

Attachment 4-2-5

WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures

WiMAX Over-The-Air General Provisioning System Specification

WMF-T33-103-R015v02

Note: This Document is reproduced without any modification with the consent of the WiMAX Forum®, which owns the copyright in them.



WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures

WiMAX Over-The-Air General Provisioning System Specification

WMF-T33-103-R015v02

WiMAX Forum[®] Approved
(2009-11-21)

WiMAX Forum Proprietary

Copyright © 2007-2009 WiMAX Forum. All Rights Reserved.

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

Copyright 2007-2009 WiMAX Forum. All rights reserved.

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

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

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

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

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

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

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

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

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

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

“WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. Third-party trademarks contained in this document are the property of their respective owners.

TABLE OF CONTENTS

1	Revision History	1
2	Document Scope	2
3	Abbreviations and Definitions	3
4	3.1 Abbreviations	3
5	3.2 Terms & Definitions	5
6	3.3 Conventions	7
7	4 References	8
8	5 Use Cases	9
9	6 OTA Provisioning Network Reference Model	11
10	6.1 Functional description	11
11	6.1.1 Provisioning Server	11
12	6.1.2 Provisioning Client	11
13	6.2 Bootstrap Message Format and Encoding	12
14	7 WiMAX General Over-the-Air Provisioning and Activation Overview	13
15	7.1 Overview	13
16	8 WiMAX Initial Bootstrap Procedure Overview	17
17	9 Requirements	18
18	9.1 General Requirements	18
19	9.1.1 Model B (Retail Model) WiMAX Devices and Their Management	18
20	9.2 Device Requirements	18
21	9.3 Provisioning Server Requirements	19
22	9.4 ASN-GW Requirements	19
23	9.5 AAA Requirements	19
24	9.6 Hotline Feature Requirements	20
25	9.7 WIB Procedure Requirements	21
26	9.7.1 Bootstrap Message Encoding	22
27	10 Security Considerations	24
28	10.1 WiMAX Bootstrap Security	24
29	10.1.1 Bootstrap Encryption Key	24
30	10.1.2 Bootstrap Information Protection	25
31	APPENDIX A. SERVICE MODES	26

1 LIST OF FIGURES

2	FIGURE 1: PROVISIONING & ACTIVATION ARCHITECTURE OVERVIEW	11
3	FIGURE 2: PROVISIONING & ACTIVATION PHASES	14
4	FIGURE 3: WIB PROCEDURE	17

5

6 LIST OF TABLES

7	TABLE 1 - MODEL B DEVICE DM REQUIREMENT	18
8	TABLE 2 - VALUES OF PROTOCOL	21
9	TABLE 3 - BOOTSTRAP MESSAGE ENCODING	22
10	TABLE 4 - ENCODING OF NONCE TLV	23
11	TABLE 5 - ENCODING OF CIPHERTEXT TLV	23
12	TABLE 6 - NONCE CONSTRUCTION (13 OCTETS)	25
13	TABLE 7 - INITIAL CCM BLOCK B_0	25
14	TABLE 8 - COUNTER BLOCK CTR_J	25
15	TABLE 9 - SERVICE MODE AVPS FOR WIMAX DECORATION	26

16

1 Revision History

Date	Revision	Description
March 26, 2008	V01	Initial version of Release 1.5.
November 6, 2009	V02	Implementation of CRs 1003 and 1006.

2 Document Scope

Many different device types will be enabled by WiMAX technologies, such as notebooks, ultra mobile devices (UMD), handsets, and consumer electronics. A WiMAX service provider would require a dynamic over the air provisioning solution to configure activate, enable subscription for, and manage these device types.

This document specifies Stage 2 and Stage 3 for general over-the-air provision and activation procedures in WiMAX.

3 Abbreviations and Definitions

3.1 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
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

OTA-General

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
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
	Message Authentication Code
MAC	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
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

OTA-General

POM	Point of Manufacturing
POS	Point of Sale
RADIUS	Remote Authentication Dial In User Service
RAPL	Roaming Agreement Preference List
RDF	Resource Description Framework
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 **3.2 Terms & Definitions**

3 The following terms & definitions are applicable to both the OMA DM [OTAOMADM] and TR-069 [OTATR069]
 4 based WiMAX OTA 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 cooperating with the operator or not).
- 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 other POA is 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
 19 Certification Authority (CA) after the CA has verified that the entity is who it says it is. Certificates can contain
 20 different types of data. For example, an X.509 Certificate includes the format of the Certificate, the serial number of
 21 the Certificate, the algorithm used to sign the Certificate, the name of the CA that issued the Certificate, the name
 22 and public key of the entity requesting the Certificate, and the CA's signature.

- 1 **Certificate Authority (CA):** An entity entrusted to issue Certificates that assert that the recipient individual,
2 computer, or organization requesting the Certificate fulfills the conditions of an established policy.
- 3 **Certificate Revocation List (CRL):** A document maintained and published by a CA that lists Certificates issued by
4 the CA that are no longer valid.
- 5 **Channel Plan:** A Channel Plan is used by the device to speed up NAP discover process. It contains physical
6 information such as channel bandwidth, center frequency, and PHY profile.
- 7 **Continuous Provisioning:** The process where a device that is already provisioned with a user account associated
8 with an active subscription with a service provider is updated with new data, parameters, and/or applications that
9 MAY replace pre-existing values or versions. The Continuous Provisioning process is based on the definition in
10 [DMRD] and includes the configuration maintenance/management use case described in the same specification.
- 11 **Contractual Agreement Preference List (CAPL):** A list consisting of Network Access Providers preferred to be
12 connected to the home network directly
- 13 **Customer Service Center (CSC):** An entity in a wireless carrier's network that receives service requests from the
14 end users and acts on such requests.
- 15 **Device Lock:** Blocking the WiMAX host device from getting activated on new operators and enforcing the device
16 to work only with the operator, which is locked, as a H-NSP.
- 17 **Device Management (DM):** Process of remotely managing device settings and applications. DM provides a
18 mechanism for the users to easily subscribe to new services and make changes to their existing services. For the
19 operators this enables a fast and easy way to introduce new services and manage provisioned services, by
20 dynamically adjusting to changes and ensuring a certain level of quality of service.
- 21 **Device Management System** A background system capable to interact with a (set of) Device(s) for the
22 purpose of Device Management.
- 23 **Device Profile:** Settings that establish the configuration of a particular device, including network settings,
24 applications, etc.
- 25 **Device Unlock:** Process of allowing the device to get activated on other Service Providers' networks.
- 26 **Host Device:** Refers to a standalone device or a sub-module in which WiMAX modem (chipset) is embedded. This
27 is the device that is to be managed as this specification defines, associated with MAC ID, and SHOULD appear in
28 DevInfo and DevDetail MOs. Examples of host device are: 1) Removable Modem (e.g., PC Card, USB Modem,
29 etc.) with embedded WiMAX chipset; 2) WiMAX sub-module physically attached to a WiMAX CPE Gateway; 3)
30 WiMAX sub-module temporarily or permanently built into a laptop; 4) WiMAX enabled consumer electronics (e.g.,
31 Digital Camera, PMP, etc.) that has the embedded WiMAX chipset.
- 32 **Management Object:** A data model for information, e.g., a configuration parameter, an image, or a file, which is a
33 logical part of the interfaces exposed by DM components and managed through the use of OAM&P.
- 34 **Model A:** Operator/service provider subsidized device, similar to the current cellular, cable modem, or DSL
35 services provisioning models. Different SKU provided for each device at POM to connect to one WiMAX network
36 or group of WiMAX networks. Model A May support self-subscription OTA or via a web portal.
- 37 **Model B:** Generic SKU retail devices. SHALL support over-the-air self-subscription and provisioning.
- 38 **Model B1:** Non-operator/service provider subsidized device.
- 39 **Model B2:** Operator/service provider subsidized device. Device contains operator/service provider specific
40 configuration.
- 41 **Multimode Device:** Device supporting two or more wireless access technologies.
- 42 **NAP Based Channel Plan:** A Channel Plan which is a subset of Root Channel Plan and is associated with a NAP.
- 43 **OMA DM:** Refers to the set of specifications developed by Open Mobile Alliance for DM.
- 44 **Prior Connect Info:** Specified in [NWGSTG3].

