



WiMAX Forum[®] Network Architecture

WiMAX IP Multimedia Subsystem (IMS) Interworking
Lawful Intercept Aspects – UNITED STATES REGION

WMF-T37-012-R020v02

WMF Approved
(2011-11-14)

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
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.

1	Table of Contents	
2	1. INTRODUCTION.....	7
3	1.1 Background.....	7
4	1.2 Scope and Purpose.....	7
5	2. NORMATIVE REFERENCES.....	9
6	3. DEFINITIONS & ACRONYMS.....	10
7	3.1 Definitions	10
8	3.2 Acronyms	12
9	4. WIMAX® SERVICES DESCRIPTION	14
10	4.1 WiMAX Services Model	14
11	4.2 General Surveillance Model	14
12	4.2.1 <i>Electronic Surveillance Model</i>	14
13	4.2.2 <i>Intercept Access Points</i>	15
14	5. WIMAX® SUBJECT IDENTIFICATION	16
15	5.1 Login Identifier.....	16
16	5.2 Equipment Identifier.....	16
17	5.3 Surveillance Subject Identification.....	16
18	6. USER PERSPECTIVE	17
19	6.1 Surveillance Events	17
20	6.1.1 <i>CII Events</i>	17
21	6.1.2 <i>CC-related Events</i>	18
22	6.2 Communications Delivery	18
23	6.3 Quality and Reliability.....	18
24	6.4 Decryption and Decompression.....	19
25	6.5 Timing Requirements	19
26	6.5.1 <i>CII Timing Requirements</i>	19
27	6.5.2 <i>CC Timing Requirements</i>	19
28	7. NETWORK PERSPECTIVE	20
29	7.1 CII Event Messages	20
30	7.1.1 <i>CII Events</i>	20
31	7.1.2 <i>Direct Signal Reporting</i>	21
32	7.1.3 <i>Serving System Reporting</i>	21
33	7.1.4 <i>Dialed Digit Extraction Reporting</i>	23
34	7.1.5 <i>Location Information</i>	23
35	7.2 CC-related Events.....	23
36	7.3 CC Delivery.....	23
37	ANNEX A. ASN.1 DEFINITIONS (NORMATIVE)	24
38	A.1 CII ASN.1.....	24
39	A.2 CC ASN.1.....	27
40	ANNEX B. OPTIONAL CII EVENT MESSAGES (INFORMATIVE)	28
41		

1 **List of Figures**

2 FIGURE 4-1 – ELECTRONIC SURVEILLANCE MODEL.....14

3

4

1 **List of Tables**

2 TABLE 7-1 – SERVINGSYSTEM MESSAGE PARAMETERS FOR TERMINAL REGISTRATION21
3 TABLE 7-2 – SERVINGSYSTEM MESSAGE PARAMETERS FOR SIP REGISTRATION22
4

1. Introduction

1.1 Background

This specification defines the interfaces between a service provider, that facilitates WiMAX® subscriber access to IMS services provided by a WiMAX Service Provider (WiMAX-SP), and a Law enforcement Agency (LEA) to assist the LEA in conducting Lawfully Authorized Electronic Surveillance (LAES) for subscription-based IMS-based Voice over Internet Protocol (VoIP) arrangements.

As used in this specification, electronic surveillance refers to the interception and monitoring of VoIP communications – i.e., Call Content (CC), Call Identifying Information (CII), or both – for a particular WiMAX Internet Protocol (IP) Multimedia Subsystem (IMS) subscriber as lawfully authorized. In this specification, an intercept subject, or more simply a subject, is an entity whose IMS service usage has been authorized by a legal instrument to be intercepted and delivered to an LEA. The identification of the subject in the authorized legal instrument is limited to subject identifiers or subject-related identifiers used by the WiMAX network or a WiMAX-SP's equipment, facility, or communication service - e.g., network address, terminal identity, subscription identity, and other IMS-specific identifiers.

As a precondition for WiMAX-SP assistance with LAES, an LEA must serve a WiMAX-SP with the necessary lawful authorization identifying the intercept subject, the communications and information to be provided. Once this lawful authorization is served on a WiMAX-SP, the WiMAX-SP shall perform the access, mediation as necessary, and delivery of the identified communications and information to the LEA via LEA-procured equipment, facilities, or services.

This specification is based on the solution found in WiMAX LI Overview [1] and ATIS-1000678 [2]. The development of this specification was also informed by other specifications addressing LI for VoIP communications including ATIS-0700005 [16] and TIA-1066 [17].

Requirements in this specification are WiMAX air interface independent.

1.2 Scope and Purpose

The scope of LAES for WiMAX is on a WiMAX-SP's Network that provides or transports the WiMAX subscriber IMS services using the WiMAX network. LAES for the following are outside the scope of this document and for future study as necessary:

- Correlation of IMS sessions within the same WiMAX-SP where multiple Delivery Functions (DF) report portions of the same session (e.g., because different DFs serve different geographic regions or different access technologies).
- Particular issues related to the design and implementation of LAES for networks providing access to IMS services through multiple access technologies (including WiMAX), and where inter-access mobility is supported between the WiMAX access and any other access technology, are not addressed in this specification.

This specification is provided for purposes of a “safe harbor” as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [3]: “a telecommunications carrier shall be found to be in compliance with the assistance capability requirements under Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with Section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or

IMSIWKLI

1 by the Commission under subsection (b), to meet the requirements of section 103.”¹ [4, 5, 6, 7]. More specifically,
2 the Lawful Interception aspects in this specification are intended to apply to WiMAX access networks and WiMAX
3 core networks providing IMS services where interworking between WiMAX access networks and IMS is provided
4 in accordance with the IP Multimedia Subsystem (IMS) Interworking specification [8].

¹ It is not the intent of this document to imply or impact any pending CALEA regulatory decisions. This document provides the mechanisms to perform lawfully authorized electronic surveillance of VoIP subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable, it is intended that a manufacturer or service provider that is in compliance with this document will have “safe harbor” under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. §1001, et seq.

