ATIS-1000031

IMPLEMENTATION GUIDELINES FOR ATIS-1000013.2007, *LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE (LAES) FOR INTERNET ACCESS AND SERVICES*

TECHNICAL REPORT

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 250 companies actively formulate standards in ATIS' 18 Committees, covering issues including: IPTV, Service Oriented Networks, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, and Billing and Operational Support. In addition, numerous Incubators, Focus and Exploratory Groups address emerging industry priorities including "Green", IP Downloadable Security, Next Generation Carrier Interconnect, IPv6 and Convergence.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, please visit < http://www.atis.org >.

ATIS-1000031, *Implementation Guidelines for ATIS-1000013.2007, Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*

Is an ATIS Standard developed by the **Lawfully Authorized Electronic Surveillance (LAES)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000031

Technical Report on

Implementation Guidelines for ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*

Alliance for Telecommunications Industry Solutions

Approved February 2010

Abstract

This document provides guidance intended to assist implementers of ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*.

FOREWORD

The information contained in this Foreword is not part of this Technical Report. As such, this Foreword may contain material that has not been subjected to public review or a consensus process.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) – formerly T1S1 – develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

This document is entitled *Implementation Guidelines for ATIS-1000013.2007, Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*. This document is the result of work by members of the Packet Technologies and Systems Committee (PTSC), working within the PTSC Lawfully Authorized Electronic Surveillance Subcommittee. This document provides guidance intended to assist implementers of ATIS-1000013.2007 and ATIS-1000013.a.2009.

Future control of this document will reside with PTSC. This control of additions to the document, such as ongoing protocol evolution, new applications, and operational requirements, will permit compatibility among U. S. networks. Such additions will be incorporated in an orderly manner with due consideration to the International Telecommunications Union – Telecommunications Standardization Sector (ITU-T) layered model principles, conventions, and functional boundaries.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, PTSC, which is responsible for the development of this Standard, had the following members:

M. Dolly, PTSC Chair
V. Shaikh, PTSC Vice-Chair
T. Jacobson, PTSC Technical Editor
C. Underkoffler, ATIS Chief Editor

Organization Represented	Name of Representative
Alcatel-Lucent	Ken Biholar Stuart Goldman (Alt).
AT&T	George Stanek Will Chorley (Alt)
Cisco Systems	Rajiv Kapoor Mike Hammer (Alt)
Department of Defense	Chris Fitzgerald Ryan Kuseski (Alt)
Embarq Corporation	Amar Ray Bill Wiley (Alt)
Ericsson Incorporated	George Foti Asok Chatterjee (Alt)
ETI Connect	Mark Uldahl David Cooke(Alt)
FBI ESTS	Janet Butkus Marybeth Paglino (Alt)
Huawei Technologies	Rouzbeh Farhoumand Spencer Dawkins (Alt)

Organization Represented	Name of Representative
IP Fabrics	Glen Myers Kevin Graves (Alt)
MetaSwitch	Duncan Archer Chris Mairs (Alt)
National Communications Systems	Nicholas Andre An Nguyen (Alt)
NeuStar	Karen Mulberry
Nokia Siemens Networks	David Francisco Nagaraja Rao (Alt)
Nortel	James McEachern Ronald Ryan (Alt)
Pen-Link, Ltd.	Mark Chapin
PSEP Canada	Liem Nguyen Sean Pope (Alt)
Qwest	Steve Showell Andrew White (Alt)
Research In Motion	Atul Asthana
Sprint	Mark Lipford Grez Schumacher (Alt)

Organization Represented	Name of Representative
Telcordia Technologies	Wesley Downum Cliff Halevi (Alt)
Tellabs Operations	Eric Geelen Mark Jones (Alt)
Tridea Works	Selvan Rengasami Ken Coon (Alt)

Organization Represented	Name of Representative
US Department of Commerce	Arthur Webster
Verint Systems Inc	Todd McDermott Greg Krebs (Alt)
Verizon Communications	Mark Desterdick David Wang (Alt)

The Lawfully Authorized Electronic Surveillance (LAES) Subcommittee was responsible for the development of this document.

TABLE OF CONTENTS

Technical Report on

Implementation Guidelines for ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*

1 SCOPE, PURPOSE, & APPLICATION

1.1 Scope

This Technical Report (TR) provides implementation guidelines for ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services* [Ref 1], and for ATIS-1000013.a.2009, *Supplement A to ATIS-1000013.2007* [Ref 2].

1.2 Purpose

The implementation guidelines in this TR are intended to assist manufacturers, product developers, and service providers in developing ATIS-1000013.2007-based lawful intercept solutions.

1.3 Application

These implementation guidelines provide additional information to assist in the use of the ATIS-1000013.2007 Standard and associated supplement(s).

The implementation guidelines identified in this TR are not intended to be considered a "safe harbor standard" under the Communications Assistance for Law Enforcement Act (CALEA) -- i.e., it is not necessary to conform to the guidelines in this TR for "safe harbor" purposes, nor does this TR change or provide additional requirements for users of the ATIS-1000013.2007 Standard and associated supplement(s). Any requirements or standards terminology (i.e., "shall," "should", etc.) are used strictly in the context of ensuring that this TR is inherently sound and provides appropriate guidance.

