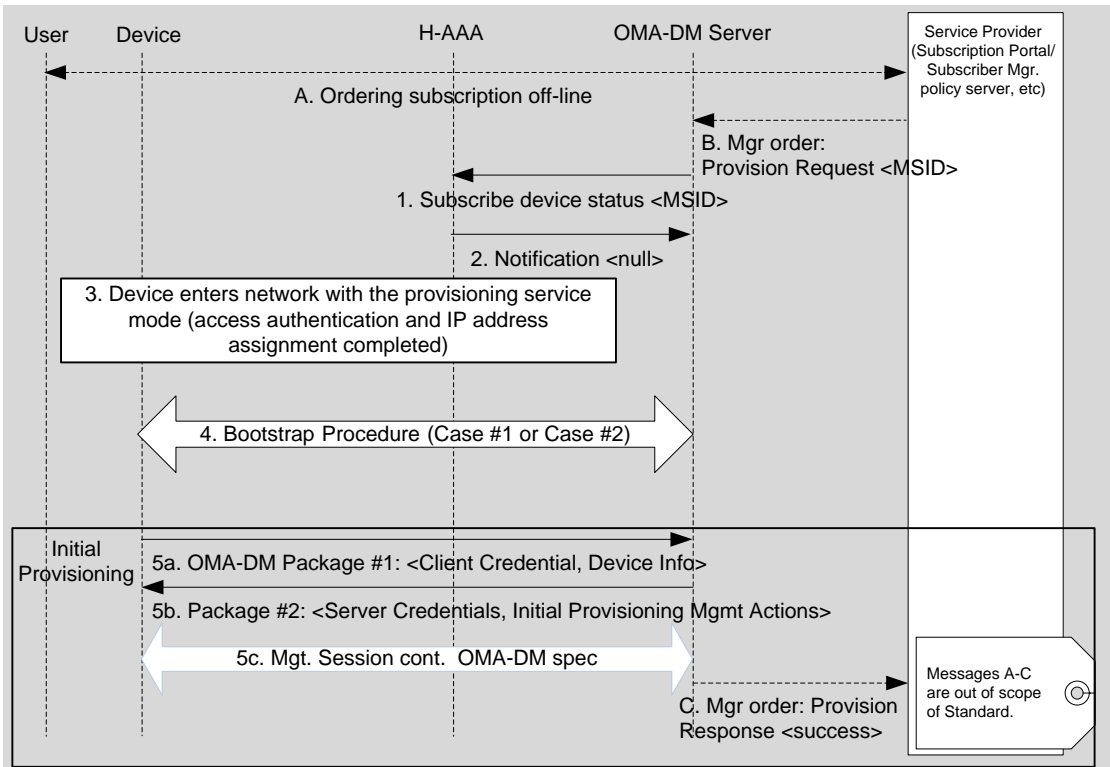


Figure 4

**- Bootstrapping & Provisioning message flow sequence with out of band subscription order**

Message flow sequence:

- A. The user establishes a business relationship with the service provider prior attaching an unprovisioned device to the service provider network.
- B. The subscription portal sends a management provision request to the OMA DM server. The request includes user credential, and MSID.
  1. OMA DM server subscribes to the device status event with the H-AAA.
  2. If the device does not have an IP Session with the network, the H-AAA SHALL send a notification with a "null" status.
  3. Device enters the network in the provisioning service mode. The access authentication and IP address assignment is completed.
  4. Device and OMA DM server SHALL perform either the case #1 or case #2 bootstrap procedure as specified in Chapter 6.2.3.
  5. Upon receiving the bootstrap document the device SHALL start an OMA DM session by sending an OMA DM Package #1 to the OMA DM server. Package #1 SHALL contain DevInfo as describer in Annex A. The OMA DM server SHALL proceed with the provisioning by managing the objects described in Annex A-C as specified in [6]. Upon successful completion of the provision phase, the OMA DM server SHALL set proper value for WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated node. Once the provisioning is completed, the OMA DM server and client SHALL terminate the DM session.
- C. The OMA DM server sends a management provision response to the subscription portal with a successful status.

The WIB procedure related error cases are defined in [23]. OMA DM session related error cases are defined in [6], [8] and [10].

## 1 **5.6 Continuous Management**

- 2 1) Devices that will be affected by the presence of a firewall blocking UDP Push notifications SHALL support  
3 client-initiated sessions tied to a timer.
- 4 2) The device using client-initiated update method (specified at WiMAX/DevCap/UpdateMethods/ClientInitiated)  
5 SHALL start a client-initiated management session to the OMA DM server of the operator every “X” number of  
6 minutes where “X” is defined under the “WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval”  
7 node.
- 8 3) The operator, upon first registration of the device on the network, SHOULD read the value of  
9 “WiMAX/DevCap/UpdateMethods/ServerInitiated” and “WiMAX/DevCap/UpdateMethods/ClientInitiated”  
10 nodes to determine the capabilities of the device. If the device reports a suggested polling interval in the  
11 “WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingInterval” node, the operator MAY set the polling  
12 interval under the Operator node accordingly. This would ensure that the devices operate at their optimum  
13 settings.

14 The WIB procedure related error cases are defined in [23]. OMA DM session related error cases are defined in [6],  
15 [8] and [10].

## 16 **5.7 Device Capabilities**

- 17 1) If the Device Capabilities (e.g. UpdateMethods) are changed, the client MAY send a notification to the DM  
18 server via a Generic Alert [6] message. The alert message includes the following data:
  - 19 • The URI of the DevCap MO – Used to identify the source
  - 20 • An alert type – The alert type “org.wimaxforum.ota.updatedevicecap” MUST be used.
- 21 2) Upon receiving the notification, the DM server SHALL update the Device Capabilities into the DM server.

---

1 **6. Security Considerations**

- 2 OMA DM security considerations SHALL use [23].

## APPENDIX A. OMA DM WiMAX<sup>®</sup> MO [NORMATIVE]

### A.1 Introduction

The size of format types are specified in [4]. The encoding of Chr type of nodes is ASCII unless otherwise specified.

Maximum length of some of the nodes is defined within the node descriptions in the following way: "Maximum length SHOULD/SHALL be ." Whenever "SHALL" is used in this context, it means that the sending entity SHALL NOT populate the node with more data than defined by maximum length and the receiving entity SHALL support lengths up to this definition. Whenever "SHOULD" is used in this context, it means that the receiving entity SHALL support lengths up to this definition and it is implementation specific of what happens if maximum length is exceeded. If "SHOULD" is used the sending entity SHOULD populate the node with data less than or equal to maximum length but it MAY put more data although it is not recommended.

A WiMAX<sup>®</sup> device's OMA DM tree MUST contain the following mandatory MOs:

- DMAcc
- DevInfo
- DevDetail
- WiMAX
- WiMAXSupp

The DMAcc, DevInfo, and DevDetail are generic OMA DM MOs defined by OMA DM WG in [11]. This document describes how these objects are used in a WiMAX device.

WiMAX MO and WiMAX Supplementary MO are WiMAX specific and described in this document.

In addition, WiMAX device MAY use, inside the WiMAXSupp, several Extensible Authentication Protocol (EAP) MOs to contain the authentication settings for different subscriptions. This is defined in [14].

A WiMAX device's OMA DM tree MAY contain the following optional MOs:

- NAP (Network Access Point)

NAP is a generic OMA DM MO defined by OMA DM WG in [3].

### A.2 Graphical Representation

Figure 5 shows the standard OMA DM tree for WiMAX<sup>®</sup> devices. The NAP MO, if included, MAY be located anywhere in the DM tree.

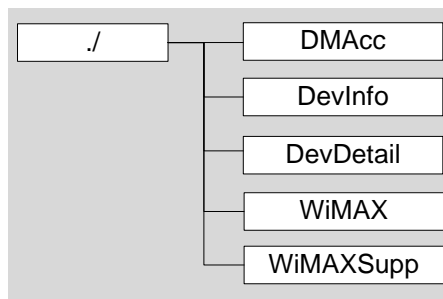


Figure 5 - Standard OMA DM tree for WiMAX devices

1 **A.3 Status and Occurrence Guidance**

2 Refer to the OMA DM ACMO Whitepaper [1] for the definition and possible values for status and occurrence of  
 3 each node.

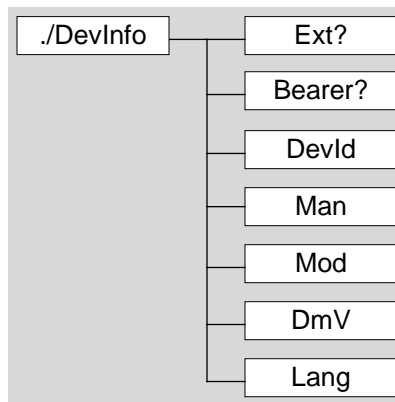
4 **A.4 DevInfo MO**

5 **A.4.1 Introduction**

6 This section describes how the standard DevInfo MO [11] is used with WiMAX devices. See the standard OMA  
 7 DM Objects definitions [11].

8 **A.4.2 Graphical Representation**

9 Figure 6 shows the standard DevInfo MO.



10  
11 **Figure 6 - Standard DevInfo MO**

12 **A.4.3 Node Descriptions**

13 **A.4.3.1 DevInfo**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

14 This interior node provides Host Device information for OMA DM server. The information is sent from the  
 15 client to the server

16 **A.4.3.2 DevInfo/Ext**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

17 This optional interior node is designated to be the only branch of the DevInfo sub tree into which  
 18 extensions can be added permanently or dynamically.

19 **A.4.3.3 DevInfo/Bearer**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

20 This optional interior node is used for stating what bearers the Host Device supports.

21 **A.4.3.4 DevInfo/DevId**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

22 This leaf node specifies globally unique identifier (GUID) for the Host Device. The identifier SHOULD be  
 23 globally unique. The Host Device MAC address (i.e. MSID) MAY be provided as a DevId for both single-

mode and dual-mode devices. WiMAX devices MAY use the MAC address as DevId in which case the format SHALL be the following.

```

<DevId> ::= < mac> “:” <mac_address>
<mac> ::= %d77.65.67
<mac_address> ::= 12 * 12 <hex>
<hex> ::= <numbers> | “A” | “B” | “C” | “D” | “E” | “F” | “a” | “b” | “c” | “d” | “e” | “f”
<numbers> ::= “0” | “1” | “2” | “3” | “4” | “5” | “6” | “7” | “8” | “9”
    
```

Examples of valid DevIds:

```

MAC:112233445566
MAC:a12233445566
MAC:A12233445566
    
```

Examples of invalid DevIds:

```

mac:1122334455
MAC:11223344556
MAC:11-22-33-44-55-66
MAC:11:22:33:44:55:66
    
```

#### A.4.3.5 DevInfo/Man

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the manufacturer identifier of the Host Device.

#### A.4.3.6 DevInfo/Mod

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the model identifier of the Host Device.

#### A.4.3.7 DevInfo/DmV

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies OMA DM client version identifier (manufacturer specified string).

#### A.4.3.8 DevInfo/Lang

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the current language setting of the Host Device. The syntax of the language tags and their use are defined in [26]. Language codes are defined by ISO in the standard ISO 639.

### A.5 DM Account MO

#### A.5.1 Introduction

This section lists the required modifications and extensions to the standard DM Account MO [11]. There MAY be multiple DMAcc MOs. A specific DMAcc MO represents a specific operator's OMA DM server.

#### A.5.2 Graphical Representation

See [11] for graphical presentation of the DMAcc MO.

1 **A.5.3 Node Descriptions**

2 **A.5.3.1 DMAcc/<X>/ServerID**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

3 This leaf node specifies a server identifier for the management server used in the management session. The  
4 ServerID MUST be unique per Home Network Service Provider (H-NSP). Each H-NSP MUST use only  
5 one ServerID value.

6 While it is not mandatory, it is recommended that one of the NSP-IDs of the operator (which are unique to  
7 that operator) be used as the ServerID.

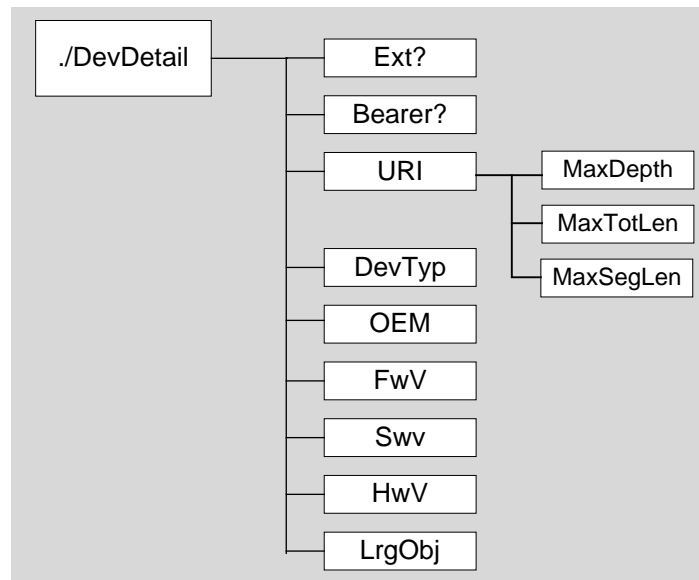
8 **A.6 DevDetail MO**

9 **A.6.1 Introduction**

10 This Section lists required modification and extensions to the standard DevDetail MO [11]. Please also refer to the  
11 OMA DM Standard Objects definitions [11].

12 **A.6.2 Graphical Representation**

13 Figure 7 shows the structure of the DevDetail MO.



14  
15 **Figure 7 - DevDetail MO**

16 **A.6.3 Node Descriptions**

17 **A.6.3.1 DevDetail/Ext**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

18 This optional interior node is designated to be the only branch of DevDetail sub tree into which extensions  
19 can be added permanently or dynamically.

20 **A.6.3.2 DevDetail/Bearer**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

21 This optional interior node is designated to be a branch of the DevDetail sub tree into which items related  
22 to the bearer that the Host Device supports are stored.

1 **A.6.3.3 DevDetail/URI**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

2 This mandatory interior node is used for information specific to URI supported by the client. See [11] for  
3 the child nodes and details.

4 **A.6.3.4 DevDetail/DevTyp**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

5 This mandatory leaf node specifies device type of the Host Device. The possible values to be used to  
6 populate this leaf node are including but not limited to the followings (The first column indicates type of  
7 the device and the second column indicates character string for the respective device types. The last column  
8 indicates whether the WiMAX/TerminalEquipment node is required or not according to the DevTyp):

9 **Table 1 - Values for DevTyp node**

Type of the Device	DevType String for Population	TerminalEquipment Node
PC Card – Single Mode	SingleModePCCard	REQUIRED
PC Card – Multi Mode	MultiModePCCard	REQUIRED
Express Card – Single Mode	SingleModeExpressPCCard	REQUIRED
Express Card – Multi Mode	MultiModeExpressPCCard	REQUIRED
USB Card – Single Mode	SingleModeUSBCard	REQUIRED
USB Card – Multi Mode	MultiModeUSBCard	REQUIRED
Basic Modem	BasicModem	OPTIONAL
SOHO Modem	SOHOModem	OPTIONAL
Personal Media Player (PMP)	PMP	OPTIONAL
Multi Mode PMP	MultiModePMP	OPTIONAL
UMPC	UMPC	OPTIONAL
Netbook	Netbook	OPTIONAL
Laptop	Laptop	OPTIONAL
Internet Tablet	InternetTablet	OPTIONAL
Single Mode Handset	SingleModeHandset	OPTIONAL
Multi Mode Handset	MultiModeHandset	OPTIONAL
PDA	PDA	OPTIONAL
Gaming Device	GamingDev	OPTIONAL
Video Phone	VideoPhone	OPTIONAL
Machine to Machine	M2M	OPTIONAL
Digital Camera	Digital Camera	OPTIONAL
Digital Camcorder	Digital Camcorder	OPTIONAL
Wearable Device	WearableDev	OPTIONAL
Multi Mode Messaging Device	MultiModeMsgDev	OPTIONAL
Electronic Book	EBook	OPTIONAL

Type of the Device	DevType String for Population	TerminalEquipment Node
Navigation Device	NavigationDev	OPTIONAL
In-Vehicle Entertainment Device	InVehicleEntDev	OPTIONAL
Home Media Gateway	HomeMediaGW	OPTIONAL
Music Player	MusicPlayer	OPTIONAL

1

2 **A.6.3.5 DevDetail/OEM**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

3 This mandatory leaf node specifies original equipment manufacturer of the Host Device.

4 **A.6.3.6 DevDetail/FwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

5 This mandatory leaf node specifies firmware version of the Host Device.

6 **A.6.3.7 DevDetail/SwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

7 This mandatory leaf node specifies software version of the Host Device.

8 In order to support the possibility of change in DDF due to software and/or firmware upgrade process, the SwV  
9 node SHALL be taken into account by the OMA DM server in the selection process of the correct DDF for the  
10 device.

