



WiMAX Forum[®] Network Architecture
Architecture, detailed Protocols and Procedures
Over-The-Air Provisioning Activation on Bootstrap

WMF-T33-117-R016v01
WiMAX Forum[®] 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
56 Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks
57 of the WiMAX Forum. All other trademarks are the property of their respective owners. Wi-Fi® is a registered
58 trademark of the Wi-Fi Alliance.

59

1	Table of Contents	
2	1. DOCUMENT SCOPE.....	6
3	2. ABBREVIATIONS AND DEFINITIONS	7
4	2.1 Abbreviations	7
5	2.2 Terms & Definitions	9
6	2.3 Conventions	11
7	3. REFERENCES.....	12
8	4. APPLICATION SCENARIOS.....	13
9	5. GENERAL REQUIREMENTS	14
10	6. USE CASES	15
11	7. WIB SERVER LOGIC FOR WIB-BASED DEVICE ACTIVATION.....	19
12	8. MS ERROR HANDLING	20
13	9. MINIMUM SET OF WIMAX® MOS TO BE SUPPORTED FOR WIB-BASED ACTIVATION.....	21
14		
15		

1 **List of Figures**

2 FIGURE 6-1 – PHASE 1 – INE / CREATE A SUBSCRIPTION.....16
3 FIGURE 6-2 – PHASE 2 – SUBSEQUENT INE / DEVICE ACTIVATION17

4
5

1 **List of Tables**

2 TABLE 7-1 – WIB SERVER ACTIONS BASED ON OTA STATUS RECEIVED FROM AN HAAA19

3

1. Document Scope

- 2 This document describes a simplified form of device activation, Activation on Bootstrap, by reference to the
- 3 relevant use cases, server logic, error handling & minimum supported MOs.

1 2. Abbreviations and Definitions

2 2.1 Abbreviations

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
ASN	Access Service Network
ASN-GW	ASN – Gateway
ATA	Analog Terminal Adapter
BEK	Bootstrap Encryption Key
BS	Base Station
BW	Band Width
CAPL	Contractual Agreement Preference List
CA	Certificate Authority
CCM	Counter with Cipher Block Chaining
CE	Consumer Electronics
CMIP	Client Mobile IP
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CSC	Customer Service Center
CSN	Connectivity Service Network
DB	Database
DDF	Device Description Framework
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DMAcc	DM Account
DNS	Domain Name System
DPI	Deep Packet Inspection
DTD	Document Type Definition
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
EMSK	Extended Master Session Key
FFT	Fast Fourier Transform
FUMO	Firmware Update Management Object
GUID	Global Unique Identifier

GW	Gateway
H-AAA	Home Authentication, Authorization and Accounting
HA	Home Agent
HTTP	Hypertext Transfer Protocol (HTTP)
H-NSP	Home Network Service Provider
H-NSP-ID	Home Network Service Provide Identifier
IMSI	International Mobile Subscriber Identity
INE	Initial Network Entry
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISF	Initial Service Flow
LDAP	Lightweight Directory Access Protocol
LSB	Least Significant Bit/Byte
MAC	Message Authentication Code Medium Access Control
MIP	Mobile IP
MO	Management Object
MS	Mobile Station (also referred to as ‘device’ in this document)
MSB	Most Significant Bit/Byte
MSID	Mobile Station Identifier
NAI	Network Access Identifier
NAP	Network Access Provider
NAP ID	Network Access Provider Identifier
NAP MO	Network Access Point Management Object
NAT	Network Address Translation
ND&S	Network Discovery & Selection
NSP	Network Service Provider
NSP ID	Network Service Provider Identifier
NW	Network
NWG	Network Working Group
OAM&P	Operation, Administration, Maintenance, and Provisioning
OMA DM	Open Mobile Alliance Device Management
OTA	Over-The-Air
PC	Personal Computer
PKI	Public Key Infrastructure
PMP	Portable Media Player

PMIP	Proxy Mobile IP
POA	Point of Activation
POM	Point of Manufacturing
POS	Point of Sale
RADIUS	Remote Authentication Dial In User Service
RAPL	Roaming Agreement Preference List
RDF	Resource Description Framework
SLA	Service Level Agreement
SKU	Stock Keeping Unit
SPI	Security Parameter Index
STB	Set-Top Box
TLV	Type Length Value
UDP	User Datagram Protocol
UMD	Ultra Mobile Device
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
V-NSP	Visited Network Service Provider
V-NSP-ID	Visited Network Service Provider Identifier
WIB	WiMAX® Initial Bootstrap
WiMAX®	Worldwide Interoperability for Microwave Access
XML	Extensible Markup Language

1

2 **2.2 Terms & Definitions**

3 The following terms & definitions are applicable to both the OMA DM [3] and TR-069 [4] based WiMAX® OTA
4 Provisioning & Activation Specifications.