Provisioning: Populating the device and the network management with data and software needed for the operation on the operator network and for improving the user experience (value added services and applications). Provisioned information SHOULD be divided into 3 groups:

- Information that can be provisioned only during activation.
- Information that can be provisioned during normal operation but only when connected to home-operator.
- Information that can be provisioned during normal operation by any operator.

Provisioning Server: Refers to a server that communicates with the device using the provisioning protocol in the provisioning process.

Roaming Agreement Preference List (RAPL): A list delivered to the device consisting of Network Service Providers preferred to be connected to when roaming.

Root Channel Plan: A Channel Plan which contains all Channel Plan Entries.

Smart Card: A smart card (or chip card, or integrated circuit card) is a miniaturized electronic card with embedded integrated circuits which can process information. This implies that it can receive input from trusted source and process the information in a standardized manner and deliver processed information as an output to trusted entities it interacts with. There are two broad categories of smart cards. The first category is memory cards (or flash memory card) used in handheld devices, digital cameras, laptops, etc., containing only non-volatile memory storage components, and perhaps some specific security logic. The second category is microprocessor cards that contain volatile memory and microprocessor components.

Service Credential: Credential used to allow the user to access the carrier services.

Terminal Equipment: 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 sub-module; 3) Embedded laptop which has WiMAX sub-module permanently built in; 4) Consumer electronics that has a WiMAX submodule.

User Profile: The User Profile is a collection of components (personal data, preferences/policies on services, networks and devices, etc.) that indicate the preferences and current configuration of a user's account. User profiles enable several users to use the same device with their own setup. The User Profile is tightly coupled with the user's identity and vice versa.

WiMAX Radio Module: Refers to WiMAX radio chipset and subsystem present in the host device and that enables WiMAX radio connectivity for the host device.

WiMAX CPE Gateway: Network equipment through which a subscriber can connect one or more PCs, laptops, or other networked devices (e.g., STB) via one or more LAN ports (e.g., Ethernet, Gigabit Ethernet WiFi, Cable Connection). The WiMAX CPE Gateway provides services, such as voice and multimedia content via a WiMAX Network. It MAY include an analog telephone adapter (ATA), and can support connectivity to an analogue telephone or an external analog Terminal Adapter. A WiMAX CPE Gateway conforms to the NWG mobility specification [NWGSTG3], and IEEE 802.16e-2005. A WiMAX CPE Gateway MAY also function as a 'layer 2 bridge' or 'layer 3 router.' It MAY support other IP stack functions like NAT(P/T) DNS/DHCP secure pass through, NAT Traversal, firewalling, parental control/DPI, security features, OAM features, and/or network diagnostics agents.

X.509: Digital Certificate Definition X.509 [RFC3280]

3.3 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

1 4 References

- [DMRD] "OMA Device Management Requirements Document, Version 1.2". Open Mobile Alliance. OMA-RD-DM-V1_2. URL:<http://www.openmobilealliance.org>
- [DMERELD] "Enabler Release Definition for OMA Device Management, v1.2," Open Mobile Alliance, OMA-ERELD-DM-V1_2, URL:<http://www.openmobilealliance.org>.
- [DSLTR069] DSL Forum TR-069, CPE WAN Management Protocol, May 2004, and Amendment 1, November 2006 URL: <http://www.dslforum.org>
- [NIST800-38C] NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004
- [NWGSTG3] WiMAX Forum, T33-001-R015v01, "Detailed Protocols and Procedures, Base Specification", Release 1.5
- [OTAOMADM] WiMAX Forum T33-104-R015v04, "Architecture, detailed Protocols and Procedures, WiMAX Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications", Release 1.5
- [OTATR069] WiMAX Forum T33-105-R015v01, "Architecture, detailed Protocols and Procedures, Over-The-Air Provisioning & Activation Protocol based on TR-069 Specification", Release 1.5
- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>
- [RFC2246] "The TLS Protocol Version 1.0", T. Dierks, C. Allen, January 1999, <http://www.ietf.org/rfc/rfc2246.txt>
- [RFC2616] "Hypertext Transfer Protocol – HTTP/1.1", R. Fielding et al, June 1999, <http://www.ietf.org/rfc/rfc2616.txt>
- [RFC2618] "HTTP Over TLS", E. Rescorla, May 2000, <http://www.ietf.org/rfc/rfc2818.txt>
- [RFC2782] "A DNS RR for specifying the location of services (DNS SRV)", A. Gulbrandsen, P. Vixie, L. Esibov, February 2000, <http://www.ietf.org/rfc/rfc2782.txt>
- [RFC3268] "Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)", P. Chown, June 2002, <http://www.ietf.org/rfc/rfc3268.txt>
- [RFC3280] "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?number=3280>
- [RFC4282] "The Network Access Identifier", B. Aboba, M. Beadles, J. Arkko, P. Eronen, December 2005, <http://www.ietf.org/rfc/rfc4282.txt>

5 Use Cases

The use cases for OTA activation provisioning of generic SKU retail Model B1 devices are:

Note: Smart Card supports is out of scope of this specification.

- 1) Out-of-band subscription establishment: User establishes a temporary, new permanent, or previously cancelled/expired subscription with a service provider without the use of a network connection from the device to be provisioned (e.g., receiving updated configuration, network ID lists and authentication information, as required, via a secure web portal). Then to activate the device, either the service provider triggers a network initiated provisioning session or the device triggers a client initiated provisioning session when the device attaches to the network.
- 2) In-band subscription establishment: User establishes a temporary, new permanent, or previously cancelled/expired subscription with a service provider through the use of a network connection from the device to be provisioned which then either triggers a network initiated provisioning session or the device triggers a client initiated provisioning session while the device is attached to the network.
- 3) The subscribed user either adds (temporarily or permanently) a new device to the active user subscription account or modifies the user subscription to replace an actively subscribed device with a different device, either through in-band or out-of-band subscription establishment methods. After which, the newly subscribed device is activated through the use of a network initiated or client initiated provisioning session while the newly subscribed device is attached to the network.