11 **A.6.3.8 DevDetail/HwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

12 This mandatory leaf node specifies hardware version of the Host Device.

13 **A.6.3.9 DevDetail/LrgObj**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

14 This mandatory leaf node indicates whether the Host Device supports the OMA DM Large Object Handling  
15 specification, as defined in [6]

16 **A.7 WiMAX<sup>®</sup> MO**

17 **A.7.1 Introduction**

18 The WiMAX<sup>®</sup> MO facilitates management of WiMAX parameters.

19 The MO Identifier for the WiMAX MO MUST be: “urn:wmf:mo:wimax-mo:1.0”

20 The WiMAX MO MUST be located in the root (/).

21 **A.7.2 Graphical Representation**

22 Figure 8 provides the structure of the WiMAX MO.

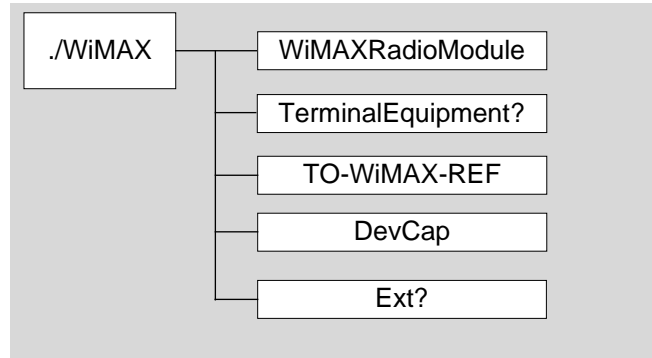


Figure 8 - WiMAX<sup>®</sup> Management Object

### A.7.3 Node Descriptions

#### A.7.3.1 WiMAX<sup>®</sup>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node specifies the WiMAX device configuration related information. This interior node as depicted in Figure 8 provides all required information about WiMAXRadioModule and Terminal Equipment and Device capabilities.

#### A.7.3.2 WiMAX<sup>®</sup>/WiMAXRadioModule

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node specifies the WiMAX radio chipset specific information. See Section A.7.4 for further details.

#### A.7.3.3 WiMAX<sup>®</sup>/TerminalEquipment

Status	Tree Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

This optional interior node specifies the Terminal Equipment device specific information. See Section A.7.5 for further details. This node is not used for stand-alone Host Devices which have built in embedded WiMAX chipset and not connected to Terminal Equipment. This node is REQUIRED for some type of devices as specified in Table 2.

#### A.7.3.4 WiMAX<sup>®</sup>/TO-WiMAX-REF

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	One	Chr	Get

This leaf node contains the link to the WiMAXSupp. See Section A.8 for further details about the WiMAXSupp. An example is presented in Annex B to show how the linkage between TO-WiMAX-REF node and WiMAXSupp is established.

This optional leaf is deprecated and is left for backwards compatibility reasons. Its value is not used. It will be removed in the next version of the spec

#### A.7.3.5 WiMAX<sup>®</sup>/DevCap

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains WiMAX device capability information. See Section A.7.6 for further details.

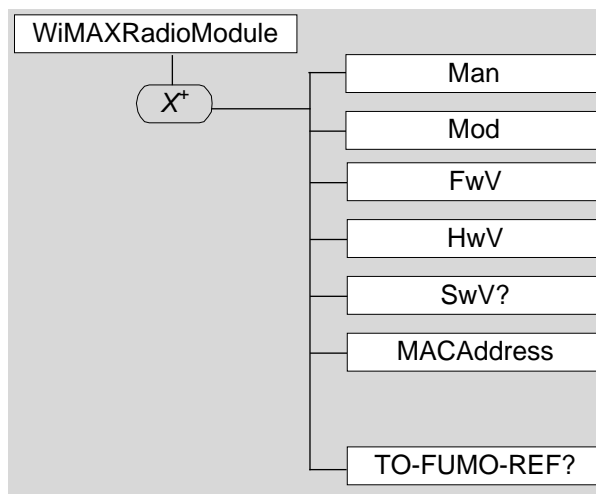
1 **A.7.3.6 WiMAX/Ext**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

2 This optional interior node is designated to be the only branch of WiMAX sub tree into which extensions  
3 can be added, permanently or dynamically.

4 **A.7.4 WiMAX® Radio Module**

5 Figure 9 shows the structure of the WiMAXRadioModule MO.



6

7 **Figure 9 - WiMAX® Radio Module**

8 **A.7.4.1 WiMAX/WiMAXRadioModule/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get

9 This interior node is a placeholder for the WiMAX radio chipsets present in the Host Device to support  
10 WiMAX bearer on the Host Device. This interior node distinguishes different WiMAX radio chipsets and  
11 subsystems that are possibly present in the Host Device. There MUST be exactly one WiMAX radio  
12 chipset and subsystem for each of these interior nodes. There should be exactly one instance of the internal  
13 node in the radio module node. In the future versions of the WiMAX MO, only one radio module will be  
14 allowed.

15 **A.7.4.2 WiMAX/WiMAXRadioModule/<X>/Man**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

16 This leaf node specifies the manufacturer of the WiMAX radio chipset embedded in the Host Device. If the  
17 manufacturer of the WiMAX chipset is not available this node SHALL contain the string “none”. The  
18 maximum length SHOULD be 50 characters.

19 **A.7.4.3 WiMAX/WiMAXRadioModule/<X>/Mod**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

20 This leaf node specifies the model of the WiMAX radio chipset embedded in the Host Device. If the model  
21 of the WiMAX radio chipset is not available this node SHALL contain the string “none”. The maximum  
22 length SHOULD be 50 characters.

1 **A.7.4.4 WiMAX/WiMAXRadioModule/<X>/FwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

2 This leaf node specifies the firmware version of the WiMAX radio chipset present in the Host Device. If  
 3 the firmware version of the WiMAX radio chipset is not available this node SHALL contain the string  
 4 “none”. The maximum length SHOULD be 50 characters.

5 **A.7.4.5 WiMAX/WiMAXRadioModule/<X>/HwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

6 This leaf node specifies the hardware version of the WiMAX radio chipset present in the Host Device. If  
 7 the hardware version of the WiMAX radio chipset is not available this node SHALL contain the string  
 8 “none”. The maximum length SHOULD be 50 characters.

9 **A.7.4.6 WiMAX/WiMAXRadioModule/<X>/SwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Chr	Get

10 This leaf node specifies the version of the software package that is installed in the Terminal Equipment  
 11 which is required for the Host Device containing the WiMAX radio chipset to operate. If the version of the  
 12 software package is not available this node SHALL contain the string “none”. The maximum length  
 13 SHOULD be 50 characters.

14 **A.7.4.7 WiMAX/WiMAXRadioModule/<X>/MACAddress**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bin	Get

15 This leaf node represents the 48-bit MSID associated with the WiMAX radio chipset and subsystem. When  
 16 displayed on the device, the 48-bit MAC address SHOULD be displayed in hexadecimal representation  
 17 with the octets of the MAC address separated by a hyphen.

18 **A.7.4.8 WiMAX/WiMAXRadioModule/<X>/CRN**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	One	68 bit HEX digits	Get

19 This leaf node represents the CRN value that was allocated to the WiMAX device as part of the device  
 20 certification process. The contents of this leaf matches the CRN part of the IPID (Integral Platform ID) that  
 21 is provided by the MS as part of the NAI during network entry.

22 WiMAX devices that have not been assign a CRN (and hence are not certified) MAY not implement this  
 23 node.

24 **A.7.5 WiMAX<sup>®</sup> Terminal Equipment**

25 This interior node describes the Terminal Equipment device information. DevInfo and DevDetail DM standard  
 26 object structure is reused to describe the terminal equipment., Figure 10 shows the structure of the  
 27 TerminalEquipment MO.

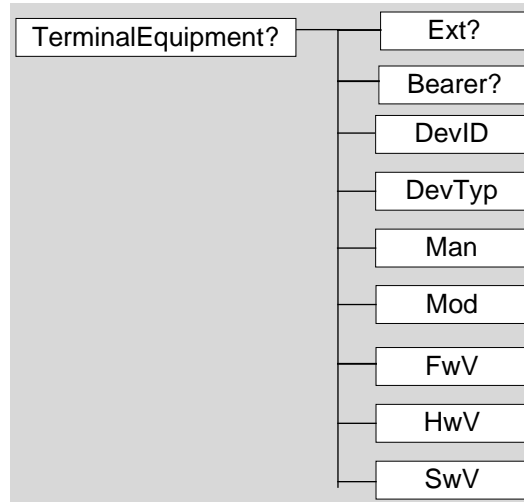


Figure 10 - Terminal Equipment

A.7.5.1 WiMAX/TerminalEquipment/Ext

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional interior node is designated to be the only branch of Terminal Equipment sub tree into which extensions can be added permanently or dynamically.

A.7.5.2 WiMAX/TerminalEquipment/Bearer

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This optional node specifies the bearer detailed information for the Terminal Equipment as defined by OMA DM. For example, it MAY contain Wi-Fi® connectivity settings.

A.7.5.3 WiMAX/TerminalEquipment/DevID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This leaf node specifies the device identifier of the Terminal Equipment. The value of this leaf node MUST be unique and formatted as a URN as defined in [27]. The value MUST be the concatenation of the node Man, the node Mod and the OEM-specific serial number of the Terminal Equipment, separated by ':'. If OEM does not supply a serial number, a GUID value in hexadecimal format MUST be used instead. The GUID value is assigned by the OMA DM client. The maximum length SHOULD be 50 characters.

Example: urn: LaptopMakerX:Model3:12345678

A.7.5.4 WiMAX/TerminalEquipment/DevTyp

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

This mandatory leaf node specifies device type of the Terminal Equipment. Possible values are including and not limited to the list in the Table 2. The maximum length SHOULD be 50 characters.

Table 2- Values for Terminal Equipment DevTyp

Type of the Device	DevType String for Population
Laptop	Laptop

Personal Media Player	PMP
Multi Mode PMP	MultiModePMP
UMPC	UMPC
Internet Tablet	InternetTablet
Gaming Device	GamingDev
Digital Camera	Digital Camera
Digital Camcorder	Digital Camcorder
Multi Mode Messaging Device	MultiModeMsgDev
E Book	EBook
Navigation Device	NavigationDev
In-Vehicle Entertainment Device	InVehicleEntDev
CPE	CPE

1 **A.7.5.5 WiMAX/TerminalEquipment/Man**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

2 This leaf node specifies the manufacturer of the Terminal Equipment. If the manufacturer of the Terminal  
3 equipment is not available this node SHALL contain the string “none”. The maximum length SHOULD be  
4 50 characters.

5 **A.7.5.6 WiMAX/TerminalEquipment/Mod**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

6 This leaf node specifies the model of Terminal Equipment. If the model of the Terminal equipment is not  
7 available this node SHALL contain the string “none”. The maximum length SHOULD be 50 characters.

8 **A.7.5.7 WiMAX/TerminalEquipment/FwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

9 This leaf node specifies the firmware version of the Terminal Equipment. Firmware refers to OEM specific  
10 SW embedded within the Terminal Equipment. If the firmware version of the Terminal Equipment is not  
11 available this node SHALL contain the value “none”. The maximum length SHOULD be 50 characters.

12 **A.7.5.8 WiMAX/TerminalEquipment/HwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

13 This leaf node specifies the hardware version of the Terminal Equipment. If the hardware version of the  
14 Terminal Equipment is not available this node SHALL contain the value “none”. The maximum length  
15 SHOULD be 250 characters.

16 **A.7.5.9 WiMAX/TerminalEquipment/SwV**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

17 This leaf node value SHALL be the concatenation of the current operating system name, the operating  
18 system version, and the operating system architecture of the Terminal Equipment separated by “:” or “.” as  
19 follows: OS\_Name:OS:OS\_Architecture (for example, Windows:XP:X86 or Windows.XP.X86). If the  
20 Operating System version of the Terminal Equipment is not available this node SHALL contain the string  
21 “none”. The maximum length SHOULD be 50 characters.

**A.7.5.10 WiMAX/TerminalEquipment/EmbeddingPlatformCertificationID**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	One	32 ASCII char	Get

This leaf node represent the embedding platform certification ID and is used by the MS when generating the platform certification ID part of the IPID that is provide by the MS as part of the NAI during network entry.

Its value is either derived from the TerminalEquipment values or pre-configured with a value that is assigned by WCB as part of the CVS certification process. In any case, it will be an ASCII string of 32 2-hex digits (a total of 64 characters).

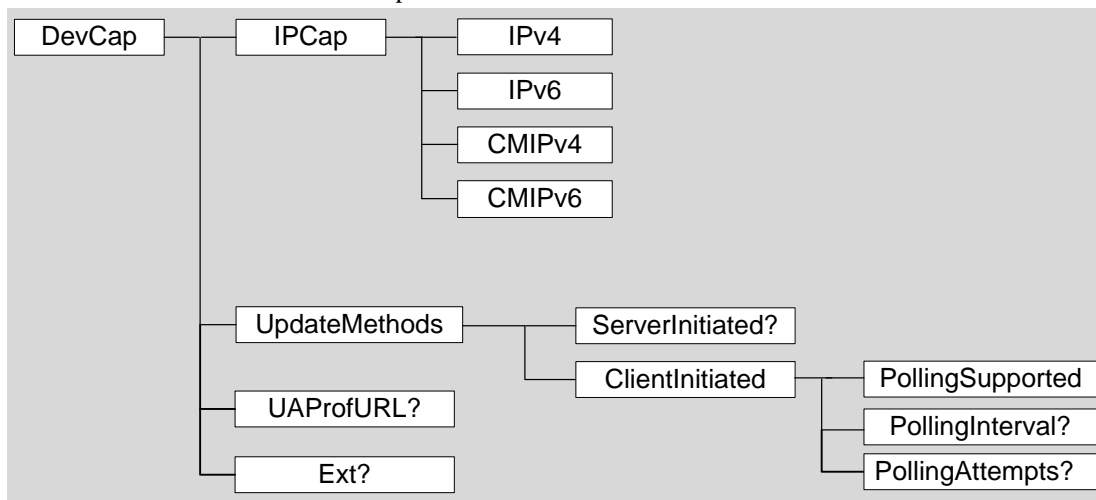
Its value is derived from the TerminalEquipment MO, the following algorithm is applied:

- The TerminalEquipment/Man value is concatenated with the TreminalEquipment/Mod generating one ASCII string (the Man part in the left hand side).
- This value is used as an input to a SHA-256 hash function generating a 32 byte value.
- This value is converted into a HEX string where each byte value is represented by a 2 digit hex string.

**A.7.6 WiMAX® Device Capabilities**

The nodes covered in this sub-section specify the different feature capabilities of the WiMAX device in order to assist the provisioning entity on the network in determining what features and associated parameters can and will be provisioned into the device. Figure 10 shows the structure of the DevCap MO.

Please note that additional capability information MAY be added to this node in the future. Figure 11 shows the structure of the DevCap MO.



**Figure 11 - WiMAX Device Capabilities**

**A.7.6.1 WiMAX/DevCap/IPCap**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains IP specific WiMAX device capability information.

1 **A.7.6.2 WiMAX/DevCap/IPCap/IPv4**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

2 This leaf node specifies if the WiMAX device is capable of supporting IPv4. 'TRUE' means that IPv4 is  
3 supported and 'FALSE' means that IPv4 is not supported.

4 **A.7.6.3 WiMAX/DevCap/IPCap/IPv6**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

5 This leaf node specifies if the WiMAX device is capable of supporting IPv6. 'TRUE' means that IPv6 is  
6 supported and 'FALSE' means that IPv6 is not supported.

7 **A.7.6.4 WiMAX/DevCap/IPCap/CMIPv4**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

8 This leaf node specifies if the WiMAX device is capable of supporting CMIPv4. 'TRUE' means that  
9 CMIPv4 is supported and 'FALSE' means that CMIPv4 is not supported.

10 **A.7.6.5 WiMAX/DevCap/IPCap/CMIPv6**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

11 This leaf node specifies if the WiMAX device is capable of supporting CMIPv6. 'TRUE' means that  
12 CMIPv6 is supported and 'FALSE' means that CMIPv6 is not supported.

13 **A.7.6.6 WiMAX/DevCap/UAProfURL**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get

14 This leaf node specifies the URL of the device capabilities via using [29], as specified in [29]. The  
15 maximum length SHALL be 1024 characters.

16 **A.7.6.7 WiMAX/DevCap/UpdateMethods**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

17 This interior node contains device capabilities related to continuous management method.

18 **A.7.6.8 WiMAX/DevCap/UpdateMethods/ServerInitiated**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Bool	Get

19 This leaf node specifies whether the device is capable of receiving Notification Initiated Session Trigger  
20 Messages sent by the OMA DM server [5]. If the value is 'FALSE', the device does not support server-  
21 initiated DM session. If the value is 'TRUE', the device supports server-initiated DM session. When this  
22 node does not exist, device behavior is the same as if the value was 'FALSE'.

23 **A.7.6.9 WiMAX/DevCap/UpdateMethods/ClientInitiated**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

24 This interior node contains information about the device's polling-based client-initiated DM capability.  
25 A device with this capability should generate a unique SessionID, as described in [6], where maximum  
26 value of SessionID SHALL NOT exceed 65535.

1 **A.7.6.10 WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingSupported**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get

2 This interior node specifies whether the device supports continuous management using client-initiated  
3 periodic polling. When the value is TRUE, the device supports client-initiated polling. If this node is not  
4 present then it is the same as being FALSE.