5 **Activation Provisioning:** The process where a device that is not provisioned for a user account currently associated
6 with an active subscription with a service provider is updated with data, parameters, and/or applications, typically
7 for the first time, associating the device with a account (paying customer) and supplying service to the device.

8 **Activation/Provisioning Points:**

- 9 ○ POM – Point of manufacturing where at least initial information MUST be provisioned.
- 10 ○ POS – Point of sale where activation and provisioning information MAY be added (depends if the
11 POS is an operator store or an entity that is cooperating with the operator).
- 12 ○ POA – Point of activation where all needed information is provisioned and ‘Device Lock’ MAY
13 be activated (in some scenarios the POS is the POA and in others the POA is done through OTA).

14 **Bootstrap:** A procedure to transfer information of device management server e.g. the address of device management
15 server, username and password to the device to enable the device to connect to the device management server and
16 establish a session with it.

17 **Certificate:** A digitally signed statement that contains information about an entity and the entity's public key, thus
18 binding these two pieces of information together. A Certificate is issued by a trusted organization (or entity) called a

- 1 Certification Authority (CA) after the CA has verified that the entity is who it says it is. Certificates can contain
2 different types of data. For example, an X.509 Certificate includes the format of the Certificate, the serial number of
3 the Certificate, the algorithm used to sign the Certificate, the name of the CA that issued the Certificate, the name
4 and public key of the entity requesting the Certificate, and the CA's signature.
- 5 **Certificate Authority (CA):** An entity entrusted to issue Certificates that asserts that the recipient individual,
6 computer, or organization requesting the Certificate fulfills the conditions of an established policy.
- 7 **Certificate Revocation List (CRL):** A document maintained and published by a CA that lists Certificates issued by
8 the CA that are no longer valid.
- 9 **Channel Plan:** A Channel Plan is used by the device to speed up NAP discovery process. It contains physical
10 information such as channel bandwidth, center frequency, and PHY profile.
- 11 **Continuous Provisioning:** The process where a device that is already provisioned with a user account associated
12 with an active subscription with a service provider is updated with new data, parameters, and/or applications that
13 MAY replace pre-existing values or versions. The Continuous Provisioning process is based on the definition in [1]
14 and includes the configuration maintenance/management use case described in the same specification.
- 15 **Contractual Agreement Preference List (CAPL):** A list consisting of Network Access Providers preferred to be
16 connected to the home network directly
- 17 **Customer Service Center (CSC):** An entity in a wireless carrier's network that receives service requests from the
18 end users and acts on such requests.
- 19 **Device Lock:** Blocking the WiMAX® host device from getting activated on new operators and enforcing the device
20 to work only with the operator, which is locked, as a H-NSP.
- 21 **Device Management (DM):** Process of remotely managing device settings and applications. DM provides a
22 mechanism for the users to easily subscribe to new services and make changes to their existing services. For the
23 operators this enables a fast and easy way to introduce new services and manage provisioned services, by
24 dynamically adjusting to changes and ensuring a certain level of quality of service.
- 25 **Device Management System:** A background system capable to interact with a (set of) Device(s) for the purpose of
26 Device Management.
- 27 **Device Profile:** Settings that establish the configuration of a particular device, including network settings,
28 applications, etc.
- 29 **Device Unlock:** Process of allowing the device to get activated on other Service Providers' networks.
- 30 **Host Device:** Refers to a standalone device or a sub-module in which WiMAX® modem (chipset) is embedded. This
31 is the device that is to be managed as this specification defines, associated with MAC ID, and SHOULD appear in
32 DevInfo and DevDetail MOs. Examples of host device are: 1) Removable Modem (e.g., PC Card, USB Modem,
33 etc.) with embedded WiMAX chipset; 2) WiMAX sub-module physically attached to a WiMAX CPE Gateway; 3)
34 WiMAX sub-module temporarily or permanently built into a laptop; 4) WiMAX enabled consumer electronics (e.g.,
35 Digital Camera, PMP, etc.) that has the embedded WiMAX chipset.
- 36 **Management Object:** A data model for information, e.g., a configuration parameter, an image, or a file, which is a
37 logical part of the interfaces exposed by DM components and managed through the use of OAM&P.
- 38 **Model A:** Operator/service provider subsidized device, similar to the current cellular, cable modem, or DSL
39 services provisioning models. Different SKU provided for each device at POM to connect to one WiMAX® network
40 or group of WiMAX networks. Model A May support self-subscription OTA or via a web portal.
- 41 **Model B:** Generic SKU retail devices. SHALL support over-the-air self-subscription and provisioning.
- 42 **Model B1:** Non-operator. Non-service provider. Not a subsidized device.
- 43 **Model B2:** Operator/service provider subsidized device. Device contains operator/service provider specific
44 configuration.
- 45 **Multimode Device:** Device supporting two or more wireless access technologies.
- 46 **NAP Based Channel Plan:** A Channel Plan which is a subset of Root Channel Plan and is associated with a NAP.