2. Normative References

- [1] WMF-T32-106-R020v01, WiMAX Forum® Network Architecture, Architecture Tenets, Reference Model and Reference Points, WiMAX Broadband Access Lawful Intercept: Overview"
- [2] ATIS-1000678.2006, LAES for VoIP Technologies in Wireline Telecommunications Networks as modified by ATIS-1000678.a.2007, Supplement A to ATIS-1000678.2006 and ATIS-1000678.b.2010, Supplement B to ATIS-1000678.2006.²
- [3] Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, October 25, 1994.³
- [4] *In the Matter of Communications Assistance for Law Enforcement Act, Order on Remand*, CC Docket No. 97-213, 17 FCC Record 6898 (2002).³
- [5] *In the Matter of Communications Assistance for Law Enforcement Act, Third Report and Order*, CC Docket No. 97-213, 14 FCC Record 16794 (1999).³
- [6] *In the matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking*, ET Document No. 04-295, 20 FCC Rcd 14989 (2005).³
- [7] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second 25 Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, 21 FCC Rcd 5360 (2006).³
- [8] WMF-T33-101-R015v02, WiMAX Forum® Network Architecture, Architecture Tenets, Reference Model and Reference Points, IP Multimedia Subsystem (IMS) Interworking", Release 1.5.
- [9] ANSI J-STD-025-B, Joint T1-TIA Standard on Lawfully Authorized Electronic Surveillance, August 2006.
- [10] ITU-T Recommendation X.690, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguishing Encoding Rules (DER), July 2002.
- [11] WMF-T32-001-R020v01, WiMAX Forum® Network Architecture, Architecture Tenets, Reference Model and Reference Points, Base Specification "
- [12] Wire and Electronic Communications Interception and Interception of Oral Communications, Title 18 of the United States Code, Chapter 119, Sections 2510 - 2522.
- [13] WMF-T33-107-R020v01, WiMAX Forum® Network Architecture, Architecture, detailed Protocols and Procedures, WiMAX Lawful Intercept - NORTH AMERICAN REGION", Release 1.5.
- [14] IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications, July 2003.
- [15] IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.
- [16] ATIS-0700005, Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-Based VoIP and Other Multimedia Services, 2007, as modified by ATIS-0700005.a, Supplement A to ATIS-0700005, Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services, 2010.
- [17] TIA-1066, LAES for cdma2000® VoIP, 2006.

² This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < <https://www.atis.org/docstore/default.aspx> >

³ This document is available from the AskCALEA website at < <http://www.askcalea.net> >.

3. Definitions & Acronyms

3.1 Definitions

Access Function (AF): Accesses and intercepts an intercept subject's communications and VoIP call identifying information unobtrusively. Comprises one or more Intercept Access Points (IAP).

Access Services Network (ASN): A complete set of network functions needed to provide radio access to a WiMAX subscriber. (See [11]).

Associate: A telecommunication user whose equipment, facilities, or service are communicating with a subject.

Call: See VoIP Call.

Call Content (CC): See section 4.2.1 and Content.

Call Content Address: The VoIP Call Content Address (CC Address) value identifies the IP address(es) and port number(s) of the CCC or pair of CCCs used for conveying the VoIP call content.

Call Identifying Information (CII): See section 4.2.1.

Call Session Control Function (CSCF): A signaling and control component within the IP Multimedia Subsystem (IMS) network that is responsible for all signaling via Session Initiation Protocol (SIP) between the Transport Plane, Control Plane, and the Application Plane of IMS. The CSCF consists of the Proxy CSCF (P-CSCF), Interrogating CSCF (I-CSCF), and the Serving CSCF (S-CSCF).

Call Content Channel (CCC) Identity: The CCC Identity (CCCI) value identifies the CCC or pair of CCCs used for conveying VoIP call content.

Collection Function (CF): Defined in [5] to be "the location where lawfully authorized intercepted communications and call identifying information is collected by a law enforcement agency (LEA)."

Communication: Any wire or electronic communication, as defined in [12].

VoIP Conference Call: An instance of a multi-party VoIP call.

Connectivity Services Network (CSN): A set of network functions that provide IP connectivity services to the WiMAX subscriber(s). (See also [11])

Content: Defined in [12], section (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."

Delivery Function (DF): Delivers intercepted communications to one or more Collection Functions in the form of call content, such as voice communications, and call identifying information, such as calling party identities and called party identities.

Destination: See call identifying information.

Direct Signal Reporting (DSR): Reporting of VoIP subject access and signaling to LEA(s) via encapsulation.

Direction: See call identifying information.

Electronic Communications: Defined in [12], section (12) to be "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."

Electronic Surveillance: 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 [VoIP] call identifying information. As used herein, surveillance refers to a single communication intercept, pen register, or trap and trace. Its usage herein does not include administrative subpoenas for obtaining a subscriber's billing records and information about a subscriber's service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