5 **A.7.6.11 WiMAX/DevCap/UpdateMethods/ClientInitiated/PollingInterval**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get

6 This leaf node specifies the device recommended value for the polling interval. This value MAY be used  
7 by the operator to configure its polling interval value. This value is presented in number of minutes. The  
8 value of this node is interpreted in the same way as WiMAXSupp/Operator/<X>/NetworkParameters/  
9 PollingInterval node in Section A10.4.7.6. When this node does not exist, device behavior is the same as if  
10 the value was zero. This OPTIONAL node MAY NOT exist if the 'PollingSupported' is FALSE.

11 **A.7.6.12 WiMAX/DevCap/UpdateMethodes/ClientInitiated/PollingAttempts**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get

12 This leaf node specifies the recommended value for polling attempts as set by the manufacturer. This value  
13 may be used by the manufacturer to configure the number of times the device will attempt to access client-  
14 initiated polling at a periodic interval. This value represents the number of times the device shall perform  
15 client-initiated polling after the initial poll.

16 It is recommended that this parameter be set to a value that will continue client polling for at least 30  
17 minutes. For example if the polling interval is set to 5 then polling attempts should be set to 5. Devices will  
18 make the first attempt after the first polling interval has expired and continue n times where n is the number  
19 of polling attempts. Setting polling attempts to a value of -1 will indicate that the MS should poll  
20 continuously. Setting the value of polling attempts to 0 will cause a device to never poll and this should  
21 never be set in the DevCap node. If it is desired by an operator that the device SHOULD never perform  
22 client initiated polling it should be set in the  
23 WiMAXSupp/Operator/<X>/NetworkParameters/PollingAttempts node of the operator.

24 This OPTIONAL node MAY NOT exist if the 'PollingSupported' is FALSE.

26 **A.7.6.13 WiMAX/Ext**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

27 This optional interior node is designated to be the only branch of DevCap sub-tree into which vendor-  
28 specific extensions can be added.

29 **A.8 WiMAX<sup>®</sup> Supplementary MO**

30 **A.8.1 Introduction**

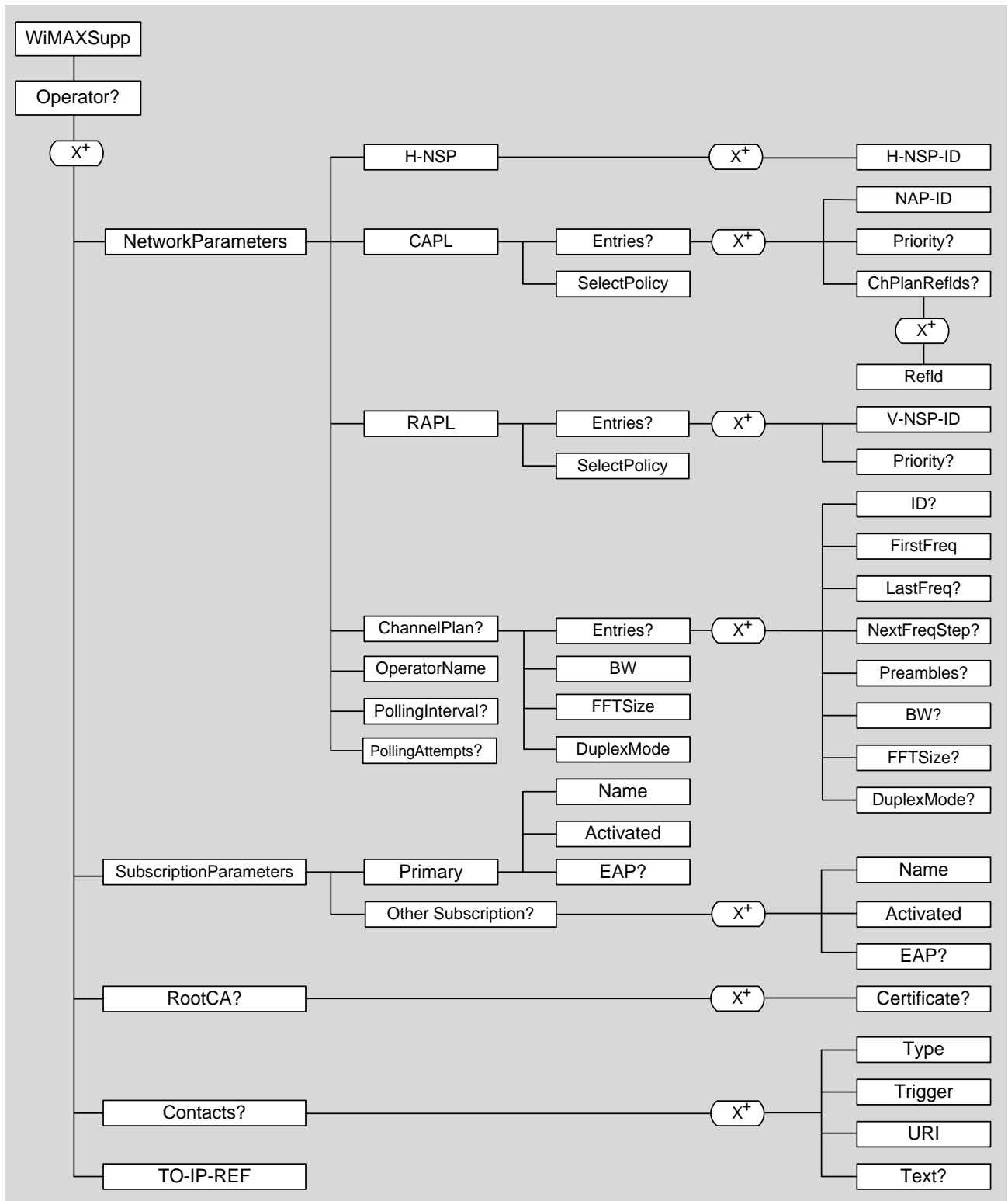
31 The WiMAX<sup>®</sup> Supplementary object facilitates management of WiMAX parameters.

32 The MO Identifier for the WiMAXSupp MUST be: "urn:wmf:mo:wimax-supp-mo:1.0"

33 **A.8.2 Graphical Representation**

34 Figure 12 provides the structure of WiMAX Supplementary MO.

1



2  
3

4

5

Figure 12 - WiMAX® Supplementary MO Tree Structure

1 **A.8.3 Node Descriptions**

2 **A.8.3.1 WiMAXSupp/Operator**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

3 This mandatory interior node lists the operator specific WiMAX parameters. See Section A.8.4 for further  
4 details.

5 **A.8.4 Operator Node**

6 **A.8.4.1 WiMAXSupp/Operator/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

7 This interior node distinguishes the different operator object and parameters. There MUST be exactly one  
8 operator node for each of these interior nodes.

9 **A.8.4.2 WiMAXSupp/Operator/<X>/NetworkParameters**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

10 This interior node contains the WiMAX network specific parameters like roaming lists, Channel Plans and  
11 home network information. See Section A.8.4.7 for further details.

12 **A.8.4.3 WiMAXSupp/Operator/<X>/SubscriptionParameters**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

13 This interior node contains the WiMAX subscription parameters like user authentication types and  
14 parameters. See Section A.8.4.8 for further details.

15 **A.8.4.4 WiMAXSupp/Operator/<X>/RootCA**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

16 This interior node contains the additional root CAs trusted by operator and is used by the device to  
17 authenticate the operator's networks. See Section A.8.4.9 for further information.

18 **A.8.4.5 WiMAXSupp/Operator/<X>/Contacts**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

19 This interior node contains multiple groups of contact addresses. Each group can be used to connect the  
20 user to different network or administrative function, such as emergency, subscription purchasing or  
21 technical support. See Section A.8.4.10 for further information.

22 **A.8.4.6 WiMAXSupp/Operator/<X>/TO-IP-REF**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

23 This interior node contains a path to the IP MO. The IP MO defines parameters for WiMAX connectivity.  
24 The IP MO is defined in [15]. See Section B.2 for further details.

25 **A.8.4.7 Network Parameters Node**

26 Network parameters node defines a set of nodes used by the device during network discovery and selection  
27 procedures, as defined in [21].

28 **A.8.4.7.1 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the H-NSP parameters. See Section A.8.4.7.8 for further details.

**A.8.4.7.2 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the CAPL. The list contains the NAP-IDs, who have direct relationship with the H-NSP. See Section A.8.4.7.9 for further details.

Figure A-1 in [20] clarifies how the business relationships are handled between subscriber, NAPs and NSPs in WiMAX.

**A.8.4.7.3 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the RAPL. The list contains the Visited Network Service Providers (V-NSP), who have direct relationship with the H-NSP. See Section A.8.4.7.10 for further details.

Figure A-1 in [20] clarifies how the business relationships are handled between subscriber, NAPs and NSPs in WiMAX.

**A.8.4.7.4 WiMAXSupp/Operator/<X>/NetworkParameters/OperatorName**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Add, Replace

This leaf node defines the human readable name of the operator, e.g., “Operator”. In the case that the “activated” node is FALSE, the operator name received from the WiMAX Medium Access Control (MAC) layer, NSP verbose name MAY be used to overwrite the value provided in the OperatorName node. The MIME type of the node SHALL be ‘text/plain; charset=utf-8’. The maximum length SHOULD be 255 bytes. In utf-8 format, each character MAY take one to four bytes.

**A.8.4.7.5 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains a Channel Plan, which holds such information as frequencies and channel BWs. The Channel Plan is used for optimizing the time used in network search. The WiMAX Forum Mobile Profile [22] defines how the Channel Plan information is mapped to the band classes. See Section A.8.4.7.11 for further details.

**A.8.4.7.6 WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies how frequently the OMA DM client SHOULD connect to the OMA DM server for polling-based client-initiated management sessions. It is only used for those devices that cannot receive server-initiated sessions. This value is presented in number of minutes.

- 1) If the value is “-1” (minus 1), then the device SHALL perform ONLY ONE polling-based client-initiated management session to the OMA DM server whenever entering the operator’s network and obtaining an IP address. The device will immediately poll and the value of PollingAttempts SHALL be ignored.
- 2) If the value is “0” (zero), then the device SHALL NOT perform any polling based client-initiated management session to the OMA DM server.

- 3) If the value is greater than zero, then the device SHALL perform a polling-based client-initiated management session to the OMA DM server every “X” minutes (the value specified in this leaf node), starting with one poll immediately after the device obtains an IP address from the operator’s network and continuing for n+1 iterations where n is the value of polling attempts. As an example if this is set to 5 and polling attempts is set to 10 the device will poll once after receiving an IP address and 10 times at 5 minute interval for a total of 11 attempts.

**A.8.4.7.7 WiMAXSupp/Operator/<X>/NetworkParameters/PollingAttempts**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the value for number polling attempts as set by the operator and it supersedes the value set in the device capabilities node set by the manufacturer. This value may be used by the operator to configure the number of times the device will attempt to access client-initiated polling at a periodic interval after the initial polling attempt. As an example if this is set to 10 and PollingInterval is set to 5 the device will poll once after receiving an IP address and 10 times after for a total of 11 attempts. Setting polling attempts to a value of -1 will indicate that the MS shall poll continuously. Setting the value of PollingAttempts to 0 will cause a device to never poll. This OPTIONAL node MAY NOT exist if the ‘PollingSupported’ is FALSE.

**A.8.4.7.8 H-NSP Node**

This node specifies the H-NSP. All the Home Network Service Provider Identifiers (H-NSP-ID) of a single H-NSP are mapped into one NSP realm and one NSP verbose name, since the NSP is selected via the realm in the Network Access Identifier (NAI) and the WiMAXSupps MOs contain only one realm in the subscription parameters.

**A.8.4.7.8.1 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node contains the H-NSP information. All of these interior nodes MUST be located in one H-NSP node.

**A.8.4.7.8.2 WiMAXSupp/Operator/<X>/NetworkParameters/H-NSP/<X>/H-NSP-ID**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the H-NSP-ID. The format of the NSP-ID is specified in [21] and 24-bit long. All NSP-IDs have the same priority.

**A.8.4.7.9 CAPL Node**

The information in this node is used in network discovery and selection phase. The node instructs which NAP SHALL be selected to establish connection to the home network. APPENDIX C represents examples how the nodes are used in network discovery and selection.

**A.8.4.7.9.1 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/SelectPolicy**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies NAP Selection Policy (defined in [Annex E.]) that SHALL be respected for CAPL. Table 3 defines the possible values for SelectPolicy node.

**Table 3 - Values for NAP Selection Policy node of CAPL**

Value	NAP Selection Policy
0	Reserved.
1	Strict Policy (defined in [32])

Value	NAP Selection Policy
2	Partially Flexible Policy (defined in [32])
3	Fully Flexible Policy (defined in [32])

**A.8.4.7.9.2 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries of CAPL.

**A.8.4.7.9.3 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of the CAPL.

**A.8.4.7.9.4 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/NAP-ID**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the NAP-ID. The format of the NAP ID is 24 bit-long integer and specified in [21].

**A.8.4.7.9.5 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/Priority**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the Priority (defined in [32]) of the NAP. Table 4 shows the possible values of the priority.

**Table 4 - Values of priority in CAPL node**

Value	Description
0	Reserved.
1	Highest priority value.
2-249	Values for other priorities.
250	Lowest priority value
251-254	Reserved.
255	Forbidden. Device is not allowed use this NAP to connect to the H-NSP.

**A.8.4.7.9.6 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanReflds**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Node	Get

This interior node allows an operator to associate one or more Channel Plan entries to a NAP and specifies a NAP Based Channel Plan for a specific NAP. See [32] for more information about NAP Based Channel Plan.

**A.8.4.7.9.7 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanReflds/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of reference IDs linking to Channel Plan entries.

**A.8.4.7.9.8 WiMAXSupp/Operator/<X>/NetworkParameters/CAPL/Entries/<X>/ChPlanReflds/<X>/Refld**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Add, Replace

This leaf node specifies a reference ID to a Channel Plan entry identified by ID located at WiMAXSuppMO/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Id. The maximum length SHALL be 20 characters.

#### A.8.4.7.10 RAPL Node

The information provided in these nodes are used in network discovery and selection phase for roaming when NAPs, which have direct connection to the H-NSP, are not available. The nodes specify which V-NSP are allowed to be used. APPENDIX C represents examples how the nodes are used in network discovery and selection.

##### A.8.4.7.10.1 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/SelectPolicy

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies V-NSP Selection Policy (defined in [32]) that SHALL be respected for RAPL. Table 5 defines the possible values for SelectPolicy node.

**Table 5 - Values for V-NSP Selection Policy Node of RAPL**

Value	V-NSP Selection Policy
0	Reserved.
1	Strict Policy (defined in [32])
2	Partially Flexible Policy (defined in [32])
3	Fully Flexible Policy (defined in [32])

##### A.8.4.7.10.2 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries of RAPL.

##### A.8.4.7.10.3 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a place holder of the RAPL.

##### A.8.4.7.10.4 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/V-NSP-ID

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the V-NSP-ID. The format of the NSP ID is 24 bit-long integer and specified in [21].

##### A.8.4.7.10.5 WiMAXSupp/Operator/<X>/NetworkParameters/RAPL/Entries/<X>/Priority

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the Priority (defined in [32]) of the V-NSP. Table 6 shows the possible values of the priority.

**Table 6 - Value of priority in RAPL node**

Value	Description
-------	-------------

0	Reserved.
1	Highest priority value.
2-249	Values for other priorities.
250	Lowest priority value
251-254	Reserved.
255	Forbidden. Device is not allowed to use this V-NSP to connect to the H-NSP.

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

**A.8.4.7.11 Channel Plan Node**

Channel Plan node specifies Channel Plan configurations that can be used in network discovery and selection procedure. It is up to the service provider how to populate the Channel Plans. More information on different kind of Channel Plans and their usage can be found from [32].

**A.8.4.7.11.1 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

This interior node contains the entries for Channel Plan

**A.8.4.7.11.2 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/BW**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the default BW value in kHz for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/BW does not specify any value for BW, this value SHALL be used.

**A.8.4.7.11.3 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/FFTSize**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the default FFT size for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/FFTSize does not specify any value for FFT size, this value SHALL be used.

**A.8.4.7.11.4 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/DuplexMode**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the default duplex modes for all the Channel Plan entries. If /ChannelPlan/Entries/<X>/DuplexMode does not specify any value for DuplexMode, this value MUST be used. See the possible values in the Section A.8.4.7.11.5.9.

**A.8.4.7.11.5 Channel Plan Entries**

Channel Plan information is used in the network discovery and selection procedures. All Channel Plan entries are part of the Root Channel Plan. The entries of Root Channel Plan SHALL be in preferred order. It is recommended to design Channel Plan entries in a way that the same physical information is not defined in multiple entries.

**A.8.4.7.11.5.1 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of the channels or channel-ranges of the Channel Plan.