- 1 **OMA DM:** Refers to the set of specifications developed by Open Mobile Alliance for DM.
- 2 **Prior Connect Info:** Specified in [2].
- 3 **Provisioning:** Populating the device and the network management with data and software needed for the operation
4 on the operator network and for improving the user experience (value added services and applications). Provisioned
5 information SHOULD be divided into 3 groups:
- 6 ○ Information that can be provisioned only during activation.
 - 7 ○ Information that can be provisioned during normal operation but only when connected to home-operator.
 - 8 ○ Information that can be provisioned during normal operation by any operator.
- 9 **Provisioning Server:** Refers to a server that communicates with the device using the provisioning protocol in the
10 provisioning process.
- 11 **Roaming Agreement Preference List (RAPL):** A list delivered to the device consisting of Network Service
12 Providers preferred to be connected to when roaming.
- 13 **Root Channel Plan:** A Channel Plan which contains all Channel Plan Entries.
- 14 **Smart Card:** A smart card (or chip card, or integrated circuit card) is a miniaturized electronic card with embedded
15 integrated circuits which can process information. This implies that it can receive input from trusted source and
16 process the information in a standardized manner and deliver processed information as an output to trusted entities it
17 interacts with. There are two broad categories of smart cards. The first category is memory cards (or flash memory
18 card) used in handheld devices, digital cameras, laptops, etc., containing only non-volatile memory storage
19 components, and perhaps some specific security logic. The second category is microprocessor cards that contain
20 volatile memory and microprocessor components.
- 21 **Service Credential:** Credential used to allow the user to access the carrier services.
- 22 **Terminal Equipment:** Refers to the device in which host device is temporarily (through PC card slot, USB port
23 etc.) or permanently (for example, embedded laptop) inserted to get WiMAX® connectivity. Examples of terminal
24 equipment are: 1) PC which has a PC card slot for peripheral devices, and PC Card (host device) is inserted in PC to
25 get WiMAX connectivity; 2) WiMAX CPE Gateway which has a WiMAX sub-module; 3) Embedded laptop which
26 has WiMAX sub-module permanently built in; 4) Consumer electronics that has a WiMAX submodule.
- 27 **User Profile:** The User Profile is a collection of components (personal data, preferences/policies on services,
28 networks and devices, etc.) that indicate the preferences and current configuration of a user's account. User profiles
29 enable several users to use the same device with their own setup. The User Profile is tightly coupled with the user's
30 identity and vice versa.
- 31 **WiMAX® Radio Module:** Refers to WiMAX® radio chipset and subsystem present in the host device and that
32 enables WiMAX radio connectivity for the host device.
- 33 **WiMAX® CPE Gateway:** Network equipment through which a subscriber can connect one or more PCs, laptops, or
34 other networked devices (e.g., STB) via one or more LAN ports (e.g., Ethernet, Gigabit Ethernet Wi-Fi®, Cable
35 Connection). The WiMAX CPE Gateway provides services, such as voice and multimedia content via a WiMAX
36 Network. It MAY include an analog telephone adapter (ATA), and can support connectivity to an analog telephone,
37 fax, or an external analog Terminal Adapter. A WiMAX CPE Gateway conforms to the NWG mobility specification
38 [2], and IEEE Std 802.16e-2005. A WiMAX CPE Gateway MAY also function as a 'layer 2 bridge' or 'layer 3
39 router.' It MAY support other IP stack functions like NAT(P/T) DNS/DHCP secure pass through, NAT Traversal,
40 firewalling, parental control/DPI, security features, OAM features, and/or network diagnostics agents.
- 41 **X.509:** Digital Certificate Definition X.509 [6]
- 42

