ATIS STANDARD

ATIS-1000069

ATIS Standard on -

Error and Exception Reporting in a Lawfully Authorized Electronic Surveillance (LAES) Environment

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.

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-1000069

ATIS Standard on

Error and Exception Reporting in a Lawfully Authorized Electronic Surveillance (LAES) Environment

Alliance for Telecommunications Industry Solutions

Approved November 16, 2018

Abstract

Current lawful intercept (LI) standards provide no means for the notification of conditions that may impact the quality, completeness, and continuation of an intercept. This specification provides an optional capability for reporting these conditions to the law enforcement collection function.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) 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.

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. The word may denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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 (Vencore Labs)
> G. Myers, PTSC LAES Chair and Technical Editor (Counter Link)
> N. Rao, PTSC LAES Vice Chair (Nokia)
> L. Mitchell, Technical Editor

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

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Lawful Intercept Error and Exception Reporting

1   Background, Scope, Purpose, & Application

1.1 Background & Scope

Current lawful intercept (LI) standards provide no means for the notification of conditions that may impact the quality, completeness, and continuation of an intercept. These conditions could be temporary or permanent errors, exceptions, and anomalies. This standard provides an optional capability for reporting these conditions to the law enforcement collection function.

This standard can be used optionally as a means of reporting certain conditions encountered during an intercept. Because messages defined in this standard have a unique object identifier, this standard can be used in conjunction with any other lawful intercept standard. How this standard is used, if at all, is determined by the service provider and by the LEA agreement.

This provides a specification for *Error and Exception Reporting in an LAES Environment*, should interested parties voluntarily choose to implement such functionality. It is not intended to be considered a "safe harbor standard" under the Communications Assistance for Law Enforcement Act (CALEA).

Any requirements or standards language (i.e., "shall," "should") is used strictly in the context of ensuring that this document is inherently sound and provides appropriate guidance to implementers.

1.2 Purpose

This standard is provided as means for conveying information that might affect the quality, completeness, and continuation of an intercept because of exceptional conditions, such as errors.

1.3 Application

The capabilities described in this standard are intended to be used for reporting errors, exceptions, and anomalies to law enforcement that might affect an ongoing interception. The reporting mechanism herein is open-ended to allow conditions specific to a service provider or specific to a particular intercept or intercept standard to be communicated. This can be considered a subset of OA&M reporting capabilities.

2   Normative References

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

> [Ref 1] ATIS-1000678.v3.2015, Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 3.[1]

> [Ref 2] RFC 4880, OpenPGP Message Format.[2]

---

[1]   This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=28232 >.

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

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Acronyms & Abbreviations

ASN.1	Abstract Syntax Notation One
ATIS	Alliance for Telecommunications Industry Solutions
CALEA	Communications Assistance for Law Enforcement Act
CC	Call Content
CF	Collection Function
CII	Call Identifying Information
DF	Delivery Function
dod	Department of Defense (United States)
IAP	Intercept Access Point
ID	Identity
IP	Internet Protocol
iso	International Standards Organization
LAES	Lawfully Authorized Electronic Surveillance
LI	Lawful Intercept
POC	Point of Contact
PTSC	Packet Technology Systems Committee
RM	Report Message

4 Lawful Intercept Error & Exception Reporting

Current LI standards specify an interface between the functions in the service provider network and the functions in the law enforcement domain. In most ATIS LI standards, this interface is known as the 'e' interface. For instance, in ATIS-1000678 [Ref 1], three types of LI information pass over the 'e' interface: call identifying information (CII), call content (CC), and certain optional messages.

4.1 Functional Model

In the model shown in Figure 4.1, the last entity in the service provider domain is the delivery function (DF), which delivers LAES information over the 'e' interface to the collection function (CF). What has been missing up to this point is a capability for the DF to report to the CF conditions that may be interfering with the intercepts. This standard fulfills that need by allowing an open-ended set of conditions to be reported over the same 'e' interface or via the Out-of-Band notification.
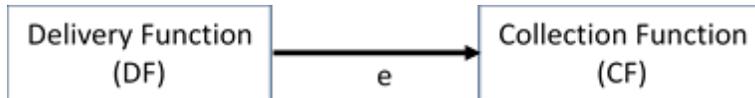
Figure 4.1 - DF to CF Interface

The conditions to be reported are completely up to the service provider. Only for the purposes of illustration, the following is an incomplete list of example conditions that, when known, might be reported:

- A connection to a CF had been broken.
- A connection to an Intercept Access Point (IAP) went down.
- A keep-alive signal from an IAP disappeared.
- The DF or an IAP did a system reset.
- An error condition was reported by an IAP.
- In a voice intercept, the call content stopped being available.
- In a voice intercept, only one side of the audio is available.
- Certain unexpected conditions or states have occurred.
- An Internet Protocol (IP) address being used for a data intercept is discovered to be allocated to a different subscriber.
- A certain number of LAES messages have been lost.
- Certain implementation limits have been exceeded (e.g., number of concurrent call legs per intercept subject, number of IP addresses per intercept subject, number of media streams per call).