**A.8.4.7.11.5.2 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/ld**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Add, Replace

This leaf node allows an operator to associate a Channel Plan entry to one or more NAPs. References to Channel Plan entries within CAPL are specified in /CAPL/Entries/<X>/ChPlanRefIds node. Entries which are referred to are part of one or more NAP Based Channel Plans. One Channel Plan entry can be associated with multiple NAPs. This optional node MUST be supported by the client that supports NAP Based Channel Plan (i.e. /CAPL/Entries/<X>/ChPlanRefIds). See APPENDIX C for recommendation on implementation details. The maximum length SHALL be 20 characters.

#### A.8.4.7.11.5.3 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FirstFreq

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node specifies the first center frequency (in kHz) for this channel range.

#### A.8.4.7.11.5.4 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/LastFreq

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the last center frequency (in kHz) for this channel range. If this value equals to the FirstFreq or the node is omitted, then this entry refers to a single channel rather than a channel range. If this field is present, NextFreqStep field SHALL be present as well.

#### A.8.4.7.11.5.5 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/NextFreqStep

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node defines the frequency step (in kHz) to reach the next central frequency when defining the frequency range using FirstFreq and LastFreq. When the node is omitted there is only one central frequency in this entry that is FirstFreq. If this field is present, LastFreq field SHALL be present as well.

The formula to calculate the next central frequencies is:

$$\text{CurrentFreq} = \text{FirstFreq}$$

$$\text{While } (\text{CurrentFreq} \leq \text{LastFreq}) \text{ CurrentFreq} = \text{CurrentFreq} + \text{NextFreqStep}$$

#### A.8.4.7.11.5.6 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/Preambles

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Add, Replace

A bitmap of 114 bits specifying the valid preambles for each channel in this channel range

The value is a hexadecimal string, which is 29 digit long. The two MSB are zeroed and the LSB indicates channel 0.

#### A.8.4.7.11.5.7 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/BW

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the individual channel BW (in kHz) for the channel in this entry.

Note: The client uses this value for the BW for this specific channel entry instead of the default BW value specified in /ChannelPlan/BW.

#### A.8.4.7.11.5.8 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries/<X>/FFTSIZE

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the size of the channel's FFT in this entry.

Note: The client uses this value for the FFT size for this specific channel entry instead of the default FFT size value specified in /ChannelPlan/FFTSize

#### A.8.4.7.11.5.9 WiMAXSupp/Operator/<X>/NetworkParameters/ChannelPlan/Entries <X>/DuplexMode

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Int	Get, Add, Replace

This leaf node specifies the duplex mode of the channel in this entry. Table 7 defines the values of the DuplexMode.

Note: The client uses this value for the duplex mode for this specific channel entry instead of the default duplex mode value specified in /ChannelPlan/DuplexMode.

**Table 7 - Values of Duplex Mode node**

Value	Description
0	Reserved
1	TDD
2	FDD
3	HFDD
4-255	Reserved

#### A.8.4.8 Subscription Parameters Node

The subscription parameter interior node contains information associated with user subscription. A user is allowed to have more than one subscription with an operator. This node enables a user and the operators to manage authentication parameters that are associated with user's subscriptions. The decision of which subscription parameters are used during network entry authentication is out of the scope of this specification.

##### A.8.4.8.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

This interior node contains the primary subscription parameters. See Section A.8.4.8.3 for further details.

##### A.8.4.8.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions

Status	Tree Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	Node	Get

This interior node contains the subscription parameters, which are associated with additional subscriptions present on the device. See Section A.8.4.8.4 for further details.

##### A.8.4.8.3 Primary Subscription parameters

This interior node contains the primary subscriber parameters.

##### A.8.4.8.3.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Name

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Add, Replace

This leaf node specifies the human readable name of the primary subscriber. The operator SHALL assure the human readable name of the primary subscriber is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

The MIME type of the node SHALL be 'text/plain; charset=utf-8'. The maximum length SHALL be 255 bytes. In UTF-8 format, each character MAY take one to four bytes.

#### A.8.4.8.3.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/Activated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get, Add, Replace

This leaf node indicates the provisioning status of the Primary Subscriber. If the value of the node is FALSE, the device SHALL enter the network in the provisioning mode when using primary subscription, by providing a WiMAX decorated NAI during the EAP negotiation that indicates the provisioning service mode as described in [23] section 8.2. Upon completion of the provisioning phase, the OMA DM server SHALL set the value to TRUE to indicate that the device SHALL use regular network entry using the provisioned parameters. As long as this leaf node value is true, all provisioned parameters should be considered by the device as the most updated parameters hence the device should first use the provisioned operator name and subscription parameters for its normal operation and only afterwards can use other alternative sources for the same parameters, if needed, such as 802.16 MAC messages. This node SHALL be included into the last OMA DM Package message from the Device Management Server to the device. When this node is sent to the device, it is able to know that all configurations are uploaded to the device.

The point of time when the OMA-Session, in which this node was set, was completed is considered as the completion point of provisioning phase by the device. (if the device needs to trigger something at the end of activation, it will use this point as the trigger).

#### A.8.4.8.3.3 WiMAXSupp/Operator/<X>/SubscriptionParameters/Primary/EAP

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

The EAP interior node contains parameters for EAP authentication methods. It contains EAP MO as specified in [14]. Only a single EAP method is allowed to be configured for the MS to use with a specific operator. In the case it is a tunneled method (such as TTLS): the definition shall include the outer and the inner method nodes.

See B.1 for further details. In case EAP node is not populated, authentication is not performed.

#### A.8.4.8.4 Other Subscription Parameters

This interior node contains subscription parameters, which are associated with additional subscriptions present on the device.

##### A.8.4.8.4.1 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node lists the entries in the Other Subscription Parameters. There MUST be exactly one OtherSubscriptions node for each of these interior nodes.

##### A.8.4.8.4.2 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Name

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Add, Replace

This leaf node defines the human readable name of an additional subscription. The operator SHALL assure the human readable name of the additional subscription is unique from all other subscriptions of the same operator, so that the operator can differentiate between subscriptions.

The MIME type of the node SHALL be 'text/plain; charset=utf-8'. The maximum length SHALL be 255 bytes. In UTF-8 format, each character MAY take one to four bytes.

##### A.8.4.8.4.3 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/Activated

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bool	Get, Add, Replace

This leaf node indicates the provisioning status of Other Subscriber. If the value of the node is FALSE, the device SHALL enter the network in the provisioning mode when using this subscription data, i.e., by providing a WiMAX decorated NAI during the EAP negotiation that indicates the provisioning service mode as described in [23] section 8.2. Upon completion of the provisioning phase, the OMA DM server SHALL set the value to TRUE to indicate that the device SHALL use regular network entry using the provisioned parameters. As long as this leaf node value is true, all provisioned parameters should be considered by the device as the most updated parameters hence the device should first use the provisioned operator name and subscription parameters for its normal operation and only afterwards can use other alternative sources for the same parameters, if needed, such as 802.16 MAC messages.

The point of time when the OMA-Session, in which this node was set, was completed is considered as the completion point of provisioning phase by the device. (if the device needs to trigger something at the end of activation, it will use this point as the trigger).

**A.8.4.8.4.4 WiMAXSupp/Operator/<X>/SubscriptionParameters/OtherSubscriptions/<X>/EAP**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	ZeroOrOne	Node	Get

The EAP interior node contains parameters for EAP authentication methods. It contains EAP MO as specified in [14]. Only a single EAP method is allowed to be configured for the MS to use with a specific operator. In the case it is a tunneled method (such as TTLS): the definition shall include the outer and the inner method nodes.

See B.1 for further details. In case EAP node is not populated authentication is not performed.

**A.8.4.9 RootCA Node**

The RootCA node contains an additional list of trusted rootCA certificates to be used during mutual authentication between the device and the network. Since the RootCA node is defined under each operator, the following practices MUST be followed:

1. For Operators:

1.1. The operator SHOULD send its trusted rootCA certificates at the end of the initial activation and provisioning flow.

1.2. The operator SHOULD update the list of trusted rootCA certificates to ensure that the device does not lose its capability to validate the network (AAA server) due to the lack of proper CA certificates.

2. For Devices:

2.1. The used root CA certificates MUST be specified by the CERT nodes of the current operator's effective EAP MO [14] in a normal network entry which uses provisioned information. The device MUST NOT use any other root CA certificates.

2.2. The device MUST EITHER use:

2.2.1. RootCA certificates embedded in the device at the point of manufacturing (POM), OR

2.2.2. The RootCA node's certificates in the mutual authentication between the device and the network (AAA server).

**A.8.4.9.1 WiMAXSupp/Operator/<X>/RootCA/<X>**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of the additional root CA Certificates trusted by a specific operator.

**A.8.4.9.2 WiMAXSupp/Operator/<X>/RootCA/<X>/Certificate**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Bin	No Get

This leaf node contains the actual binary Root Certificate. The format of Root CA SHALL be X.509 and DER.

#### A.8.4.10 Contacts Node

This node contains a number of contact info nodes an operator MAY wish to make available to its subscribers. Two types, one for technical support and another for subscription portal, are mandatory, others are available for use by operators.

##### A.8.4.10.1 WiMAXSupp/Operator/<X>/Contacts/<X>

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	OneOrMore	Node	Get, Add, Delete

This interior node is a placeholder of multiple support contact addresses.

##### A.8.4.10.2 WiMAXSupp/Operator/<X>/Contacts/<X>/Type

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Int	Get, Add, Replace

This leaf node defines a URI contact type that will be made visible to the user.

**Table 8 - Values of URI Type**

Value	Availability	Description
0	Reserved	Mandatory contact node for the operator's technical support contact information.
1	Reserved	Mandatory contact node for operator's subscription portal contact information.
2 – 199	Reserved	Reserved for future use.
200 -255	Available	Operator defined URI types (e.g., My account, FAQ, etc.)

##### A.8.4.10.3 WiMAXSupp/Operator/<X>/Contacts/<X>/Trigger

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Null	Exec

This leaf node specifies a trigger to start the contact action or process. The client device SHOULD indicate to a user interface application that there is a message waiting for the user. The user interface application SHOULD, upon receipt of user approval, execute the URI within the context of the device.

For example, if the device is a laptop the user interface application MAY launch the default web browser for a "http://" prefixed URI or MAY launch a VoIP client application for a "sip://" prefixed URI.

The types of actionable URI prefixes are outside the scope of this specification and are implementation specific.

The execution of the URI-based contact action or process SHALL be performed either synchronously as part of the current DM session (i.e., run to completion before executing the next DM operation or terminating the current DM session) or asynchronously from the current DM session (i.e., run in parallel with the DM session continuing to execute the next DM operations and/or terminating the current DM session). After execution of the URI-based contact action or process, the client MAY issue a generic alert, as described in [6], to the DM server indicating the result of the contact action or process after it completes or fails. The URI of the WiMAX Supplementary MO SHALL be sent as the source element of the generic alert in order to allow the DM server to identify the origin of the alert. The definition of the alert type returned as the meta type element in the generic alert is beyond of scope of this document but MAY be defined in future revisions of this spec.

##### A.8.4.10.4 WiMAXSupp/Operator/<X>/Contacts/<X>/URI

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get, Add, Replace

1 This leaf node specifies a contact address in URI format.

2 The URI string will most often be a telephone number (e.g., tel:+ 911), a SIP VoIP contact (e.g.,  
 3 sip:alice@wonderland.com) or a URL (e.g., http://wireless.com/TechnicalSupport). Other URI resource  
 4 types MAY be specified, but the device MAY NOT implement support for all URI formats. The maximum  
 5 length SHALL be 1024 characters.

6 **A.8.4.10.5 WiMAXSupp/Operator/<X>/Contacts/<X>/Text**

Status	Tree Occurrence	Format	Min. Access Types
OPTIONAL	ZeroOrOne	Chr	Get, Add, Replace

7 This leaf node specifies a simple string that can be displayed to the user for the given contact type. For  
 8 example this could be “Technical Support” or “Subscription Portal”. The maximum length SHOULD be  
 9 255 characters.

10

## APPENDIX B. OMA Connectivity Management Objects [Normative]

### B.1 OMA EAP Management Object

This section describes how the generic EAP MO [14] is used in WiMAX<sup>®</sup>. The statuses and descriptions of the nodes are modified according to the following table to fit the generic EAP MO to the WiMAX needs. The definitions for the usage of the nodes listed in this table **MUST** be followed. The non-listed nodes **MUST** be used as specified in [14].

This section defines the EAP MO usage and configuration for different EAP methods but does not define whether a method is optional or mandatory to implement.

The definition of the mandatory supported Methods are as defined in [21].

Node	Status	Comment
EAP/<X>/METHOD-TYPE	[14]	See the node description [14]. The node can be used for referring to EAP methods which do not require using expanded EAP type identifiers, e.g. EAP-TLS, EAP-TTLS, and EAP-AKA.
EAP/<X>/VENDOR-ID	[14]	See the node description [14]. The node <b>MUST</b> be used for Plain-MSCHAPV2. VENDOR-ID <b>MUST</b> be 24757 (WMF) for Plain-MSCHAPV2.
EAP/<X>/VENDOR-TYPE	[14]	See the node description [14]. The node <b>MUST</b> be used for Plain-MSCHAPV2. VENDOR-TYPE <b>MUST</b> be 1 for Plain-MSCHAPV2.
EAP/<X>/PASSWORD	[14]	See the node description [14]. The maximum length in WiMAX is 253 characters. <b>REQUIRED</b> for Plain-MSCHAPv2.
EAP/<X>/PROVISIONED-PSEUDO-IDENTITY	[14]	In WiMAX this leaf node contains the provisioned pseudonym identity to be used in the first network entry, when EAP-AKA is used for the user authentication. When this node is present, the provisioned pseudonym identity <b>SHALL</b> be used and the permanent identity <b>SHALL NOT</b> be sent to the network during the first authentication. If this node is not present then the permanent identity is used for the first authentication.

Node	Status	Comment
EAP/<X>/USE-PRIVACY	[14]	<p>In WiMAX EAP-AKA, there are two possible ways the device can operate upon receipt of a permanent identity request from the AAA server [RFC 4187 Section 4.1.6]. This leaf node defines which way the device SHALL perform upon that request, i.e., AT_PERMANENT_ID_REQ. If the value of this node is TRUE and if the device has a pseudonym identity available then the permanent identity SHALL NOT be sent to the network even if it is explicitly requested by the server. If this node is FALSE or missing, then the permanent identity SHALL be sent to the network when the permanent identity is requested by the server. If the device has no pseudonym identity available then the permanent identity SHALL be sent to the network when requested, regardless of this node.</p> <p>In other WiMAX EAP methods excluding EAP-TLS, e.g., EAP-TTLS, if this node is TRUE then the device SHALL use a randomly generated username in outer EAP-Response/Identity. If this node is FALSE or missing then any type of identity conforming to each EAP method can be used.</p> <p>Realm portion of the NAI (Network Access Identified) is still required to route authentication to the home network in all cases.</p>
EAP/<X>/EAP-AKA/USE-CHECKCODE	REQUIRED	In WiMAX, if USE-CHECKCODE is TRUE then AT_CHECKCODE SHALL be included in EAP-Response/AKA-Challenge or EAP-Response/AKA-Reauthentication message. If this is FALSE or missing then AT_CHECKCODE is not sent by the device. However, regardless of this node, AT_CHECKCODE MUST be used when new attributes are included in EAP-Request/AKA-Identity or EAP-Response/AKA-Identity message [RFC 4187 Chapter 8.2].
EAP/<X>/ VFY-SERVER-REALM	REQUIRED for EAP_TLS and EAP_TTLS	<p>In WiMAX:</p> <p>If this node is omitted or set to TRUE the MS SHALL verify the server realm in the certificate as defined in [21].</p> <p>If this node is set to FALSE – the MS SHALL skip realm verification.</p>
EAP/<X>/CERT	REQUIRED	See the node description [14].
EAP/<X>/CERT/<X>/CERT-TYPE	[14]	<p>See the node description [14].</p> <p>At least DEVICE and CA certificate types are REQUIRED in WiMAX.</p>
EAP/<X>/CERT/<X>/SER-NUM	REQUIRED	See the node description [14].
EAP/<X>/CERT/<X>/ISSUER	REQUIRED	See the node description [14].