The use cases for OTA activation provisioning of partially provisioned Service Provider subsidized Model A and B2 type devices are:

- 4) The device has been partially provisioned with data specific to a given service provider X before it is acquired by the user. The device can only be provisioned for service with service provider X. OTA provisioning completes the configuration of the device.
 - a. User subscription is performed out-of-band and device is activated over the air in service provider's X network as in case 1.
 - b. User subscription is performed in-band in service provider's X network and device is activated over the air in service provider's X network as in use case 2.
 - c. User subscription with service provider X already exists. User subscription is modified in-band or out-of-band. The subscribed user either adds (temporarily or permanently) a new device to the active user subscription account or modifies the user subscription to replace an actively subscribed device as in use case 3.

The use cases for OTA continuous provisioning for Model A and Model B type devices are:

- 5) When the device is attached to the network, the service provider triggers a network initiated update to the configuration information stored in the device (e.g., user subscription data, ND&S configuration information, change the device lock/unlock state, etc.) when the service provider determines it is needed to update or change the behavior of the device.
- 6) When the device is attached to the network, the user or support personnel triggers a client initiated update to the configuration information stored in the device (e.g., user subscription data, ND&S configuration information, change the device lock/unlock state, etc.) when it is determined that improvements in the device behavior are needed.

The use cases for OTA re-provisioning for Model A and Model B type devices are:

- 7) A subscribed and activated device is attached to the network, the device uses the device authentication and the initial provisioning and activation decoration since the device wishes to be fully re-provisioned by the server. The network performs full initial provisioning and activation flow with the device as it is an initial activation with Out Of band (OOB) subscription.

The use case for OTA deferred provisioning for Model B type device is:

OTA-General

- 8) User establishes a subscription with a service provider. The subscription is obtained out-of-band or in-band. After subscription, the device is considered activated by the NW but the NW does not have the ability to initially provision the MS with any parameter hence the device is not aware of the activation. However, the non activated-aware device is still capable of completing network entry as an un provisioned device and receive some level of service. At a later date, once the network deploys a DM server – it can perform initial provisioning of the device during the next network entry.

The use cases for OTA activation provisioning based on smart card are:

- 1) A smart card is inserted into the device for the first time. The smart card contains information that provides contact information for the provisioning server in the Service Provider network as well as a set of shared secrets with the provisioning server to define a trust relationship. The smart card allows the device to connect to a correct network and get provisioned. It can be used by all device type models (A and B).
- 2) A smart card is inserted into a used device that might contain erroneous provisioning parameters from a previous configuration. The device will use the information in the smart card to obtain a proper set of parameters and then gets provisioned using these parameters.

6 OTA Provisioning Network Reference Model

The OTA Provisioning architecture is based on WiMAX Release 1 Network Reference Model.

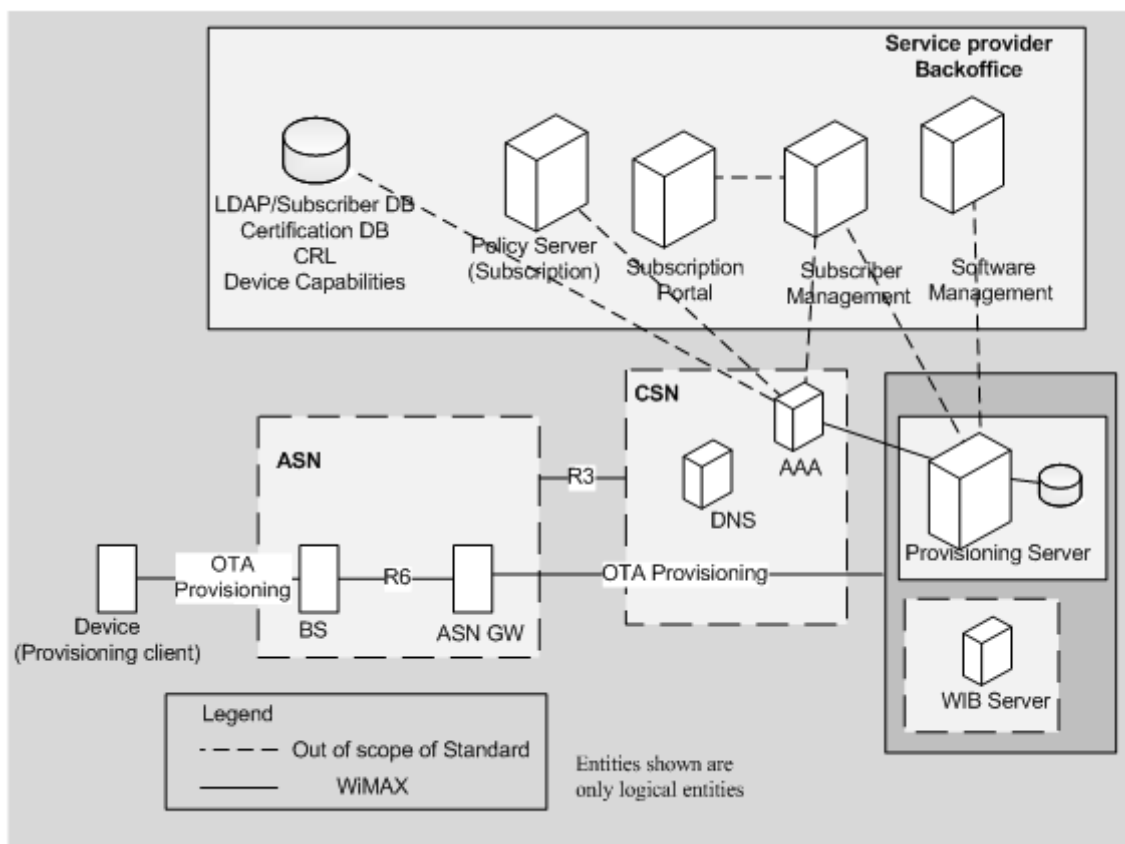


Figure 1: Provisioning & Activation Architecture Overview

6.1 Functional description

6.1.1 Provisioning Server

The provisioning server is a management authority that has the right to perform a specific device management function on a device or to manipulate a given data element or parameter.

For networks that support OMA DM based activation and provisioning, the provisioning server SHALL support the WiMAX OTA Provisioning & Activation based on OMA DM [OTAOMADM].

For networks that support DSL TR-069 based activation and provisioning, the provisioning server SHALL support the WiMAX OTA Provisioning & Activation based on TR-069 protocol, as specified in [OTATR069].

6.1.2 Provisioning Client

The provisioning client is an agent in the device that is an extension of the provisioning protocol to support WiMAX requirements as specified in this document.

For devices that support OMA DM based activation and provisioning, the provisioning client SHALL support the WiMAX OTA Provisioning & Activation based on OMA DM, as specified in [OTAOMADM].

For devices that support DSL TR-069 based activation and provisioning, the provisioning client SHALL support the WiMAX OTA Provisioning & Activation based on TR-069, as specified in [OTATR069].

6.2 Bootstrap Message Format and Encoding

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

- **OMA Client Provisioning** - This profile specifies alignment of two existing enablers – OMA Client Provisioning [ERELDCP] and OMA Device Management [ERELDDM]. The profile defines how the information provisioned using OMA Client Provisioning can be transferred to the management tree specified in the OMA Device Management.
- **OMA Device Management** - This profile defines how the OMA Device Management [ERELDDM] can be used for bootstrapping.