4.2 Error & Exception Reporting over a Separate Interface

This section describes the reporting of outages/restoral of the e interface via a separate means, which may be an automated or human source.

4.3 Out-of-Band Notification

When an LI service outage is detected, the Service Provider (SP) shall notify the LEA expeditiously by sending an out-of-band notification. Additional messages with updated information may also be sent. When the service is restored, a second out-of-band message shall be sent for service restoral. If ATIS-1000069 Report Message (RM) is implemented, an RM may be sent to the CF over the 'e' interface in lieu of the second out-of-band message with details of the error/outage condition.

Out-of-band methods are a phone call or email. The LEA contact information (e.g., phone number, email address) is provided in conjunction with the lawful authorization.

In the case of email, the email shall be secured. The manner of securing the email is up to the service provider. For instance, OpenPGP [Ref 2] is a widely used method that provides confidentiality and authentication.

No details of the LI information pertaining to the actual interception shall be passed insecurely. The notification shall contain minimum necessary information (e.g., IP and port, based upon operator policy or something mutually agreed during the setup of the LI) to identify the affected 'e' interface.

The following is an example of a notification message that has a minimum set of information:

1. **Essential details:**
   a. The Point of Contact (POC) at the LEA this message is intended for.
   b. The exact date and time when the outage started.
   c. The agreed upon identification of the interception, (unique name agreed during the LI setup).

         i.   example: X-123456789

2. **The expected duration:**
   a. can be an estimated time to repair.
   b. can be unknown.
3. **Reason ("The Why"):**
   a. Why is this happening?
4. **Closing:**
   a. Give a contact number and the POC at the service provider to contact.

5 Reporting Capabilities

Reporting occurs whenever the DF determines that a situation or condition should be reported to the CF. This clause describes the reporting messages.

5.1 Report Message Requirements

Each message contains the unique object ID specific to this standard. This allows the CF to treat these messages separately and unambiguously from the LI messages that might otherwise be received.

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

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

Note that although optional and conditional parameters are considered to be OPTIONAL syntactically in the Abstract Syntax Notation One (ASN.1) syntax, the inclusion requirements in this clause take precedence over the ASN.1 definitions.

6 Error & Exception Messages

The Report message is the only message defined in this standard.

6.1 Lawful Intercept Error & Exception Reporting Messages

Table 6.1 – Report Message

Parameter	MOC	Description
Report type	M	The report can be an event, a condition, a notice, or other. Generally, an event is a one-time occurrence (although it may repeat itself). A condition is something with persistence, and something that can presumably have a beginning and an end. A notice is a notification about something to happen in the future.
Timestamp	M	This is the date and time of this report. The timestamp is reported to at least the thousandth of a second and shall report either coordinated universal time or local time with the local time differential from coordinated universal time.
Summary	M	This is text summarizing the condition being reported. The text is completely implementation dependent but should be usable for display to a human operator of the CF.
Details	O	If further, more detailed information is available about the condition, it may be placed in this textual parameter.

SystemID	O	If the condition is associated with a specific system or network element whose identity is known, an identifier of that may be placed in this parameter. In the case of an IAP, this would contain the IAP system identifier.
CaseIdentity	O	If the condition is associated with a specific case, the identifier of that case may be placed in this parameter.