1  
2 The following table includes the WiMAX forum definition of VENDOR-ID and VENDOR-TYPE for the different  
3 inner Methods:

Method	Vendor-ID	Vendor-TYPE
PLAIN MSCHAPv2	24757 (WMF)	1

PLAIN CHAP	24757 (WMF)	2
Reserved	24757 (WMF)	3-239
Vendor specific type	24757 (WMF)	240-255

1 For model B devices – the nodes must be populated with the values in the table for the specified inner methods.

2

### 3 **B.1.1 Method Related Parameters**

4 The following Table 9 provides an overview of the EAP settings used together with each EAP Method.

5

**Table 9 - EAP Method versus Used Parameters**

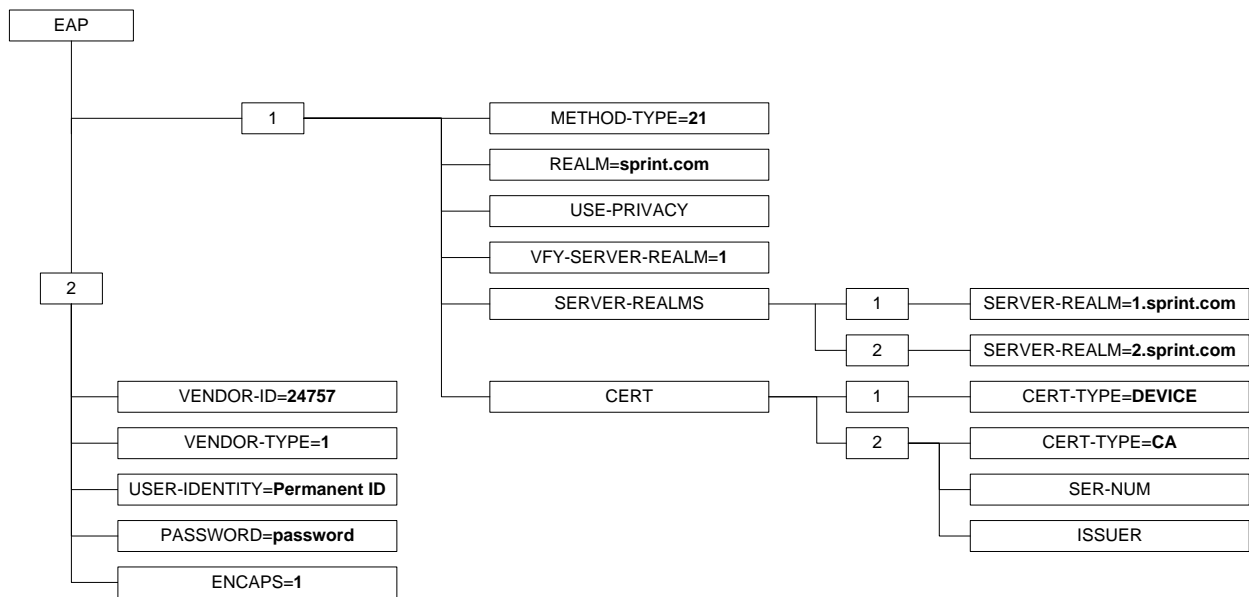
EAP Method/Used Parameters	EAP-AKA	EAP-TLS	EAP-TTLS	PLAIN-MSCHAPv2	Plain CHAP
METHOD-TYPE	X	X	X		
VENDOR-ID				X	X
VENDOR-TYPE				X	X
USER-IDENTITY	X	X	X	X	X
PASSWORD				X	X
REALM	X	X	X		
PROVISIONED-PSEUDO-IDENTITY	X				
USE-PRIVACY	X	X	X		
EAP-AKA/USE-CHECKCODE	X				
ENCAPS	X	X		X	X
VFY-SERVER-REALM		X	X		
SERVER-REALMS/<X>/SERVER-REALM		X	X		
CA-CERT					
CERT-TYPE		X	X		
ISSUER		X	X		
SER-NUM		X	X		
DEVICE-CERT					
CERT-TYPE		X	X		

6

7

1 **B.1.2 Example: EAP-TTLSv0 and Plain-MSCHAPv2**

2 Figure 13 illustrates how EAP-TTLSv0 and PLAIN-MSCHAPv2 parameters can be used and linked together using  
 3 the ENCAPS node.



4

5 **Figure 13 - Example of EAP-TTLSv0 and PLAIN-MSCHAPv2 parameters**

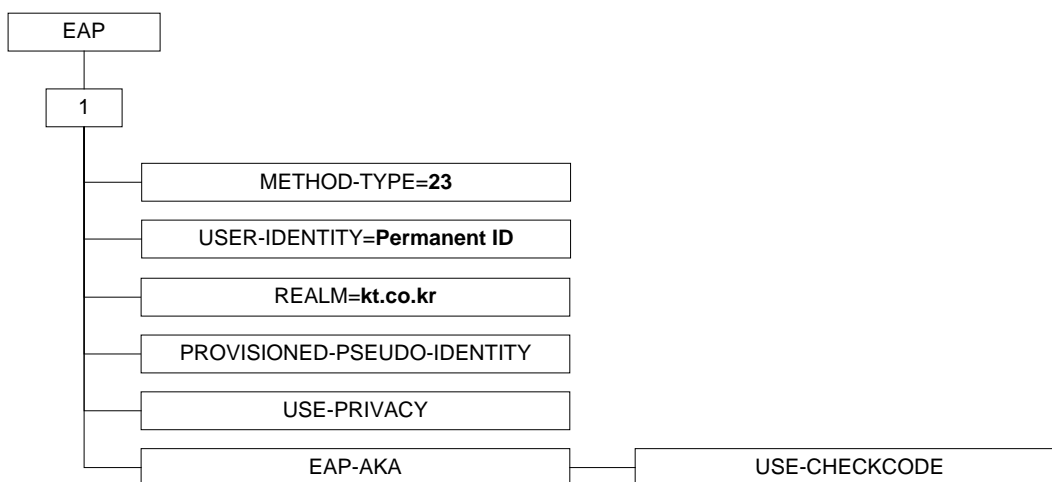
6 Example: EAP-TLS, EAP-TTLSv0 and Plain-MSCHAPv2

7 In the case the device falls back from TTLS to TLS as defined in NWGSTG3 4.4.1.4.1.1.1 – all the parameters for  
 8 the TLS authentication will be taken from the TTLS node which is node number 1 in this example.

9

10 **B.1.3 Example: EAP-AKA in Stand alone Mode**

11 Figure 14 illustrates an example of how the leaf nodes can be constructed in the EAP node when the EAP-AKA is  
 12 used for the user authentication.

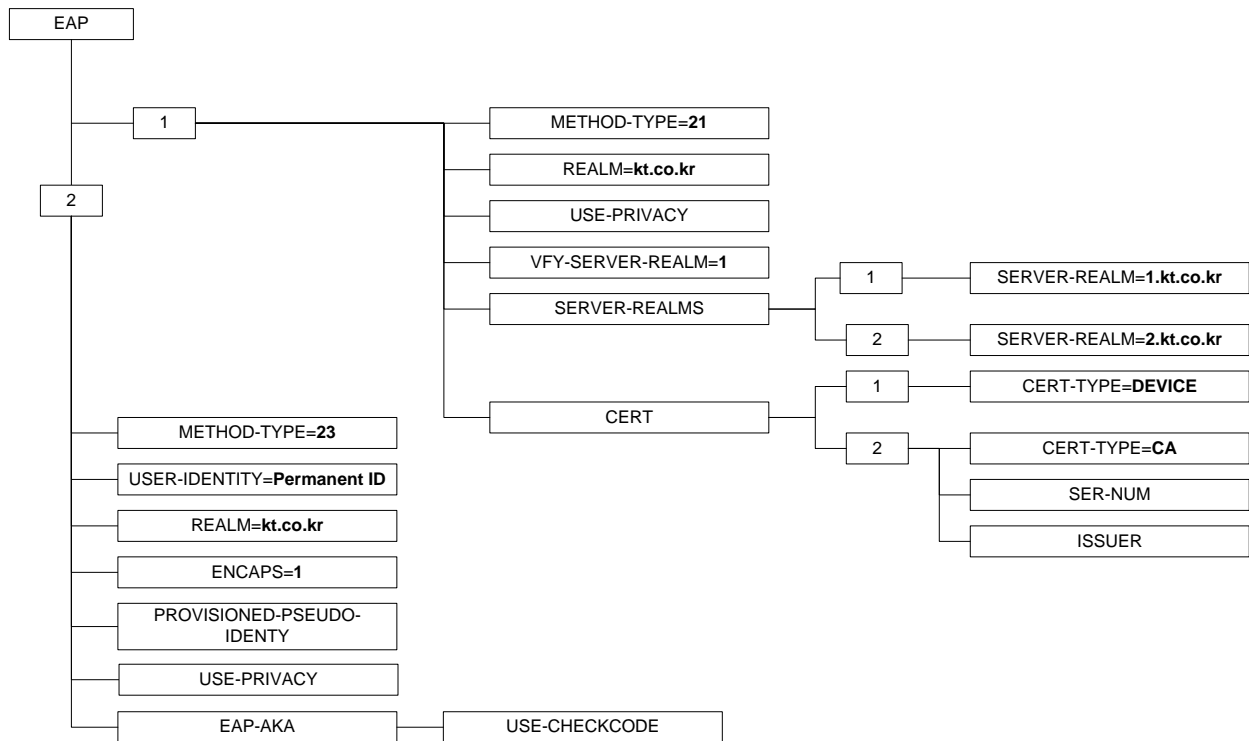


13

14 **Figure 14 - Example of EAP-AKA parameters**

1 **B.1.4 Example: EAP-AKA with EAP-TTLS Encapsulation**

2 Figure 15 illustrates an example of how the leaf nodes can be constructed in the EAP node when the EAP-AKA is  
3 used with EAP-TTLS encapsulation for the device and user authentication.



4  
5 **Figure 15 - Example of EAP-AKA and EAP-TTLS parameters**

6 **B.2 OMA IP Management Object**

7 This Section describes how the generic IP MO [15] is used in WiMAX. The description of the nodes is in [15] but  
8 the status of some nodes MUST be changed as the following table for WiMAX to fit the generic IP MO to the  
9 WiMAX needs.

Node	Status	Comment
MIPv4/SharedSecret	REQUIRED	Contains the NAI configuration for the MIPv4 registration. In WiMAX, the SharedSecret key is generated dynamically and locally. See [21].
MIPv4/SharedSecret/NAI/<X>/Use-Pseudo	REQUIRED	Indicates to the MIPv4 stack to use pseudo username in the MIPv4 registration.
MIPv4/Protocol/	REQUIRED	Specifies the MIPv4 protocol configuration.
MIPv4/Protocol/RevTun	REQUIRED	In WiMAX, the value SHOULD be TRUE.
MIPv4/Protocol/RetryCount	REQUIRED	See the node description in [15].
MIPv4/Protocol/RetryTimer	REQUIRED	See the node description in [15].
MIPv4/Protocol/RegPeriod	REQUIRED	See the node description in [15].
MIPv4/Protocol/RegPeriodRel	REQUIRED	See the node description in [15].
MIPv4/Protocol/NatTraversal	OPTIONAL	NAT Traversal is not used in WiMAX so this node SHOULD not be supported.

MIPv6/SharedSecret	REQUIRED	Contains the NAI configuration for the MIPv6 registration. The SharedSecret key is generated dynamically and locally. See [21].
MIPv6/SharedSecret/NAI/<X>/Use-Pseudo	REQUIRED	Indicates to the MIPv6 stack to use pseudo username in the MIPv6 registration.
MIPv6/Protocol/	REQUIRED	Specifies the MIPv6 protocol configuration.
MIPv6/Protocol/RouteOpt	REQUIRED	In WiMAX the value MAY be FALSE.
MIPv6/Protocol/RetryCount	REQUIRED	See the node description in [15].
MIPv6/Protocol/RetryTimer	REQUIRED	See the node description in [15].
MIPv6/Protocol/BindingLifeTime	REQUIRED	See the node description in [15].
MIPv6/Protocol/BindingLifeTimeRel	REQUIRED	See the node description in [15].
MIPv6/Protocol/SignalingProtection	REQUIRED	In WiMAX the value SHOULD be AUTHOPT.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19

### B.3 OMA NAP Management Object

#### B.3.1 Definitions for OMA Network Access Point (NAP) Management Object

The WIMAX sub-tree specified in this Section SHALL be placed under the BearerParams node in [3]. See B.3.2 for examples. Device Management servers SHALL support OMA NAP MO for WiMAX bearer configuration while devices MAY support it.

##### B.3.1.1 ../BearerType

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The *BearerType* node value specified in [3] MUST be “WIMAX”.

##### B.3.1.2 ../AddrType

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The *AddrType* in the OMA NAP MO specified in [3] MUST be supported and the value MUST be from the Table 10:

**Table 10 - NAP Address Types**

AddrType	Description
NAI	The Addr field SHALL identify a unique subscription under the WiMAX Supplementary MO. The Addr value SHALL be formatted as an NAI [28]

##### B.3.1.3 ../Addr

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

The username portion of the NAI is used to identify a unique subscriber under the operator’s subscription parameters. The primary subscription is identified with an empty username, i.e. using the value “@realm”. A subscription other than the primary is identified with a non-empty username and in this case the value of the username SHALL be the same as the name of the dynamic node under *WiMAXSupp/SubscriptionParameters/OtherSubscriptions/<X>*, e.g. “1@realm”.

1 **B.3.1.4 ../BearerParams/WIMAX**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Node	Get

2 This interior node contains the WiMAX bearer specific parameters for Network Access Point Management  
3 Object.

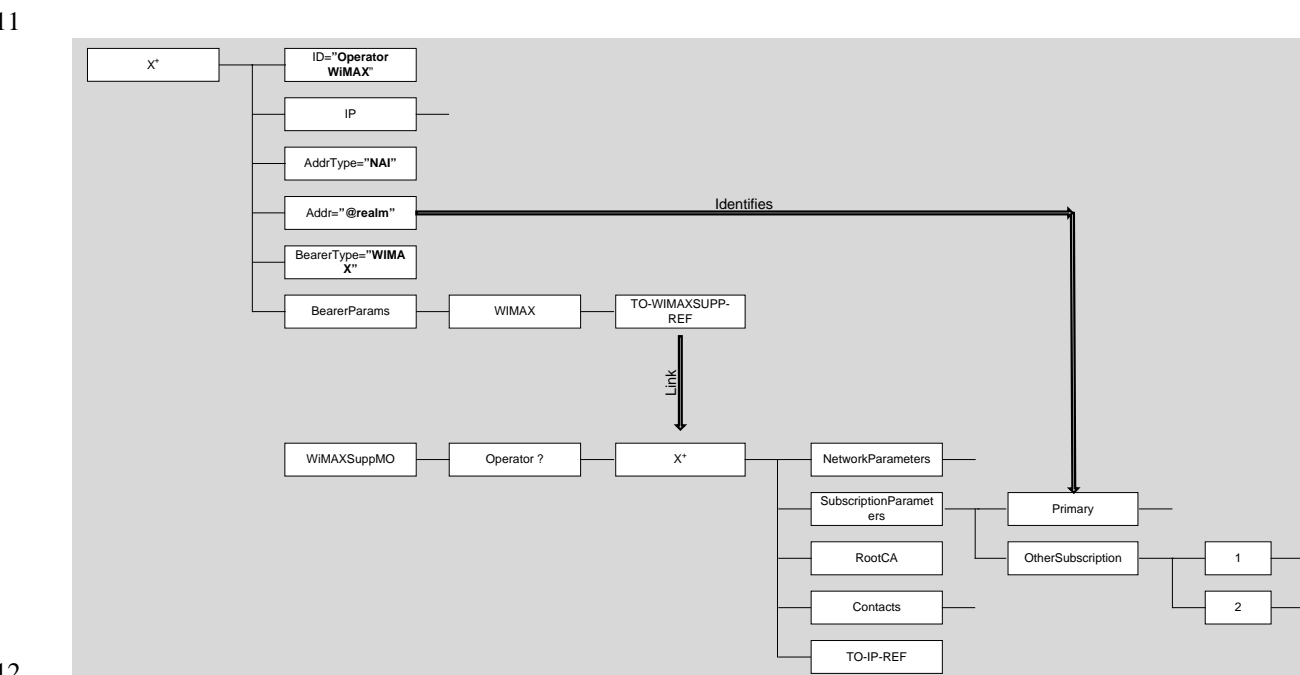
4 **B.3.1.5 ../BearerParams/WIMAX/TO-WIMAXSUPP-REF**

Status	Tree Occurrence	Format	Min. Access Types
REQUIRED	One	Chr	Get

5 This interior node specifies a link to the operator specific dynamic node *WiMAXSupp/Operator/<X>*.

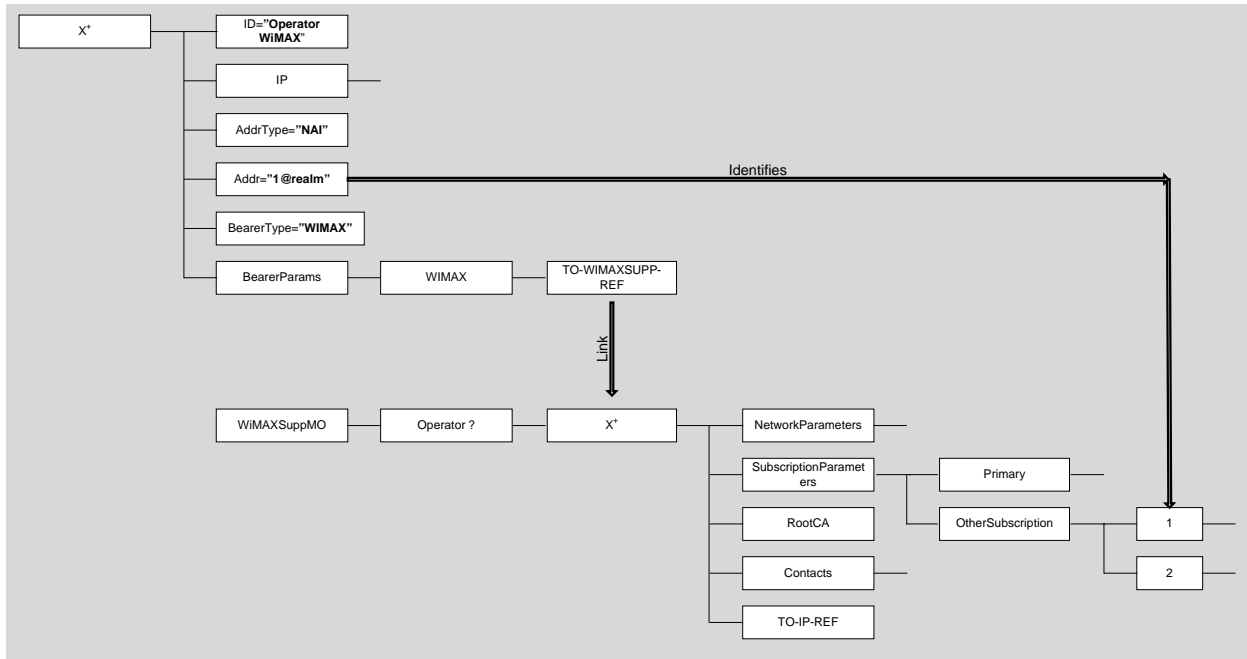
6 **B.3.2 Example: Linkage Between the OMA Network Access Point (NAP) MO WiMAX  
7 Supplementary MO**

8 The Figure 16 shows how the OMA NAP MO is used to specify a WiMAX Bearer configuration using the primary  
9 subscription parameters. The primary subscription is identified by an Addr value “@realm”, where the username is  
10 empty.



