



## **WiMAX Forum® Network Architecture**

Architecture Tenets, Reference Model and Reference Points

WiMAX Broadband Access Lawful Intercept: Overview

**WMF-T32-106-R020v01**

WMF Approved

(2011-09-16)

**WiMAX Forum Proprietary**

Copyright © 2011 WiMAX Forum. All Rights Reserved.

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

2  
3 Copyright 2011 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 by the WiMAX Forum members, provided that all  
7 copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be  
8 duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

9  
10 Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance  
11 of the following terms and conditions:

12  
13 **THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST**  
14 **EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND**  
15 **STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE,**  
16 **NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX**  
17 **FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND**  
18 **DISCLAIMS ANY WARRANTIES TO THE CONTRARY.**

19  
20 Any products or services provided using technology described in or implemented in connection with this document may be  
21 subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely  
22 responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all  
23 required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable  
24 jurisdiction.

25  
26 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
27 **APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY**  
28 **OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.**

29  
30 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE**  
31 **SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY**  
32 **CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.**

33  
34 The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any  
35 technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any  
36 technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual  
37 property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology,  
38 standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies,  
39 technologies, standards, and specifications, including through the payment of any required license fees.

40  
41 **NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH**  
42 **RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED**  
43 **INTO THIS DOCUMENT.**

44  
45 **IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD**  
46 **PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING,**  
47 **WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL**  
48 **PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY**  
49 **USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS**  
50 **MEMBERS RELATING TO THE USE OF THIS DOCUMENT.**

51  
52 The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is  
53 solely responsible for determining whether this document has been superseded by a later version or a different document.

54  
55 “WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the  
56 WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks of the WiMAX  
57 Forum. All other trademarks are the property of their respective owners.

1	<b>Table of Contents</b>	
2	<b>1. DOCUMENT SCOPE.....</b>	<b>4</b>
3	<b>2. ABBREVIATIONS AND TERMINOLOGY .....</b>	<b>5</b>
4	2.1 Abbreviations .....	5
5	2.2 Terminology .....	5
6	<b>3. REFERENCES.....</b>	<b>7</b>
7	<b>4. LAWFUL INTERCEPT NETWORK PERSPECTIVE .....</b>	<b>8</b>
8	4.1 Network Reference Model.....	8
9	4.2 Functional Entities.....	9
10	4.2.1 Administration Function (ADMF) .....	9
11	4.2.2 Delivery Function (DF).....	9
12	4.2.3 Collection Function/Law Enforcement Monitoring Function (CF/LEMF) .....	9
13	4.2.4 Intercept Access Point (IAP) .....	9
14	4.3 Communication among Functional Entities .....	9
15	4.3.1 ADMF and IAPs.....	9
16	4.3.2 DFs and IAPs .....	10
17	4.3.3 ADMF and DFs.....	10
18	4.3.4 DFs and CFs .....	10
19	4.4 Intercept Information Associated with Various WiMAX Network Elements .....	10
20	4.4.1 AAA .....	10
21	4.4.2 HA .....	10
22	4.4.3 ASN-GW or ASN.....	10
23	4.5 Lawful Intercept Identities.....	11
24	4.5.1 WiMAX identifiers .....	11
25	4.5.2 WiMAX Identity Hiding and LI.....	11
26		
27		

1 **LIST OF FIGURES**

2 FIGURE 4-1 - LAWFUL INTERCEPTION NETWORK REFERENCE MODEL FOR WIMAX .....8

3

4

## 1. Document Scope

2 This specification provides an overview of the WiMAX architecture in relation to Lawful Intercept (LI) for WiMAX  
3 based Broadband Access Services and Internet Protocol (IP) Multimedia Subsystem (IMS)-based Voice over IP  
4 (VoIP) services as stated in [1].

5 The material in this document is a conceptual overview of the LI service and LI model for WiMAX for Voice, Data  
6 and IP associated signaling. This version of the document covers only packet data and IMS-based VoIP services.  
7 Non-IMS-based VoIP and other services are for further study.