- 1 **Intercept:** Defined in [12], section(4) to be “the aural or other acquisition of the content of any wire, electronic, or
2 oral communication through the use of any electronic, mechanical, or other device.”
- 3 **Intercept Access Point (IAP):** A point within a telecommunication system or VoIP network where some of the
4 [VoIP] communications or [VoIP] call identifying information of an intercept subject’s equipment, facilities and
5 services are accessed.
- 6 **Intercept Subject:** Intercept Subject is defined based on the identifiers described in Section 5.
- 7 **Internet Protocol (IP) Multimedia Subsystem (IMS):** A generic architecture for offering multimedia services
8 (e.g., voice over IP), defined by 3rd Generation Partnership Project (3GPP).
- 9 **Lawfully Authorized Electronic Surveillance (LAES):** see Electronic Surveillance.
- 10 **Law Enforcement (LE):** The broad community of Law Enforcement Agencies that have an interest in LAES.
- 11 **Law Enforcement Administrative Function:** Controls the LEA’s Collection Function.
- 12 **Law Enforcement Agency (LEA):** A government entity with the legal authority to conduct electronic surveillance
13 (e.g., the Federal Bureau of Investigation or a local police department).
- 14 **Mediation Function (MF):** A function that maps (rather than encapsulates) VoIP subject access and network
15 signaling messages onto e-interface messages (as defined in this standard).
- 16 **Mobile Station (MS):** Generalized mobile equipment set providing connectivity between subscriber equipment and
17 a base station (BS). The Mobile Station may be a host or a customer premises equipment (CPE) type of device that
18 supports multiple hosts.
- 19 **Origin:** See Call Identifying Information.
- 20 **Proxy-CSCF (P-CSCF):** See Call Session Control Function
- 21 **Real-time Transport Protocol (RTP):** A packet based communication protocol that adds timing and sequence
22 information to each packet to allow the reassembly of packets to reproduce real time audio and video information.
23 RTP is defined in RFC 3550 [14].
- 24 **Service Provider (SP):** An entity that provides telecommunication services to customers and other users. A SP
25 may or may not operate a network. A SP may or may not be a customer of another SP. A SP may or may not be a
26 WiMAX-SP.
- 27 **Serving-CSCF (S-CSCF):** See Call Session Control Function.
- 28 **IP Session:** A set of multimedia senders and receivers and the data streams flowing from senders to receivers.
- 29 **Session Initiation Protocol (SIP):** An Internet Engineering Task Force (IETF)-defined signaling protocol used for
30 controlling multimedia communication sessions such as voice and video calls over IP. SIP is defined in RFC 3261
31 [15].
- 32 **Subject:** See intercept subject.
- 33 **Surveillance:** See electronic surveillance.
- 34 **Termination:** An incoming VoIP call attempt. See also call identifying information.
- 35 **Tunnel:** A capability that enables networks, network elements, or devices to exchange data or packets via
36 intermediate networks, while hiding the protocol details from the intermediate networks. Tunneling is generically
37 implemented by encapsulating an end-to-end network protocol within packets that are natively carried over the
38 intermediate networks.
- 39 **Voice over IP (VoIP):** A family of transmission technologies that converts voice calls into data packets for
40 transmission over the Internet or other IP-based networks.
- 41 **VoIP Call:** A sequence of events beginning with an initial connection or facility request and ending with the final
42 release of all facilities used. A VoIP call may have one or more legs.

IMSIWKL I

1 **WiMAX Service Provider (WiMAX-SP):** An entity that provides telecommunication services to customers and
 2 other users through WiMAX technology. A WiMAX-SP may or may not operate a network. A WiMAX-SP may or
 3 may not be a customer of another WiMAX-SP.

4 **WiMAX-SP Administrative Function:** Controls the WiMAX-SP's AF and DF.

5 **Wireline:** Refers to traditional wire-based telephone service.

6

7 3.2 Acronyms

AF	Access Function
ASN	Access Service Network
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
ATIS	Alliance for Telecommunication Industry Solutions
BER	Basic Encoding Rules
C	Conditional (parameter)
CALEA	Communications Assistance for Law Enforcement Act
CF	Collection Function
CC	Call Content (see section 3.1)
CII	Call Identifying Information (see section 3.1)
CmC	Communication Content
CmII	Communication Identifying Information
CSN	Connectivity Service Network
CUI	Charging User Identifier
DSR	Direct Signal Reporting
DF	Delivery Function
FCC	Federal Communications Commission
IAP	Intercept Access Point
ID	Identifier
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ITU	International Telecommunication Union
LAES	Lawfully Authorized Electronic Surveillance
LE	Law Enforcement
LEA	Law Enforcement Agency
M	Mandatory (parameter)
MAC	Media Access Control
MF	Mediation Function
MS	Mobile Station
NAI	Network Access Identifier
NAP	Network Access Provider

IMSIWK LI

NSP	Network Service Provider
O	Optional (parameter)
PANI	P-Access Network Info
P-CSCF	Proxy Call Session Control Function
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
S-CSCF	Serving Call Session Control Function
SIP	Session Initiation Protocol
SP	Service Provider
TDM	Time Division Multiplex
US	United States
VoIP	Voice over IP
WiMAX-SP	WiMAX Service Provider

1

4. WiMAX® Services Description

4.1 WiMAX Services Model

WiMAX IMS-based VoIP architectures and services are defined in [8].

4.2 General Surveillance Model

4.2.1 Electronic Surveillance Model

The functions needed to perform LAES are broadly categorized as access, delivery, collection, service provider administration, and law enforcement administration [12]. These functions are described herein without regard to their implementation. The relationship between these functional categories is shown in Figure 4-1. As shown, the Access Function (AF), Delivery Function (DF), and WiMAX-SP Administration Function are the responsibility of the WiMAX-SP, and the Collection Function (CF) and Law Enforcement Administration Function are the responsibility of the LEA. The use of these functions to perform an interception is initiated by receipt of a specific lawful authorization.

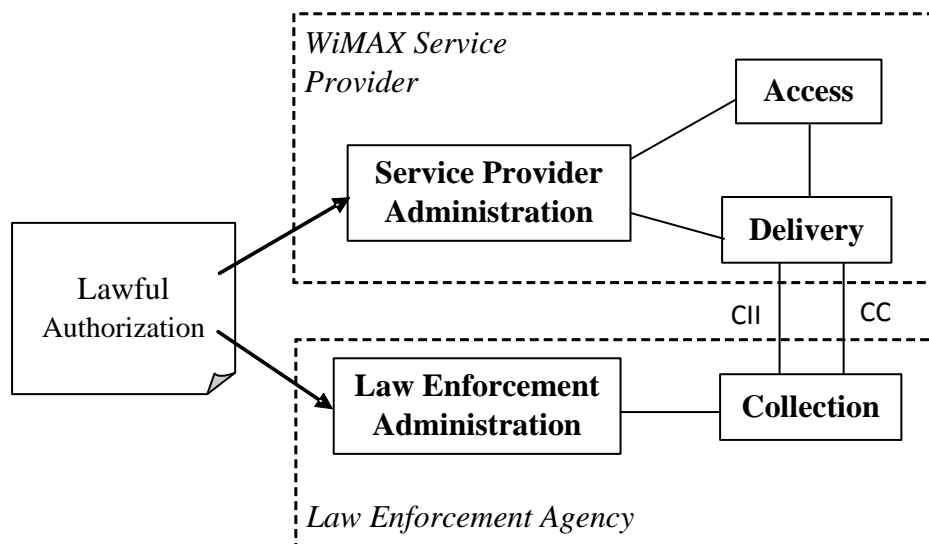


Figure 4-1 – Electronic Surveillance Model

Call Content is the stream(s) of VoIP packets sent from the subject to one or more associates, or from one or more associates to the subject. Note that when certain codecs are used voice content may be combined with video or other multi-media content. In those cases VoIP packets are considered to include the combined voice/video or voice/multi-media packets. CC also includes VoIP packet streams sent from various network entities (e.g., a voice mail server) to the subject, or from the subject to various network entities, in the bearer plane. [12] defines the term *content* as “when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication.”

