



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

Architecture, detailed Protocols and Procedures

WIMAX Lawful Intercept - NORTH AMERICAN REGION

**WMF-T33-107-R020v01**

WiMAX Forum<sup>®</sup> 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  
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.

58

1	<b>TABLE OF CONTENTS</b>	
2	<b>1. INTRODUCTION.....</b>	<b>6</b>
3	1.1 Background.....	6
4	1.2 Scope and Purpose.....	6
5	<b>2. NORMATIVE REFERENCES.....</b>	<b>8</b>
6	<b>3. DEFINITIONS &amp; ACRONYMS.....</b>	<b>10</b>
7	3.1 Definitions .....	10
8	3.2 Acronyms .....	12
9	<b>4. WIMAX® SERVICESDESCRIPTION .....</b>	<b>14</b>
10	4.1 WiMAX Services Model .....	14
11	4.2 General Surveillance Model .....	15
12	4.2.1 <i>Electronic Surveillance Model</i> .....	15
13	4.2.2 <i>Intercept Access Points</i> .....	16
14	<b>5. WIMAX® SUBJECT IDENTIFICATION.....</b>	<b>17</b>
15	5.1 Login Identifier .....	17
16	5.2 Equipment Identifier.....	17
17	<b>6. USER PERSPECTIVE .....</b>	<b>18</b>
18	6.1 Introduction .....	18
19	6.2 Surveillance Events .....	18
20	6.2.1 <i>Access Attempt</i> .....	18
21	6.2.2 <i>Access Accepted</i> .....	18
22	6.2.3 <i>Access Failed</i> .....	18
23	6.2.4 <i>Access Session End</i> .....	18
24	6.2.5 <i>Access Rejected</i> .....	18
25	6.2.6 <i>Access Signaling Message Report</i> .....	18
26	6.2.7 <i>Packet Data Session Start</i> .....	19
27	6.2.8 <i>Packet Data Session Failed</i> .....	19
28	6.2.9 <i>Packet Data Session End</i> .....	19
29	6.2.10 <i>Packet Data Session Already Established</i> .....	20
30	6.2.11 <i>Packet Data Header Report</i> .....	20
31	6.2.12 <i>Packet Data Summary Report</i> .....	20
32	6.2.13 <i>ServingSystem Event Reporting for Terminal Registration</i> .....	21
33	6.2.14 <i>Virtual Private Network (VPN) Security Association Establishment</i> .....	21
34	6.2.15 <i>Virtual Private Network (VPN) Security Association Release</i> .....	21
35	6.3 General Requirements .....	21
36	6.3.1 <i>Subject Communications</i> .....	21
37	6.3.2 <i>Communications Delivery</i> .....	21
38	6.3.3 <i>Timing Requirements</i> .....	22
39	6.3.4 <i>Performance and Quality</i> .....	22
40	6.3.5 <i>Security and Reliability over the Interface between DF and CF</i> .....	22
41	6.3.6 <i>Encryption and Compression</i> .....	23
42	6.3.7 <i>Isolation</i> .....	23
43	6.3.8 <i>Privacy and Authentication</i> .....	23
44	6.3.9 <i>Transparency</i> .....	23
45	6.3.10 <i>Correlation</i> .....	23
46	6.3.11 <i>Location Information Reporting</i> .....	24

1	6.3.12	<i>Handling of Tunneled Packets</i> .....	24
2	6.3.13	<i>WiMAX Femto Access Points</i> .....	24
3	<b>7.</b>	<b>NETWORK PERSPECTIVE</b> .....	<b>25</b>
4	7.1	Introduction .....	25
5	7.2	Definitions for “Mandatory,” “Optional,” and “Conditional” Parameters.....	25
6	7.3	Message Reporting .....	25
7	7.3.1	<i>Access Attempt Message</i> .....	25
8	7.3.2	<i>Access Accepted Message</i> .....	25
9	7.3.3	<i>Access Failed Message</i> .....	25
10	7.3.4	<i>Access Session End Message</i> .....	25
11	7.3.5	<i>Access Rejected Message</i> .....	25
12	7.3.6	<i>Access Signaling Message Report Message</i> .....	25
13	7.3.7	<i>Packet Data Session Start Message</i> .....	25
14	7.3.8	<i>Packet Data Session Failed Message</i> .....	26
15	7.3.9	<i>Packet Data Session End Message</i> .....	26
16	7.3.10	<i>Packet Data Session Already Established Message</i> .....	26
17	7.3.11	<i>Packet Data Header Report Message</i> .....	26
18	7.3.12	<i>Packet Data Summary Report Message</i> .....	26
19	7.3.13	<i>Virtual Private Network (VPN) Security Association Establishment</i> .....	27
20	7.3.14	<i>Virtual Private Network (VPN) Security Association Release</i> .....	27
21	7.4	Additional Message Reporting .....	27
22	7.4.1	<i>ServingSystem Event Reporting for Terminal Registration</i> .....	27
23	<b>8.</b>	<b>CMC DELIVERY</b> .....	<b>28</b>
24	<b>APPENDIX A.</b>	<b>(NORMATIVE)</b> .....	<b>29</b>
25	A.1	ASN.1 Definitions .....	29
26	A.1.1	<i>WiMAX CmII Abstract Syntax Module</i> .....	29
27	<b>APPENDIX B.</b>	<b>RELIABLE DELIVERY (INFORMATIVE)</b> .....	<b>32</b>
28	B.1	Short-Term Pull Buffering.....	32
29	B.2	Short-Term Push Buffering .....	32
30	<b>APPENDIX C.</b>	<b>OPTIONAL MESSAGES (INFORMATIVE)</b> .....	<b>33</b>
31	C.1	Optional Surveillance Status Messages .....	33
32	C.2	WiMAX CmII Optional Messages Abstract Syntax Module .....	33
33	<b>APPENDIX D.</b>	<b>INTERCEPTED COMMUNICATION CONTENT DELIVERY (NORMATIVE)</b> .....	<b>35</b>
34	D.1	WiMAX CmC Delivery Format .....	35
35	D.2	WiMAX CmCC Abstract Syntax Module .....	35
36	<b>APPENDIX E.</b>	<b>CANADIAN LOCATION REPORTING (NORMATIVE)</b> .....	<b>36</b>
37	E.1	Location information reporting.....	36
38	E.1.1	<i>Location_Update message definition</i> .....	36
39	E.1.2	<i>Location_Update message information elements definitions</i> .....	36
40	E.1.3	<i>Location_Message ASN.1</i> .....	37
41	E.2	Delivery over the communications delivery interface .....	38
42	<b>APPENDIX F.</b>	<b>LBS AND USI REPORTING</b> .....	<b>39</b>
43	F.1	User Perspective .....	39
44	F.1.1	<i>Reporting of Subject Communications for LBS-USI</i> .....	39

1	F.1.1.1 LBS Communications.....	39
2	F.1.1.2 USI Communications.....	39
3	F.2 Network Perspective.....	39
4	<i>F.2.1 LBS-USI Request Message</i> .....	39
5	<i>F.2.2 LBS-USI Response Message</i> .....	40
6	F.3 LBS-USI ASN.1 .....	41

7

1 **TABLE OF FIGURES**

2 FIGURE 1– WIMAX LI NETWORK SERVICES MODEL .....14  
3 FIGURE 2 – ELECTRONIC SURVEILLANCE MODEL .....15

4

5

6 **TABLE OF TABLES**

7 TABLE 1 – PACKET DATA HEADER REPORT MESSAGE PARAMETERS.....26  
8 TABLE 2 – PACKET DATA SUMMARY REPORT MESSAGE PARAMETERS .....26  
9 TABLE 3 – SERVINGSYSTEM MESSAGE PARAMETERS FOR TERMINAL REGISTRATION.....27  
10 TABLE 4 – LOCATION\_UPDATE MESSAGE.....36

11

---

# 1. Introduction

## 1.1 Background

This specification defines the interfaces between a service provider that facilitates WiMAX® subscriber access to the Internet, or to 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 Internet Access and Services (IAS) arrangements.

As used in this specification, electronic surveillance refers to the interception and delivery of communications – i.e., Communications Content (CmC), Communications Identifying Information (CmII), or both – for a particular Mobile Station (MS), WiMAX Femto Access Point (WFAP), or other user equipment as lawfully authorized. In this specification, an intercept subject, or more simply a subject, is a WiMAX subscriber MS, whose communications have been authorized by a legal instrument to be intercepted and delivered to an LEA. The identification of the subject is limited to subject identifiers, subject-related identifiers, or equipment identifiers used by the WiMAX Service or a WiMAX-SP equipment, facility, or communication service - e.g., network address, terminal identity, subscription identity.

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, and service areas where the communications and information are 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 ATIS-1000013-2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services (IAS) [16], as modified by ATIS-1000013.a-2009 Supplement A to ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services (IAS) [20], and WiMAX Lawful Broadband Access Intercept Part 0 – Overview [19].

## 1.2 Scope and Purpose

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

- Lawful Intercept (LI) for non-Internet Protocol (IP) services (e.g., Ethernet CS);
- Correlation of 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);
- Possible additional requirements specific to Multicast/Broadcast Service (MCBS);
- Possible additional requirements related to reporting of WFAP Closed Subscriber Group (CSG) information;
- Possible additional requirements related to Local Breakout; and
- Possible requirements specific to communications that undergo Network Address Translation by the WiMAX-SP.

For the U.S., this specification is provided for purposes of a “safe harbor” as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [1]: “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

- 1 telecommunication support services shall be found in compliance with Section 106, if the carrier,  
2 manufacturer, or support service provider is in compliance with publicly available technical  
3 requirements or standards adopted by an industry association or standard-setting organization, or by  
4 the Commission under subsection (b), to meet the requirements of section 103.”<sup>1</sup> [2, 3, 14, 15].
- 5 This specification is also intended for use in Canada to meet the Canadian requirements and  
6 capabilities for LAES. See Annex E Canadian Requirements for Canadian specific requirements and  
7 capabilities.