2 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Technical Report are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] ATIS-1000013.2007, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services*, 2007.[1]

[Ref 2] ATIS-1000013.a.2009, *Supplement A to ATIS-1000013.2007*, January 2009[1].

[1] This document is available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. < http://www.atis.org >

[Ref 3] IETF RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*, February 2006.[2]

[Ref 4] IETF RFC 4664, *Framework for Layer 2 Virtual Private Networks (L2VPNs)*, September 2006.[2]

[Ref 5] ATIS-1000021, *Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment*, October 2007.[1]

[Ref 6] IETF RFC 4301, *Security Architecture for the Internet Protocol*, December 2005.[2]

[Ref 7] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008.[2]

[Ref 8] IETF RFC 2131, *Dynamic Host Configuration Protocol*, March 1997. [2]

[Ref 9] IETF RFC 1533, *DHCP Options and BOOTP Vendor Extensions*, October 1993. [2]

[Ref 10] IETF RFC 3046, *DHCP Relay Agent Information Option*, January 2001. [2]

[Ref 11] IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*, June 2000. [2]

[Ref 12] IETF RFC 2866, *RADIUS Accounting*, June 2000. [2]

3 ACRONYMS & ABBREVIATIONS

AACmII	Access Associated Communication Identifying Information
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CACmII	Content Associated Communication Identifying Information
CALEA	Communications Assistance for Law Enforcement Act
CmC	Communication Content
CmII	Communication-Identifying Information
DHCP	Dynamic Host Configuration Protocol
IAP	Intercept Access Point
IAS	Internet Access and Services
IASP	Internet Access or Services Provider
ISP	Internet Service Provider
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LI	Lawful Intercept
MAC	Media Access Control
MPLS	Multi-Protocol Label Switching
PVC	Permanent Virtual Circuit
RADIUS	Remote Authentication Dial In User Service
TLS	Transport Layer Security
VPN	Virtual Private Network

[2] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

4 OVERVIEW OF ATIS-100013.2007

The focus of ATIS-1000013.2007 is on lawfully authorized electronic surveillance (LAES) for the portion of the network that facilitates subscriber access to the Public IP network. Subscribers may obtain Internet Access and Services (IAS) from a provider that uses owned, leased, or re-sold facilities. IAS transport methods include xDSL, cable, Wi-Fi, and WiMAX.

The IAS surveillance model provides a framework within which the lawful intercept (LI) capabilities can be analyzed. The IAS model represents a number of cases where an intercept subject has, gains, or is granted access to physical facilities provided by the Access Network (e.g., fixed DSL) and the subject uses those physical facilities to invoke and utilize services provided by a service provider. IAS services may be provided by the Access Network provider or a third party service provider (e.g., ISP). In gaining access to IAS services, the subject (or equipment, like a PC) may be required to register for service. This registration for service may occur in the Access Network Domain, the ISP Domain, or both Domains. In some cases (e.g., fixed DSL), no registration for service may be required in the Access Network Domain as the service is fixed or pre-defined and associated with the subject.

For IAS, physical (e.g., bandwidth) and logical (e.g., IP address) resources may be dynamically allocated to the intercept subject's device. In IAS, dynamic allocation of resources may occur in both the Access Network Domain (e.g., assign physical facilities) and the ISP Domain (e.g., assign logical session).

5 IMPLEMENTATION GUIDELINES

The following are implementation guidelines for ATIS-100013.2007.

5.1 Dynamic IP Addresses Management

This section applies to implementations where packets are isolated for interception based on dynamic IP addresses. In this case, it is essential to ensure that a dynamic IP address is assigned to the intercept subject so that only the intercept subject's communications are captured. When using this isolation method, implementations may need to detect assignments and releases of dynamic IP addresses to the intercept subject.

Clauses 5.1.1 and 5.1.2 provide some implementation guidelines for detecting assignments and releases of dynamic IP addresses using DHCP [Ref 8] and RADIUS [Ref 11], [Ref 12].

5.1.1 Dynamic IP Address Assignment by DHCP

When DHCP is used in the network to assign dynamic IP addresses, one approach for detecting assignment and release is to have the DHCP server(s) notify the CmC IAPs of assignments and releases of IP addresses. The DHCP server(s) would also be reporting the assignments and releases of dynamic IP addresses as AACmII. Interfaces for doing this are beyond the scope of this Implementation Guide.

Another approach uses observation of DHCP packets on the network. Dynamic IP address assignment to an intercept subject whose identifier is something other than an IP address (e.g., MAC address, DHCP option 61 [Ref 9], DHCP option 82 [Ref 10]) can be done by a state machine that examines

DHCPDISCOVER, DHCPREQUEST, and DHCPACK packets on the network. Explicit releases of IP addresses by an intercept subject can be detected by monitoring for DHCPRELEASE packets.