Call Identifying Information, as defined in [3] is “dialing or signaling information that identifies the origin, direction, destination, or termination of each [VoIP] communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.” [4] states that “*destination* is a party or place to which a [VoIP] call is being made (e.g., called party); *direction* is a party or place to which a [VoIP] call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); *origin* is a party initiating a [VoIP] call (e.g., calling party), or a place from which a [VoIP]

IMSIWKLI

- 1 call is initiated; and *termination* is a party or place at the end of a communication path (e.g., the called or call-
2 receiving party, or the switch of a party that has placed another party on hold).”
- 3 The *Access Function*, consisting of one or more Intercept Access Points (IAP), accesses and intercepts an intercept
4 subject’s CC and CII unobtrusively. The IAPs may vary between WiMAX-SPs.
- 5 The *Delivery Function* delivers intercepted communications to one or more CFs. The DF shall deliver intercepted
6 communications in the form of CC and CII.
- 7 The *Collection Function* collects and analyzes the CC and CII received from the DF. It is defined to be the location
8 where lawfully authorized intercepted CC and CII is collected by a LEA.
- 9 The *WiMAX-SP Administration Function* controls the WiMAX-SP’s AF and DF.
- 10 The *Law Enforcement Administration Function* controls the LEA’s CF.

11 **4.2.2 Intercept Access Points**

12 With respect to WiMAX, IAPs are places in the network where CII and CC are intercepted. There are two
13 fundamental types of WiMAX IAPs:

- 14 1. WiMAX VoIP Call Identifying Information IAPs (CII-IAPs); and
- 15 2. WiMAX VoIP Call Content IAPs (CC-IAPs).

16 CII-IAPs and CC-IAPs are associated with CII and CC intercept functions respectively that perform the actual
17 interception of CII and CC. These CII and CC intercept functions are incorporated into one or more network
18 elements. CII and CC intercept functions may be collocated within the same network element, or may be distributed
19 among many network elements. The interfaces for transport of CII and CC information from the CII and CC IAPs
20 to the Delivery Function are outside the scope of the WiMAX specifications.

21 **4.2.2.1 CII-IAPs**

22 CII-IAPs capture information necessary to generate CII and present it to the DF, or to the Mediation Function (MF)
23 as defined in [1]. The CII-IAP(s) can reside in a number of places. CII-IAPs shall be placed such that reasonably
24 available CII can be intercepted whether the WiMAX-SP provides the Access Services Network (ASN),
25 Connectivity Services Network (CSN), or both for a specific communication. The specific placement of CII-IAP(s)
26 in a WiMAX network is a WiMAX-SP design decision.

27 **4.2.2.2 CC-IAPs**

28 A CC-IAP intercepts all VoIP packets to and from an intercept subject.

29 A CC-IAP intercepts the subject’s content and presents it to the DF or to the MF. The CC-IAP(s) can reside in a
30 number of places. When the WiMAX-SP supports interworking, CC-IAPs shall be placed such that all CC in the
31 network of the WiMAX-SP can be intercepted whether the WiMAX-SP provides the ASN, CSN, or both for a
32 specific communication. The specific placement of CC-IAP(s) in a WiMAX network is a WiMAX-SP design
33 decision.

1 **5. WiMAX® Subject Identification**

2 This section identifies types of entities that may be the subject of surveillance. When the subject of a surveillance is
3 a subscriber, the subject's access to the WiMAX services can be divided into two categories defined by the way the
4 subject activity is identified in the network.

5 **5.1 Login Identifier**

6 The subject is uniquely identified through a login process. As a result of a successful login process, an intercept may
7 be based on information, such as:

- 8 • A single IP address, a set of IP addresses or an IP subnet/IP prefix assigned to the subject at
9 login;
- 10 • Account-session-id assigned to the subject's session at login; or
- 11 • The subject's Charging User Identifier (CUI).

12 Note that in the case of multiple logins by the subject, multiple cases of the above conditions may be required for the
13 same subject.

14 **5.2 Equipment Identifier**

15 The subject is identified through an address or interface that uniquely identifies the subject's equipment or session.
16 The intercept resulting from equipment identification may be based on information such as:

- 17 • Media Access Control (MAC) address or set of MAC addresses associated with the subject's
18 equipment;
- 19 • Static IP address, which could be a single IP address, a set of IP addresses or an IP subnet/IP
20 prefix assigned to the subject's equipment.

21 Note that in some cases the subject may be associated with multiple equipment identifiers.

22 **5.3 Surveillance Subject Identification**

23 The subject of a surveillance can either be a subscriber or an identified instance of a conference. Identification of the
24 conference is service specific and outside the scope of this specification.

25

6. User Perspective

This section presents the law enforcement user perspective requirements for LAES for IMS-based VoIP for US WiMAX® network communication-related events [8].

6.1 Surveillance Events

This section identifies communication-related events (termed surveillance events) that generate CII and CC.

6.1.1 CII Events

A CII event is a user action or signal, or action taken by the network on behalf of a user, that may cause a communication state change. These events are generally reflected by protocol messages that convey the state change. These events are not intended to reflect a particular technology, but to describe the event in general. The mapping is intended to report those events based upon analysis of the intercepted messages.