---

<sup>1</sup> It is not the intent of this document to imply or impact any pending CALEA regulatory decisions related to IAS. This document provides the mechanisms to perform lawfully authorized electronic surveillance of IAS subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable to IAS, 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
- 2 [1] Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, October 25, 1994.<sup>2</sup>
- 3 [2] In the Matter of Communications Assistance for Law Enforcement Act, Order on Remand, CC Docket No. 97-  
4 213, 17 FCC Record 6898 (2002).<sup>2</sup>
- 5 [3] In the Matter of Communications Assistance for Law Enforcement Act, Third Report and Order, CC Docket  
6 No. 97-213, 14 FCC Record 16794 (1999).<sup>2</sup>
- 7 [4] Wire and Electronic Communications Interception and Interception of Oral Communications, Title 18 of the  
8 United States Code, Chapter 119, Sections 2510 – 2522.<sup>2</sup>
- 9 [5] ITU-T Recommendation X.680, Information technology - Abstract Syntax Notation One (ASN.1):  
10 Specification of basic notation, July 2002.<sup>3</sup>
- 11 [6] Section 3 of the WiMAX Forum Specification adopts some of the definitions from ATIS-1000013.2007, as  
12 modified by ATIS-1000013.a-2009.
- 13 [7] IETF RFC 793, Transmission Control Protocol, September 1981.<sup>4</sup>
- 14 [8] Sections 4-8 of the WiMAX Forum Specification (excluding Section 7.4) reproduce in substantial part the  
15 corresponding sections of ATIS-1000013.2007, as modified by ATIS-1000013.a-2009, and adapts them for use  
16 in WiMAX™ networks.
- 17 [9] IETF RFC 791, Internet Protocol Darpa Internet Program Protocol Specification, September 1981.<sup>4</sup>
- 18 [10] IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998.<sup>4</sup>
- 19 [11] Packet Technologies in Wireline Telecommunications Networks, Version 2, January 2006.<sup>4</sup>
- 20 [12] ANSI J-STD-025-B, Joint T1-TIA Standard on Lawfully Authorized Electronic Surveillance, August 2006.
- 21 [13] Annex A and Annex C use ATIS definitions from ATIS-1000013.2007, as modified by ATIS-1000013.a-2009,  
22 supplemented by definitions that are specific to WiMAX networks.
- 23 [14] *In the matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services,*  
24 *First Report and Order and Further Notice of Proposed Rulemaking*, ET Document No. 04-295, 20 FCC Rcd  
25 14989 (2005).<sup>2</sup>
- 26 [15] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services,*  
27 *Second Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, 21 FCC Rcd 5360  
28 (2006).<sup>2</sup>
- 29 [16] ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services.
- 30 [17] WiMAX Forum, WMF-T32-001-R016v01 and WMF-T32-004-R015v01, “Architecture Tenets, Reference  
31 Model and Reference Points” Base Specification (Release 1.6) and Informative Annex (Release 1.5)
- 32 [18] Annex D adopts the ASN.1 format directly from ATIS-1000013.a-2009.
- 33 [19] WiMAX Forum WMF-T32-106-R02015v01, "Architecture Tenets, Reference Model and Reference Points,  
34 WiMAX Broadband Access Lawful Intercept: Overview", Release 2.01.5.
- 35 [20] ATIS-1000013.a.2009 Supplement A to ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance  
36 (LAES) for Internet Access and Services.

---

<sup>2</sup> This document is available from the AskCALEA website at < <http://www.askcalea.net> >.

<sup>3</sup> This document is available from the International Telecommunications Union. < <http://www.itu.int/ITU-T/> >

<sup>4</sup> 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> >

- 1 [21] ITU-T Recommendation X.690, Information technology - ASN.1 encoding rules: Specification of Basic  
2 Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguishing Encoding Rules (DER), July  
3 2002.<sup>3</sup>
- 4 [22] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.<sup>4</sup>
- 5 [23] IETF RFC 4960, Stream Control Transmission Protocol, September 2007.<sup>4</sup>
- 6 [24] IETF RFC 4340, Datagram Congestion Control Protocol (DCCP), March 2006.<sup>4</sup>
- 7 [25] WMF - T32-002 WiMAX Forum® Network Architecture (Stage 2: Architecture Tenets, Reference Model and  
8 Reference Points)
- 9 [26] WMF-T33-118-R016v01 "Architecture, detailed Protocols and Procedures: Femtocells Core Specification".
- 10 [27] WMF-T33-115-R015v01 "WiMAX Forum® Network Architecture: Universal Services Interface (USI) An  
11 Architecture for Internet+ Service Model"
- 12 [28] WMF-T33-110-R015v01 "WiMAX Forum® Network Architecture: Protocols and Procedures for Location  
13 Based Services"
- 14 [29] Amendment\_ASN\_LR-R020v01-A\_T33-001\_T33-109 "WiMAX Forum® Network Architecture:  
15 Architecture, Detailed Protocols and Procedures: ASN Local Routing: Amendment to T33-001-R020v01 and  
16 T33-109-R020v01"
- 17 [30] WMF-T32-001-R016v01, "Architecture Tenets, Reference Model and Reference Points, Base Specification",  
18 Release 1.6.
- 19

---

## 3. Definitions & Acronyms

### 3.1 Definitions

**Access-Associated Communications Identifying Information (AACmII):** CmII associated with communication between the subject and the WiMAX network for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the WiMAX network by the subject.

**WiMAX Network:** See Section 2.1.29 of [30].

**Access Service Network (ASN):** See Section 2.1.2 of [30].

**Connectivity Service Network (CSN):** See Section 2.1.10 of [30].

**Access Session:** The interval during which the user is authorized to access the WiMAX network. Packet data sessions occur within an access session.

**Closed Subscriber Group (CSG):** A CSG is defined in [26].

**Communication Content (CmC):** The full IP packet streams to and from the subject.

**Communication-Identifying Information (CmII):** Information that identifies the origin, direction, destination, or termination of each communication generated or received by a subject by means of any equipment, facility, or service of a WiMAX-SP.

Communications Identifying Information can be one of two types:

- 1) Access Associated Communications Identifying Information; or
- 2) Content Associated Communications Identifying Information.

Communications Identifying Information is “reasonably available” to a WiMAX-SP if it is present in the WiMAX-SP network and can be made available without the provider being unduly burdened with network modifications. CmII is delivered by the set of messages defined in this specification and the set of mandatory and conditional parameters contained therein.

**Communication:** Any wire or electronic communication, as defined in [4].

**Content Associated Communications Identifying Information (CACmII):** Communication Identifying Information associated with the delivery and routing of the subject’s packets in the network (i.e., the headers of the IP packets).

**Dynamic IP Address:** An IP address that is temporarily assigned to a subscriber’s equipment for a limited or specified duration.

**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 communication 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.

**Full Content Broadband Intercept Order:** Delivery of both CmC and AACmII information to LEA is authorized.

**Intercept:** Defined in [4] section 2510 (4) to be “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.”

**Intercept Access Point (IAP):** A point within a WiMAX-SP domain where some of the communications or communications identifying information of an intercept subject’s equipment, facilities, and services are accessed.

- 1 **Intercept Subject:** A WiMAX subscriber whose communications, communications identifying  
2 information, or both, have been authorized by a court to be intercepted and delivered to a Law  
3 Enforcement Agency. The identification of the intercept subject is limited to identifiers used  
4 to access the particular equipment, facility, or communication service (e.g., network address,  
5 terminal identity, subscription identity).
- 6 **Law Enforcement Agency (LEA):** A government entity with the legal authority to conduct electronic  
7 surveillance (e.g., the Federal Bureau of Investigation or a state or local police department).
- 8 **Limited Broadband Intercept Order:** Delivery of only CmII (AACmII and CACmII) information to  
9 LEA is authorized.
- 10 **Location Information:** Location information identifies the location of the subject's terminal.
- 11 **Mobile Station (MS):** A Mobile station is defined in [25].
- 12 **Packet:** An IP packet is defined in [9, 10].
- 13 **Packet Data Session:** The interval during which the user is granted resources to send or receive  
14 packets to or from the WiMAX network. Packet data sessions occur within an access  
15 session.
- 16 **Session:** A set of multimedia senders and receivers and the data streams flowing from senders to  
17 receivers. Access Sessions and Packet Data Sessions are specific types of sessions.
- 18 **Static IP Address:** An IP address that is permanently assigned to a subscriber's equipment.
- 19 **Stream:** A set of IP packets sharing the same IP addresses and the IP next-layer protocol. The packets  
20 also share the same flow label if the protocol is IPv6 and layer-4 ports if the IP protocol is  
21 TCP, UDP, SCTP, or DCCP.
- 22 **Subject:** See *intercept subject*.
- 23 **Subject Domain:** The subject domain is composed of the intercept subject and the intercept subject's  
24 equipment and facilities. The intercept subject's equipment may include, but is not limited to,  
25 personal computers, PDAs, MSs, gaming equipment, hubs, routers, switches, firewalls, local  
26 wireless access points, and any other equipment used by the subject to access the Internet. The  
27 subject's facilities include, but are not limited to, all customer premise wiring and customer  
28 premise equipment (CPE), whether owned by the subject or provider, used to facilitate access  
29 to the Internet.
- 30 The physical equipment and facilities in the subject domain support the logical functions of  
31 registration (when required), reservation, and packet transfer to and from the Internet. The  
32 registration function may be a fixed capability between the CPE and provider equipment for  
33 some access capabilities.
- 34 **Subscriber Identity:** Uniquely identifies the subscriber to the WiMAX service. This is the alias used  
35 by the WiMAX-SP to identify the intercept subject (e.g., userID, Service Acct ID, Charging  
36 User ID). There can be more than one form of identity used.
- 37 **Surveillance:** See Electronic Surveillance.
- 38 **WiMAX Femto Access Point (WFAP):** A WiMAX Femto Access Point is defined in [26].
- 39 **WiMAX Service Provider (WiMAX-SP):** Operator of a WiMAX network providing access to  
40 physical facilities provided by the WiMAX network that allows the intercept subject to invoke  
41 and utilize services provided by an Internet service provider. The services could be provided  
42 by the WiMAX-SP or by a third party service provider (e.g., Internet service provider).
- 43

