ATIS-1000075

ATIS Standard on -

Cloud Services Impacts on Lawful Interception Study

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 and major U.S. contributor to 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.

Published by

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

ATIS-1000075

ATIS Standard on

Cloud Services Impacts on Lawful Interception Study

Alliance for Telecommunications Industry Solutions

Approved December 16, 2016

Abstract

This document is the result of a study of lawful interception (LI) of certain cloud services. This is a joint study among ATIS' PTSC LAES and WTSC LI.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers.

This study shall be a joint effort among Packet Technologies and Systems Committee (PTSC) Lawfully Authorized Electronic Surveillance (LAES) subcommittee and Wireless Technologies and Systems Committee (WTSC) Lawful Intercept (LI) subcommittee to ensure that all stakeholders can exercise appropriate influence on its development. The PTSC LAES is the assigned subcommittee responsible for coordinating the joint effort with WTSC LI to develop this document.

PTSC LAES develops and recommends standards, technical requirements, and technical reports related to LAES of packet-mode technologies in a wireline environment. PTSC LAES is a subcommittee of PTSC, which 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.

WTSC LI develops, maintains, amends, and enhances American National Standards and other ATIS deliverables related to lawful intercept within the Global System for Mobile Communications (GSM) family. WTSC LI is a subcommittee of WTSC, which develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

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 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 Communications Sciences)

G. Myers, PTSC LAES Chair (Counter Link)

N. Rao, PTSC LAES Vice Chair (Nokia)

The PTSC LAES Subcommittee was responsible for coordinating the joint effort with WTSC LI and developing this document.

Table of Contents

Table of Figures

ATIS Standard on –

Cloud Services Impacts on Lawful Interception Study

1 Scope, Purpose, & Application

1.1 Scope

This document is the result of a study of lawful interception (LI) of certain cloud services. This is a joint study among the ATIS Packet Technologies and Systems Committee (PTSC) Lawfully Authorized Electronic Surveillance (LAES) subcommittee, Wireless Technologies and Systems Committee (WTSC) Lawful Intercept (LI) subcommittee, and the Cloud Services Forum (CSF).

For the purposes of this study, a cloud service is a service that is available to a person with access to the public Internet or that is implemented atop cloud-computing resources. Thus such services are usually independent of access networks, where LI has often been focused.

Also, for the purposes of this study, the set of cloud services is restricted to a subset with the following attributes:

- The principal users of the service are people.
- The users have identities defined and known by the cloud service.
- A principal function of the cloud service is communication or the sharing of private information among specific users.
- The cloud service is potentially subject to a lawful intercept.

To differentiate the providers of this type of cloud service from other services upon which they might be built, the term “user service provider (USP)” is used herein to mean the provider of those cloud services fitting the above attributes.

This document is a technical study of interception of cloud services. Purposely, legal matters, implications, and questions are excluded. Also, any findings that result from this study are not intended to imply that the topic of lawful interception of cloud services falls under specific laws of any country, such as the U.S. Communications Assistance for Law Enforcement Act (CALEA) statute.

1.2 Purpose

The purpose of this study is to identify and analyze:

- The challenges, impacts, and obstacles of meeting LI requirements for cloud services.
- The extent to which existing ATIS LI standards meet these requirements.
- The deltas that may exist between existing and needed LI capabilities.
- What new work may be required to achieve a fuller set of LI capabilities.

1.3 Application

The findings that result from this study will provide appropriate guidance to ATIS committees for use in their standards development work to enable lawful interception of cloud services.

2 Informative References

The following standards or organizations are provided for informative purposes. They address related or similar areas to the ATIS Cloud Study. At the time of publication, the editions indicated were valid. All standards are subject to revision.