43 2.3 Conventions

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

1 **3. References**

- [1] “DM Requirements Document, Version 1.2”. Open Mobile Alliance. OMA-RD-DM-V1_2.
[URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [2] WMF-T33-001-R016, WiMAX Forum® Network Architecture-Detailed Protocols and Procedures, Base Specification
- [3] WMF-T33-104-R016, WiMAX Forum®, Network Architecture- Architecture, detailed Protocols and Procedures, WiMAX® Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications
- [4] WMF-T33-105-R015, WiMAX Forum®, Network Architecture- Architecture, detailed Protocols and Procedures, Over-The-Air Provisioning & Activation Protocol based on TR-069 Specification
- [5] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997,
<http://www.ietf.org/rfc/rfc2119.txt>
- [6] “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, R. Housley et.al., April 2002, <http://www.ietf.org/rfc/rfc3280.txt>

4. Application Scenarios

- 1
- 2 WIB-based activation scenario is defined as an optional capability for a device and a network. The scenario provides
- 3 a solution for basic device activation and is not applicable for extensive device provisioning (i.e. it is not a
- 4 replacement for Device Management using OMA-DM or TR-069 session), if such Device Management capabilities
- 5 (e.g. FUMO or DRMD) are required.
- 6 The network, initially deploying WIB-based activation framework, may be later evolved to provide full OTA
- 7 Provisioning/ Management capabilities. The devices, initially activated using WIB-based activation, may be later
- 8 migrated into full management using OTA Provisioning/ Management framework. Before migration can take place,
- 9 the device continues to initiate WIB at every network entry. When the network is ready for migration to full OTA
- 10 Provisioning/Management, the WIB server will re-bootstrap the device with OMA-DM account information. The
- 11 device will then connect to the OMA-DM server and continue with full provisioning as specified in [OTA General
- 12 Spec, OMA-DM Spec].
- 13 WIB-based activation option is defined and only applicable for devices that support WIB.

1 **5. General Requirements**

- 2 The device that supports OMA-DM WIB-based activation SHALL announce this capability as one of the supported
- 3 options in the Protocol field of the WIB bootstrap request message. If an MS announces its support of OMA-DM
- 4 WIB-based device activation, the WIB Server MAY include the activation MOs in the Bootstrap response message.

6. Use Cases

The following message flow presents one of the possible use cases for the bootstrap-based device activation.

The procedure consists of the following phases:

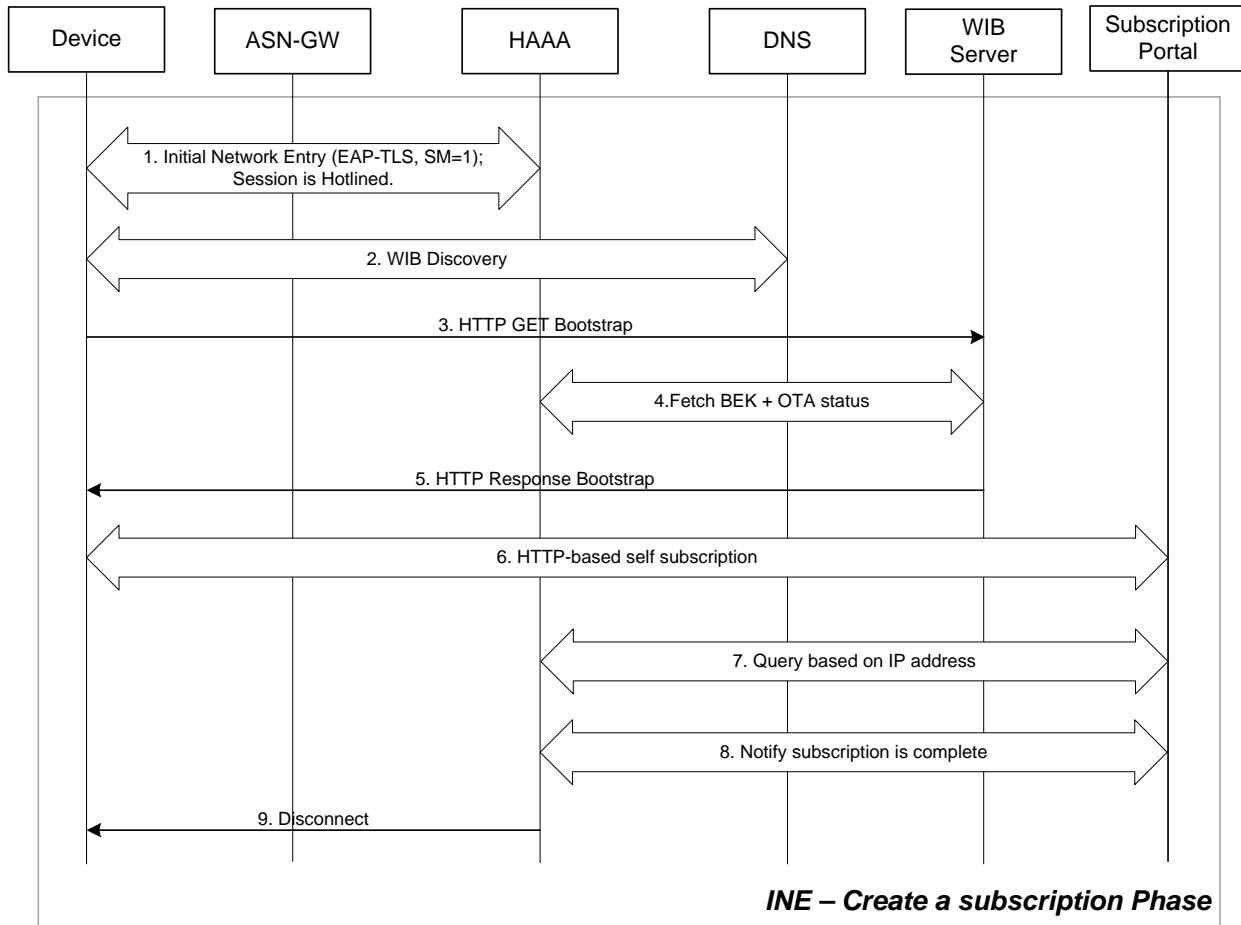
- 1) MS INE – Create a subscription.
- 2) Subsequent INE – Device activation.
- 3) Subsequent INE – For an activated device (if needed).

In essence, the first time an un-subscribed device performs INE to the WiMAX® network (Phase 1), it performs the bootstrap by going to the WIB Server. At this phase, the device receives a bootstrap document that MAY include Managed Objects including operator/network-specific parameters, but not the DM Account (DMAcc) and subscription activation parameters. The device's IP session is re-directed to the Operator's Subscription Portal where the user may create a subscription.

Once the subscription is created, the Network may trigger device deregistration (MS Network Exit) which follows the new INE initiated by the device (Phase 2). This time, when the device completes a subsequent INE, it may be granted with normal IP session processing according to the subscription SLA. The device performs WIB and is provided with Managed Object including subscription activation parameters (device activation flag is set) - because the WIB Server identifies there is a subscription.

Depending on the answer, replace the text with the following: Subsequent network entry (Phase 3), the device performs WIB. The WIB server can send updated configuration to the device. WIB based activation can only be used to set or modify the Management Objects specified in Annex E [3] specification.