8 Laws of individual nations and regional institutions, and sometimes licensing and operating conditions define a need  
9 to intercept telecommunications traffic and related information in modern telecommunications systems. It has to be  
10 noted that lawful interception shall always be done in accordance with the applicable national or regional laws and  
11 regulations.

12 See the following regional specifications for the specific LI reporting requirements and capabilities:

- 13 a) WiMAX Lawful Intercept - NORTH AMERICAN REGION [3]
- 14 b) IMS INTERWORKING – LI ASPECTS – US REGION [6].

---

## 2. Abbreviations and Terminology

### 2.1 Abbreviations

ADMF	Administrative Function
ASN	Access Service Network [2]
ASN-GW	ASN Gateway
CF	Collection Function
CUI	Charging User Identifier
DF	Delivery Function
HA	Home Agent
AAA	Authentication, Authorization, and Accounting [2]
IAP	Intercept Access Point
IP	Internet Protocol
IMS	IP Multimedia Subsystem
LEMF	Law Enforcement Monitoring Function
LI	Lawful Intercept
MF	Mediation Function
MS	Mobile Station
NRM	Network Reference Model
VoIP	Voice over IP
WiMAX-SP	WiMAX Service Provider

### 2.2 Terminology

*For the purpose of this document, the terms and definitions presented in [2] apply, in addition to the terms and definitions found below.*

<b>AAA</b>	See [2].
<b>Administration Function</b>	Responsible for administrating a lawful authorization.
<b>ASN</b>	See [2].
<b>ASN-GW</b>	Gateway function connecting ASN and CSN. See [2].
<b>Authentication</b>	A method (e.g. based on username/password) by which a network confirms a subscriber's identity.
<b>Authorization</b>	The process by which a network grants access to resources to a user. Usually follows Authentication.
<b>Broadband Intercept Order</b>	A lawful authorization (e.g., court order) with jurisdiction that authorizes the interception of the broadband-based wire or electronic communications of an intercept subject.
<b>Communication</b>	Any wire, wireless, or electronic communication.

## Lawful-Intercept-Overview

<b>Collection Function/Law Enforcement Monitoring Function (CF/LEMF)</b>	Designated as the transmission destination for the results of interception relating to a particular intercept subject.
<b>Delivery Function (DF)</b>	The Delivery Function is responsible for delivering intercepted communications and information to one or more CF/LEMFs.
<b>Electronic Surveillance</b>	The statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of communication identifying information. As used herein, <i>surveillance</i> refers to a single communication intercept.
<b>Home Agent (HA)</b>	Mobility anchor point in the CSN used in Client Mobile IP and Proxy Mobile IP.
<b>H-NSP</b>	See [2].
<b>Intercept</b>	The aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
<b>Intercept Access Point (IAP)</b>	A point within an Telecommunications Services Provider domain where some of the communications or communications identifying information of an intercept subject's equipment, facilities and services are accessed.
<b>Intercept Subject</b>	A subscriber whose communications, communications identifying information, or both, have been lawfully authorized to be intercepted and delivered to a Law Enforcement Agency. The identification of the intercept subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, mobile identity, subscription identity).
<b>Lawful Authorization</b>	Permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/access provider/service provider. Typically this refers to a warrant or order issued by a lawfully authorized body.
<b>Law Enforcement Agency (LEA)</b>	A government entity with the legal authority to conduct electronic surveillance (e.g., the Federal Bureau of Investigation or a state or local police department).
<b>Subject</b>	See <i>intercept subject</i>
<b>Surveillance</b>	See <i>electronic surveillance</i>