12  
13 **Figure 16 - Linkage Between NAP MO and WiMAXSupp (Primary Subscription)**

14 The Figure 17 shows how the OMA NAP MO is used to specify a WiMAX Bearer configuration using a non-  
15 primary subscription parameters. The non-primary subscription is identified by Addr value “1@realm”, where the  
16 “1” is the name of the dynamic node of the non-primary subscription.



1

2

**Figure 17 - Linkage Between NAP MO and WiMAXSupp (Other Subscriptions)**

---

## 1 **APPENDIX C. CAPL, RAPL and Channel Plan Examples**

2 [Add a new Annex into NWG Rel 1, Version 1.2.0, Stage 3]

3 All examples in this section refer to the situation where the device is using an operator controlled CAPL and  
4 RAPL from a single operator, a user controlled CAPL and RAPL (having higher priority than the  
5 operator controlled CAPL and RAPL), does not exist and prior connection information is not available.

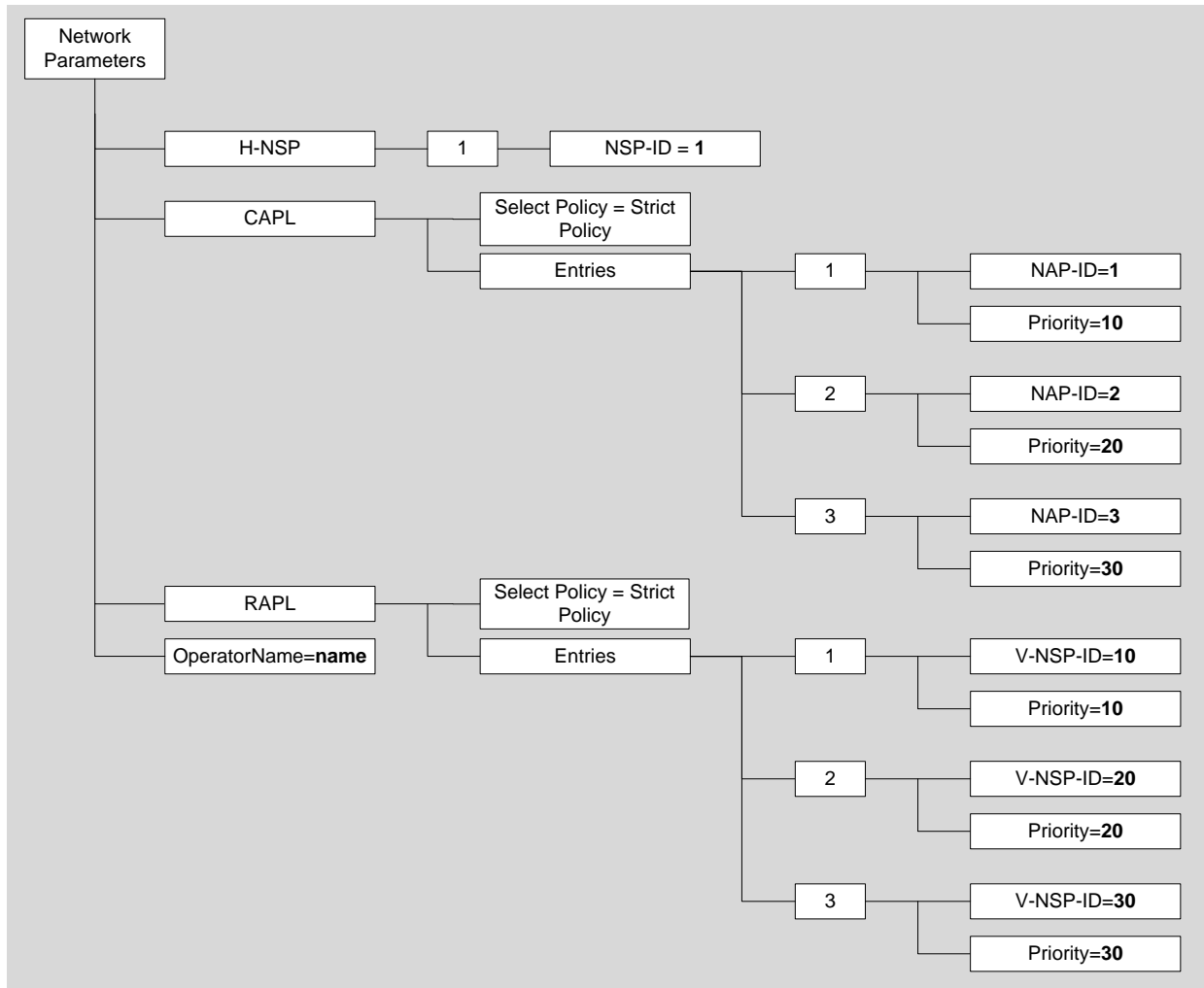
6 The operator is recommended to configure the selection policy and priorities of the NAPs and V-NSPs taking into  
7 account the time to acquire a connection and its effect on the user experience. In addition, when several H-NSPs  
8 exist in a device, connection to a particular H-NSP may be skipped if an acceptable NAP (according to configuration  
9 information) is not found before a valid attempt to connect to another H-NSP occurs (acceptable NAP of the  
10 other H-NSP found).

### 11 **C.1 Parameters used in CAPL and RAPL nodes**

#### 12 **C.1.1 Example: Strict CAPL and RAPL with Priority – Networks Available**

13 Figure 18 and Figure 19 illustrate an example of how CAPL and RAPL can be used in a strict way, which means  
14 that only NAPs in CAPL, and V-NSPs in RAPL, are allowed to be used for establishing the connection to the  
15 network.

1



2

3 **Figure 18 - An example configuration how strict CAPL and RAPL are used with priority**

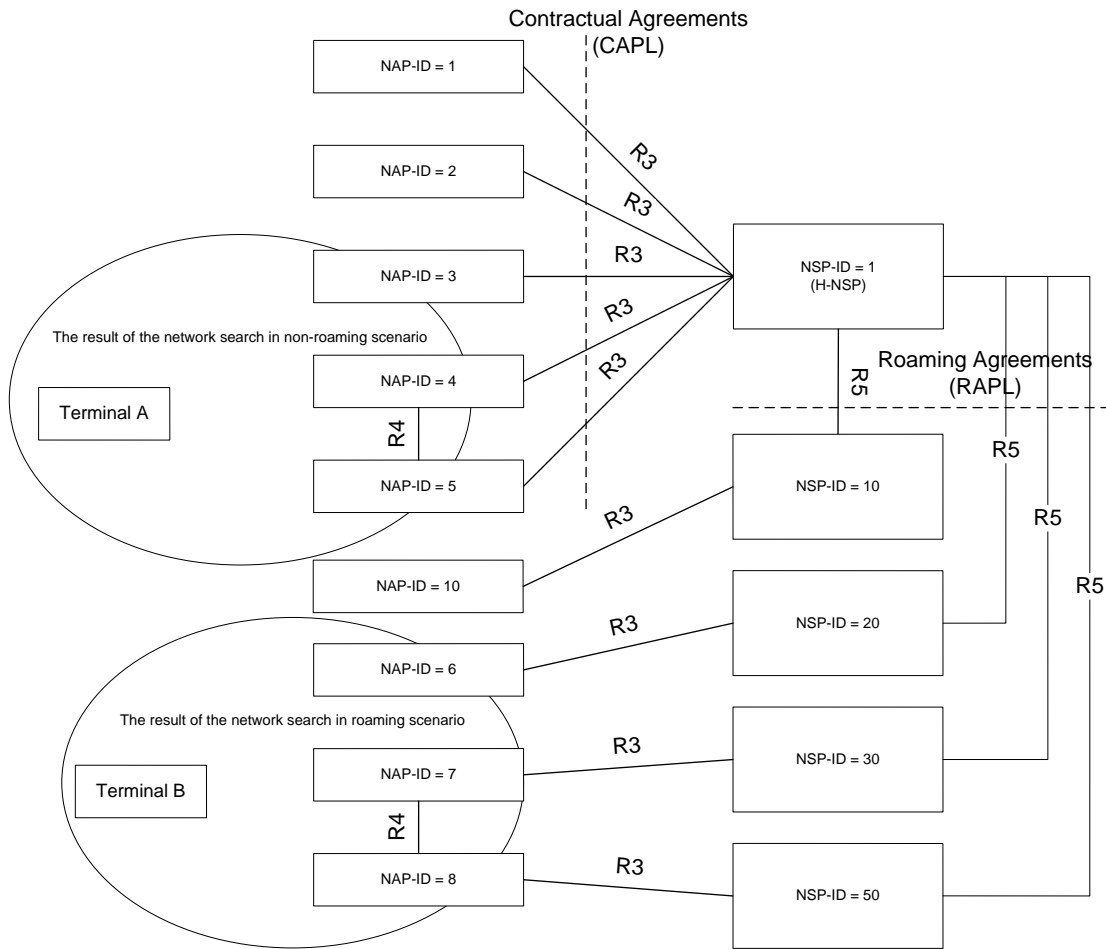
4 Network Service Provider MAY have Contractual Agreement with NAPs, which are not in the CAPL due to

5 - Deployment and agreement reasons; different access types e.g., fixed, portable or mobility MAY have  
6 different kind of configurations and network coverage restrictions.

7 - The provisioned information in the device is not up-to-date.

8 These same reasons MAY apply to RAPL as well.

1 Note! Strict CAPL MAY be used when the RAPL is flexible and vice versa.



2

3

**Figure 19 - Network setup**

4 **C.1.1.1 Non-roaming Scenario with Terminal A:**

5 The result of the network search is

6 NAP-ID = 3 -> NSP-ID = 1

7 NAP-ID = 4 -> (not in CAPL)

8 NAP-ID = 5 -> (not in CAPL)

9 The device SHALL use NAP-ID=3 to connect to the home network, since it is the only NAP found in the network  
10 search that is in the CAPL.

11 **C.1.1.2 Roaming Scenario with Terminal B:**

12 The result of the network search is

13 NAP-ID = 6 -> NSP-ID = 20 -> NSP-ID = 1

14 NAP-ID = 7 -> NSP-ID = 30 -> NSP-ID = 1

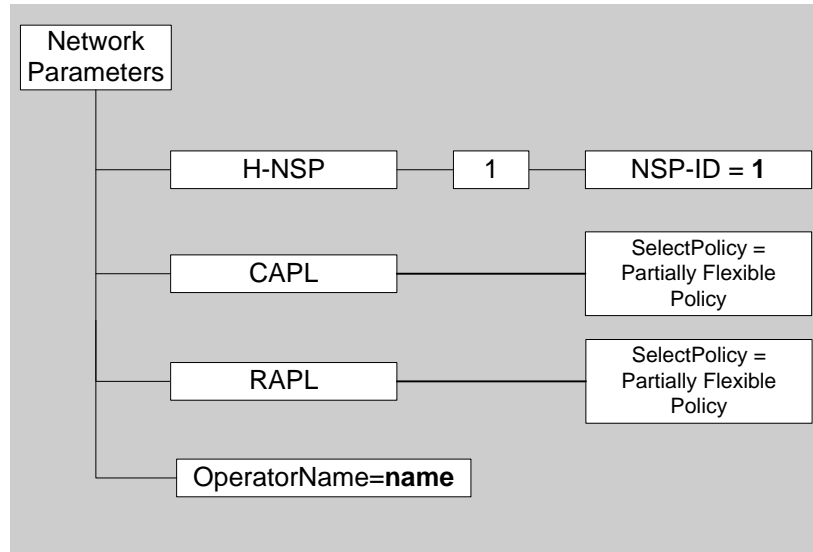
15 NAP-ID = 8 -> NSP-ID = 50 -> NSP-ID = 1

16 NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device SHALL use NAP-ID = 6  
17 and V-NSP-ID = 20 to connect to the home network, since NSP-ID=20 has the highest priority in the RAPL.

1 **C.1.2 Example: No Restrictions in CAPL and RAPL**

2 Figure 20 illustrates an example of how the device is allowed to establish connection to any NAP or V-NSP, which  
3 has direct connection to the H-NSP, in non-roaming and roaming scenario.

4



5

6 **Figure 20 - An example configuration of no restrictions in CAPL and RAPL**

7 **C.1.2.1 Non-roaming Scenario:**

8 The device is allowed to use whatever NAP, which has a direct connection to the H-NSP.

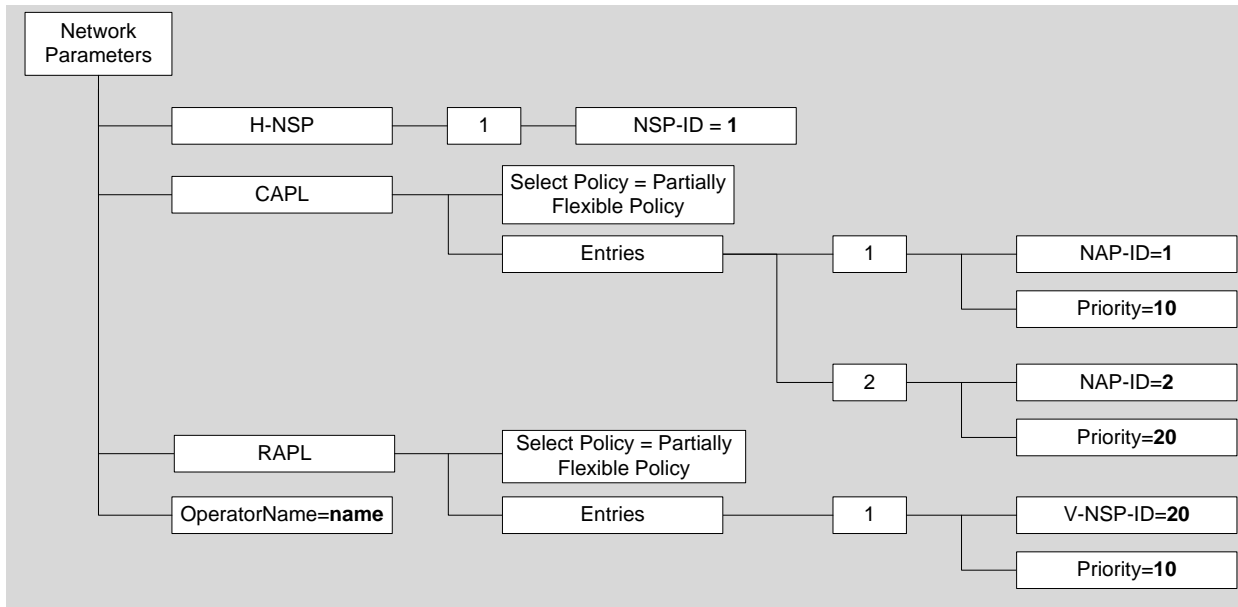
9 **C.1.2.2 Roaming Scenario:**

10 NAPs which have direct connection to the H-NSP are not found and therefore the device resorts to RAPL. The  
11 device is allowed to use whatever V-NSP, which has direct connection to the H-NSP. Determination of how the  
12 device knows that a V-NSP has direct connection to the H-NSP is out of scope of this specification.

13 **C.1.3 Example: Flexible CAPL and RAPL with Priority**

14 Figure 21 and Figure 22 illustrate an example of how the operator can specify a set of NAPs and V-NSPs and  
15 still allow the device to establish connections using NAPs and/or V-NSPs, which are not listed in CAPL or RAPL.