[678] ATIS-1000678.v3, *LAES for Voice over Packet Technologies in Wireline Telecommunications Networks*, Version 3.[1]

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

[005] ATIS-0700005, *Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services*; ATIS-0700005-2010a, *Supplement A for Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services.*[3]

[025-B] J-STD-025-B, *Lawfully Authorized Electronic Surveillance*.[4]

[500-292] NIST Special Publication 500-292, *NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology*, September 2011.[5]

[800-145] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, September 2011.[5]

[042] ATIS-1000042, *Support for Lawfully Authorized Electronic Surveillance (LAES) of Advanced Voice over Packet (VoP) Conferencing*.[6]

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

3.1.1 Intercept Access Point (IAP): A point within a service-provider's network where information is intercepted.

3.1.2 "X" as a Service (XaaS) Provider: A provider of the "X" service. For instance, Infrastructure as a Service (IaaS) denotes infrastructure as a service.

3.1.3 User Service Provider (USP): A cloud service provider whose principal users are people who are potentially subject to a lawful interception.

3.1.4 Intercept Subject: A subscriber of a service whose communications have been authorized by a legal authority such as a court to be intercepted and delivered to a Law Enforcement Agency.

3.2 Acronyms & Abbreviations

API	Application Program Interface
ATIS	Alliance for Telecommunications Industry Solutions
CALEA	Communications Assistance for Law Enforcement Act

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

[2] Available at: < https://www.atis.org/docstore/product.aspx?id=22665 >.

[3] Available at: < https://www.atis.org/docstore/product.aspx?id=22706 >.

[4] Available at: < https://www.atis.org/docstore/product.aspx?id=26133 >.

[5] This document is available from the National Institute of Standards and Technology (NIST) at: < https://www.nist.gov/ >.

[6] Available at: < https://www.atis.org/docstore/product.aspx?id=26149 >.

CC	Communications Content
CII	Communications Identifying Information
CSF	Cloud Services Forum
CSP	Cloud Service Provider
DF	Delivery Function
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IAP	Intercept Access Point
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LI	Lawful Interception
LTE	Long Term Evolution
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
NaaS	Network as a Service
NAT	Network Address Translation
OTT	Over the Top
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
PaaS	Platform as a Service
RTP	Real-time Transport Protocol
SaaS	Software as a Service
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TSP	Telecommunications Service Provider
TTP	Trusted Third Party
URI	Uniform Resource Identifier
USP	User Service Provider

VoIP	Voice over Internet Protocol
XaaS	“X” as a Service
XaaSP	“X” as a Service Provider
WTSC	Wireless Technologies and Systems Committee

4 Introduction

As discussed in the Scope clause, this technical study paints a picture of where LI technology must move in order to cope with the rise of cloud services. Also as explained in the Scope, the discussions are limited to those where the principal users are people or organizations of people, where the users have some form of identity, and where the specific cloud service is one where rational people can agree that there is a reasonable likelihood that a request from a law enforcement agency for an intercept (e.g., court order) could be issued for the communications of a user of that cloud service

4.1 Cloud-Based Communications

The term “communications” has both obvious and non-obvious forms. From a cloud perspective, services with “obvious” communications are:

- Voice communications (e.g., “over the top” Voice over Internet Protocol [VoIP]).
- Voice with video communications.
- Online conferencing (which can include many types of communications – voice, video, chat, shared screens, document sharing).
- Email.
- File sharing.
- Social networking (e.g., in Facebook, there many different forms of communications).

A few examples of less-obvious communications, which also fall within the scope of this study, are:

- Inter-player communications in massive multiplayer online games.
- Interaction in virtual worlds.
- Blogs.
- Online store usage (e.g., “If I order this, it signals this”, wish lists).

These services don’t require communications between multiple defined users or organizations. For instance, a common way to hide communications among people with email is to give everyone the same user ID and hide the communications in never-to-be-sent messages in the drafts folder. One could also envision a need to intercept the traffic between a customer and his online bank.

There are two subjects that this study purposely avoids as much as possible. One is the oft-used “XYZ as a service” when discussed as part of the cloud. The rationale is that these are just broad categories that don’t give us much insight into LI needs. It is reasonable to expect that “infrastructure as a service” and “platform as a service,” as commonly used, describe services that are quite unlikely to have LI needs. For other categories, such as “communications as a service” and “storage as a service,” there may be services within them to which LI needs likely apply, but it is more useful to identify such services individually (with the recognition that the list will grow over time.)