WiMAX devices MUST support the OMA Device Management profile for the bootstrap message. This means the UDP payload of the bootstrap message MUST be formatted in accordance with [ERELDDM], and then encrypted as described in [OTAGEN] Security Consideration section.

Support for OMA Client Provisioning over WiMAX is not prohibited, but is not recommended either.

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

7 WiMAX General Over-the-Air Provisioning and Activation Overview

7.1 Overview

The Figure 2 illustrates the overview of the activation & provisioning procedure. This procedure consists of following three phases:

- 1) Pre-Provisioning.
- 2) Subscription and Provisioning.
- 3) Post-Provisioning.

The Figure 2 covers the following use cases:

- 1) User has established business relationship (existing subscription) with service provider. Provisioning an un-provisioned device when the device is attached to the network.
- 2) User establishes business relationship with service provider while attached to the network with an un-provisioned device and the device receives provision data.
- 3) The subscribed user either adds a new device to the user subscription account or replaces an existing device with a new device.
- 4) Service provider updates the information stored in an already activated device (e.g., user subscription data, etc.) when it is needed (i.e., continuous provisioning). Refer back to section 5 for detailed description of these use cases.
- 5) User has established business relationship with service provider, device lost provisioned data. Re-provisioning an already provisioned device (according to server information) when the device is attached to the network.

Working Assumption:

- 1) One or more specific provisioning protocol clients are installed in the device.
- 2) The default subscriber policy and hotline rules are installed at the H-AAA by the network service provider. The procedure for installing these rules are outside the scope of the specification.
- 3) The hotline function is RECOMMENDED.

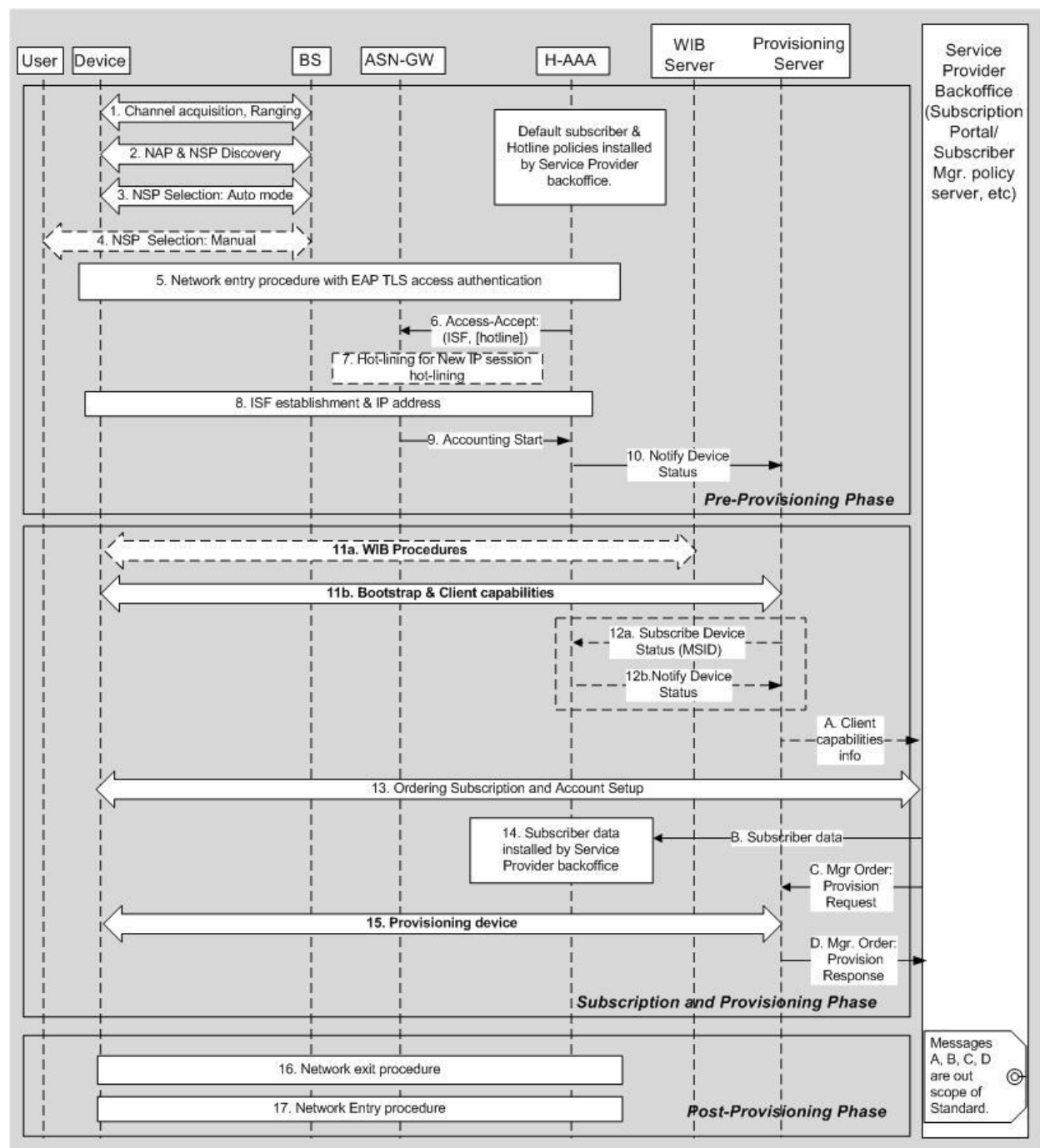


Figure 2: Provisioning & Activation Phases

The Model A, B1, and B2 devices SHALL perform all of these phases. There MAY be a slight variation within each phase for each device model or use case. The detailed procedure is specified in the following sections and the [OTAOMADM] or the [OTADSLTR069] specification. The following paragraph describes some of the main procedures within each of the phases.

Pre-Provisioning Phase (Steps 1-10):

1. The device performs channel acquisition and ranging.
2. The device detects one or more available WiMAX NAPs and discovers available NSPs associated with one or more NAPs.

OTA-General

3. The device discovers available NSPs associated with one or more NAPs and an NSP based on some preference criteria (if available).
4. The device identifies accessible NSPs and selects an NAP and an NSP based on some preference criteria (if available). Or, the user performs NSP manual selection.
5. The device performs Network entry procedures with a special decorated NAI for entering the provisioning mode. The Network entry procedures SHALL be based on [NWGSTG3].
6. The NSP MAY decide to authorize limited access to the device for the purpose of creating a business relationship with the user. The limited access is controlled by using the Hotline procedure [NWGSTG3], where the H-AAA will notify the ASN-GW that the device is to be hot-lined, via the ISF authorization, i.e., Access Accept.
7. The H-AAA MAY activate hot-lining if decided by the Network Service Provider. If the Network Service Provider has decided that un-provisioned devices have to be put in the hot-lined state, the hot-lining can be activated either in the ASN-GW or in the HA (it depends on the ASN-GW and the HA capabilities). The H-AAA provides the hotline attributes. In the example, the hotline attributes are provided to the ASN-GW. The hot-lining MAY be as simple as blocking all IP traffic between the device and other hosts, detail of hot-lining rule, see section 8.6 .
8. The device performs the DHCP procedure to obtain a point of attachment address Based on the ISF data, the ASN-GW initiates the data path setup with a proper classifier installed.
9. ASN-GW sends accounting start information to H-AAA.
10. Upon receiving accounting start information, the H-AAA informs the provisioning server of the device status.