6.1.1.1 CII Mapped Event Reporting

The following event messages defined in [2] are used to report CII:

- Answer
- Change
- Origination
- Redirection
- Release
- ConferencePartyChange
- TerminationAttempt
- Connection
- ConnectionBreak
- NetworkSignal
- SubjectSignal
- MediaAndAddressReporting

6.1.1.2 Direct Signal Reporting

The DirectSignalReporting event message, as defined in [2], is used to report signaling that cannot be mapped to one of the messages defined in Section 6.1.1.1.

6.1.1.3 Serving System Reporting

The serving system identification information includes the identity of the ASN and CSN systems currently assigned to provide service for the Mobile Station (MS). Information regarding the occurrence of the event (e.g., identity of the ASN and CSN systems providing intercept access, time, date) should be included. Where a WiMAX-SP provides both the ASN and CSN during a VoIP call, the reported serving ASN and CSN systems may be the same.

The ServingSystem event message shall be used to report the system identity of both the ASN and CSN currently serving the intercept subject (i.e., resulting from MS registration).

The ServingSystem event message shall also be used to report addressing and contact information registered by the intercept subject (i.e., registered via the Session Initiation Protocol (SIP) “REGISTER” method).

6.1.1.4 Dialed Digit Extraction Reporting

In IMS-based VoIP, when the intercept subject dials or signals digits in the VoIP content stream after the session is connected to another SP’s service for processing and routing, the WiMAX-SP shall isolate and report to the LEA the dialed or signaled digits, when reasonably available, as CII to the LEA. The WiMAX-SP that reports the CII dialed digit extraction information is not obligated to assure that the connection is with another SP’s service.

IMSIWKLI

1 The WiMAX-SP shall support a dialed digit extraction capability, with a toggle feature that can activate/ deactivate
2 this capability (per lawful authorization) and report the dialed or signaled digits, when reasonably available, as CII.
3 See Annex F of [2] for additional information.

4 Note: The CII Dialed Digit Extraction event reporting is not required for other IMS-based multimedia services.

5 Note: The session that is connected to another SP's service for processing and routing may be provided by the same
6 WiMAX-SP.

7 **6.1.1.5 Location Information Reporting**

8 When authorized and reasonably available, location information shall be provided for the Answer, Origination, and
9 Release events to identify the location of the intercept subject's mobile station (MS).

10 **6.1.2 CC-related Events**

11 The following messages, as defined in [2], are used to report CC-related events:

- 12 • CCOpen
- 13 • CCChange
- 14 • CCClose
- 15 • CCUnavailable
- 16 • UUContent

17 CC-related events shall only be reported to an LEA for an intercept subject when that LEA is authorized to receive
18 CC for that intercept subject.

19 **6.2 Communications Delivery**

20 The WiMAX-SP shall deliver to the LEA all CC present in its network and all reasonably available CII regardless of
21 whether it provides the ASN, CSN, or both for a particular VoIP communication. Various transport technologies
22 can be used for delivery of intercepted communications between the WiMAX-SP's DF or MF and the LEA's CF.
23 The transport technology chosen shall be agreed between the WiMAX-SP and LEA.

24 There are a variety of circumstances and protocols where the intercept subject's VoIP packets are tunneled by the
25 WiMAX-SP (i.e., encapsulated within a packet that typically has different IP addresses). For a WiMAX-SP's tunnel
26 carrying an intercept subject's VoIP packets, if that WiMAX-SP's tunnel is originated or terminated in the WiMAX-
27 SP's network, interception shall be performed on the subject's VoIP packets.

28 A WiMAX-SP is not required to ensure that the intercepted CII and CC was also received by the subject or
29 associates. For example, when packets sent to a MS are intercepted, it is not known whether the packets are actually
30 received by the MS because of the potential for extraordinary network conditions (e.g., network congestion/failure
31 and air interface problems).

32 Once Lawful Interception is activated, interception should occur expeditiously. However, interception may be
33 initiated for a VoIP call that is ongoing at the time of intercept activation. Once deactivated, Lawful Interception
34 should end expeditiously.

35 **6.3 Quality and Reliability**

36 The quality of service associated with the result of interception of communication content should be (at least) equal
37 to the quality of service of the original content of communication.

38 The reliability associated with the result of interception of VoIP communications content should be (at least) equal
39 to the reliability of the original content of communication. The reliability associated with the interception of VoIP
40 communication identifying information should be (at least) equal to the reliability of the original SIP signaling and
41 other (i.e., terminal registration) signaling.

1 **6.4 Decryption and Decompression**

2 A WiMAX-SP shall be responsible for decrypting or decompressing, or ensuring the LEA's ability to decrypt or
3 decompress, any communication or signaling encrypted or compressed by a subscriber or customer, when the
4 encryption or compression was provided by the WiMAX-SP and the WiMAX-SP possesses the information
5 necessary to decrypt or decompress the communication or signaling. A WiMAX-SP that provides the LEA with
6 information about how to decrypt or decompress a communication or signaling (e.g., identifying the type of
7 compression software used to compress the communication or signaling, directing the LEA to the appropriate
8 vendor that can provide decryption or decompression equipment, or providing the encryption key used to encrypt the
9 communication or signaling) fully satisfies its obligation under the preceding sentence.

10 Informative note: It is LE's preference that the WiMAX-SP deliver decrypted and decompressed communications.

11 **6.5 Timing Requirements**

12 Timing information enables law enforcement agencies to associate CII with the content of communication. Timing
13 information includes two elements:

- 14 • Event Time-stamp: Each surveillance message shall contain a time-stamp that is recorded within a specific
15 amount of time from when the event triggering the surveillance message was detected (i.e., the time
16 difference between the time the CII triggering event was detected and the time recorded in the time-stamp).
- 17 • Event Timing: Surveillance messages shall be sent to the LEA within a defined amount of time after the
18 information pertaining to the CII triggering event is available at the IAP.

19 **6.5.1 CII Timing Requirements**

20 The following timing requirements shall apply to the delivery of CII:

- 21 • Each surveillance message shall be sent by the Delivery Function to the Collection Function within eight
22 (8) seconds of receipt by the IAP of the information pertaining to the CII triggering event at least 95% of
23 the time.
- 24 • Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CII
25 event triggering the surveillance message was detected.