The other subject avoided as much as possible is the law. This study is a technical study and does not take into account current law, what future laws might be, or what future laws should be. Thus this study has three goals:

1. Identify specific cloud services for which there is reasonable likelihood that a lawful authorization for an interception of a user's communications could be issued.
2. Where possible, identify how existing LI standards could apply to those services, including how they might need to be extended.
3. Identify the need for new standards or even completely different approaches to interception of cloud services.

Section 5 provides a service-independent overview of the relationships among the cloud service users, the access paths (e.g., Broadband cable supplier, Long Term Evolution [LTE] provider, Wi-Fi provider), and the cloud services with which that user is interacting.

Section 6 looks at the manner in which intelligence is distributed in an LI solution and suggests some approaches that could differ significantly from today's LI standards.

Section 7 dissects a couple of case studies in detail, looking at specific LI capabilities needed for those specific services.

Section 8 contains a European Telecommunications Standards Institute (ETSI) Comparison.

Section 9 provides the conclusion.

Please note that the document herein is not a "layman's" document; it uses terminology from the networking and LI environments and assumes the reader has a basic understanding of both.

4.2 Cloud Services & Law Enforcement General Expectations

Cloud implementations of telecommunication services have the potential of complicating lawful interception . Whatever services had LI requirements before continue to do so if they are implemented over a cloud service, such as IaaS, Platform as a service (PaaS), Software as a service (SaaS), Network as a Service (NaaS), etc., in effect over any "cloudified" (XaaS) layer. Existing LI obligations for these services do not change if they are partially or fully implemented in a Cloud.

Because Cloud implementations have the potential to affect LI solutions, existing intercept standards may still be relevant and useful, but gaps may appear. To assist in defining these gaps, this document describes which LI solutions may be impacted as services are implemented fully or partially in a Cloud.

Service Providers fully or partially implement services that currently require a LI solution. The following is a list of LI requirements that are fulfilled by Service Providers to accommodate LI solutions in a traditional network environment. In a Cloud environment these same requirements are applicable. The Cloud environment must consider how these LI obligations are fulfilled.

a. **<u>Authentication and Isolation</u>:** The Service Provider shall ensure that only communications associated with the intercept subject's, if reasonably available, are intercepted and delivered to the Law Enforcement Agency (LEA). The Service Provider shall ensure that the captured communication originates from or is directed to the intercept subject's if reasonably available.

b. **<u>Proportionality</u>:** The Service Provider shall ensure that only authorized communications are intercepted.

c. **<u>Completeness</u>:** The Service Provider shall ensure that all of the intercept subject's messages and communications, both to and from the intercept subject's if reasonably available, shall be intercepted for the entire period authorized by the intercept order.

d. **<u>Performance:</u>** The Service Provider shall be capable of provisioning multiple simultaneous intercepts per intercept subject, for multiple intercept subjects. The Service Provider shall be capable of delivering intercept information to three (3) LEAs simultaneously per intercept subject per service.

e. **<u>Invisibility/Undetectability</u>:** The Service Provider shall perform interception in such a manner that the intercept subject or the intercept subject's terminal equipment cannot detect that the intercept is being performed. The interception shall be undetectable to all non-authorized persons (i.e., employees, subscribers, other LEAs). If a particular offered cloud-based service uses resources offered by a different provider, then the interception shall remain undetectable to that different provider. LI activation and invocation shall remain undetectable to the users, and among all involved service providers.

f. Confidentiality/Access Control: Only authorized persons shall have access to or knowledge of an intercept, intercept capabilities, intercept-related equipment, and intercept communications and data in the service provider's network.

g. Correlation: The Service Provider shall ensure the interception is accomplished in a way that can associate the communication-identifying information with the communication to which it pertains.

h. Availability and Reliability: The Service Provider shall use appropriate performance and reliability mechanisms and parameters to enable the intercept to be performed in a manner that eliminates the likelihood that the intercept will be corrupted.