Subscription and Provisioning Phase (Steps 11-15):

The actual order of these steps MAY vary depending on the implementation of the subscription portal subsystem, and the device model. During the entire Subscription and Activation phase the subscription portal should be used as the mean to interact with the user and deliver messages to him (such as “activation in process”, “your device was successfully activated” etc...).

The key steps in this phase are the following:

11. The bootstrap procedure is performed. According to the device type, one of the following two steps or both are performed.
 - a. The device and the provisioning server perform a WIB procedure. The WIB procedure is a method to allow the client to advertise the DM OTA protocol it supports, the network to select the DM OTA protocol to be used, and to deliver DM OTA protocol specific bootstrap information. This is an optional step for some type of devices.
 - b. The device and the provisioning server perform a Bootstrapping & Device capabilities procedure. The Bootstrapping procedure is a method for the provisioning server to deliver the bootstrap information to the device. The bootstrap information MAY contain the provisioning server contact information and credentials. The bootstrapping procedure MAY be part of the WIB procedure. The device capabilities information MAY be delivered to the provisioning server through DM session following the bootstrapping procedure.
12. The provisioning server MAY subscribe device status to the H-AAA server if necessary. Then if the status of the device is changed the H-AAA server sends a notification message to the provisioning server.
 - A. The device capabilities information is delivered to subscription portal.
13. The user creates a business relationship enabling access via the selected NSP to the subscription portal. Based on the user input and device capabilities, the subscription portal creates a user account.
 - B. The user account information is delivered to a data base where the H-AAA and the provisioning server have access to the information.
14. The user account information is stored in the database.
- C. The subscription portal requests the provisioning server to initiate the provisioning process.
15. A management session is established between the provisioning client and the server to deliver the provisioning data. The provisioning procedure is a method for the device to acquire and store the provisioning data, i.e., managed objects. Either the provisioning client or the server MAY initiate the management session.
 - D. The provisioning server responses the provisioning results to the subscription portal.

Post-Provisioning Phase (Steps 16-17):

OTA-General

1 16. Upon completion of the provisioning phase, the H-AAA will request the ASN-GW to initiate the network
2 exit procedure [NWGSTG3].

3 17. If the NW-Exit procedure was initiated within 90 seconds from the time of provisioning completion, the
4 device will treat this NW-Exit as the last phase of OTA activation and then perform the network exit and
5 re-entry procedure using the new credentials to ensure the network access keys are properly installed and
6 used.

7 If NW-Exit happened past that time, the device uses its normal ND&S algorithm.

8
9 Note that during continuous provisioning, the service provider updates the information stored in the device already
10 associated and provisioned with an active user account. The continuous provisioning operation only requires the step
11 15 at a minimum.

8 WiMAX Initial Bootstrap Procedure Overview

The WiMAX Initial Bootstrap (WIB) procedure enables the discovery and negotiation of the device management (DM) OTA protocol to be used between the device and the network. The procedure consists of WIB server discovery using DNS SRV records [RFC2782], and WIB OTA protocol negotiation using simple HTTP between the device and the WIB server.

The device initiates the WIB server discovery and protocol negotiation upon obtaining a point of attachment IP address using DHCP, and provides information about the OTA protocols it supports to the WIB server using the HTTP GET method. The WIB server uses the information provided by the client, selects an appropriate OTA protocol, and provides OTA protocol specific bootstrap information about the selected protocol in the HTTP response. If a mutually supported OTA protocol cannot be selected, the WIB server responds with an HTTP error, and the OTA provisioning cannot proceed. With the successful execution of the bootstrapping process, a secure path between the device's DM client and the DM provisioning server can be established and the protocol specific provisioning process for the device can begin.

WIB server is a functional entity that enforces OTA DM protocol for a particular domain, and MAY store the configuration bootstrap information, MAY act as a proxy to deliver the bootstrap information, or MAY redirect the device to another server that can deliver the bootstrap information. The figure below illustrates the WIB procedure.

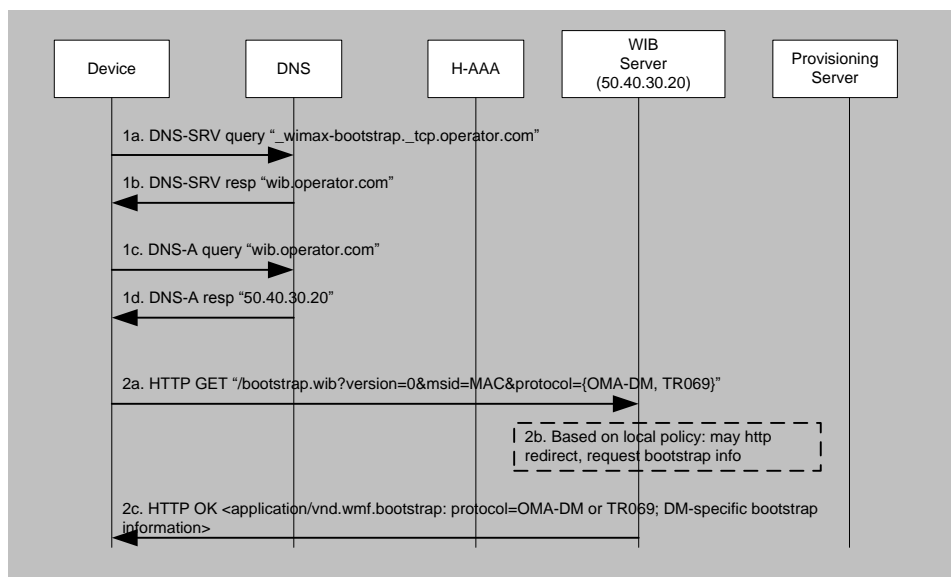


Figure 3: WIB procedure

9 Requirements

B1 and B2 devices SHALL be able to support all the functions specified in this section. However, during the actual OTA provisioning operation, A and B2 type devices with sufficient pre-configured information SHALL NOT be required to follow all the steps specified here.

9.1 General Requirements

1. OMA DM SHALL be mandatory for provisioning all Model B (retail) WiMAX devices, i.e., for all WiMAX retail devices OMA DM is the default OTA provisioning mechanism.
2. In addition to OMA DM, TR-069 SHALL be also mandatory for provisioning Model B (retail) WiMAX devices classified as CPE gateway, and this option is selectable by the service provider at initial DM protocol discovery phase.
3. WIB procedure MUST be run on devices supporting a provisioning protocol other than OMA DM.
4. WIB procedure MUST be run on devices supporting only OMA DM if they cannot support OMA DM server initiated bootstrap, i.e., the UDP Push bootstrap.
5. All networks supporting OTA provisioning MUST support WIB procedure.
6. Networks supporting OMA DM MUST start the OMA DM server initiated bootstrap immediately after notification from AAA (i.e., UDP Push).
7. The device MUST use the first bootstrap message it successfully received (either WIB or UDP Push) and silently discard all subsequently received bootstrap messages.
8. In the case of WIB, after initial DM protocol discovery the device SHALL be provisioned using the negotiated protocol.
9. Network MUST respond to device provisioning request {sm=1} even if device is considered provisioned by the network. The network SHALL initiate a provisioning flow with the device.