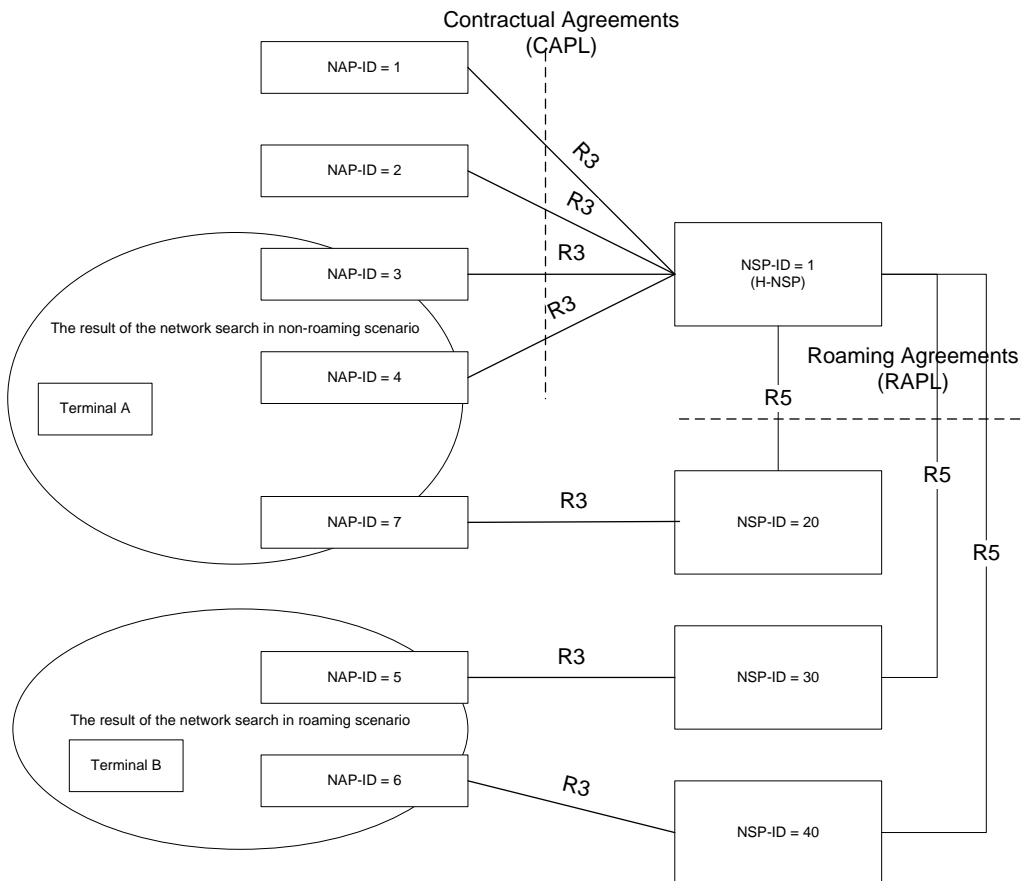
1



2

3

**Figure 21 - An example configuration of flexible CAPL and RAPL with priority**



4

5

**Figure 22 - Network setup**

1 **C.1.3.1 Non-roaming Scenario with Terminal A:**

2 The result of the network search is

3 NAP-ID = 3 -> NSP-ID = 1

4 NAP-ID = 4 -> NSP-ID = 1

5 NAP-ID = 7 -> NSP-ID = 20 -> NSP-ID = 1

6 The device MAY use either NAP-ID = 3 or NAP-ID = 4 to connect to the home network. It is implementation  
7 specific which one is selected. However the device SHALL NOT use NAP-ID = 7 because it does not have direct  
8 connection to the H-NSP and the result of the network search contained NAPs, which have direct connection to the  
9 H-NSP.

10 **C.1.3.2 Roaming Scenario with Terminal B:**

11 The result of the network search is

12 NAP-ID = 5 -> NSP-ID = 30 -> NSP-ID = 1

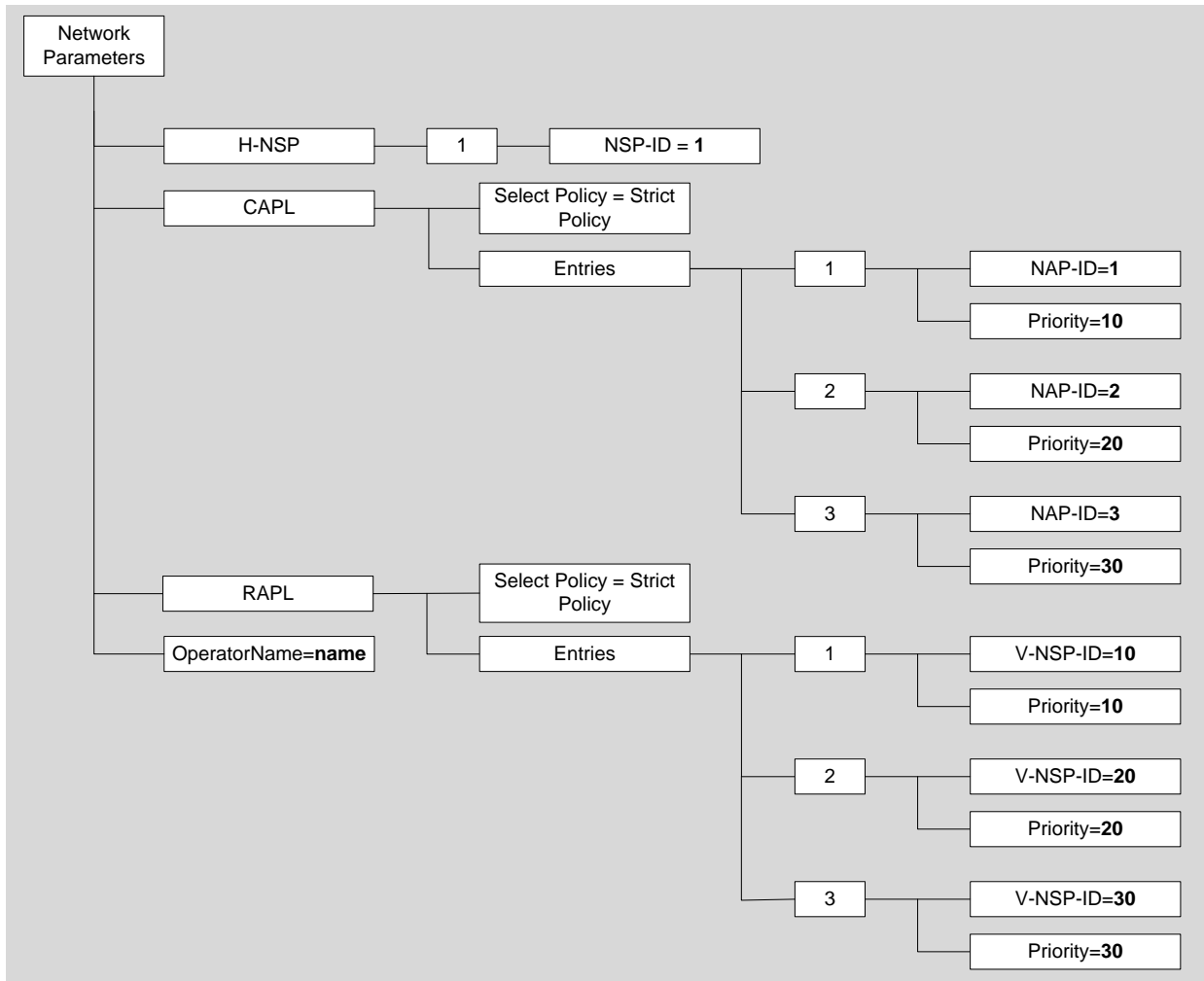
13 NAP-ID = 6 -> NSP-ID = 40 -> NSP-ID = 1

14 NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device MAY use either NAP-ID  
15 = 5 or NAP-ID = 6 to connect to the home network via NSP-ID = 30 or NSP-ID = 40. It is implementation specific  
16 which one is selected.

17 **C.1.4 Example: Strict CAPL and RAPL with Priority – Networks Not Available**

18 Figure 23 and Figure 24 illustrate an example of how CAPL and RAPL can be used in a strict way, which means  
19 that only NAPs, which are listed in CAPL, and V-NSPs, which are listed in RAPL, are allowed to be used to connect  
20 the network. In this example the terminal is not allowed to connect to the network because the network search does  
21 not return any NAPs or V-NSPs which are in CAPL or RAPL.

1



2

3

**Figure 23 - An example configuration how strict CAPL and RAPL are used with priority**

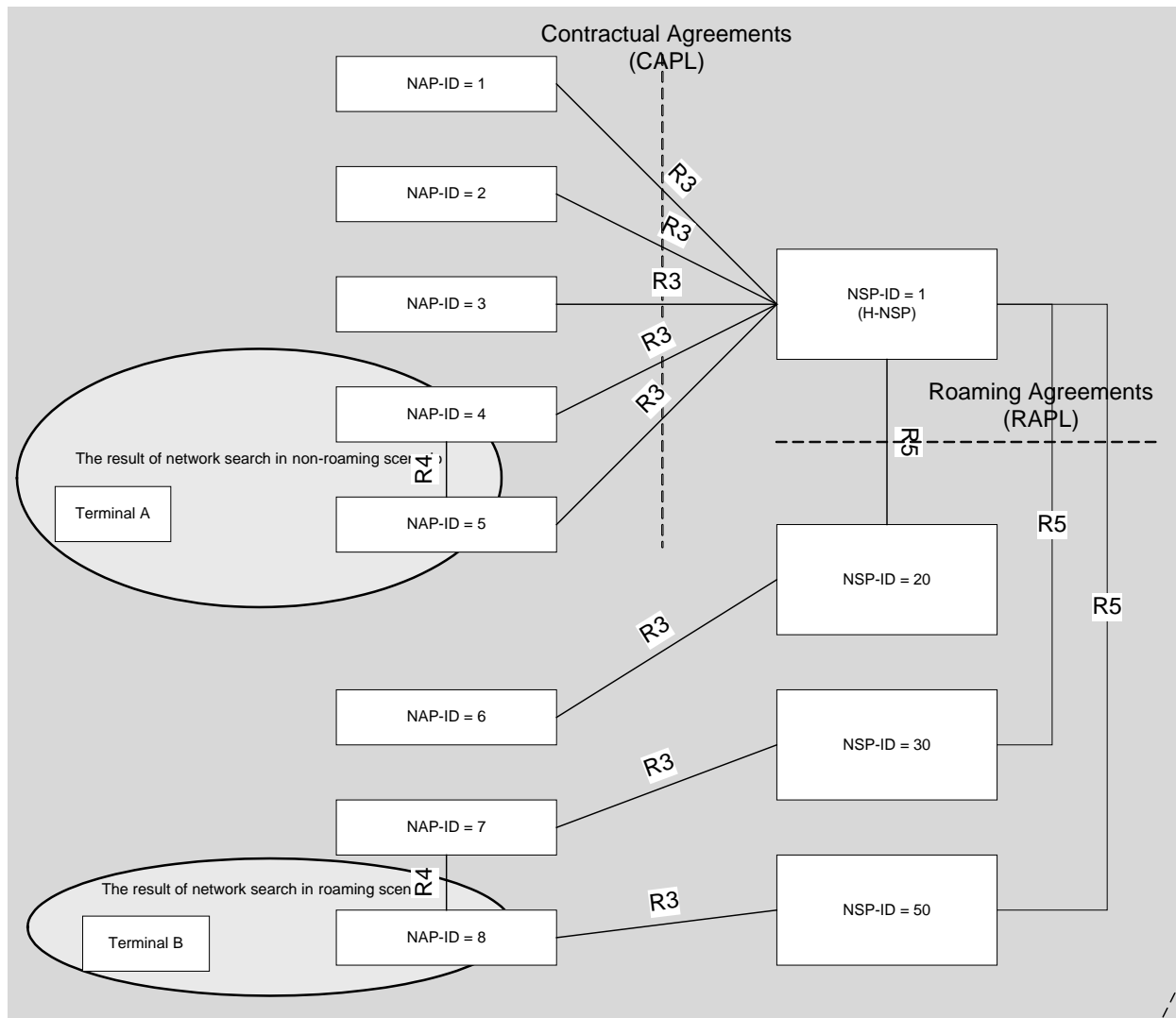


Figure 24 - Network setup

**C.1.4.1 Non-roaming Scenario with Terminal A:**

The result of the network search is

NAP-ID = 4 -> NSP-ID = 1

NAP-ID = 5 -> NSP-ID = 1

The device is not allowed to connect to any of the networks, since the result of the network search did not contain any NAPs, which are listed in CAPL nor have any of the found NAPs, which have direct connection to any of the V-NSPs listed in RAPL.

**C.1.4.2 Roaming Scenario with Terminal B:**

The result of the network search is

NAP-ID = 8 -> NSP-ID = 50 -> NSP-ID = 1

NAPs listed in CAPL are not found and therefore the device resorts to RAPL. The device is not allowed to connect any of the networks, since the result of the network search did not contain any V-NSPs, which are listed in RAPL.

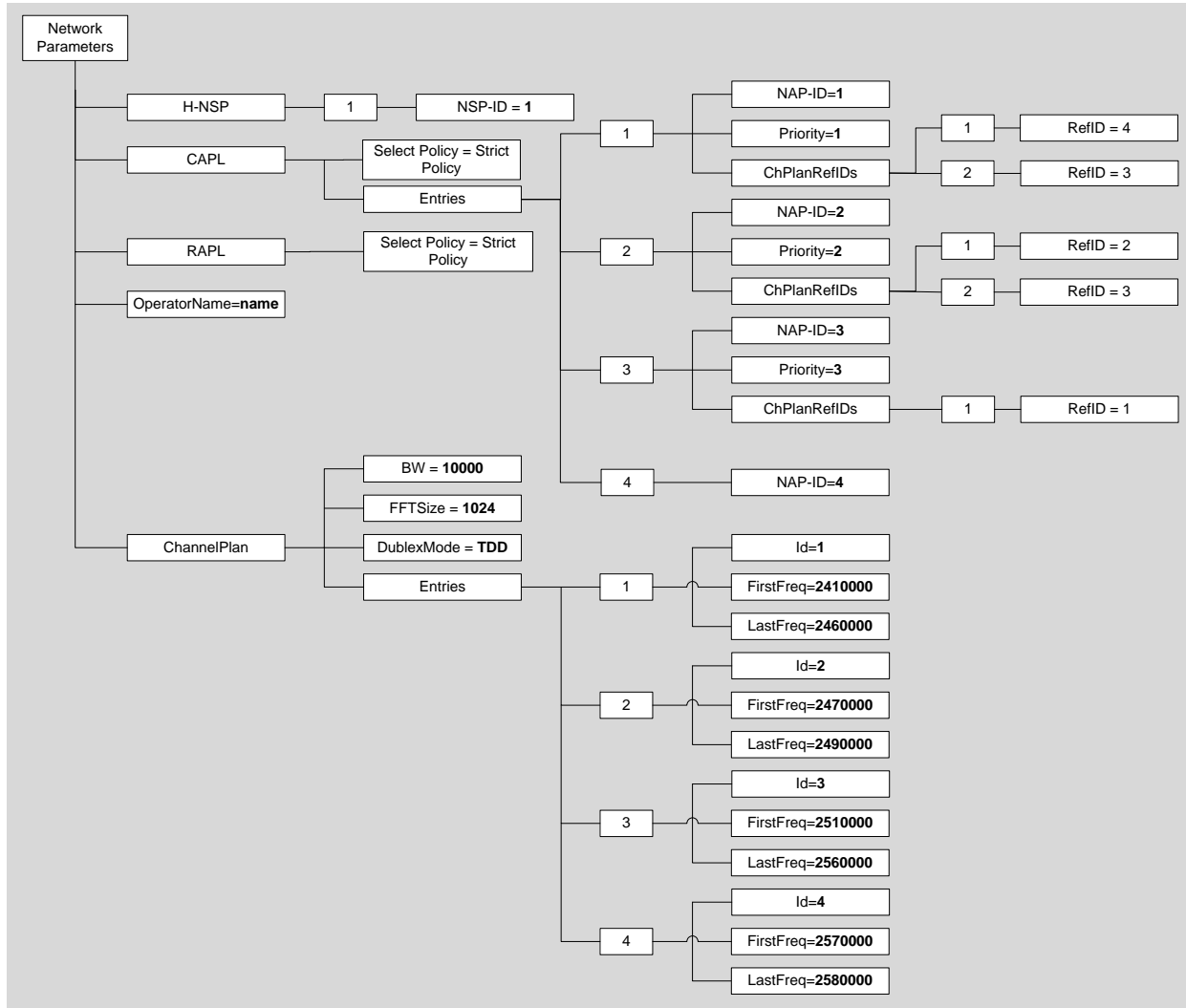
1 **C.2 Channel Plan Usage**

2 This section describes how the NAP based and root channel plan is used in network discovery and selection phases.

3 **C.2.1 Example: Network Search – Preferred NAPs Found**

4 Figure 25 and Figure 26 illustrate an example of how the NAP selection is carried out when NAP Based Channel  
5 Plan or Root Channel Plan or Full Search is used and preferred NAP is found during the search. The configuration  
6 forbids the device to roam and to connect using other NAPs, which are not in the CAPL. The channel plan  
7 information is used in network search, when the device is not connected to the network, and it does not have any  
8 “Prior Connect Info” record. Please note that values in the channel plan are exemplary.