26 **6.5.2 CC Timing Requirements**

27 The following timing requirements shall apply to the delivery of CC:

- 28 • Time-stamps shall be provided with encapsulated intercepted packets delivered to the CF, unless timing is
29 provided by other means, such as when the underlying user transport method in the payload provides
30 timing and sequencing (e.g., Real-time Transport Protocol (RTP) [14]). Note that timestamps are lost if
31 VoIP is converted to Time Division Multiplex (TDM).
- 32 • Intercepted VoIP content shall be expeditiously transmitted by the IAP towards the DF with its
33 interception.

34

7. Network Perspective

This section identifies the triggers for reporting CII event messages and the information contained in those event messages. It also describes the application level CC delivery format and associated delivery information.

Note that when different SPs provide ASN and CSN functionality for an intercept subject, the ability to detect triggering events and the availability of intercept data may be limited because of various factors (e.g., use of tunneling or encryption). In all cases a WiMAX-SP providing ASN functionality, CSN functionality, or both shall deliver intercept data as defined in the section to the extent it is available and lawfully authorized.

Each message is described as consisting of a set of parameters. Each parameter is either:

- Mandatory (M) --- Required for the message;
- Conditional (C) --- Required in situations where a condition (defined in the usage column) is met; or
- Optional (O) --- Provided at the discretion of the implementation.

The information to be carried by each parameter is identified. Please note that both optional and conditional parameters as described in this section are considered to be OPTIONAL syntactically in Abstract Syntax Notation One (ASN.1) provided in Annex A.

7.1 CII Event Messages

This section identifies event messages and their triggers used to report VoIP CII events. The messages described in this section emulate for a WiMAX environment the LAES of VoIP service specified in [2], which was itself drawn from the LAES for Public Switched Telecommunications Network (PSTN) service defined in [9].

This specification provides two methods of reporting VoIP CII:

1. Mapped SIP signaling information (or Mapped); or
2. Direct Signal Reporting (DSR).

“Mapped” is a method characterized by mapping SIP-based WiMAX VoIP signaling information into CII event messages described in section 6.1.1.1. (e.g., mapping a SIP INVITE to an Origination event). The “DSR” method is characterized by directly reporting appropriate SIP-based WiMAX VoIP signaling as CII (see Section 6.4 of [2]).

A CII event shall be reported as either a DSR message or a Mapped message. CII in Mapped Messages is the principal delivery mechanism for events covered by this specification. CII in DSR messages is a supplemental delivery mechanism, used only when the required information elements cannot reasonably be accommodated in the Mapped Messages.

7.1.1 CII Events

The following LAES messages, which are defined in [2], are utilized for WiMAX IMS-based VoIP CII reporting:

- Answer
- Change
- Origination
- Redirection
- Release
- ConferencePartyChange
- TerminationAttempt
- Connection
- ConnectionBreak
- NetworkSignal
- SubjectSignal
- MediaAndAddressReporting

7.1.2 Direct Signal Reporting

The DSR message, as specified in [2], allows reporting CII signaling events that are not mapped onto the CII event messages defined in this document (e.g., for new SIP methods or responses or extensions).

7.1.3 Serving System Reporting

The ServingSystem event message is used to report both SIP registration and terminal registration.

In the Serving System message the identity of a service provider (SP) may be provided in the form of a unique identifier of the provider or of a network element (e.g., ASN gateway) controlled by that SP.

When the information is available at an IAP, the SP reporting a Serving System event message shall identify both the ASN and CSN serving the VoIP call at the time of the report regardless of whether the reporting SP provides ASN functionality, CSN functionality, or both. Examples of data that may be used to identify the SP providing the CSN functionality in the SystemIdentity information element in Tables 1 and 2 include the Network Service Provider (NSP) Identifier (ID) and the “realm” component of the Network Access Identifier (NAI) as defined in [11]. Examples of data that may be used to identify the SP providing the ASN functionality in the AsnSystemIdentity information element in Table 7-1 and Table 7-2 include a unique identifier for the ASN Gateway, such as the IP address or Anchor Data Path Function ID, and Operator ID (i.e., Network Access Provider (NAP) ID) as defined in [11]. The WiMAX-SP should report the most granular identifier of the provider of the ASN and CSN functionality reasonably available (e.g., ASN Gateway identifier should be preferred when available rather than Operator ID).

7.1.3.1 Serving System Reporting for Terminal Registration

This ServingSystem Event reports terminal registration. The ServingSystem event message shall be triggered when the intercept subject’s MS is authorized for service with another SP or in another service area. The event may be reported when the intercept subject registers in the home network. If the intercept subject’s MS registers with a SP providing both ASN and CSN functionality, the SP may report only a single ServingSystem event message (i.e., a single ServingSystem with the SP identified in both the SystemIdentity and AsnSystemIdentity parameters).

The ServingSystem message includes the following parameters when used to report terminal registration:

Table 7-1 – ServingSystem Message Parameters for Terminal Registration

Information Element	M/O/C	Conditions
Caselidentity	M	
IAPSystemIdentity	C	Include to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	
RegisteringPartyIdentity	M	Identifies the party for whom terminal registration, is being attempted.
SystemIdentity	C	Include when reasonably available to identify the SP providing CSN functionality.
AsnSystemIdentity	C	Include when reasonably available to identify the SP providing ASN functionality .

7.1.3.2 Serving System Reporting for SIP Registration

This ServingSystem event message reports a registration, a change, or an attempted change to the serving SP or intercept subject’s addressing information (e.g., for personal mobility).

The ServingSystem event message shall be triggered when:

- A request to register or deregister an intercept subject’s addressing information is directed or forwarded to a registrar (e.g., a SIP Proxy forwards a Register request to a SIP Registrar);

IMSIWKLI

- 1 • A request to register or deregister an intercept subject's addressing information is processed, failed, or
2 timed out by a registrar (e.g., a SIP Registrar processes a SIP Register request); or
3 • When the intercept subject is authorized for service by a SP.