[Note: In R1.5, OMA DM will not support all the CPE parameters. These will be worked in future releases.]

9.1.1 Model B (Retail Model) WiMAX Devices and Their Management

The following Table 1 provides the classification of Model B WiMAX devices and their Device Management protocol.

Table 1 - Model B device DM requirement

Type of device	DMRequirements at device
WiMAX CPE Gateway	OMA DM- Mandatory; TR-069 - Mandatory
other WiMAX devices	OMA DM - Mandatory

9.2 Device Requirements

In order to acquire provisioning data, the device SHALL perform the following steps:

- 1) The device SHALL perform device authentication as a part of the network entry procedure as defined in [NWGSTG3] Section 4.3 (Network Entry and Exit), with the following sub-clauses:
 - a. When the device responds with an EAP Response/Identity message providing the NAI, the device SHALL include the WiMAX OTA provisioning service mode attribute value pair (avp), i.e. 'sm=1', in the WiMAX decoration of the NAI to indicate that the device is entering the network to perform OTA provisioning and activation. The NAI format MUST conform to [NWGSTG3].

- b. The WiMAX decoration MUST be used to indicate to the AAA server that the device wishes to perform OTA provisioning and activation. The WiMAX decoration of the NAI SHALL be '{sm=1}' for the WiMAX OTA provisioning and activation. For example, a correctly decorated NAI for OTA provisioning is '{sm=1}ms-id@realm'. The device SHALL use the procedures defined in [NWGSTG3] to determine the realm and to construct the NAI.
 - c. For model B devices, the MS SHALL follow the procedure of comparing the extracted domain name from the server certificate with the realm used in the NAI as defined in [NWGSTG3] but SHALL skip the procedure of comparison of realms between extracted domain name from server certificate against configured list of realms.
- 2) The device SHALL obtain a point of attachment address, as defined in [NWGSTG3].
 - 3) The device SHALL support the network exit procedure specified in the [NWGSTG3].
 - 4) When provisioning data is updated to the device via continuous management, the device SHALL take all authentication related parameters into use in the next authentication or re-authentication and all other parameters at latest during the next initial network entry.
- All authentication related error case procedures defined in [NWGSTG3] SHALL be followed.

9.3 Provisioning Server Requirements

In the case of OMA DM activation and provisioning solution, the provisioning server SHALL support the OMA DM Protocol [DMERELD] and the [OTAOMADM] specification.

In the case of DSL TR-069 activation and provisioning solution, the provisioning server SHALL support the TR-069 Protocol [DSLTR069] and the [OTATR069] specification.

The provisioning server MAY subscribe to the device event status with the H-AAA when receiving the bootstrapping or provisioning request. When subscribing to the device event status, the subscription message SHALL include at least the MAC address of the device as an MSID.

If the provisioning server receives a message which contains invalid attributes or the message format is not valid or the message does not contain all the mandatory attributes the provisioning server SHALL ignore the received message and respond to the sender with an appropriate response message if it is available.

9.4 ASN-GW Requirements

The ASN-GW SHALL conform to [NWGSTG3] with the following sub-clauses:

1. Upon receiving the EAP Response/Identity from the device the ASN-GW (NAS) SHALL perform the network entry procedure as specified in the [NWGSTG3] specification.
2. The ASN-GW SHALL process the Access-Accept message as specified in the [NWGSTG3] specification.
3. Upon successful establishment of an IP session with the device, the ASN-GW SHALL send the Accounting-Request Start message.
4. The ASN-GW SHALL support the network exit procedure based on the Network Trigger, as specified in [NWGSTG3] Section 4.5.2.1.2.(Network Trigger).

9.5 AAA Requirements

The H-AAA receives a RADIUS Access Request containing an EAP message attribute set to the NAI value received in an EAP-Response Identity from the device. The H-AAA SHALL process the Access-Request, Access- Accept, and Accept-Reject messages as specified in the [NWGSTG3] specification in Section 4.4 (Authentication, Authorization and Accounting).

Upon successful device authentication using the provisioning mode (i.e., {sm=1}), the H-AAA SHALL send an Access-Accept message as defined in the [NWGSTG3] specification in Section 4.4 and SHALL perform the following steps:

- 1) The H-AAA MAY set the hotline attribute for network access control.

- 2) The H-AAA SHALL use the access policy of the provisioning mode to create the Initial Service Flow (ISF).
If the NW has provisioning capabilities, It is recommended that, for non subscribed MSs, the access policy of the provisioning mode SHOULD limit access to only the subscription portal, the WIB server and the provisioning server (if available), as well as limit the number of pre-provisioned service flows.
(The NW may have a different policy for subscribed devices that enters in the provisioning mode i.e. re-provisioning).
If the NW does not have provisioning capabilities the use of the provisioning access policy by the H-AAA is expected only in the case that the MS does not have a subscription. After Subscription has been obtained, it is up to the operator to decide the level of access the H-AAA allows for this MS.

Upon the reception of the Accounting-Start message, the H-AAA SHALL send a notification to the WIB and provisioning servers (if they are available) containing the computed BEK, the MSID, the IP address of the device, and the value of the Session-Timeout Attribute [NWGSTG3]. The notification protocol is out of the scope of this document.

In the case where the provisioning server subscribes to the event status of a specific device, the H-AAA server SHALL notify the event status to the provisioning server by delivering the computed BEK, the MSID, the IP address of the device, and the value of Session-Timeout Attribute, upon receiving the Accounting Start message. The protocol of subscription and notification of the event status method is out of the scope of this document.

Upon completion of the provisioning phase, the H-AAA SHALL initiate the network exit procedure, as specified in the [NWGSTG3] specification in Section 4.5.2.1.2. The method of detecting the completion of the provisioning phase is out of the scope of this document.

When provisioning data is updated to the device via continuous management, H-AAA SHALL take all authentication related parameters into use in the next authentication or re-authentication.

All AAA related error case procedures defined in [NWGSTG3] SHALL be followed.

9.6 Hotline Feature Requirements

The Hotline feature as defined in the [NWGSTG3] specification MAY be used with the WiMAX Over-The-Air provisioning and activation procedure to enhance the user experience and to provide network access control.

The H-AAA MAY activate hot-lining, depending on the policy of the Network Service Provider, i.e., Network Service Provider MAY decide that un-provisioned or non-activated device(s) entering the network have to be hot-lined. How the H-AAA is aware of this decision is out of the scope of this document.

The Hot-lining function of the Hot-Lining Device (HLD) MAY be implemented in the ASN-GW or the HA depending on their capabilities. The Hot-line-Session-Timer and Hot-Lining Rules are provided by the H-AAA. As an alternative to the Hot-Lining Rules, the Hot-line-Profile-ID MAY be provided by the H-AAA, and then a set of rules per each different Hot-line-Profile-ID SHALL be configured in the ASN-GW or the HA.