### 3. References

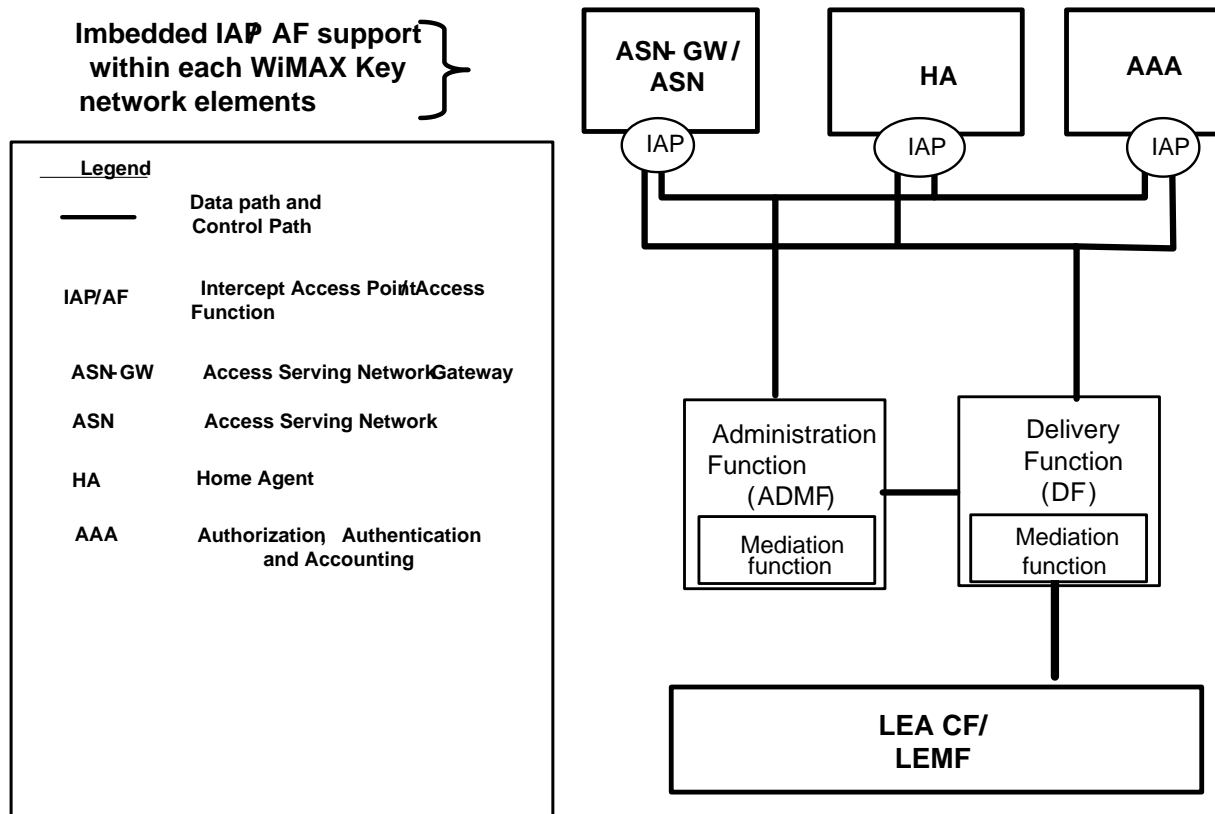
- 1 [1] WiMAX Forum Requirements and Recommendations for WiMAX Forum™ Mobility Profiles, Release 1.5,  
2 www.wimaxforum.org.
- 3 [2] WiMAX Forum, WMF-T32-001-R016v01, T32-004-R015v01, T32-005-R010v05, “Architecture Tenets,  
4 Reference Model and Reference Points” Base Specification, Annex and Abbreviations, Release 1.6.
- 5 [3] WiMAX Forum T33-107-R020v01, "Architecture, detailed Protocols and Procedures, WIMAX Lawful  
6 Intercept - NORTH AMERICAN REGION", Release 2.0.
- 7 [4] ETSI ES 201 158 ETSI Standard, Telecommunications security; Lawful Interception (LI); Requirements for  
8 network functions.
- 9 [5] ETSI TS 102 232-3 Technical Specification; Lawful Interception (LI); Handover Interface and Service-Specific  
10 Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services.
- 11 [6] WiMAX Forum T37-012-R020v01, "WiMAX Forum Network Architecture, WIMAX IP Multimedia  
12 Subsystem (IMS) Interworking", Release 2.0.
- 13