1

2 **3.2 Acronyms**

AAA	Authorization, Authentication, and Accounting
AACmII	Access Associated CmII
ASN	Access Service Network
ANSI	American National Standards Institute
A-PDU <i>or</i> APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One [5]
ASP/iASP	Application Service Provider/Internet Application Service Provider
ATIS	Alliance for Telecommunication Industry Solutions
CACmII	Content Associated CmII
CALEA	Communications Assistance for Law Enforcement Act.
CF	Collection Function
CHAP	Challenge Handshake Authentication Protocol
CmC	Communication Content
CmII	Communication-Identifying Information.
CPE	Customer Premise Equipment
CSG	Closed Subscriber Group
CSN	Connectivity Service Network
CUI	Charging User Identifier
DCCP	Datagram Congestion Control Protocol
DHCP	Dynamic Host Configuration Protocol
DF	Delivery Function
FCC	Federal Communications Commission
GMT	Greenwich Mean Time
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
IAS	Internet Access and Services
IP	Internet Protocol
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LI	Lawful Intercept
LBS	Location Based Services
LR	Location Requestor
LS	Location Server
L-ID	Long-lived USI Identifier
MAC	Media Access Control
MF	Mediation Function
MOC	Mandatory Optional Conditional
MS	Mobile Station
NAI	Network Access Identifier

NAP	Network Access Provider
NSP	Network Service Provider
PDU	Protocol Data Unit
RADIUS	Remote Authentication Dial In User Service
SP	Service Provider
S-ID	Short-lived USI Identifier
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol [7]
UDP	User Datagram Protocol
USI	Universal Services Interface
VPN	Virtual Private Network
WFAP	WiMAX Femto Access Point

## 4. WiMAX® ServicesDescription

### 4.1 WiMAX Services Model

The WiMAX LI Network Services Model is based on a combination of the ATIS Internet Access and Services model [16] and the WiMAX Network Reference Model [17]. The WiMAX LI Network Services Model consists of the following:

1. the Subject Domain involving the WiMAX subscriber's equipment; and
2. the WiMAX Network Services Provider's (NSP) Domain, serving the Subject, consists of:
  - an ASN(s); and
  - a CSN.

For roaming situations, the WiMAX Visited Network consists of both an ASN(s) and a Visited CSN.

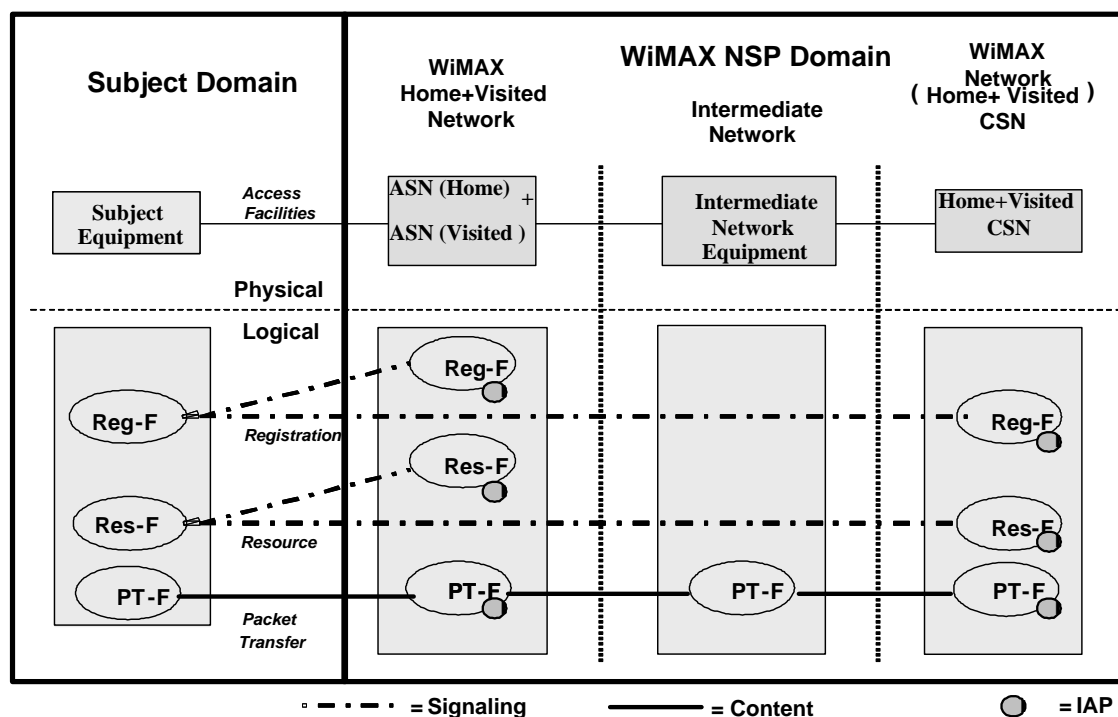


Figure 1– WiMAX LI Network Services Model

Description of components of Figure 1:

- a. The following logical functions are presented in Figure 1:
  - *Registration Function (Reg-F)* – Registration, for the purposes of this document, is defined as any login or authentication process required of the subject by the service provider to gain access to the Internet.
  - *Resource Function (Res-F)* – Resource reservation for the purposes of this document is defined as reserving resources (e.g., bandwidth) as necessary for access, and granting the subject access to the Internet. Resource reservation is recognized by providing the subject with one or more valid IP addresses, an IP address prefix or IP subnet address ranges that allow the subject to access the

1 Internet. Quarantined addresses, or addresses assigned for the purposes of registration are not  
 2 included as resources assigned in the network.

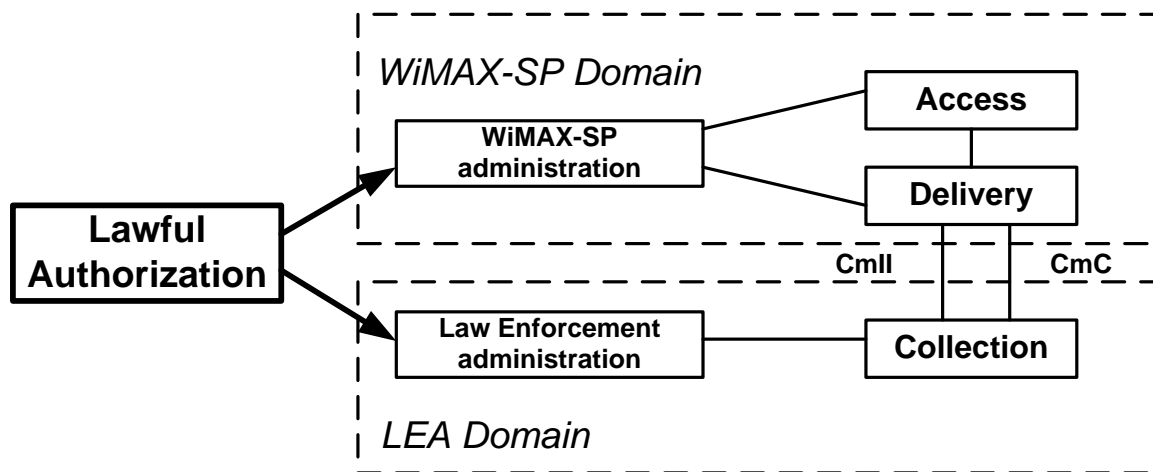
3 • *Packet Transfer Function (PT-F)* - For the purposes of this document, the packet transfer function  
 4 is defined as the process of transferring Layer 3 IP packets to and from the WiMAX network. For  
 5 packet transfer to occur, the subject needs to have completed Reg-F and Res-F, if required. For the  
 6 network to perform PT-F, the network elements need to be able to recognize the Layer 3 packet  
 7 structure and be able to handle the packets. Only those network elements that recognize the Layer 3  
 8 packet structure (i.e., IP header fields) and handle the packets can perform the packet transfer  
 9 function.

10 b. IAPs are possible Intercept Access Points. See section 4.2.2 Intercept Access Points.

## 11 4.2 General Surveillance Model

### 12 4.2.1 Electronic Surveillance Model

13 The functions needed to perform LAES are broadly categorized as access, delivery, collection, service  
 14 provider administration, and law enforcement administration [12]. These functions are described  
 15 herein without regard to their implementation. The relationship between these functional categories is  
 16 shown in Figure 2. As shown, the Access Function (AF), DF, and WiMAX-SP Administration  
 17 Function are the responsibility of the WiMAX-SP, and the Collection Function (CF) and Law  
 18 Enforcement Administration Function are the responsibility of the LEA. The use of these functions to  
 19 perform an interception is initiated by receipt of a specific lawful authorization.  
 20



21  
 22

23 **Figure 2 – Electronic Surveillance Model**

24 The *Access Function*, consisting of one or more IAPs, accesses and intercepts an intercept subject's  
 25 CmC and CmII unobtrusively. The IAPs may vary between WiMAX-SPs.

26 The *Delivery Function* delivers intercepted communications to one or more CFs. The DF shall deliver  
 27 intercepted communications in the form of CmC and CmII.

28 The *Collection Function* collects and analyzes the CmC and CmII received from the DF. It is defined  
 29 to be the location where lawfully authorized intercepted CmC and CmII is collected by a LEA.

30 The *WiMAX-SP Administration Function* controls the WiMAX-SP's AF and DF.

31 The *Law Enforcement Administration Function* controls the LEA's CF.

## 4.2.2 Intercept Access Points

With respect to WiMAX, IAPs are places in the network where lawful intercept of CmII and CmC occurs. There are two fundamental types of WiMAX IAPs:

1. WiMAX Communication Identifying Information IAPs (CmII-IAPs); and
2. WiMAX Communication Content IAPs (CmC-IAPs).

CmII-IAPs and CmC-IAPs are associated with CmII and CmC intercept functions respectively that perform the actual interception of CmII and CmC. These CmII and CmC intercept functions are incorporated into one or more network elements. CmII and CmC intercept functions may be collocated within the same network element, or may be distributed among many network elements. The interfaces for transport of CmII and CmC information from the CmII and CmC IAPs to the DF is outside the scope of the WiMAX specifications.

### 4.2.2.1 CmII-IAPs

CmII-IAPs capture information necessary to generate CmII and present it to the DF, or to the Mediation Function (MF) as defined in [16]. The CmII-IAP(s) can reside in a number of places. CmII-IAPs shall be placed such that reasonably available CmII can be intercepted whether the WiMAX-SP provides the ASN, CSN, or both for a specific communication. The specific placement of CmII-IAP(s) in a WiMAX network is a WiMAX-SP design decision.