If the hot-lining is activated, the Hotline-Profile or the Hot-Lining-Rules SHALL be configured in the way that:

- The Hotline-Profile and Hotline-Rules SHALL NOT affect CMIP and DHCP traffic.
- Traffic between the device and the DNS server SHALL be passed.
- Traffic between the device and the provisioning server SHALL be passed.
- HTTP traffic between the device and the subscription portal SHALL be passed.
- Additional other special traffic MAY be allowed depending on the policy of the Network Service Provider. (e.g., HTTP traffic to some other special servers)
- Other HTTP traffic MAY be redirected to an Operator Portal.
- Additional other traffic MAY be allowed depending on the policy of the Network Service Provider.

9.7 WIB Procedure Requirements

A device that does not support OMA DM or TR-069 server initiated bootstrap SHALL use the WIB procedure (Section 8) based on DNS and HTTP. The device SHALL perform a DNS SRV query [RFC2782] to resolve the location of the WIB server upon IP session establishment. The Service in the SRV query SHALL be “wimax-bootstrap”. The protocol in the SRV query SHALL be “tcp”. If the target NSP realm is available the Name in the SRV query SHALL be the domain of the target NSP realm. If the target NSP realm is not available from the 802.16 SBC-RSP, the Name in the SRV query SHALL be the Domain Name obtained from DHCP procedure (DHCP option 15 [RFC2132]). The DNS server SHALL resolve this domain name to the FQDN of the WIB server of the NSP.

DNS related error cases are defined in [RFC2782] specification. If the device is not able to understand the received DNS SRV response message or the device did not receive the message it MAY send a new DNS SRV query to the network until the maximum retry count is exhausted. If the WIB server address resolution is successful, the device SHALL open a HTTP session [RFC2616] to the WIB server to inform the WIB server of the supported DM OTA protocol(s), and retrieve the bootstrap information. The device SHALL use the HTTP GET method with the Request-URI “/bootstrap.wib?version=VERSION&msid=MAC&protocol={ PROTOCOL}”. The device SHALL provide the MAC address in the URI using the MSID query parameter and SHALL indicate the WIB HTTP protocol version in the URI using the “version” parameter (see Table 3 for supported versions). The device SHALL provide a comma-separated list of the supported provisioning protocols in the “protocol” parameter the values are specified in Table 2.

Table 2 - Values of PROTOCOL

PROTOCOL	Value
OMA DM	0
TR-069	1
Reserved	2 - 65535

For example, when assuming the following parameters;

VERSION = 0

MAC = 001122334455

PROTOCOL = OMA-DM

WIB Server Domain = wibserver.foo.com

The URI will be “http://wibserver.foo.com/bootstrap.wib?version=0&msid=001122334455&protocol={0}”

When assuming the following parameters for a device that supports both OMA-DM and TR-069;

VERSION = 0

MAC = 001122334455

PROTOCOL = OMA-DM or TR-069

WIB Server Domain = wibserver.bar.com

The URI will be "http://wibserver.bar.com./bootstrap.wib?version=0&msid=001122334455&protocol={0,1}"

If the “protocol” parameter is not present, the server SHALL behave as if “OMA DM” was specified. The device MAY provide additional optional parameters in the Request-URI. The following optional parameters are defined: “vendor” and “model”. These parameters can be used by the device to notify the network of the vendor name and model ID of the device itself. The network MAY use this information to select the DM protocol to be used and to determine the bootstrap information. The device SHALL provide an Accept Header [RFC2616] containing the media type defined for the bootstrap (application/vnd.wmf.bootstrap).

WIB server SHALL respond to the device with one of the following HTTP responses:

1. 200 OK. If the WIB server can provide the bootstrap information for the device identified with the MAC address, the WIB server SHALL reply with an HTTP 200 OK message containing the bootstrap information in the response body encoded as specified in section 10.1. The Content-Type of the reply SHALL be “application/vnd.wmf.bootstrap”.
2. 302 Found. If the WIB server does not support bootstrap information delivery but can redirect the device to another server that can provide the bootstrap information, the WIB server SHALL reply with an HTTP 302 Found message containing the URI to the location of the bootstrap information. Upon receiving the redirect the device SHALL open an HTTP session to the indicated URL and SHALL use the HTTP GET method with the new server. The new server SHALL support the WIB HTTP query with the parameters and responses specified in this chapter.
3. 400 Bad Request. If the WIB server does not understand the request due to malformed syntax, corrupted packet, decode error, unsupported WIB protocol revision, etc., it SHALL reply with an 400 Bad Request message which indicates the failure of the OTA provisioning procedure.
4. 403 Forbidden. If the HTTP GET message contains an OTA Provisioning protocol which is not supported by the associated WiMAX network of the WIB server or is not allowed for the requested and known device (e.g. non-CPE device identified via MAC address requesting only TR-069 protocol). In this case the WIB server SHALL reply with an HTTP 403 Forbidden message which indicates the failure of the OTA provisioning procedure.
5. 404 Not Found. If the server cannot provide the bootstrap information or redirect the device to another server, it SHALL reply with an HTTP 404 Not Found message which indicates the failure of the OTA provisioning procedure.

If the device does not receive the WIB HTTP response message or the device is not able to understand it the device MAY send a new WIB HTTP GET message to the network until the maximum retry count is exhausted. It is not in the scope of this document to define the value for max retries.

In order to ensure robustness of WIB protocol independent of the exact NW provisioning implementation, it is recommended that the device will retry WIB procedure several times spread over a minimum period of 10 minutes before deciding that the retry counter is exhausted (for example 10 retries, 1 every minute).

In all WIB procedure error cases occurring during initial provisioning the device SHOULD perform network exit procedure as described in [NWGSTG3] after the maximum retry count is exhausted.

9.7.1 Bootstrap Message Encoding

The bootstrap information SHALL be provided to the device using the format defined for the bootstrap, i.e., application/vnd.wmf.bootstrap. The bootstrap information consists of a fixed size header followed by a variable size data as described below.

Table 3 - Bootstrap Message Encoding

	Header			Data
Field	Version	Protocol	Length	Data
Number of Octets	2	2	4	Variable (0 – 2 ¹⁶ -9)

Octet Significance	MSB LSB	MSB LSB	MSB LSB	DM protocol specific
Value	0 1 – 65535 = Reserved	Protocol Value defined in Table 1	Data length as a number of octets	DM protocol specific

The version field SHALL contain the value 0 for this version of the protocol. The protocol field SHALL be a value taken from the Table 1. The data portion SHALL contain DM specific bootstrap information encrypted and authenticated using AES-CCM as described in Section 10.1 WiMAX Bootstrap Security. The encrypted bootstrap document and the nonce value MAY be transmitted to the client in a Type-Length-Value (TLV) encoded message as described in Table 5 and Table 6. The exact type and number of TLVs used in the WIB response is specified in the relevant documents [OTAOMADM] and [OTATR69].

The size of the type field SHALL be two octets, the size of the length field SHALL be four octets, and the size of the value field SHALL be 13 octets for the nonce value and 0 - 2^{16} -34 octets for the ciphertext value. The TLVs that SHALL be used are described in Table 5 and Table 6.