4 The ServingSystem message includes the following parameters when used to report SIP registration:

5 **Table 7-2 – ServingSystem Message Parameters for SIP Registration**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	C	Include to identify the system containing the IAP, when the underlying data carriage does not imply that system.
Time Stamp	M	
RegisteringPartyIdentity	M	Identifies the party for whom terminal registration, is being attempted.
SystemIdentity	C	Include when reasonably available to identify the SP providing CSN functionality.
AsnSystemIdentity	C	Include when reasonably available to identify the SP providing ASN functionality .
RequestIdentity	C	Included to identify an address registration or deregistration request within a system, when available.
AddressRegistrationType	C	Indicates whether an address registration, address deregistration, or both were detected. Provided when appropriate.
RegisteringPartyIdentity	C	Identifies the party for whom address registration, deregistration, or both, are being attempted. Provided when appropriate.
RequestingPartyIdentity	C	Included to identify the party requesting the address registration, deregistration, or both, when different from the RegisteringPartyIdentity.
RegistrarIdentity	C	Identifies the registrar to which the address registration request, deregistration request, or both, are destined. Provided when appropriate.
RequestAddressInformation	C	Address information attempted to be registered, deregistered, or both, when present.
ResponseAddressInformation	C	Address information included in the response to the attempt to register, deregister, or both register and deregister address information, when present.
FailureReason	C	Included to indicate the reason that an address registration, deregistration, or both, were unsuccessful, when the registration, deregistration, or both are unsuccessful.
ExpirationPeriod	C	Included to identify the address-independent registration lifetime applicable to the registered addresses, when known.
Protocol-Specific Parameters	C	Included, when protocol-specific parameter information from VoIP signaling protocols (e.g., SIP message contents) are to be mapped into this message. For detailed descriptions of the mapping of this information, see the protocol-specific mapping annexes of [2] (e.g. Annex B on SIP mappings).
EncapsulatedSignalingMessage	O	The signaling message received from the intercept subject, sent to the intercept subject, or sent or received on behalf of the intercept subject, which stimulated the

		sending of the ServingSystem message.
--	--	---------------------------------------

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35

7.1.4 Dialed Digit Extraction Reporting

The DialedDigitExtraction Message defined in [2] shall be used to report subject-dialed or signaled digits in the VoIP content stream after the session is established from the perspective of the WiMAX-SP when those digits are reasonably available. The digits may be reported on a digit-by-digit basis, accumulated until a buffer is filled, accumulated until a timer expires, or accumulated until the VoIP call is released.

The DialedDigitExtraction message shall be triggered when covered by the lawful authorization and when:

- Digit-by-digit reporting is performed and a digit is detected; or
- Digit accumulation is performed and the first of the following occurs:
 - a. A maximum of 32 digits have been accumulated in the buffer;
 - b. 20 seconds have elapsed since detection of the first digit in the buffer; or
 - c. The call or session is released.

7.1.5 Location Information

When authorized and required, location information is included in a CII event message as follows:

- If location information for the subject is reasonably available in a SIP PANI header, it shall be reported and other location information may be reported.
- If location information for the subject is not reasonably available in a SIP PANI header, other subject location information shall be reported if reasonably available.

Location information from a SIP PANI header shall be reported in the location parameter. The locationType sub-parameter of the location parameter shall contain the access-type specification from the SIP PANI header (e.g. WMF-Mobile WiMAX) and the location sub-parameter shall contain the access-info specification from the SIP PANI header (e.g. wimax-bs-id=nnnnnsssss). If reasonably available, other location information may be reported in the location parameter or in the protocolSpecificParameters parameter.

7.2 CC-related Events

The following LAES messages, which are defined in [2], shall be utilized for WiMAX IMS-based VoIP CC-related event reporting:

- CCOpen
- CCChange
- CCClose
- CCUnavailable
- UUContent.

7.3 CC Delivery

The CCDelivery Application Protocol Data Unit (APDU), which is defined in [2], shall be used to encapsulate communications content packets for transfer over the CC delivery interface.

1 **ANNEX A. ASN.1 Definitions (Normative)**

2 This annex provides the Abstract Syntax Notation One (ASN.1) definitions for this specification. CII and CC
3 corresponding to ASN.1 definitions shall be encoded according to Basic Encoding Rules (BER) [10].

4 **A.1 CII ASN.1**

5 WiMAX-LAES-IMS-VoIP-CII-Abstract-Syntax-Module

6 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) ims-voip(4) cii(0) version-1(0)}

7
8 DEFINITIONS IMPLICIT TAGS ::=

9
10 BEGIN

11
12 IMPORTS

13
14 Answer,
15 CCClose,
16 CCOpen,
17 Change,
18 Origination,
19 Redirection,
20 Release,
21 ServingSystem,
22 TerminationAttempt,
23 ConferencePartyChange,
24 Connection,
25 ConnectionBreak,
26 DialedDigitExtraction,
27 NetworkSignal,
28 SubjectSignal,
29 DirectSignalReporting,
30 MediaAndAddressReporting,
31 CCChange,
32 CCUnavailable,
33 UUContent,
34 FeatureManagement,
35 SurveillanceStatus,
36 AddressRegistrationType,
37 CallIdentity,
38 Cause,
39 EncapsulatedSignalingMessage,
40 IAPSystemIdentity,
41 IPAddress,
42 PartyIdentity,
43 ProtocolSpecificParameters,
44 SipHeader,
45 SystemIdentity

46
47 FROM T1S1-LAES-VoP-Abstract-Syntax-Module

48 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-678(0) cii(0) common(0) version-4(3)}