CmII may be categorized as Access Associated CmII (AACmII) or Content Associated CmII (CACmII).

- Access Associated CmII*: CmII associated with communication between the subject and the WiMAX-SP domain for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the WiMAX network by the subject. All AACmII signaled between the subject and the network shall be reported to law enforcement.
- Content Associated CmII*: CmII associated with the delivery and routing of the subject's content in the network, derived from specific fields in the Layer 3 headers and Layer 4 headers of the IP packets as defined in 6.2.11 and 6.2.12. Two options exist for delivering CACmII:
  - Delivering the records for the specified header fields of each intercepted packet to law enforcement; or
  - Delivering summary records.

### 4.2.2.2 CmC-IAPs

A CmC-IAP intercepts the full packets to and from an intercept subject.

The CmC-IAP intercepts the subject's content and presents it to the DF or to the MF as defined in [16]. The CmC-IAP can reside in a number of places. When the WiMAX-SP supports interworking, CmC-IAPs shall be placed such that all CmC in the network of the WiMAX-SP can be intercepted whether the WiMAX-SP provides the ASN, CSN, or both for a specific communication. The specific placement of CmC-IAP(s) in a WiMAX network is a WiMAX-SP design decision.

---

## 1 **5. WiMAX® Subject Identification**

2 The subject's access to the WiMAX services can be divided into two categories defined by the way the  
3 subject activity is identified in the network.

### 4 **5.1 Login Identifier**

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

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

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

12 When subject activity is identified in the network through login identification, the subject (or subject's  
13 equipment) may be required to transmit and receive "signaling" packets – e.g., Challenge Handshake  
14 Authentication Protocol (CHAP) packets and CHAP v2 packets – to perform Registration Function  
15 (Reg-F) and Reservation Function (Res-F) in order to gain access (e.g., authentication and  
16 authorization) to the network and to receive resources (e.g., IP address). Interception of the subject's  
17 CmII and CmC is available only after the subject has been identified in the network. Signaling prior to  
18 the identification of the subject in the network, or during the period when a subject's equipment has  
19 been placed in this "quarantine" state, cannot be intercepted as the subject has not been identified in  
20 the network.

### 21 **5.2 Equipment Identifier**

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

- 25 • MAC address or set of MAC addresses associated with the subject's equipment;
- 26 • Static IP address, which could be a single IP address, a set of IP addresses or an IP subnet/IP prefix  
27 assigned to the subject's equipment;

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

29 When subject activity is identified in the network through equipment identification, login AACmII  
30 may not be available. For example, with pre-paid access the user log-in information may not be  
31 known and therefore may not be reported as AACmII.

---

## 6. User Perspective

### 6.1 Introduction

Section 6 presents the user perspective requirements for LAES for WiMAX-SP network. The user in this case is the LEA.

Section 6.2 presents communication-related events that represent or generate communication-identifying information (termed “surveillance events”) in the WiMAX-SP network.

Section 6.3 presents general capabilities needed for LAES for IAS.

### 6.2 Surveillance Events

This clause presents surveillance events that cause CmII to be reported. The events are based on ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20].

#### 6.2.1 Access Attempt

This event occurs when an Authentication, Authorization and Accounting (AAA) server detects an intercept subject or a surveiled WFAP attempting to enter or re-enter a WiMAX network.

#### 6.2.2 Access Accepted

This event occurs when the intercept subject, associated CPE network device, or a surveiled WFAP has successfully authenticated with a network AAA server, or Home Agent (or functional equivalent).

If the WiMAX-SP allows multi-login, where the same user identity and password is used multiple times to establish multiple concurrent and distinct access sessions, separate Access Accepted events shall be provided for each session.

#### 6.2.3 Access Failed

This event occurs when network authentication has failed and an access session has not been successfully established for an intercept subject or a surveiled WFAP with an AAA server.

#### 6.2.4 Access Session End

This event occurs when a AAA server detects that the intercept subject’s or a surveiled WFAP’s access has been disconnected and the access session is terminated. The following are example cases:

- The intercept subject initiates a disconnect request to the network;
- The subscriber equipment experiences a loss of power; or
- The network terminates the session due to expiration of timers or loss of signal to subject.

#### 6.2.5 Access Rejected

This event occurs at an AAA server when an intercept subject’s or a surveiled WFAP’s login procedure (authentication or authorization) to the network is successfully completed, but the access attempt is rejected for other reasons. The following is an example case:

- The Access Rejected message would be generated when a subject is already logged on, attempts a second login with a valid ID and password, but the network does not allow multiple logins.

#### 6.2.6 Access Signaling Message Report

This event occurs when the WiMAX system receives a signaling message from the intercept subject or a surveiled WFAP, or sends a signaling message to the intercept subject or a surveiled WFAP, and the event is not defined by one of the other clauses in section 6.2.

1 Examples of such a signaling message are a Remote Authentication Dial In User Service (RADIUS<sup>5</sup>),  
2 or Diameter<sup>6</sup> - detected in the network.

3 This event also occurs when the WiMAX network signals to a network node that a Local Routing  
4 capability as described in [29] may/must be enabled or disabled for one or more service flows of the  
5 subject and such enabling or disabling could disrupt the intercept. Examples of intercept disruption  
6 include cases where there is no IAP at the Local Routing point or the Local Routing point is located in  
7 another service provider's network. If the enabling or disabling of the Local Routing capability would  
8 be transparent to the intercept (e.g., no change in the availability of intercept data or the DF reporting  
9 the data) then reporting of the enabling/disabling is not required. Note that [29] contains requirements  
10 describing circumstances under which ASN Gateway Local Routing may and may not be  
11 enabled/disabled for subject communications.

### 12 **6.2.7 Packet Data Session Start**

13 This event occurs when an intercept subject or a surveiled WFAP successfully completes any login process  
14 required by the network and whenever one or more IP addresses or prefixes/subnets are assigned to the subject's  
15 equipment.

### 16 **6.2.8 Packet Data Session Failed**

17 This event occurs when an intercept subject's or a surveiled WFAP's login procedure to the network is  
18 successfully completed, but the intercept subject is denied access to the network. An example of this  
19 is:

- 20 • When the IP addresses or other network resources to accommodate the subject's use of the network  
21 are not available.

### 22 **6.2.9 Packet Data Session End**

23 This event occurs when an intercept subject or a surveiled WFAP ends a packet data session with the network. In  
24 cases in which the intercept is based on a subject's IP addresses or prefixes/subnets that are allocated dynamically  
25 (see clause 6.2.10), the Packet Data Session End event is considered to occur, and shall be reported, in the  
26 following cases:

- 27 • The IP address associated with a packet data session is explicitly released (e.g., by a DHCPRELEASE  
28 [22], or by release of a Mobile IP session);  
29
- 30 • The IP address associated with a packet data session is no longer assigned to the subject or the  
31 surveilled WFAP. This may include the following situations:
  - 32 • The WiMAX network terminates a subject's session after a pre-established time period or  
33 inactivity period (e.g., a DHCP lease expiration);
  - 34 • The WiMAX network terminates the subject's session for other reasons (e.g., resource  
35 condition or administrative controls); or
  - 36 • The WiMAX network detects the intercept subject's equipment disruption of connectivity  
37 (e.g., loss of physical layer or data link layer) and after a specified time, terminates the  
38 subject's packet data session.

---

<sup>5</sup> For more information, see IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. This document is available from the Internet Engineering Task Force (IETF). < <http://www.ietf.org> >

<sup>6</sup> For more information, see IETF RFC 3588, *Diameter Base Protocol*. This document is available from the Internet Engineering Task Force (IETF). < <http://www.ietf.org> >

### 1 **6.2.10 Packet Data Session Already Established**

2 This event occurs when the WiMAX system detects that surveillance begins on an intercept subject's  
3 communications for any packet data session of the intercept subject that is already established<sup>7</sup>, regardless  
4 of whether the intercept subject is actively transmitting or receiving packets, as in the following examples:

- 5 • Lawful electronic surveillance commences on an intercept subject who already has an established  
6 access session with the subscribed-to WiMAX-SP (e.g., the login event may have occurred prior to  
7 surveillance starting), whether or not the intercept subject is actively transmitting or receiving  
8 packets at the time;
- 9 • Lawful electronic surveillance commences on an intercept subject who is identified by an  
10 equipment identifier (as described in 5.2) and delivery of either CmC or CACmII is initiated; or
- 11 • A Mobile Station performs a Handover from a normal basestation or another WFAP to a surveilled  
12 WFAP.

13 Where packets are isolated based on IP addresses it is essential to track the assignment and release of  
14 dynamic IP addresses so the communications of the intercept subject are not missed and only the  
15 communications of the intercept subject are captured. The Packet Data Session Already Established event  
16 shall report the current dynamic IP addresses of an intercept subject when the WiMAX-SP determines that  
17 the subject has already been assigned one or more dynamic IP addresses prior to the start of the intercept.

### 18 **6.2.11 Packet Data Header Report**

19 This event is used to provide CACmII packet header reports on a per packet basis (non-summarized  
20 reporting) when reporting of CmC is not authorized for the intercept. The event is triggered by each  
21 packet of a packet stream sent or received by the subject or a surveiled WFAP. The report event  
22 provides source and destination information derived from the packet headers and the number of bytes  
23 for each packet. IP addresses and the IP next-layer protocol are always reported, the flow label is  
24 reported if the packet is IPv6, and the layer-4 ports are reported if the IP protocol is TCP, UDP, SCTP  
25 [Ref 23], or DCCP [Ref 24].

### 26 **6.2.12 Packet Data Summary Report**

27 This event is used to provide CACmII summary reports when reporting of CmC is not authorized for  
28 the intercept. The event may be triggered by the start of a packet stream, interim report of a packet  
29 stream, or end of a packet stream. An interim report can also be triggered by: a) expiration of a timer;  
30 b) reaching a count limit; or c) a change in information being counted (e.g., the IP Address being  
31 counted changes). The report event provides source and destination information derived from the  
32 packet headers and summary information for the number of packets and number of bytes destined to or  
33 originated by the subject or a surveiled WFAP for each stream set, and the time of the first and last  
34 packets associated with each stream set. IP addresses and the IP next-layer protocol are always  
35 reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported if the IP  
36 protocol is TCP, UDP, SCTP [Ref 23], or DCCP [Ref 24].