Table 4 - Encoding of Nonce TLV

Field	Type	Length	Value
Number of Octets	2	4	13
Octet Significance	MSB LSB	MSB LSB	MSB LSB
Contents	0 = Nonce	13	The nonce value selected by the server.

Table 5 - Encoding of Ciphertext TLV

Field	Type	Length	Value
Number of Octets	2	4	Variable (0 – 2^{16} -34)
Octet Significance	MSB LSB	MSB LSB	MSB LSB
Contents	1 = Ciphertext	Value field length as a number of octets	Encrypted bootstrap

Additional TLVs MAY be used by WiMAX OMA DM or WiMAX TR-069 protocols to carry protocol specific bootstrap information. However, the total length of the entire bootstrap information payload SHALL NOT exceed 65535 octets. The format of these additional TLVs is specified in the relevant documents [OTAOMADM] [OTATR069].

The device SHALL discard the bootstrap message and SHOULD perform network exit procedures as described in [NWGSTG3] if the device receives a bootstrap message which is malformed, contains invalid attributes or values of attributes which the device does not support, or there is some other error in parsing the bootstrap message.

If the bootstrap message contains duplicate TLVs, including the value field, the first TLV SHALL be accepted and the other ones SHALL be ignored. The device SHALL ignore the unrecognized TLVs in the bootstrap message.

10 Security Considerations

In order to ensure secure communication between the device and server the following describes the minimum set of cipher-suites that SHALL be supported by the device and server.

The OMA DM and TR-069 servers SHALL support a subset of the cipher suites defined in [RFC3268]. The servers SHALL implement the following set of cipher suites listed in priority order from the highest to the lowest.

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

The OMA DM and TR-069 device SHALL support at least one of these cipher suites. The device and server SHALL negotiate the strongest cipher suite available to both end points as a part of the establishment of the TLS connection.

It is recommendation that the device SHOULD be configured to support TLS_RSA_WITH_3DES_EDE_CBC_SHA.

The implications of this are that the OMA DM server and TR-069 server have to use RSA-based certificates and support at least one of 3DES, AES-128, and AES-256 for the TLS-based communication with the device. The device and server are free to add any other cipher suite which is considered to have similar or stronger cryptographic properties to their capability lists, but the definitions here SHOULD serve as the minimum and therefore common baseline.

The procedures described here define a method for protecting the OTA transport of the OMA DM or TR-069 bootstrap information which contains configuration data as well as credentials necessary for subsequent OMA DM or TR-069 transactions. The method described here is generic in that the key and the encryption method are independent of the provisioning protocol.

This specification does not address the storage or secure usage of this bootstrap information once it has been delivered to the device. This specification deals solely with the method in which the bootstrap information is secured for delivery to the mobile station. It is the responsibility of implementations to ensure that the keys, credentials and all other related content is appropriately secured during processing within the device.

10.1 WiMAX Bootstrap Security

The bootstrapping procedure is intended to enable the secure delivery of bootstrap data to the device. The bootstrap process utilizes temporary keys derived from the Extended Master Session Key (EMSK) to authenticate and protect the bootstrap information. To perform this function a new key is computed at the device and the AAA.

10.1.1 Bootstrap Encryption Key

The Bootstrap Encryption Key (BEK) is derived from the EMSK as follows.

BEK = the 16 most significant (leftmost) octets of HMAC-SHA256(EMSK, "bek@wimaxforum.org"). The bek@wimaxforum.org is ascii and is not null terminated.

The lifetime of the BEK is set to the lifetime of the EMSK.

The BEK is bound to the EMSK which is already bound to the device so no additional key binding is necessary in the BEK key derivation procedure.

The AAA delivers the BEK, MSID and the device's IP address to the entity which is delivering the bootstrap information to the device. The method the AAA server uses to deliver the BEK to the WIB and/or Provisioning Server is out of scope of this document, but security controls are assumed to be in place for it. The BEK key is then used to authenticate and encrypt the bootstrap document for secure delivery to the device per the detailed description in the following section.

10.1.2 Bootstrap Information Protection

The bootstrap information SHALL be protected utilizing AES in the CCM mode [NIST800-38C]. 'tlen' SHALL be 64 and 't' SHALL be 8. The number of the octets in the message authentication code field SHALL be set to 8. Consistent with the CCM specification the 3-bit binary encoding $[(t-2)/2]$ of bits 5, 4, and 3 of the 'Flags' octet in B0 SHALL be 011.

The size 'q' of the length field 'Q' SHALL be set to 2. Consistent with the CCM specification, the 3-bit binary encoding $[q-1]$ of the 'q' field in bits 2, 1 and 0 of the 'Flags' octet in B0 SHALL be 001.

The length 'a' of the associated data string 'A' SHALL be set to 0.

The nonce value SHALL be 13 octets long (15-q) as shown in Table 6. The octets 0 through 7 SHALL be set to a 64-bit cryptographic quality random number (RAND). The octets 8 through 12 are reserved and set to zero.

Note: The set of nonce values used with a given BEK MUST not contain duplicate values since using the same nonce more than once compromises the security properties of AES-CCM. The use of a sufficiently large random number along with the expectation that the bootstrap information will be encrypted and transmitted a small number of times relative to the size of the random number is expected to maintain the security of AES-CCM for this application.

Table 6 - Nonce Construction (13 Octets)

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12
Field	RAND							Reserved					
Value	Random Value							0x0000000000					

The provisioning server generates a cryptographic quality random number, populates the RAND field of the nonce and processes the bootstrap information with AES-CCM. The provisioning server then transmits the protected document to the device. Upon the reception of a protected bootstrap message the device decrypts and authenticates the document.

Consistent with the AES-CCM specification, the initial block B0 is formatted as shown in Table 7.

Table 7 - Initial CCM Block B₀

Octet Number	0	1	13	14	15
Octet Significance		MSB LSB		MSB LSB	
Number of Octets	1	13		2	
Field	Flags	Nonce		Length	
Value	0x19	As specified in Table 2		0	

Consistent with the AES-CCM specification, the counter blocks Ctr_j are formatted as shown in

Table 8 - Counter block Ctr_j

Octet Number	0	1	13	14	15
Octet Significance		MSB LSB		MSB LSB	
Number of Octets	1	13		2	
Field	Flags	Nonce		Counter	
Value	0x1	As specified in Table 2		j	

APPENDIX A. Service Modes

The service mode attribute value pairs (avp) that can be used in the WiMAX NAI decoration are listed in Table 1. The device can use these avps in the WiMAX decoration of the NAI to indicate a special intent in its network entry. The device SHALL only use the service mode avps in the WiMAX decoration of the EAP outer identity [NWGSTG3] Section 4.4.1.3.1 (Outer Identity). The network MAY have special access policies for the different service modes. WiMAX Decoration SHALL contain only one Service Mode at time. If several Service Mode decorations are used, the first Service Mode is applied and all the rest are ignored.

Table 9 - Service mode avps for WiMAX decoration

Service mode avp	Description
sm=0	Reserved
sm=1	OTA provisioning
sm=2	Emergency Service support