49
50 CaseIdentity,

51 TimeStamp

52

IMSIWK LI

```

1 FROM Laesp-j-std-025-b
2 {iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-b(2) version-1(0)}
3
4 WiMAX-LAES-IMS-VoIP-CC-DeliveryHeaderModule-OID
5
6 FROM WiMAX-LAES-IMS-VoIP-CC-Module
7 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) ims-voip (4) cc(1) version-1(0)};
8
9 WiMAX-LAES-IMS-VoIP-CII-Abstract-Syntax-Module-OID ::= OBJECT IDENTIFIER
10
11 protocolIdentifier OBJECT IDENTIFIER ::= {WiMAX-LAES-IMS-VoIP-CII-Abstract-Syntax-Module-OID}
12
13 LAESProtocol ::= CHOICE {
14     enhancedProtocol          WiMAX-LAES-IMS-VoIP-CII-Protocol,
15     laesMessage               WiMAX-LAES-IMS-VoIP-CII-Message
16 }
17
18 WiMAX-LAES-IMS-VoIP-CII-Protocol ::= SEQUENCE {
19     protocolIdentifier        OBJECT IDENTIFIER,
20     wimaxLaesImsVoipCiiMessage WiMAX-LAES-IMS-VoIP-CII-Message
21 }
22
23 WiMAX-LAES-IMS-VoIP-CII-Message ::= CHOICE {
24     wimax-laes-ims-voip-answer          [1] Answer,
25     wimax-laes-ims-voip-ccClose        [2] CCClose,
26     wimax-laes-ims-voip-ccOpen         [3] CCOpen,
27     wimax-laes-ims-voip-change         [4] Change,
28     wimax-laes-ims-voip-origination    [5] Origination,
29     null-6                              [6] NULL,
30     -- [6] reserved by [025B] for Packet Envelope
31     wimax-laes-ims-voip-redirectation  [7] Redirection,
32     wimax-laes-ims-voip-release        [8] Release,
33     wimax-laes-ims-voip-servingSystem  [9] ServingSystem,
34     wimax-laes-ims-voip-termAttempt    [10] TerminationAttempt,
35     null-11                             [11] NULL,
36     -- [11] reserved by [025B] for Connection Test
37     wimax-laes-ims-voip-conferencePartyChange [12] ConferencePartyChange,
38     wimax-laes-ims-voip-connection      [13] Connection,
39     wimax-laes-ims-voip-connectionBreak [14] ConnectionBreak,
40     wimax-laes-ims-voip-dialedDigitExtraction [15] DialedDigitExtraction,
41     wimax-laes-ims-voip-networkSignal   [16] NetworkSignal,
42     wimax-laes-ims-voip-subjectSignal   [17] SubjectSignal,
43     wimax-laes-ims-voip-directSignalReporting [18] DirectSignalReporting,
44     wimax-laes-ims-voip-mediaAndAddressReporting [19] MediaAndAddressReporting,
45     wimax-laes-ims-voip-ccChange        [20] CCChange,
46     wimax-laes-ims-voip-ccUnavailable   [21] CCUnavailable,
47     wimax-laes-ims-voip-surveillanceStatus [22] SurveillanceStatus,
48     -- Optional message
49     wimax-laes-ims-voip-featureManagement [23] FeatureManagement,
50     -- Optional message
51     wimax-laes-ims-voip-uuContent       [24] UUContent
52 }
53
54 ServingSystem ::= SEQUENCE {
55     caseId                [0] CaseIdentity,
56     iAPSystemId           [1] IAPSystemIdentity OPTIONAL,

```

IMSIWKLI

```

1      timestamp                [2] TimeStamp,
2      systemIdentity            [3] SystemIdentity            OPTIONAL,
3      null4                     [4] Null -- Included for backward compatability
4      requestId                 [5] CallIdentity            OPTIONAL,
5      registrationType          [6] AddressRegistrationType  OPTIONAL,
6      registering                [7] PartyIdentity            OPTIONAL,
7      requesting                 [8] PartyIdentity            OPTIONAL,
8      registrar                  [9] PartyIdentity            OPTIONAL,
9      requestAddressInfo        [10] CHOICE {
10         generic                [0] SEQUENCE OF SEQUENCE {
11             address              [0] PartyIdentity,
12             expirationPeriod     [1] INTEGER}, -- in seconds
13         sip                      [1] SET OF SipHeader}        OPTIONAL,
14     responseAddressInfo        [11] CHOICE {
15         generic                [0] SEQUENCE OF SEQUENCE {
16             address              [0] PartyIdentity,
17             expirationPeriod     [1] INTEGER}, -- in seconds
18         sip                      [1] SET OF SipHeader}        OPTIONAL,
19     failureReason              [12] Cause                    OPTIONAL,
20     expirationPeriod           [13] CHOICE {
21         generic                [0] INTEGER, -- for all addresses, in seconds
22         sip                      [1] SipHeader}                OPTIONAL,
23         -- Maps SIP Expires header
24     protocolSpecificParameters [14] ProtocolSpecificParameters OPTIONAL,
25     signalingMsg                [15] SET OF EncapsulatedSignalingMessage OPTIONAL,
26     asnSystemIdentity           [16] SystemIdentity          OPTIONAL
27 }
28
29 Location ::= SET OF LocationInfo
30
31 LocationInfo ::= SEQUENCE {
32     locationType                [0] UTF8String,
33     locationData                 [1] UTF8String
34 }
35
36 END -- of WiMAX-LAES-IMS-VoIP-CII-Abstract-Syntax-Module
37

```

```
1 A.2 CC ASN.1
2 WiMAX-LAES-IMS-VoIP-CC-Abstract-Syntax-Module
3 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) ims-voip (4) cc(0) version-1(0)}
4
5 DEFINITIONS IMPLICIT TAGS ::=
6
7 BEGIN
8
9 IMPORTS
10
11 IAS-CC-APDU
12 FROM IAS-LAES-CmCC-Abstract-Syntax-Module
13 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmcc(1) version-4(3)};
14
15 wimax-LAES-IMS-VoIP-CC-Abstract-Syntax-Module-OID ::= OBJECT IDENTIFIER
16
17 WiMAX-CC-APDU ::= IAS-CC-APDU
18
19 END -- WiMAX-LAES-IMS-VoIP-CC-Abstract-Syntax-Module
```

1 **ANNEX B. Optional CII Event Messages**
2 **(Informative)**

3 The following LAES messages, which are defined in Annex D of [2], may be utilized for WiMAX IMS-based VoIP
4 CII event reporting:

- 5 • SurveillanceStatus
6 • FeatureManagement.

7