37 The Packet Data Summary Report can be used as the single reporting event for CmII associated with IP headers  
38 from subscriber content when reporting the information in other events would be redundant.

39 Packet Data Summary Reports are reported per IAP.

---

<sup>7</sup> There are a number of approaches to determine whether the subject's packet data session has already been established. One approach is to obtain the subject's session status by contacting service provider's user login database (e.g., RADIUS log records). In this approach, the determination of Packet Data Session Already Established relies on the completeness of Res-F. In another approach, the IAP uses the equipment identification to identify the subject and intercepts the subject's packets. The IAP then determines that the packet data session has already been established when data packets are intercepted.

### 6.2.13 ServingSystem Event Reporting for Terminal Registration

This event occurs when the intercept subject's MS or the WFAP that is the subject of an intercept order is authorized for service with a SP, including the home network, or in another service area

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

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

### 6.2.14 Virtual Private Network (VPN) Security Association Establishment

This event occurs when a VPN connection is established between an intercept subject host and a destination host using a WiMAX-SP VPN system as the intercept subject's VPN endpoint. A VPN Security Association Establishment event is considered to occur and shall be reported in the following case:

- The intercept subject establishes a (transport mode) VPN with participation of a WiMAX-SP VPN network system.

Note: A VPN connection can be established in a tunneling mode whereby only the endpoints – the intercept subject host and a destination host – participate in the set up of the protected security association and exchange encrypted IP packet payloads. All intermediary network elements (the WiMAX-SP in this case) see only the source and destination IP addresses of the endpoints in the unencrypted IP headers, but the port addresses remain hidden within the encrypted packet contents. However, if a WiMAX-SP system participates in the VPN connection establishment (transport mode VPN) on behalf of the intercept subject, the event and associated information can be detected by the WiMAX-SP.

### 6.2.15 Virtual Private Network (VPN) Security Association Release

This event occurs when a VPN connection that was established by a WiMAX-SP domain system on behalf of the intercept subject supporting protected IP communications with a remote IP address terminates. The VPN Security Association Release event is considered to occur in the following cases:

- Either the local or remote end of the VPN ends the security association.
- The VPN security association is terminated due to inactivity or an error.

## 6.3 General Requirements

### 6.3.1 Subject Communications

The WiMAX-SP shall ensure that the complete communications (i.e., full packet stream to and from the subject's equipment, facilities, and service under a full content order, or packet headers to and from the subject's equipment, facilities, and service under an order that requires only the delivery of CmII) of the subject are intercepted regardless of whether it provides the ASN, CSN, or both for a particular communication.

### 6.3.2 Communications Delivery

Various delivery methods and associated technologies can be used to support the communications delivery interface between an WiMAX-SP and law enforcement. These delivery methods carry the CmII and CmC defined in this specification. Arrangement for these delivery methods (e.g., TCP/IP, UDP/IP) and the underlying technologies (e.g., private T1, internet, Ethernet/fiber) are made between

1 the WiMAX-SP and the LEA and accordingly affect information carried in the CmC delivery header  
2 and the timeliness of the delivered CmII and CmC.

3 The format for delivery of CmII across the communications delivery interface is specified in Annex  
4 A.1. The format for delivery of CmC across the communications delivery interface is specified in  
5 Section 8 and Annex D.

### 6 **6.3.3 Timing Requirements**

#### 7 **6.3.3.1 Timing Requirements for CmII**

8 Timing information includes two elements:

- 9 a. **Event Time-stamp:** Each surveillance message shall contain a time-stamp that is recorded  
10 within a specific amount of time from when the event triggering the surveillance message was  
11 detected (i.e., the time difference between the time the CmII triggering event was detected and  
12 the time recorded in the time-stamp).
- 13 b. **Event Timing:** Surveillance messages shall be sent to the LEA within a defined amount of  
14 time after the information pertaining to the CmII triggering event is available at the IAP. The  
15 preferred precision is in milliseconds when reasonably available.

16 The following timing requirements shall apply to the delivery of CmII:

- 17 • Each surveillance message shall be sent by the DF to the CF within eight (8) seconds of receipt by  
18 the IAP of the information pertaining to the CmII triggering event at least 95% of the time.
- 19 • Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when  
20 the CmII event triggering the surveillance message was detected. The time-stamp shall include a  
21 Greenwich Mean Time (GMT) offset, if available.

#### 22 **6.3.3.2 Timing Requirements for CmC**

23 The following timing requirements shall apply to the delivery of CmC:

- 24 • Time-stamps shall be provided with encapsulated intercepted packets delivered to the CF, unless  
25 timing is provided by other means such as a guaranteed method for timely delivery of content from  
26 access to the delivery function, in which case timestamping may occur at the delivery function.

### 27 **6.3.4 Performance and Quality**

28 The WiMAX-SP shall be capable of performing multiple intercepts per subject.

29 The WiMAX-SP shall be capable of performing intercepts on multiple subjects.

30 The WiMAX-SP shall be capable of performing intercepts for multiple LEAs for the same subject. The  
31 intercepts shall not be detectable among LEAs.

32 The quality of the communication delivery interface is defined by the negotiation between the  
33 WiMAX-SP and the LEA.

### 34 **6.3.5 Security and Reliability over the Interface between DF and CF**

35 The equipment, facilities or services for delivering CmII and CmC over the interface between DF and  
36 CF are procured by the LEA, and their specifications are outside the scope of this Standard. Security  
37 and reliability are a function of those equipment, facilities, or services procured (e.g., private line,  
38 public internet, point-to-point). When feasible based on the delivery equipment, facilities, or services  
39 procured by the LEA, the WiMAX-SP shall offer a method to ensure that the intercepted CmII and  
40 CmC are delivered to the LEA securely and reliably. When the WiMAX-SP provides buffering of  
41 intercept data as defined in Annex B, the SHA-256 hashing function, at a minimum, shall be used.  
42 Hash values shall be retained by the WiMAX-SP for five years, or as otherwise negotiated with the  
43 LEA on a per-case basis.

### 1 **6.3.6 Encryption and Compression**

2 If the WiMAX-SP uses encryption in the network, the WiMAX-SP shall deliver the intercepted data to  
3 the LEA in unencrypted form or provide the encryption keys and specify the encryption method. If the  
4 intercepted data is available at the IAP in both encrypted form and unencrypted form, the WiMAX-SP  
5 shall provide it to the LEA in unencrypted form.

6 If the WiMAX-SP uses compression in the network, the WiMAX-SP shall deliver the intercepted data  
7 to the LEA in uncompressed form, or identify the means to decompress. If the intercepted data is  
8 available at the IAP in both compressed form and uncompressed form, the WiMAX-SP shall provide it  
9 to the LEA in uncompressed form.

### 10 **6.3.7 Isolation**

11 While the intercept is active, the WiMAX-SP shall ensure that only authorized communications are  
12 intercepted, according to the surveillance order served.

13 The WiMAX-SP shall ensure that only communications associated with the subject's equipment are  
14 intercepted. Communications not associated with the subject's equipment, facilities, or services shall  
15 not be delivered to the LEA.

16 For purpose of this specification, when the subject of an intercept order is a WFAP, an MS connected  
17 to the WFAP via the Reference Point R1 is considered to be a subject of an intercept order for the  
18 duration of the connection.

### 19 **6.3.8 Privacy and Authentication**

20 The WIMAX-SP shall not monitor or permanently record the subject communications.

21 The WIMAX-SP shall ensure that the captured communication originates from or is directed to the  
22 subject's equipment, facilities, or service.

### 23 **6.3.9 Transparency**

24 The WiMAX-SP shall perform the intercept in such a manner that the subject, the operator of a  
25 surveilled WFAP, or an MS at a surveilled WFAP cannot reasonably detect that the intercept is being  
26 performed.

27 The intercept shall be transparent to all non-authorized employees of the WiMAX-SP as well as to all  
28 other non-authorized persons.

29 Nothing, from the subject's point of view, should be detectable as the result of LAES. The subject's  
30 service parameters shall not be impacted by the intercept in such a way that the surveillance is  
31 detectable. Note that replication of packets may cause some latency, but this latency should not be  
32 reasonably detectable by the subject.

33 Note that it is understood that interception of subject communications in networks utilizing Local  
34 Routing capabilities, as defined in [29], could lead to situations where additional latency or other  
35 performance changes may be detectable by the subject. When WiMAX-SPs follow the requirements  
36 in [29] regarding the enabling/disabling of ASN Gateway Local Routing for the communications of LI  
37 subjects, for purposes of this specification it will be assumed that the subject's terminal equipment  
38 cannot reasonably detect that the intercept is being performed.

### 39 **6.3.10 Correlation**

40 The WiMAX-SP shall ensure that the intercepted information is correlated to the appropriate type of intercept order  
41 (i.e., "limited" or "full content"), for a subject. When multiple intercept orders exist for the same subject, the  
42 reporting of each order is correlated to the specified type of intercept order.

### 6.3.11 Location Information Reporting

When location information is lawfully authorized and is reasonably available, the WiMAX Network shall report location type and the actual location. The WiMAX Network shall report all location information reasonably available, which may include multiple sets of location information, for example:

locationType = "streetaddress", location = "100 First Street",

locationType = "IP", location = "10.17.123.12".

locationType = "Cell ID", location = BSId value of the basestation / WFAP.

Identical information from different sources (e.g., two identical Cell IDs) may be reported only once; however, when different sources provide different values for the same type of location information (e.g., two different values of latitude/longitude coordinates) both shall be reported.

The level of detail of the reported location information should be commensurate with the level of detail of the location information reasonably available at the IAP. For a subject that is connected to the WiMAX ASN, the location information typically contains the Cell ID.

Note: Because the WFAP is a consumer device location information reported by the WFAP cannot be trusted. Because a WFAP may be nomadic or mobile the physical location represented by a WFAP cell ID may change over time. Therefore additional information may be required to determine the location of the WFAP or an MS attached to a WFAP.