## 4. Lawful Intercept Network Perspective

This section provides an overview of a network reference model for Lawful Intercept (LI), new functional entities and interface reference points that may be needed for enabling LI. See the North American specifications [3] for the North American view of the General Surveillance Model (Section 4.2.1), Intercept Access Points (Section 4.2.2), and specific broadband LI requirements (Section 6.3). See the ETSI specifications [4] for the European view of the General Requirements (Section 4) and Handover Interface (Section 5) and see ETSI specification [5] for the European view of the Intercept Related Information (IRI) events (Section 6). See the US Region LI for IMS-based VoIP specification [6] for US-specific IMS-based VoIP LI requirements (Section 8).

### 4.1 Network Reference Model

The LI network reference model for WiMAX® consists of an Administrative Function (ADMf), Delivery Functions (DFs), Intercept Access Points (IAPs), and LEA Collection Functions (CFs). IAPs are co-located with one or more of the WiMAX network elements or interfaces. The ADMf and the DF may be co-located or may be separate entities, depending on the deployment scenario.



**Figure 4-1 - Lawful Intercept Network Reference Model for WiMAX®**

Note that while IAPs are placed on network entities such as a ASN-GW/ASN, HA, and AAA, the placement of IAPs is implementation dependent and IAPs may be placed elsewhere in the WiMAX-SP's network such as on firewalls, routers, or interfaces between network elements (e.g., bearer path). Network elements not part of the WiMAX NRM are beyond the scope of this specification.

## 4.2 Functional Entities

### 4.2.1 Administration Function (ADMF)

The ADMF performs the following functions:

- Interfaces with LEAs, as necessary, to obtain information regarding Broadband Intercept Orders;
- Interfaces with IAPs as necessary to enable (e.g., activation, deactivation, interrogation, as well as invocation) an intercept;
- Interfaces with DFs as necessary to enable (e.g., activation, deactivation, interrogation, as well as invocation) an intercept;
- Informs IAPs and DFs of changes to the observed subject's identity (e.g., CUI) as necessary; and
- Ensures the privacy of each LEAs Intercept Order (i.e., ensures that one LEA is not aware of another LEAs intercept order)

The ADMF may include a Mediation Function (MF). The MF performs the following functions:

- Formats information between the LEA and ADMF as described in national/regional specifications.

### 4.2.2 Delivery Function (DF)

The DF performs the following functions:

- Interfaces with IAPs as necessary to enable an intercept and obtain intercepted communications;
- Interfaces with an ADMF as necessary to enable an intercept; and
- Interfaces with CFs as necessary to deliver formatted intercepted communications.; and
- Ensures the privacy of each LEAs Intercept Order (i.e., ensures that one LEA is not aware of another LEAs intercept order).

The DF may include a Mediation Function (MF). The MF performs the following functions:

- Formats the intercepted communications for delivery to a CF/LEMF.

### 4.2.3 Collection Function/Law Enforcement Monitoring Function (CF/LEMF)

CFs perform the following functions:

- Receives formatted intercepted communications from the DFs.

### 4.2.4 Intercept Access Point (IAP)

IAPs can be part of ASN or CSN, e.g., ASN Gateway (ASN-GW)/ASN, Authentication, Authorization and Accounting (AAA) Server, or Home Agent (HA)

IAPs perform the following functions:

- Intercepts authorized subject communications and delivers the intercepted communications to DFs;
- Interface with an ADMF and DFs as necessary to enable an intercept.

## 4.3 Communication among Functional Entities

### 4.3.1 ADMF and IAPs

The following may be exchanged as necessary:

- intercept subject identity;

## Lawful-Intercept-Overview

- 1                   • communications to be intercepted;
- 2                   • lawful authorization identifier; and
- 3                   • Other information to enable (e.g., activation, deactivation, interrogation, as well as invocation)
- 4                   intercept.

**4.3.2 DFs and IAPs**

6 The IAPs send intercepted communications to DFs. The following may be exchanged as necessary:

- 7                   • intercept subject identity;
- 8                   • communications to be intercepted;
- 9                   • lawful authorization identifier;
- 10                  • correlation identifier; and
- 11                  • Other information to enable (e.g., activation, deactivation, interrogation, as well as invocation)
- 12                  intercept.