7   Implementation Perspective

The Stage 3 description for LAES Error and Exception Reporting messages is defined in the form of ASN.1 in this clause.
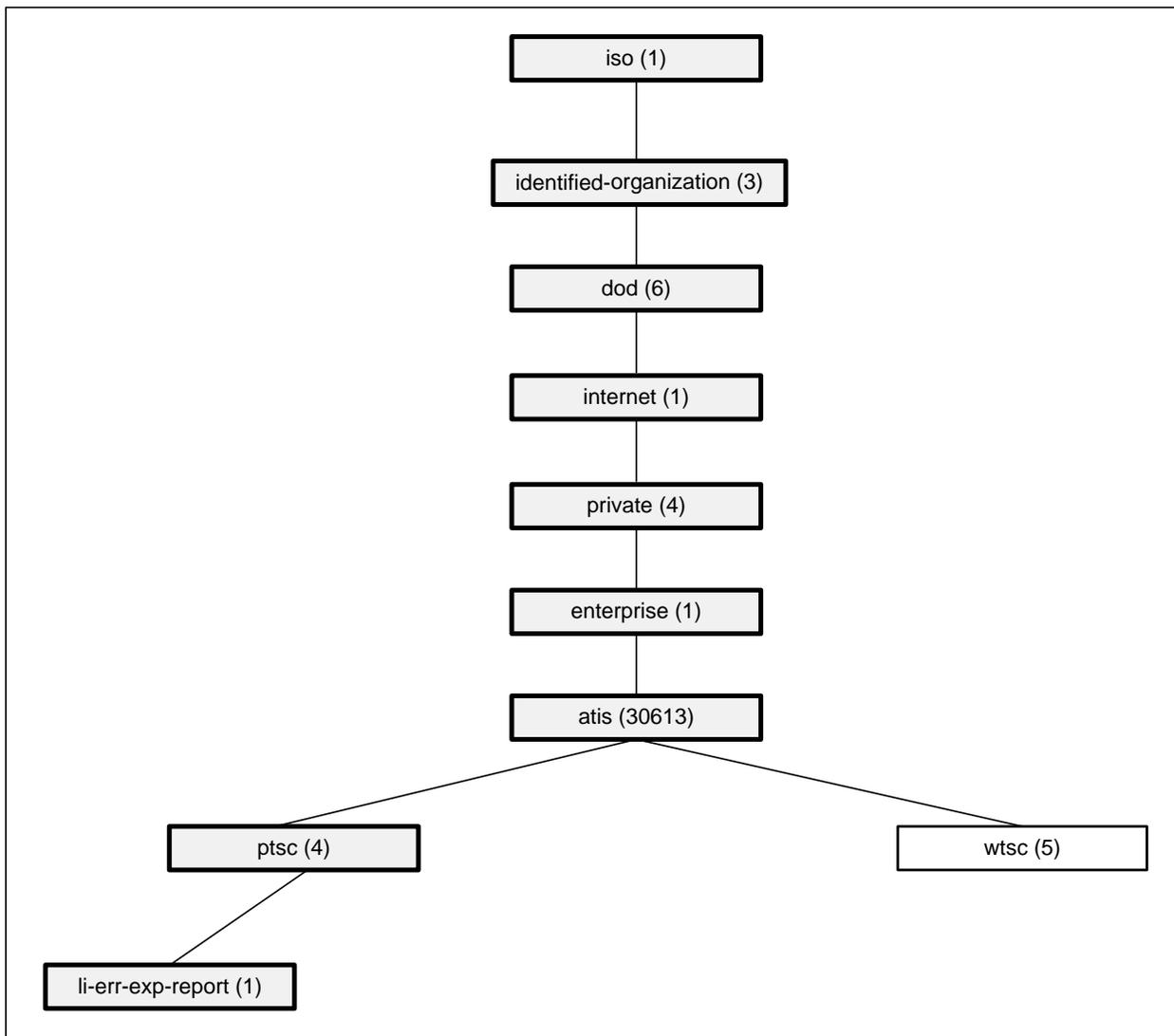
7.1 *Object Identifier Tree*

Figure 7.1 - Object Identifier Tree

7.2   Abstract Syntax Error & Exception Reporting Module

```
EREP-LAES-Abstract-Syntax-Module

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atis(30613)
ptsc(4) li-err-exp-report(1) version-1(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

eREP-LAES-OID OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6) internet(1)
private(4) enterprise(1) atis(30613) ptsc(4) li-err-exp-report(1) version-1(1)}


GenProtocol ::= SEQUENCE {
      eREP-LAES-OID        [0]    OBJECT IDENTIFIER,
      genMessage           [1]    GenMessage
}


GenMessage ::= CHOICE {
      reportMessage        [0]    ReportMessage,

      …

}


ReportMessage ::= SEQUENCE {
      reportType           [0]    ReportType,
      timestamp            [1]    GeneralizedTime,
      summary              [2]    VisibleString,
      details              [3]    VisibleString        OPTIONAL,
      systemId             [4]    VisibleString        OPTIONAL,
      caseIdentity         [5]    VisibleString        OPTIONAL,
      …
}


ReportType ::= ENUMERATED {
      event         (0),
      condition     (1),
      notice        (2),
      other         (3),

      …

}

END
```