### 6.3.12 Handling of Tunneled Packets

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

### 6.3.13 WiMAX Femto Access Points

When the intercept subject is a WFAP and surveillance of a WFAP is allowed by national or regional law or regulation, intercepted communication shall include communication directed to and from the WFAP itself as well as communication directed to any MS accessing the network via the subject WFAP. CmII intercepted for a WFAP reports signaling messages received from the WFAP, or sent towards the WFAP, when those messages neither originate at nor are directed toward an MS connected to the WFAP. This CmII shall be reported with the Subscriber Identity parameter populated with the identity of the WFAP. Signaling messages received from an MS connected to the WFAP or sent toward an MS connected to the subject WFAP shall be reported with the Subscriber Identity parameter populated with the identity of the MS. Similarly, CmC intercepted for a WFAP reports user plane communications received from the WFAP, or sent towards the WFAP, when those communications do not originate at, nor are directed towards an MS connected to the WFAP. The CmC may include configuration messages for the WFAP, such as the messages used to manage a Close Subscriber Group at the WFAP. CmC intercepted for MSs connected to the network via the subject WFAP reports user plane communications received from an MS connected to the WFAP or sent towards an MS connected to the WFAP.

---

## 7. Network Perspective

### 7.1 Introduction

This clause identifies messages, describes the information to be reported for each WiMAX® CmII message, and describes the application level CmC 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.

### 7.2 Definitions for “Mandatory,” “Optional,” and “Conditional” Parameters

The value in the Mandatory/Optional/Conditional (MOC) column in the Message Parameter tables in this document indicates whether inclusion of the indicated parameter in the indicated message is *Mandatory* (M), *Optional* (O), or *Conditional* (C).

- A *Mandatory* (M) value means that the sender of the message shall always include this parameter in the message.
- An *Optional* (O) value means that the sender of the message may include this parameter in the message.
- A *Conditional* (C) value means that the sender of the message shall include this parameter in the message when the criteria specified in the *Conditions* column are met.

### 7.3 Message Reporting

The messages and associated information listed in this clause are reported as specified in ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20] unless otherwise noted.

#### 7.3.1 Access Attempt Message

See ATIS-1000013.2007 6.2.1 [16].

#### 7.3.2 Access Accepted Message

See ATIS-1000013.2007 6.2.2 [16], as modified by ATIS-1000013.a.2009 [20].

#### 7.3.3 Access Failed Message

See ATIS-1000013.2007 6.2.3 [16], as modified by ATIS-1000013.a.2009 [20].

#### 7.3.4 Access Session End Message

See ATIS-1000013.2007 6.2.4 [16], as modified by ATIS-1000013.a.2009 [20].

#### 7.3.5 Access Rejected Message

See ATIS-1000013.2007 6.2.5 [16], as modified by ATIS-1000013.a.2009 [20].

#### 7.3.6 Access Signaling Message Report Message

See ATIS-1000013.2007 6.2.6 [16].

#### 7.3.7 Packet Data Session Start Message

See ATIS-1000013.2007 6.2.7 [16], as modified by ATIS-1000013.a.2009 [20].

1 **7.3.8 Packet Data Session Failed Message**

2 See ATIS-1000013.2007 6.2.8 [16].

3 **7.3.9 Packet Data Session End Message**

4 See ATIS-1000013.2007 6.2.9 [16], as modified by ATIS-1000013.a.2009 [20].

5 **7.3.10 Packet Data Session Already Established Message**

6 See ATIS-1000013.2007 6.2.10 [16], as modified by ATIS-1000013.a.2009 [20].

7 **7.3.11 Packet Data Header Report Message**

8 The Byte Count sub-parameter of the Header Set parameter is defined as the number of bytes  
 9 contained in the packet triggering the event. If the packet is IPv4 the number of bytes is the value  
 10 contained in the Total Length field [9]. If the packet is IPv6 the number of bytes is the value  
 11 contained in the Payload Length field [10].

12 **Table 1 – Packet Data Header Report Message Parameters**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Header Set	M	

13  
 14

15 **7.3.12 Packet Data Summary Report Message**

16 The Stream Period sub-parameter of the Stream Set parameter defines the period of time  
 17 during which packets associated with a given stream set were sent or received by the Subject.  
 18 The stream period is defined by the time of the first packet sent during the time period  
 19 covered by the Packet Data Summary Report and the time of last packet sent during the time  
 20 period covered by the Packet Data Summary Report. The time of the first and last packets  
 21 are reported in units of milliseconds.

22 The Byte Count sub-parameter of the Stream Set parameter is defined as the sum of the number of  
 23 bytes contained in each packet of the stream triggering the event. If the packet is IPv4 the number  
 24 of bytes is the sum of the values contained in the Total Length field of each packet [9]. If the  
 25 packet is IPv6 the number of bytes is the sum of the values contained in the Payload Length  
 26 field of each packet [10].

27 **Table 2 – Packet Data Summary Report Message Parameters**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Stream Set	M	

28  
 29

**7.3.13 Virtual Private Network (VPN) Security Association Establishment**

See ATIS-1000013.2007 Table C.2 [16].

**7.3.14 Virtual Private Network (VPN) Security Association Release**

See ATIS-1000013.2007 Table C.3 [16].

**7.4 Additional Message Reporting**

The messages in this clause are to be reported in addition to the ones specified in clause 7.3. The Information Element definitions (e.g., Case Identity, IAP System Identity, Location Information) are as specified in Section 6.1.1 of ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20].

**7.4.1 ServingSystem Event Reporting for Terminal Registration**

As defined in this Specification, the ServingSystem Event is used to report terminal and WFAP registration. The ServingSystem Message shall be triggered when:

- the MS is authorized for service,
- the WFAP is authorized for service.

When known, the SP reporting a Serving System event message shall identify both the ASN and CSN serving the IP session 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 [30]. Examples of data that may be used to identify the SP providing the ASN functionality in the AsnSystemIdentity information element in Tables 1 and 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 [30]. 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, such as IP address, should be preferred when available rather than Operator ID).

When used to report the registration of a WFAP, the ‘SubscriberIdentity’ parameter is used to report the MAC address of the WFAP.

**Table 3 – ServingSystem Message Parameters for Terminal Registration**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
SystemIdentity	C	Include when reasonably available to identify the WiMAX-SP providing the CSN functionality.
AsnSystemIdentity	C	Include when reasonably available to identify the SP providing ASN functionality
Location Information	C	Provide when reasonably available and lawfully authorized.

---

1 **8. CmC Delivery**

2 Delivery of CmC for WiMAX® Internet Access is based on the Abstract Syntax Notation One (ASN.1)  
3 CmC delivery method in the ATIS Internet Access and Services standard [16], as modified by ATIS-  
4 1000013.a.2009 [20]. See Annex D. in this specification for the ASN.1 delivery format for WiMAX  
5 CmC delivery.  
6

---

## APPENDIX A. (Normative)

### A.1 ASN.1 Definitions

This annex provides the Abstract Syntax Notation One (ASN.1) [5] definitions for this specification. CmII and CmC corresponding to ASN.1 definitions shall be encoded according to Basic Encoding Rules (BER) [Ref 21].

#### A.1.1 WiMAX CmII Abstract Syntax Module

```
WiMAX-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmii(0) version-3(2)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

    Access-Attempt,
    Access-Accepted,
    Access-Failed,
    Access-Session-End,
    Access-Rejected,
    Access-Signaling-Message-Report,
    Packet-Data-Session-Start,
    Packet-Data-Session-Failed,
    Packet-Data-Session-End,
    Packet-Data-Session-Already-Established,

    CasIdentity,
    IAPSystemIdentity,
    IpAddress,
    Location,
    PacketDataSessionID,
    SubscriberIdentity,
    TimeStamp,
    Value
FROM IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2(1)};

    VPNSecurityEstablishment,
    VPNSecurityRelease
FROM IAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii-optional(2) version-2(1)};

wimax-LAES-CmII-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmii(0) version-3(2)}

wimax-CmII-Protocol-Identifier OBJECT IDENTIFIER ::= {wimax-LAES-CmII-Abstract-Syntax-Module-
OID}

WiMAXProtocol ::= SEQUENCE
{
    wimax-CmII-Protocol-Identifier OBJECT IDENTIFIER,
    wimaxMessage WiMAXMessage
}
```

```

1
2 WiMAXMessage ::= CHOICE {
3     access-Attempt           [0] Access-Attempt,
4     access-Accepted         [1] Access-Accepted,
5     access-Failed           [2] Access-Failed,
6     access-Session-End     [3] Access-Session-End,
7     access-Rejected         [4] Access-Rejected,
8     access-Signaling-Message-Report [5] Access-Signaling-Message-Report,
9     session-Start           [6] Packet-Data-Session-Start,
10    session-Failed          [7] Packet-Data-Session-Failed,
11    session-End              [8] Packet-Data-Session-End,
12    session-Already-Established [9] Packet-Data-Session-Already-Established,
13    data-Header-Report       [10] Packet-Data-Header-Report,
14    data-Summary-Report      [11] Packet-Data-Summary-Report,
15    serving-System           [12] ServingSystem,
16    vPN-Security-Establishment [13] VPNSecurityEstablishment,
17    vPN-Security-Release     [14] VPNSecurityRelease
18 }
19
20 -- WiMAX Message Definitions
21
22 Packet-Data-Header-Report ::= SEQUENCE
23 {
24     caseld           [0] Caseldentity,
25     iAPSystemId     [1] IAPSystemIdentity,
26     timestamp       [2] TimeStamp,
27     subscriberIdentity [3] SubscriberIdentity,
28     headerSet       [4] HeaderSet,
29     ...
30 }
31
32 Packet-Data-Summary-Report ::= SEQUENCE
33 {
34     caseld           [0] Caseldentity,
35     iAPSystemId     [1] IAPSystemIdentity,
36     timestamp       [2] TimeStamp,
37     subscriberIdentity [3] SubscriberIdentity,
38     streamSet       [4] StreamSet,
39     ...
40 }
41
42 ServingSystem ::= SEQUENCE
43 {
44     caseld           [0] Caseldentity,
45     iAPSystemId     [1] IAPSystemIdentity,
46     timestamp       [2] TimeStamp,
47     subscriberIdentity [3] SubscriberIdentity,
48     systemIdentity  [4] SystemIdentity OPTIONAL,
49     locationInformation [5] Location OPTIONAL,
50     asnSystemIdentity [6] SystemIdentity OPTIONAL,
51     ...
52 }
53
54 -- WiMAX Parameter Definitions
55
56 HeaderSet ::= SEQUENCE
57 {
58     packetDataSessionID [0] PacketDataSessionID,
59     sourceIPAddress      [1] IpAddress,
60     destinationIPAddress [2] IpAddress,
61     protocol             [3] INTEGER,
62     byteCount            [4] INTEGER,

