ATIS-1000013.v2.2015(R2020)

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000013.v2.2015(R2020), *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2*

Is an American National 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-1000013.v2.2015(R2020)

[Revision and Consolidation of ATIS-1000013.2007 and ATIS-1000013.a.2009]

American National Standard for Telecommunications

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services, Version 2

Alliance for Telecommunications Industry Solutions

Approved July 21, 2015

American National Standards Institute, Inc.

Abstract

Internet Access and Services can be obtained by establishing a subscription based arrangement. This standard provides capabilities to lawfully intercept communications of subscription-based Internet Access and Services arrangements.

NOTE - Annex A, *ASN.1 Definitions*, of this Standard has also been formatted as a separate plain text file and electronically packaged with this standard.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

This document is entitled *Lawfully Authorized Electronic Surveillance for Internet Access and Services*. This standard is the result of work by members of the Alliance for Telecommunications Industry Solutions (ATIS) Packet Technologies and Systems Committee (PTSC), working within the PTSC Lawfully Authorized Electronic Surveillance (LAES) Subcommittee. This standard defines the interfaces between an Internet Access or Services Provider and a Law Enforcement Agency to assist the Law Enforcement Agency in conducting lawfully authorized electronic surveillance for Internet Access and Services.

This version of the standard provides clarifications, corrections, and enhancements to ATIS-1000013.2007, and adds an informative annex on *Byte Count Reporting in an Internet Access and Services LAES Environment*.

It is not the intent of this document to imply or impact any pending regulatory decisions related to Internet Access and Services. This document provides the mechanisms to perform lawfully authorized electronic surveillance of Internet Access and Services subject to the appropriate legal and regulatory environment.

Future control of this document will reside with ATIS PTSC. This control of additions to the specification, 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 ITU-T layered model principles, conventions, and functional boundaries.

> **NOTE - A buffering solution for use with this standard is addressed in ATIS-1000021, *Technical Report on Data Buffering (Short Term Storage) in an LAES Environment*.**

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

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communication Sciences)

G. Myers, PTSC LAES Chair (Counter Link)

N. Rao, PTSC LAES Vice-Chair (Nokia Networks)

The **LAES** Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard for Telecommunications –

Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services

1 Introduction

1.1 Background

This Standard defines the interfaces between a service provider that facilitates subscriber access to the Internet and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for subscription-based Internet Access and Services (IAS) arrangements. This Standard is provided for purposes of a "safe harbor" as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [Ref 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 telecommunication support services shall be found in compliance with Section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103."[1] [Ref 2, 3, 14, 15].

As used in this Standard, electronic surveillance refers to the interception and delivery of communications for a particular IAS subscriber as lawfully authorized. The said communications may include Communication Identifying Information (CmII) with or without the Communication Content (CmC).

In this Standard, an intercept subject, or more simply a subject, is an IAS subscriber 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 or subject-related identifiers used by the Internet Access or Services Provider's (IASP) equipment, facility, or communication service – e.g., network address, terminal identity, subscription identity.

As a precondition for an IASP's assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve an IASP 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 an IASP, the IASP 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.

1.2 Scope & Purpose

The focus of LAES for IAS is on the network(s) that provide subscriber connectivity to the Internet. IAS may be provided by a set of independent or related entities – e.g., a Digital Subscriber Line (DSL) provider, cable provider, Wireless Fidelity (Wi-Fi®) provider, or a WiMAX®[2] provider and an Internet Service Provider (ISP). This document does not address mobile IP capabilities as defined by the Internet Engineering Task Force (IETF).

---

[1] 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] For fixed/nomadic wireless (e.g., as a wireline access alternative).