1 **Phase 1: MS INE – Create a subscription phase**



2

3

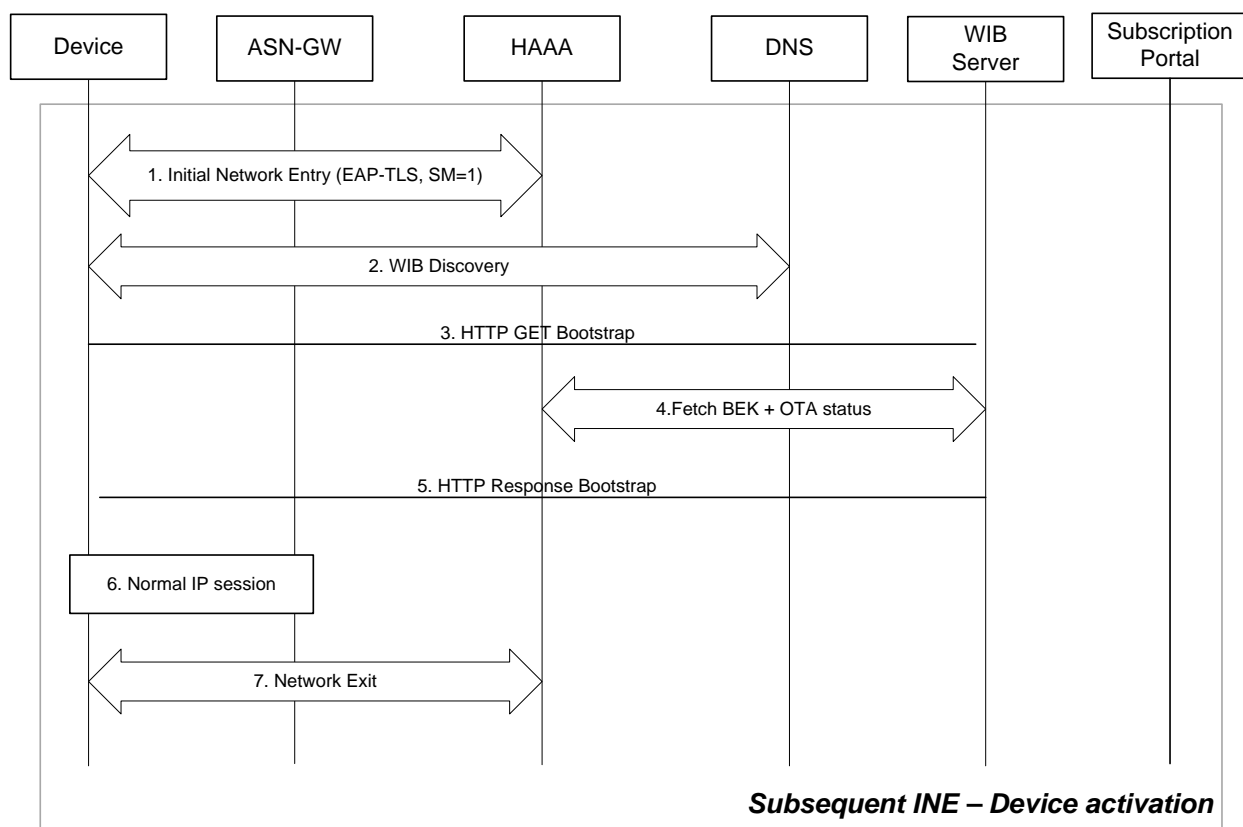
Figure 6-1 – Phase 1 – INE / Create a subscription

- 4 1. The device performs INE. Device signals its need for provisioning using NAI decoration - SM=1. AAA
 5 authenticates the device using EAP-TLS and identifies the device is unsubscribed (AAA checks the DB to
 6 identify a subscription based on MAC address). The AAA authorizes a network entry and activates
 7 Hotlining. The AAA captures active session information: SM=1, the MAC address and the fact that there
 8 is no subscription.
- 9 2. The device performs WIB server discovery via DNS procedure.
- 10 3. The device sends the HTTP based WIB bootstrap request (GET) to the WIB server. The device announces
 11 its support of “OMA-DM bootstrap-based device provisioning” mode by setting the Protocol field value in
 12 the WIB bootstrap request message.
- 13 4. The WIB server contacts the HAAA and provides the MAC address of the MS extracted from the WIB
 14 bootstrap request message. The HAAA uses the MS’ MAC address to look for the session record and
 15 returns back the BEK key, and OTA Status which includes SM=1 and whether there is a subscription (note
 16 that at this stage device has no subscription).
- 17 5. The WIB server returns back the HTTP based Boot-Record (protected by the BEK key). The Managed
 18 Objects returned in the boot record may include operator-specific information and trigger Internet Browser
 19 on the device side (as specified in OMA). Because there is no subscription at the moment, the Managed
 20 Object does not include subscription-specific info and subscription activation flag.

- 1 6. The Device/User opens Internet Browser. HTTP session is Hotlined by the network (ASN-GW/ HA) – http
- 2 traffic is redirected to the Subscription Portal. User communicates with the Subscription portal to create an
- 3 account. This can be achieved by using the Hotlined HTTP redirection to redirect the user’s browser to the
- 4 subscription portal.
- 5 7. The Subscription Portal queries HAAA about WiMAX® session status using the HTTP session source IP
- 6 address. The AAA responds back to the Subscription Portal with information such as Device MAC, etc.
- 7 8. Once the subscription is complete, the Subscription Portal updates the operator’s OSS/BSS with the newly
- 8 created subscription (not shown in the figure) and notifies the HAAA that the subscription is complete
- 9 (including the selected service profile).
- 10 9. The HAAA updates the Device’s subscription status and initiates MS Network Exit.