9



10

11

**Figure 25 - Example Configuration**

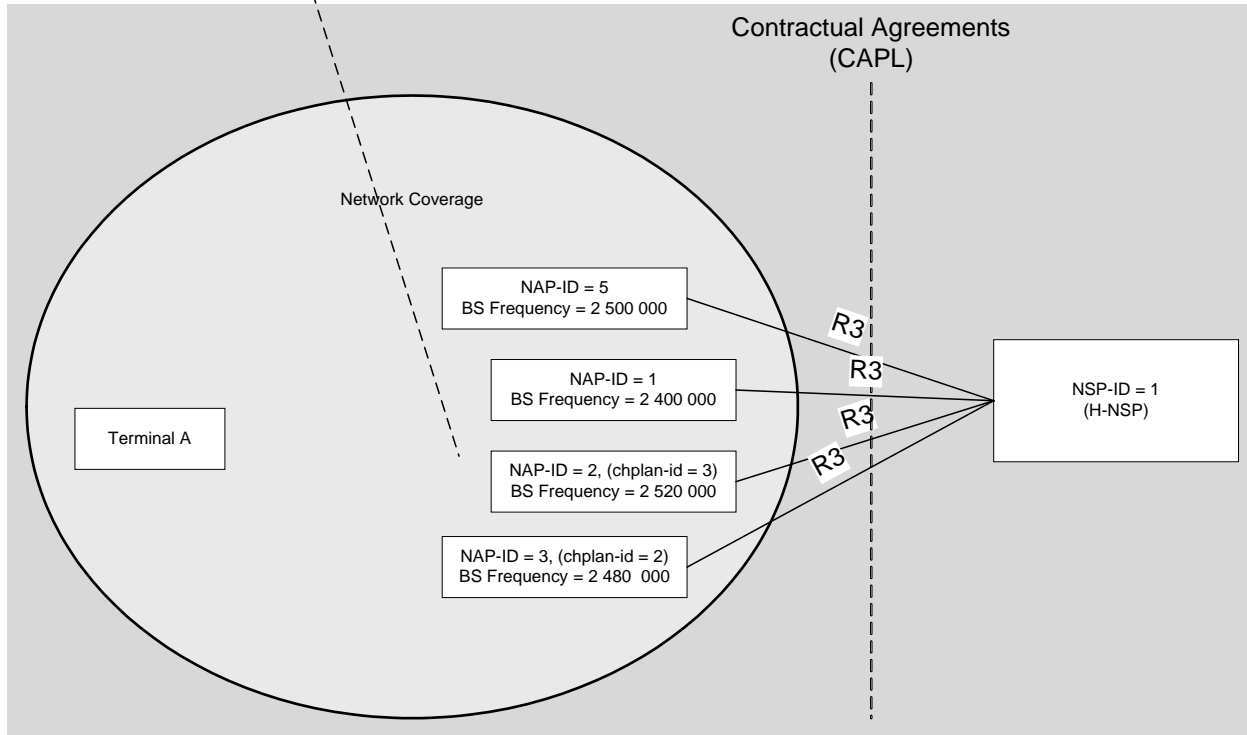


Figure 26 - Network Coverage and Setup

**C.2.1.1 NAP selection based on NAP Based Channel Plan**

Device is allowed to select NAP-ID= 2 even though it is not the most preferred NAP, but it is the highest priority of found NAPs. As NAP-ID=1 is not found from the frequencies of the NAP-ID=1's channel plan entries, the device can ignore the priority of NAP-ID=1.

**C.2.1.2 NAP selection based on Root Channel Plan**

Device is allowed to select NAP-ID= 2 even though it is not the most preferred NAP, but it is the highest priority of found NAPs. As NAP-ID=1 is not found from the frequencies indicated by the Root Channel Plan, the device can ignore the priority of NAP-ID=1.

**C.2.1.3 NAP selection based on Root Channel Plan, if NAPs in CAPL would not have priorities**

The device is allowed to select any of the NAPs from the CAPL. However if the device searches the frequencies in the order given in the Root Channel Plan it first finds NAP-ID=3.

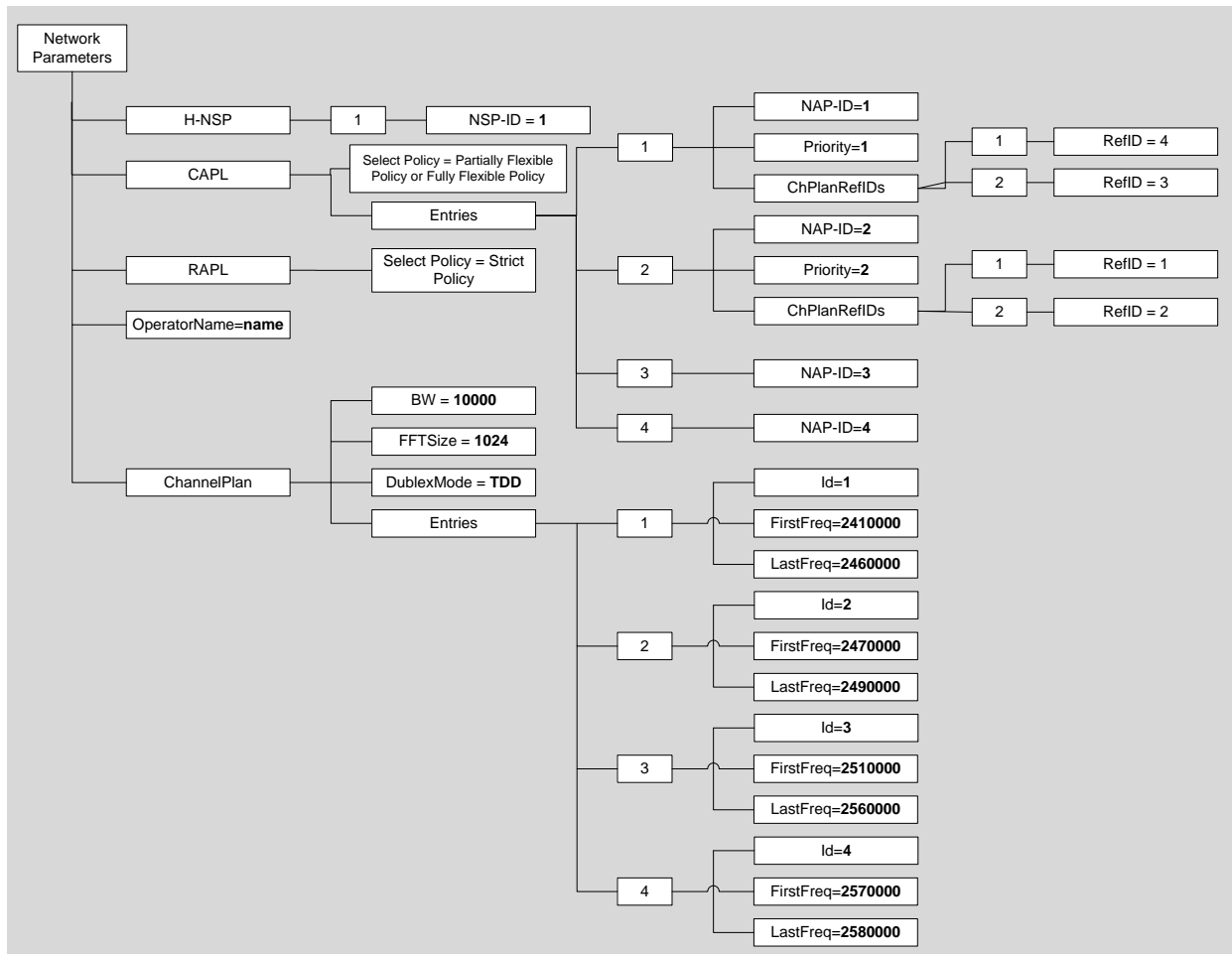
**C.2.1.4 NAP selection based on full search if channel plan configuration is not provided**

Device SHALL select NAP-ID = 1, since it is the most preferred NAP and highest priority of found NAPs.

**C.2.2 Example: Network Search – Flexible CAPL**

Figure 27 and Figure 28 illustrate an example of how the NAP selection is carried out when NAP Based Channel Plan, Root Channel Plan or full network search is used and the NAP Selection Policy in CAPL is set to Partially Flexible Policy or Fully Flexible Policy. The configuration forbids the device to roam. The channel plan information is used in network search, when the device is not connected to the network, and it does not have any "Prior Connect Info" record. Please note that values in the channel plan are exemplary.

1

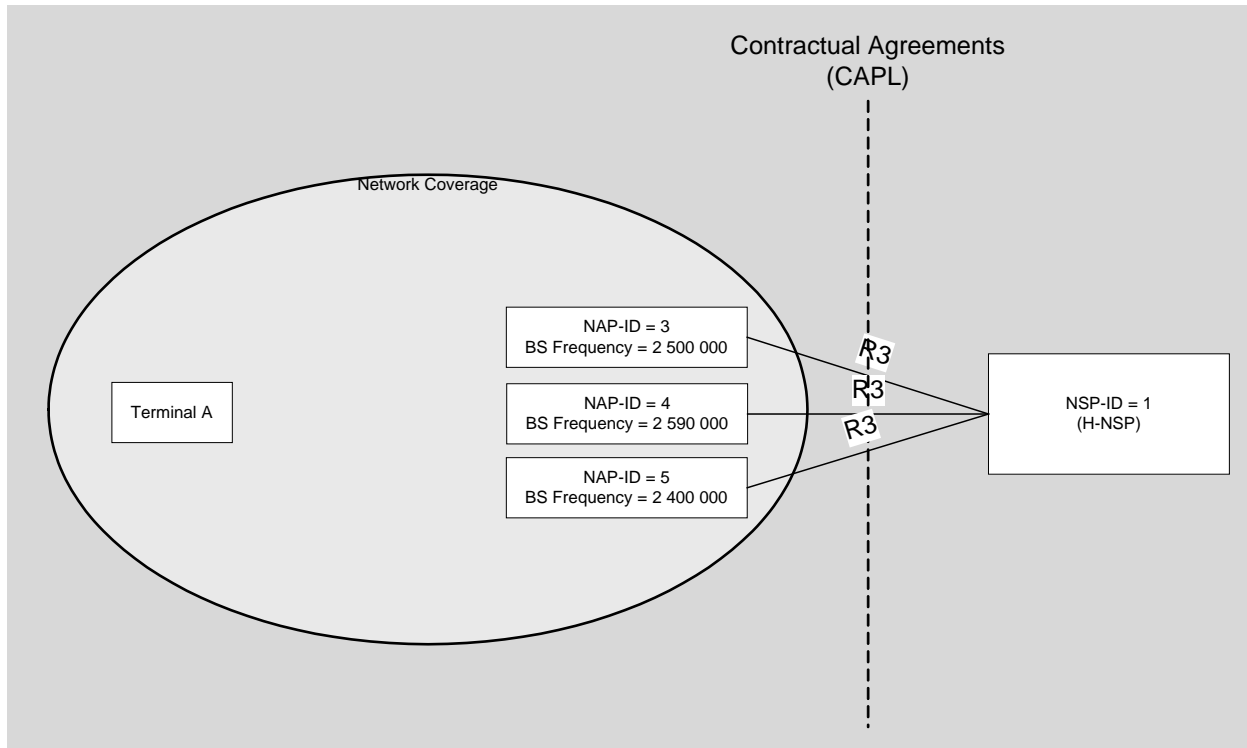


2

3

Figure 27 - Example Configuration

1 **C.2.2.1 NAPs Not Found From the Channel Plan**



2

3

**Figure 28 - Network Coverage and Setup**

4 **NAP Selection** when NAP Selection Policy is set to Partially Flexible Policy

5 Device is allowed to select either NAP-ID=3 or NAP-ID=4, because NAPs with priority are not found and NAP  
6 Selection Policy is set to Partially Flexible Policy which means that the device SHALL respect NAPs in CAPL  
7 before selecting other NAP which is connected to the H-NSP. In other words the device is not allowed to select  
8 NAP-ID=5. It is implementation specific which one is selected.

9 **NAP selection** when NAP Selection Policy is set to Partially Flexible Policy

10 Device is allowed to select either NAP-ID=3, NAP-ID=4 or NAP-ID=5, because NAPs, which do not have priority,  
11 in CAPL are handled with same priority as NAPs which are not in the CAPL. It is implementation specific which  
12 one is selected.

13

---

## 1 **APPENDIX D. Ensuring Management Authority Control of** 2 **MOs**

3 To ensure that a MO or specific node cannot be added or altered by an unauthorized management authority (e.g., a  
4 rogue service provider), DM provides an ACL mechanism to prevent this from happening.

5 An ACL is a node property that lists the only management servers allowed to add, replace and/or get the value of the  
6 nodes in the data structure.

7 Exact details on how the ACL property is formatted and how it behaves are included within the OMA DM Tree and  
8 Description specification [12].

9 In addition, ACLs MAY be used by management authorities to lock out whole areas of the DM data structure, to  
10 either ensure that SLAs are met, or the device is totally secured from malicious/unsecured management (e.g. such a  
11 requirement MAY apply to government-provisioned devices). To accomplish this, it is recommended that these  
12 ACLs are provisioned as embedded management operations during the bootstrap via factory provisioning or via the  
13 UICC (e.g., in the case of dual mode devices).

14

---

## 1 **APPENDIX E. Mandatory MOs For Supporting Model B** 2 **Devices [Normative]**

3 The following WiMAXSupp MOS SHALL be set by networks for supporting model B devices:

- 4 • WiMAXSupp/Operator/<x>/NetworkParameters/OperatorName
- 5 • WiMAXSupp/Operator/<x>/NetworkParameters/H-NSP/<x>/H-NSP-ID (with at least one H-NSP-ID)
- 6 • WiMAXSupp/Operator/<x>/NetworkParameters/CAPL/\* (with at least one NAP entry)
- 7 • WiMAXSupp/Operator/<x>/SubscriptionParameters/Primary/Activated
- 8 • WiMAXSupp/Operator/<x>/SubscriptionParameters/Primary/EAP... (with the MOs that are required for  
9 the specified EAP method) – only if the network enforces an EAP method that is different from the  
10 default TLS method.

11

---

## APPENDIX F. Maximum sizes of Elements in WiMAXSupp for Model B devices [NORMATIVE]

Model B devices are expected to enable the user to subscribe to more than one operator. For each operator, the device will be provisioned with information in the WiMAXSupp/Operator entry.

The purpose of this ANNEX is to specify minimum number of operators a Model B device is expected to support (which is translated to the amount of WiMAXSupp/Operator entries to be supported) and to the maximum instances of sub elements of the operator entry (number of channel plan nodes – for example) in order to ensure devices implement sufficient storage for storing the entire provisioned information.

Model B devices SHALL support the various amounts and sizes that are specified in this ANNEX.

If a network attempts to provision more elements than supported, the device SHALL return a ‘Device full’ (420) status code and will not store the information.

Having defined these limits, devices may support larger amounts of operators but are not required to do so.

If the number of provisioned WiMAXSupp/Operator MOs has reach the specified limit and a user attempts to subscribe to a new operator, the subscription will fail with the following behavior:

1. During the OMA-DM session, the device SHALL return a ‘Device full’ (420) status code on the ‘Add’ command
2. The network SHOULD place descriptive information in the subscription portal to inform the user of the failure and the reason for the failure
3. The device MAY implement some logic that informs the user about the problem and suggest ways to overcome it in order for the user to succeed in the next attempt. The exact logic is out of scope from this specification.

Size limits:

The amount of WiMAXSupp/Operator nodes shall be at least 16.

For each operator the following maximum number of entries is:

- /WiMAXSupp/Operator/<x>/NetworkParameters:
  - /NetworkParameters/H-NSP/<x>/H-NSP-ID – 1 entry
  - /NetworkParameters/CAPL/Entries/<x>/\* – 16 entries
  - CAPL REFids – like channel plan entries (32)
  - /NetworkParameters/RAPL/Entries/<x>/\* – 64 entries
  - /NetworkParameters/ChannelPlan/Entries/<x>/\* – 32 entries
  - /NetworkParameters/OperatorName – 255 characters
- /WiMAXSupp/Operator/<x>/SubscriptionParameters:
  - /SubscriptionParameters/ – only Primary
  - /SubscriptionParameters/Primary/EAP/<x>/\* - 1 EAP method (1 entry is EAP-TLS is used and 2 entries if EAP-TTLS is used)
- EAP – related:
  - Realm- 64 bytes
  - UserIdentity – 64 bytes

- 1           o Password – 64 bytes
- 2           o Certificates – None
- 3           o Server Realm – up to 16 entries each up to 64 bytes
- 4       • /WiMAXSupp/Operator/<x>RootCA:
  - 5           o None (4 entries each up to 4K bytes)
- 6       • /WiMAXSupp/Operator/<x>Contacts
  - 7           o /Contacts/<x>/\* – 4 entries
  - 8           o URI – up to 128 bytes
  - 9           o Text – up to 255 characters

10

11 Other limits:

12 The dynamic tag string (<x>) length is 32 characters for operator tags (WiMAXSupp/Operator/<x>) and 16 for the  
13 rest. Networks are encouraged to use numeric values when possible (for example: as tags for the different CAPL  
14 entries, for the different ChannelPlan entries etc...)

15

16

17

18