```

```
1      sourcePortNumber [5] INTEGER OPTIONAL,  
2      destinationPortNumber [6] INTEGER OPTIONAL,  
3      ipv6FlowLabel [7] INTEGER OPTIONAL  
4  }  
5  
6  StreamPeriod ::= SEQUENCE  
7  {  
8      startTime [0] TimeStamp,  
9      endTime [1] TimeStamp,  
10 }  
11  
12 StreamSet ::= SET OF SEQUENCE  
13 {  
14     packetDataSessionID [0] PacketDataSessionID,  
15     sourceIpAddress [1] IpAddress,  
16     destinationIpAddress [2] IpAddress,  
17     packetCount [3] INTEGER,  
18     protocol [4] INTEGER,  
19     byteCount [5] INTEGER,  
20     streamPeriod [6] StreamPeriod,  
21     sourcePortNumber [7] INTEGER OPTIONAL,  
22     destinationPortNumber [8] INTEGER OPTIONAL,  
23     ipv6FlowLabel [9] INTEGER OPTIONAL  
24 }  
25  
26 SystemIdentity ::= Value  
27  
28 END -- WiMAX-LAES-CmII-Abstract-Syntax-Module  
29  
30  
31
```

---

## 1 **APPENDIX B. Reliable Delivery (Informative)**

2 It is important that intercept information be delivered in as reliable and robust a way as possible from  
3 the DF to the LEA. To this end, there are a number of suggested mechanisms.

### 4 **B.1 Short-Term Pull Buffering**

5 ATIS-1000021 "Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment"<sup>8</sup>  
6 defines a mechanism where CmII and CmC are stored in files rather than being transported in real time. The files  
7 and their contents are described in detail in ATIS-100021 as well as the mechanisms to determine how often files are  
8 created and for accessing them. In summary, within a case, CmII is stored as ASN.1 messages, CmC is stored in  
9 Packet CAPture (PCAP) format, and log files provide auxiliary information, such as hashes of the CmII and CmC  
10 files. The LEA CF uses Secure Shell version 2 (SSH2) and Secure FTP (SFTP) to pull the files out, and may then  
11 verify hashes before deleting the files. SSH2 and SFTP provide the LEA with strong authentication and encryption.  
12 The specifics of the PCAP format used is also defined in ATIS-1000021.

### 13 **B.2 Short-Term Push Buffering**

14 An alternative mechanism may be created where the DF builds CmII and CmC files and "pushes" them up to the CF  
15 using SSH2 and SFTP. The specifics about file formats, file naming conventions, and file granularity (how often a  
16 new file is started) can be taken directly from ATIS-100021. Push buffering generally requires less storage space  
17 outside of the CF; it is recommended that transmission of intercept files be specifiable with a range of time values,  
18 with a maximum of at least 15 minutes, and with a range of size values, with a maximum of at least 10 MB. With  
19 push buffering, having a separate hash file per intercept file (rather than the log file) is preferable, but one should  
20 use at least the strength of hash specified in ATIS-1000021 (SHA-256).

---

<sup>8</sup> See ATIS-1000021-2007 Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment. < <http://www.atis.org> >

---

## APPENDIX C. Optional Messages (Informative)

### C.1 Optional Surveillance Status Messages

The following optional messages as defined in Annex C.1 of ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20] are also defined for usage of WiMAX LAES at the option of the WiMAX-SP:

- Service Change
- Virtual Private Network (VPN) Security Association Establishment
- Virtual Private Network (VPN) Security Association Release
- Surveillance Activation
- Surveillance Continuation
- Surveillance Change
- Surveillance Deactivation.

If the Surveillance Continuation message is used as a heartbeat, AND if no packets were detected for the duration of the summary timer, then the Packet Data Summary Report shall not be sent.

If the Surveillance Continuation message is not used as a heartbeat mechanism, then null Packet Data Summary Reports shall be sent at the expiration of the Summary Timer.

### C.2 WiMAX CmlI Optional Messages Abstract Syntax Module

```
WiMAX-LAES-CmlI-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) optional-cmii(1) version-3(2)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
IMPORTS
ServiceChange,
SurveillanceActivation,
SurveillanceContinuation,
SurveillanceChange,
SurveillanceDeActivation
FROM IAS-LAES-CmlI-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii-optional(2) version-2(1)};
wimax-LAES-CmlI-Optional-Messages-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) optional-cmii(1) version-3(2)}
wimax-CmlI-Optional-Protocol-Identifier OBJECT IDENTIFIER ::=
{wimax-LAES-CmlI-Optional-Messages-Abstract-Syntax-Module-OID}
WiMAXOptionalProtocol ::= SEQUENCE
{
  wimax-CmlI-Optional-Protocol-Identifier OBJECT IDENTIFIER,
  wimaxOptionalCmlIMessage WiMAXOptionalCmlIMessage
}
```

```
1
2 WiMAXOptionalCmIIMessage ::= CHOICE
3 {
4     serviceChange                [0] ServiceChange,
5     null-1                        [1] NULL,
6     -- [1] reserved by [Ref 16] for vpnSecurityEstablishment --
7     null-2                        [2] NULL,
8     -- [2] reserved by [Ref 16] for vpnSecurityRelease --
9
10    surveillanceActivation         [3] SurveillanceActivation,
11    surveillanceContinuation       [4] SurveillanceContinuation,
12    surveillanceChange             [5] SurveillanceChange,
13    surveillanceDeActivation       [6] SurveillanceDeActivation
14 }
15
16 END -- WiMAX-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
```

---

## 1 **APPENDIX D. Intercepted Communication Content Delivery** 2 **(Normative)**

### 3 **D.1 WiMAX CmC Delivery Format**

4 The ASN.1 in this annex is defined for the delivery of WiMAX CmC to the LEAs.

### 5 **D.2 WiMAX CmCC Abstract Syntax Module**

```
6  
7 WiMAX-LAES-CmCC-Abstract-Syntax-Module  
8 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmcc(2) version-2(1)}  
9  
10 DEFINITIONS IMPLICIT TAGS ::=  
11  
12 BEGIN  
13  
14 IMPORTS  
15  
16 IAS-CC-APDU  
17 FROM IAS-LAES-CmCC-Abstract-Syntax-Module  
18 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmcc(1) version-2(1)};  
19  
20 wimax-LAES-CmCC-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=  
21 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmcc(2) version-2(1)}  
22  
23 wimax-CmCC-Protocol-ID OBJECT IDENTIFIER ::= {wimax-LAES-CmCC-Abstract-Syntax-Module-  
24 OID}  
25  
26 WiMAX-CC-APDU ::= IAS-CC-APDU  
27  
28 END -- WiMAX-LAES-CmCC-Abstract-Syntax-Module
```

## APPENDIX E. Canadian Location Reporting (Normative)

### E.1 Location information reporting

Additional location information reporting beyond the basic capabilities provided in this specification (see section 7.0) may be required to meet Canadian regulator requirements or operator license requirements. A Location\_Update message is defined in this annex to be used in conjunction with the other LAES reporting messages in this specification to report the location of the intercept subject.

The Location\_Update message may be triggered by events such as the following:

- when an event is detectable in the network at an IAP and when location information is reasonably available at an IAP: or
- the mobile terminal is powered up and a connection is made to the wireless network; or
- the mobile terminal is powered down and is disconnected from the wireless network; or
- the mobile terminal is entering a new location area (e.g., normal location update); or
- the mobile terminal periodically provides an update of its location while connecting to the wireless network (e.g., periodic location update); or
- location information is available via location services or presence services; or
- location information is available at a shared Network Access Provider (NAP).

Note that IAP placement and where and when events are detected are implementation dependent.

#### E.1.1 Location\_Update message definition

The Location\_Update message is defined as specified in Table 2.

**Table 4 – Location\_Update Message**

Information Element	MOC	Conditions
CaseIdentity	M	
IAPSystemIdentity	C	Provide when known.
ObservedSubjectIdentities	C	Provide when known.
TimeStamp	M	
Location_Information	M	

#### E.1.2 Location\_Update message information elements definitions

The following information elements are defined for use with the Location\_Update message:

- 1) **Case Identity** – Identifies the case.
- 2) **IAP System Identity** – Identifies the network element containing the IAP.
- 3) **Observed Subject Identities** – Identities of the subject observed at the IAP (e.g., International Mobile Subscriber Identity (IMSI), Mobile Station ID (MSID), Simple Internet Protocol Uniform Resource Locator (SIP URL), User Name)
- 4) **Time Stamp** – Identifies the date and time of the Location\_Update event.
- 5) **Location Information** – Location information associated with the intercept subject. The location information consists of the following information fields:

- 1 a) **Location Type** – The type of the location reported (e.g., “Type = BS ID”, “Type = geo
- 2 coordinates”).
- 3 b) **Location** – The actual location (e.g., “BS ID = 10”).
- 4 c) **Time of Location** – The time the location was recorded if different from the time of the
- 5 Location\_Update event.