Implicit releases of IP addresses can also occur, the most-common example being the expiration of the lease time period assigned to the dynamic IP address by a DHCP server. In such cases, there is nothing directly observable on the network because the subscriber is assumed to obey the lease-expiration time originally given by the DHCP server in the DHCPACK packet, and the DHCP server assumes it is free to reassign this IP address to a different subscriber. There are at least two ways of implementing this:

1. The IAP has a state machine that tracks the lease time for each assigned dynamic IP address. If the lease time of an IP address of an intercept subject expires, the IAP assumes that the IP address is no longer associated with the intercept subject and ceases intercepting packets identified by this IP address.
2. The IAP monitors the network for DHCPOFFER or DHCPACK packets (as it does above for IP address assignment), and if it detects an IP address that is currently being used to identify packets of an intercept subject being reassigned to a different subscriber, it ceases intercepting packets identified by this IP address.

To handle the case when an intercept starts after a dynamic IP address(es) has been assigned to the intercept subject, a mechanism should exist to communicate the currently assigned IP address(es) to the appropriate IAP(s).

5.1.2 Dynamic IP Address Assignment Controlled by RADIUS

When RADIUS is used in the network to control assignment of dynamic IP addresses, one approach for detecting the assignment and release is to have the RADIUS server(s) notify the CmC IAPs of assignments and releases of dynamic IP addresses. The RADIUS server(s) would also be reporting the assignments and releases of dynamic IP addresses as AACmII. Interfaces for doing this are beyond the scope of this Implementation Guide.

Another approach uses observation of RADIUS packets on the network. In this approach, the following events need to be detected:

1. An identifier of an intercept subject appears in a RADIUS Access-Attempt message, and the corresponding Access-Accept message contains a Framed-IP-Address attribute. This is an assignment of a dynamic IP address to the intercept subject.
2. An IP address currently associated with an intercept subject appears in a Framed-IP-Address attribute in a RADIUS Access-Accept message, and the corresponding Access-Attempt message did not have an identifier of this intercept subject. This should be treated as a release of the dynamic IP address from the intercept subject.
3. A RADIUS Accounting-Start or Interim-Update message has a Framed-IP-Address attribute and an identifier of an intercept subject. This is an assignment of a dynamic IP address to an intercept subject.
4. A RADIUS Accounting-Stop message has a Framed-IP-Address attribute and an identifier of an intercept subject. This is a release of the dynamic IP address from the intercept subject.
5. An IP address currently associated with an intercept subject appears in a Framed-IP-Address attribute in a RADIUS Accounting-Start or Interim-Update message, with an identifier of a subscriber other than the intercept subject. This should be treated as a release of the IP address from the intercept subject.

Cases 2 and 5 above are similar to the implicit-release situation of DHCP discussed earlier, where there is nothing directly observable on the network about the release.

To handle the case when an intercept starts after a dynamic IP address(es) has been assigned to the intercept subject, a mechanism should exist to communicate the currently assigned IP address(es) to the appropriate IAP(s).

5.2 Case Identity

Because the systems on the receiving end of the 'e' interface sometimes use the case identity as a file or directory name, case identity should be limited to the following characters: alphanumeric; hyphen (-); underscore (_); and period (.).

Note that the case identity is assigned by the LEA with coordination between the LEA and the IASP.

5.3 Security and Integrity

Mechanisms for meeting the Security and Integrity requirements of [Ref 1] and [Ref 2] include the following:

- Private leased lines with appropriate bandwidth;
- Frame relay and ATM PVCs with appropriate bandwidth;
- BGP/MPLS IP provider provisioned Virtual Private Network (VPN) with appropriate bandwidth [Ref 3];
- Layer 2 provider provisioned VPNs with appropriate bandwidth [Ref 4];
- The buffering mechanism described in ATIS-1000021 [Ref 5];
- IPsec security protocols (i.e., from the DF to the CF) [Ref 6]; and
- Transport Layer Security (TLS) [Ref 7].

NOTE: One or more of these mechanisms may be used to provide security and integrity. Other mechanisms that are based upon standard protocols may also be used. The IASP and the LEA need to negotiate and agree on the mechanism(s) to be used.

5.4 Location Information

Location information in the access messages and packet-data messages is intended to provide information about the subject's current location when reasonably available and when lawfully authorized. When not lawfully authorized, the optional Location field in the messages should be omitted. When lawfully authorized but unknown (i.e., location is unknown or not reasonably available), the location-type subfield in the ASN.1 Location should be set to the string value "Unknown".

5.5 Access Signaling Message Report

Although the Access Signaling Message Report may be used in lieu of the other access messages, it is preferable to the LEA to generate the access messages when possible. The Access Signaling Message Report may also be used to supplement the access messages by reporting access-related information that does not map to the other access messages.

5.6 Handling of Tunneled Packets

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

5.7 Redundant CACmII Reporting

When the lawful authorization includes CmC, the content packets including the IP packet headers are delivered to the LEA, and the information contained in CACmII (i.e., the Packet Data Header Reports and Packet Data Summary Reports) is redundant. In this case, it is recommended not to deliver CACmII.