**4.3.3 ADMF and DFs**

14 The following may be exchanged as necessary:

- 15                  • intercept subject identity;
- 16                  • communications to be intercepted;
- 17                  • lawful authorization identifier;
- 18                  • CF information (e.g., network address of CF); and
- 19                  • Other information to enable (e.g., activation, deactivation, interrogation, as well as invocation)
- 20                  intercept.

**4.3.4 DFs and CFs**

22 Formatted intercepted communications is delivered from the DFs to the CFs.

**4.4 Intercept Information Associated with Various WiMAX Network Elements**

24 This section identifies subject communications events or communications status that may be detected by the IPAs at  
25 various WiMAX Network Elements and reported to the DFs as required by the regional LAES specifications:.

**4.4.1 AAA**

- 27                  • HAAA/VAAA authentication and authorization event (e.g., RADIUS event such as Access
- 28                  Attempt).

**4.4.2 HA**

- 30                  • MIP4 registration event;
- 31                  • MIP6 BU event;
- 32                  • indication that the Subject is already ‘online’; and
- 33                  • a Subject packet data session is already established.

**4.4.3 ASN-GW or ASN**

- 35                  • successful or unsuccessful packet data session establishment event;
- 36                  • packet data session termination event; and

- 1                   • indication that the Subject is ‘online’.

## 2   **4.5        Lawful Intercept Identities**

### 3   **4.5.1    WiMAX identifiers**

4   For the purpose of this document, the identifiers presented in [2] apply.

### 5   **4.5.2    WiMAX Identity Hiding and LI**

6   WiMAX enables the service provider to hide the identity of the subscriber from various elements in the network and  
7   across the wireless link. As part of Authentication, a pseudo identity can be used by the MS (i.e., PseudoNAI)  
8   instead of the real subscription identity. In this case, the real subscription identity is only available in the home CSN  
9   AAA server but is not known to other network entities to e.g. identify a data session. This pseudo identity can be  
10   changed frequently. The service provider uses a Charging User Identifier (CUI) to correlate the various sessions for  
11   a single subscriber. The CUI is under the control of the H-NSP and is used as a longer lived identifier that is  
12   available to all of the network entities contributing to LI, regardless of the pseudo identity value.

13   If the service provider elects to use pseudo identities within the home network and with visited networks, the CUI is  
14   used to correlate subscriber’s identity and intercepted information without the network elements actually knowing  
15   the subscriber’s true identity. Based on the above described properties the CUI can serve as an intercept subject  
16   identifier in these cases. The CUI protects the subscriber’s anonymity, while still providing a constant correlation  
17   value for detecting interception events and reporting to LEA.

18   An example of the procedures needed to use the CUI as the intercept subject identifier is as follows:

- 19       1. The LEA needs to take a legal warrant to the home service provider of the intercept subject. The request  
20        would include holding the CUI constant during the length of the warrant or, if the CUI is changed by the  
21        home service provider, the LEA is notified as quickly as possible. The home service provider would  
22        provide the value of the CUI to LEA. Note: The CUI is always distributed to the required network elements  
23        in the AAA path, not to provide any indication of the existence of a legal warrant.
  - 24       2. LEA would take the CUI and applicable legal warrants to the service providers that are to perform  
25        interception. The intercept subject’s identity to these service providers would be the CUI. Any changes to  
26        the CUI would be relayed to these service providers by the LEA. Use of CUI among operators protects the  
27        intercept subject’s identity as intended with the pseudo identity and yet provides a constant correlation  
28        identifier for detecting intercept events and reporting to LEA.
  - 29       3. All interceptions for the intercept subject would be reported to the LEA using the CUI.
  - 30       4. Once the Warrant expires or is withdrawn, the CUI information is no longer used by any of the service  
31        providers, home or visited. The home service provider may change the value of CUI according to normal  
32        operating procedures.
- 33