### 6 E.1.3 Location\_Message ASN.1

7 Canadian-Messages-Abstract-Syntax-Module

8 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) canadian-cmii(3) version-2(1)}

9  
 10 DEFINITIONS IMPLICIT TAGS ::=

11 BEGIN

12 IMPORTS

13  
 14 CaselIdentity,  
 15 IAPSystemIdentity,  
 16 TimeStamp

17 FROM IAS-LAES-CmII-Abstract-Syntax-Module

18 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2(1)};

19 canadian-messages-OID OBJECT IDENTIFIER ::=

20 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) canadian-cmii(3) version-2(1)}

21 CanadianProtocol ::= SEQUENCE {

22     protocolIdentifier     OBJECT IDENTIFIER (canadian-messages-OID),  
 23     messages               CanadianMessages

24 }

25 CanadianMessages ::= CHOICE {

26     Location-update       [1] Location-Update

27 }

28 -- Message Definitions

29 Location-Update ::= SEQUENCE {

30     caselid                [0] CaselIdentity,  
 31     iAPSystemId           [1] IAPSystemIdentity            OPTIONAL,  
 32     observedSubjectIDs    [2] ObservedSubjectIdentities    OPTIONAL,  
 33     timestamp             [3] TimeStamp,  
 34     location-Information   [4] Location-Information

35 }

36 -- Information Elements Definitions

37 Location-Information ::= SEQUENCE

38 {  
 39     locationType           [0] UTF8String,  
 40     location               [1] UTF8String,  
 41     locationTime          [2] TimeStamp                    OPTIONAL  
 42 }

43 ObservedSubjectIdentities ::= SET OF UTF8String

44 END -- Canadian-Messages-Abstract-Syntax-Module

45

1 **E.2 Delivery over the communications delivery interface**

- 2 Delivery of CmII and CmC should be via a reliable delivery method. The specifics of the method for delivery over  
3 the communication delivery interface are determined by WiMAX-SP and LEA arrangements (See Section 6.3.5).

---

## 1 APPENDIX F. LBS and USI Reporting

2 This annex is normative for Canada and informative for the US.

### 3 F.1 User Perspective

4 Additional event reporting beyond the basic capabilities provided in this specification (see section 6) may be  
5 required to meet Canadian regulator requirements or operator license requirements. A LBS-USI Request message  
6 and a LBS-USI Response message are defined in this annex to be used to report the LBS and USI related events  
7 defined below.

#### 8 9 10 F.1.1 Reporting of Subject Communications for LBS-USI

11 WiMAX has defined capabilities that allow various network elements to communicate information about a subject  
12 using LBS and USI. Such communications between a network element acting on behalf of the subject to an  
13 associate may be required to be intercepted.

##### 14 F.1.1.1 LBS Communications

15 WiMAX LBS capabilities are defined in [28]. The WiMAX-SP shall intercept communications between a LR and  
16 the LS (i.e., LBS Location Requests and Location Responses) associated with an intercept subject or intercept  
17 subject's service under the following circumstances:

- 18 • Reporting of LR to LS communications is required by law or regulation;
- 19 • The data to be reported has not been otherwise reported; and
- 20 • The identity of the LR involved in the communications has not otherwise been reported.

##### 21 F.1.1.2 USI Communications

22 WiMAX USI capabilities are defined in [27]. The WiMAX-SP shall intercept communications between an  
23 ASP/iASP and the USI System (i.e., USI Requests and USI Responses) associated with an intercept subject or  
24 intercept subject's service under the following circumstances:

- 25 • Reporting of ASP/iASP to USI System communications is required by law or regulation;
- 26 • The data to be reported has not been otherwise reported; and
- 27 • The identity of the ASP/iASP involved in the communications has not otherwise been reported.

### 28 29 F.2 Network Perspective

#### 30 31 F.2.1 LBS-USI Request Message

32 The LBS-USI Request Message is used to report requests for LBS or USI application data about a subject or a  
33 subject's service from a LBS Server or USI System. The LBS-USI Request Message shall be triggered when:

- 34 • A WiMAX-SP LBS Server receives a LBS Location Request (as described in [28]) where the user  
35 MS identity in the LBS Location Request is associated with the intercept subject; or
- 36 • A WiMAX-SP USI System receives a USI Request (as described in [27]) message where the Short-  
37 Lived USI Identity (S-ID) or Long-Lived USI Identity (L-ID) in the USI Request is associated with  
38 the intercept subject.

39 The Requestor Identity parameter is used to report the identity of the entity sending the request. It may be  
40 the identity of another user or it may be the identity of another WiMAX-SP or third party application server.  
41 It may or may not be the same as the identity embedded in the LBS Location Request or USI Request that  
42 the WiMAX-SP uses to authenticate the request (see Requesting Party below).

- 1 The Server Identity parameter is used to report the identity of the LBS Server or USI System that received  
 2 the LBS Location Request or USI Request.
- 3 The Request Identity parameter uniquely identifies the request for the Case Identity, Subscriber Identity, and  
 4 IAP System indicated.
- 5 The Requesting Party parameter is used to report the identity of the entity on whose behalf the LBS Location  
 6 Request or USI Request is sent. This is the identity contained in the LBS Location Request or USI Request  
 7 that the WiMAX-SP authenticates prior to providing the LBS Location Response or USI Response. It may  
 8 be the identity of another user or it may be the identity of another WiMAX-SP or third party application  
 9 server.
- 10 The LBS-USI Application parameter is used to report the type of USI or LBS application to which the  
 11 request pertains (e.g., USI Location Update, USI E-Payment Authorization, LBS Location Request). Where  
 12 the USI application is one defined in [27], the value reported should be the name of the service as used in  
 13 [27].
- 14 The Encapsulated Request Message parameter is used to report the request message sent from the Location  
 15 Requestor to the LBS Server or from the ASP/iASP to the USI System.

16 **Table 5 – LBS-USI Request Message Parameters**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Requestor Identity	M	
Server Identity	M	
Request Identity	M	
Requesting Party	C	Provide when reporting of CmC is authorized
LBS-USI Application	C	Provide when reporting of CmC is authorized
Encapsulated Request Message	C	Provide when reporting of CmC is authorized

17

18 **F.2.2 LBS-USI Response Message**

19 The LBS-USI Response Message is used to report responses to requests for LBS or USI application data about a  
 20 subject or a subject's service from a LBS Server or USI System. The LBS-USI Response Message shall be  
 21 triggered when:

- 22 • A WiMAX-SP LBS Server sends a LBS Location Response (as described in [28]) where the LBS  
 23 Location Response was prompted by an earlier LBS Location Request associated with the intercept  
 24 subject's MS; or
- 25 • A WiMAX-SP USI System sends a USI Response (as described in [27]) where the Short-Lived USI  
 26 Identity (S-ID) or Long-Lived USI Identity (L-ID) in the USI Response is associated with the  
 27 intercept subject.

28 The Requestor Identity parameter is used to report the identity of the entity to which the response is sent. It  
 29 may be the identity of another user or it may be the identity of another WiMAX-SP or third party application  
 30 server. It may or may not be the same as the requestor identity embedded in the LBS Location Request or  
 31 USI Request that prompted the response.

32 The Server Identity parameter is used to report the identity of the LBS Server or USI System that sent the  
 33 LBS Location Response or USI Response.

1 The Request Identity parameter identifies the request that prompted the response and is identical to the  
 2 Request Identity reported for that request (see section F.2.1). If the request that prompted the response was  
 3 not reported (e.g., because the LBS-USI Request event occurred prior to the start of the intercept) then the  
 4 Request Identity uniquely identifies the response for the Case Identity, Subscriber Identity, and IAP System  
 5 indicated.

6 The LBS-USI Application parameter is used to report the type of USI or LBS application to which the  
 7 request pertains (e.g., USI Location Update, USI E-Payment Authorization, LBS Location Request). Where  
 8 the USI application is one defined in [27], the value reported should be the name of the service as used in  
 9 [27].

10 The Encapsulated Response Message parameter is used to report the response message sent from the LBS  
 11 Server to the Location Requestor or from the USI System to the ASP/iASP.

12 **Table 6 – LBS-USI Response Message Parameters**

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
Requestor Identity	M	
Server Identity	M	
Request Identity	M	
LBS-USI Application	C	Provide when reporting of CmC is authorized
Encapsulated Response Message	C	Provide when reporting of CmC is authorized

13

### 14 **F.3 LBS-USI ASN.1**

15 LBS-USI-Abstract-Syntax-Module

16 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) lbs-usi(5) version-1(0)}

17

18 DEFINITIONS IMPLICIT TAGS ::=

19

20 BEGIN

21

22 IMPORTS

23

24 CaseIdentity,

25 IAPSystemIdentity,

26 Location,

27 ProtocolSignal

28 SubscriberIdentity,

29 TimeStamp,

30 Value

31 FROM IAS-LAES-CmII-Abstract-Syntax-Module

32 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2(1)};

33

34 lbs-usi-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=

35 {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) lbs-usi(5) version-1(0)}

36

37 lbs-Usi-Protocol-Identifier OBJECT IDENTIFIER ::= {lbs-usi-Abstract-Syntax-Module-OID}

38

39 LBS-USI-Protocol ::= SEQUENCE

40 {

```
1     lbs-usi--Protocol-Identifier    OBJECT IDENTIFIER,
2     lbs-usiMessage                 LBS-USIMessage
3 }
4
5 LBS-USIMessage ::= CHOICE {
6     lbs-usi-Request                [0] LBS-USI-Request,
7     lbs-usi-Response               [1] LBS-USI-Response
8 }
9
10 -- LBS-USI Message Definitions
11
12 LBS-USI-Request ::= SEQUENCE
13 {
14     caseld                          [0] CaselIdentity,
15     iAPSystemId                     [1] IAPSystemIdentity,
16     timestamp                       [2] TimeStamp,
17     subscriberIdentity              [3] SubscriberIdentity,
18     requestorIdentity              [4] Value,
19     serverIdentity                  [5] Value,
20     requestIdIdentity               [6] INTEGER,
21     requestingParty                 [7] Value,
22     lbs-usiApplication              [8] Value OPTIONAL,
23     encapsulatedRequestMessage     [9] ProtocolSignal OPTIONAL,
24     ...
25 }
26
27 LBS-USI-Response ::= SEQUENCE
28 {
29     caseld                          [0] CaselIdentity,
30     iAPSystemId                     [1] IAPSystemIdentity,
31     timestamp                       [2] TimeStamp,
32     subscriberIdentity              [3] SubscriberIdentity,
33     requestorIdentity              [4] Value,
34     serverIdentity                  [5] Value,
35     requestIdIdentity               [6] INTEGER,
36     lbs-usiApplication              [7] Value OPTIONAL,
37     encapsulatedRequestMessage     [8] ProtocolSignal OPTIONAL
38     ...
39 }
40
41 END -- LBS-USI-Abstract-Syntax-Module
42
43
```