11

12 **Phase 2: Subsequent MS INE – Device activation phase**



13

14 **Figure 6-2 – Phase 2 – Subsequent INE / Device activation**

- 15 1. The device performs a subsequent INE. The device signals its need for provisioning using NAI decoration
- 16 (SM=1) because subscription activation flag is not set. The HAAA authenticates the device using EAP-
- 17 TLS and identifies there is a valid subscription for the device. The HAAA authorizes an MS network entry
- 18 with the subscribed SLA parameters.
- 19 2. Steps (2) is the same as steps (2) in Phase 1.
- 20 3. Steps (3) is the same as steps (3) in Phase 1.
- 21 4. WIB server contacts the HAAA and provides the MAC address of the MS extracted from the WIB
- 22 bootstrap request message. The HAAA uses the MS’ MAC address to look up for the WiMAX® session

- 1 record and returns back the BEK key, and OTA Status which includes SM=1 and whether there is a
2 subscription (at this stage, the device has a subscription).
- 3 5. The WIB server returns back the Boot-Record (protected by the BEK key). Phase 2 Managed Objects
4 returned in the boot record will include subscription parameters and will set the subscription activation flag.
- 5 6. From the moment the device has been authenticated and authorized (step 1), a normal IP session may be
6 allowed. (operator decision with regards to the user authentication dependency)
- 7 7. A network exit procedure may be triggered by either the MS or the network.

8

9 **Phase 3: Subsequent MS INE – For an activated device**

- 10 When the activated device with a valid subscription performs INE, the HAAA authenticates the device using the
11 selected EAP method and identifies there is a valid subscription for this device. The HAAA authorizes MS network
12 entry with the subscribed SLA parameters.
- 13 The device, now containing activated subscription, will not be using “outer” NAI decoration (SM=1) and will go to
14 the WIB server first whenever it needs to open an OMA-DM session but does not have a valid DM account. This
15 optional phase if executed, presents a n o pportunity for t he N etwork t o modify t he d evice’s M anaged O bjects
16 (defined in Annex E [3]) for an already activated device whenever it is required.

1 **7. WIB Server logic for WIB-based device activation**

2 The following table lists WIB Server actions based on OTA Status received from an HAAA (as described in Phase
3 1/2, step 4).

4 **Table 7-1 – WIB Server actions based on OTA Status received from an HAAA**

NAI decoration - Service Mode Value	Subscription	Action
1	No	Send Bootstrap response without Activation Managed Object.
1	Yes	Send Bootstrap response with Activation Managed Object.
No SM	No	Treat this case as if SM=1 with no subscription.
No SM	Yes	Send empty bootstrap protected by BEK. Ignored by device if no update required. Updated bootstrap when applicable.

5

1 **8. MS Error Handling**

2 MS will ignore any unsupported MO received in the bootstrap response message. In the case of bootstrap-based
3 device activation, the last parameter MS receives is “Activation flag”. If any of the received MOs is unsupported,
4 the “Activation flag” SHALL be ignored. MS MAY use the received and correctly processed MOs as activation
5 parameters in the subsequent INEs. As long as “Activation flag” is not set, the MS SHALL continue using NAI
6 decoration in indicating device provisioning request (i.e. { sm=1}) during the subsequent INEs until device
7 provisioning succeeds (i.e. until “activation flag” is set). The absence of NAI decoration “sm=1” may be interpreted
8 by CSN as the implicit acknowledge for bootstrap provisioning success.

9. Minimum set of WiMAX® MOs to be supported for WIB-based activation

- 1
2
3 The device that announces its support of “OMA-DM WIB-based activation” mode SHALL support the mandatory
4 Management Objects defined in Annex E [3] and SHOULD comply with the WiMAX® Retail Profile package for
5 OTA OMA-DM activation.
- 6 OMA-DM WIB-based device activation is intended to provide capability to create device activation awareness and
7 as such, the device SHALL support minimum set of OMA-DM parameters for activation-awareness [as referred by
8 OTA OMA-DM retail package for device activation]. The network implementing OTA OMA-DM WIB-based
9 device activation SHOULD NOT rely on this method for provisioning of the parameters not defined in OTA OMA-
10 DM activation WiMAX Retail Profile package.