i. Timestamps: The Service Provider shall use a timestamp of an accuracy of at least 200 ms relative to the detection of the event at the Intercept Access Point (IAP) and a precision of at least 1 ms. The timestamp shall report coordinated universal time or local time with the local time differential from coordinated universal time.

j. Location: When authorized, the location information of the intercept subject shall be reported. If there are multiple forms of location information in the network, all shall be reported if available.

k. Non-Repudiation: The Service Provider shall securely keep and retain sufficient records of service subscriptions to document that the intercepted communications were associated with the intercept subject's, if reasonably available.

l. Encoding/Encryption/Compression: If the Service Provider provides or controls encoding, compression, and/or encryption for the intercept subject or at least is knowledgeable of this processing, the service provider must either transmit the communication content in a decoded, decompressed and/or decrypted form, or provide the information (e.g., encoding method, compression method, encryption keys) needed by the LEA collection system to reverse this processing and obtain the clear form of the communications. It is law enforcement's preference that the communications be delivered in a decoded, uncompressed, and/or decrypted form. This preference is greater if proprietary or specialized encoding, compression, and/or encryption had been used. If the Service Provider transmits the communication content toward the LEA collection system in an encoded, compressed, and/or encrypted form and the encoding, compression, and/or encryption is proprietary, the Service Provider needs to make the proprietary algorithms available to Law Enforcement. Licensing of proprietary algorithms is beyond the scope of this document and would be handled between Law Enforcement and the licensor.

m. Non-Alteration of Communication Content: The Service Provider shall ensure against alteration of communication content. The Service Provider must not intentionally alter communication content (other than what is necessary based on the requirement concerning encoding/encryption/compression) unless otherwise lawfully authorized.

n. Real-Time Access: The Service Provider shall have the ability to deliver in real-time the intercept subject's communications upon transmission to or from the intercept subject's equipment, facility, or service if reasonably available.

o. Control of geography: To adhere to laws pertaining to jurisdiction, the Intercept Access Points need to be in the same jurisdiction as the court order.

5 Overview of LI Implications on Cloud-Based Services

5.1 Challenge

Unlike classic telecommunications services for which LI solutions were developed in the past, cloud-based services bring new challenges to the horizon. To name a few:

- Device perspective: Users may access the services from a variety of devices: computer, tablet, mobile smart phone, or other devices such Kindle®[7], ROKU®[8], IPTV®[9], etc.

[7] Kindle is a registered trademark of Amazon.com, Inc.

[8] ROKU, is a registered trademark of Roku, Inc. .

[9] IPTV is a registered trademark of Cisco Systems.

- Access perspective: Users may access cloud-based services via a variety of access networks: home internet access – cable or DSL, enterprise LAN, school, hotel rooms; WiFi Hot Spots – shopping malls, airports; Mobile access – HSPA, LTE, etc.
- Location perspective: Users may access the service at different locations: home, shopping mall, train, bus, airplane, another country, etc.
- Protocol perspective: Different protocols may be used in providing/granting the service to the users: Session Initiation Protocol (SIP), Extensible Markup Language (XML), Hypertext Transfer Protocol (HTTP), or Diameter, RADIUS, etc.
- Service perspective: Users may access a variety of cloud-based services: playing online games, chat during a game, watching a video stream, downloading a book, web-based conferencing, web-based chat which may include text, audio, or video, etc.

In some situations, LI may only apply to a Telecommunications Service Provider (TSP) that leases the infrastructure; for example, from a cloud service provider.

For simplicity of argument, the cloud can be divided into two layers, as illustrated in Figure 5.1. The top layer is the User Service Provider (USP), the entity that owns the subscriber relationship, and the bottom is the XaaS Provider (XaaSP), which provides the cloud service to the USP. A Cloud Service Provider (CSP) can be one of many varieties of XaaSP. The USP can provision any number of services on the XaaSP infrastructure, such as telecom, email, or a number of LI modules. The XaaSP is contracted by the USP to physically instantiate the services that the top layer sells to individual users.

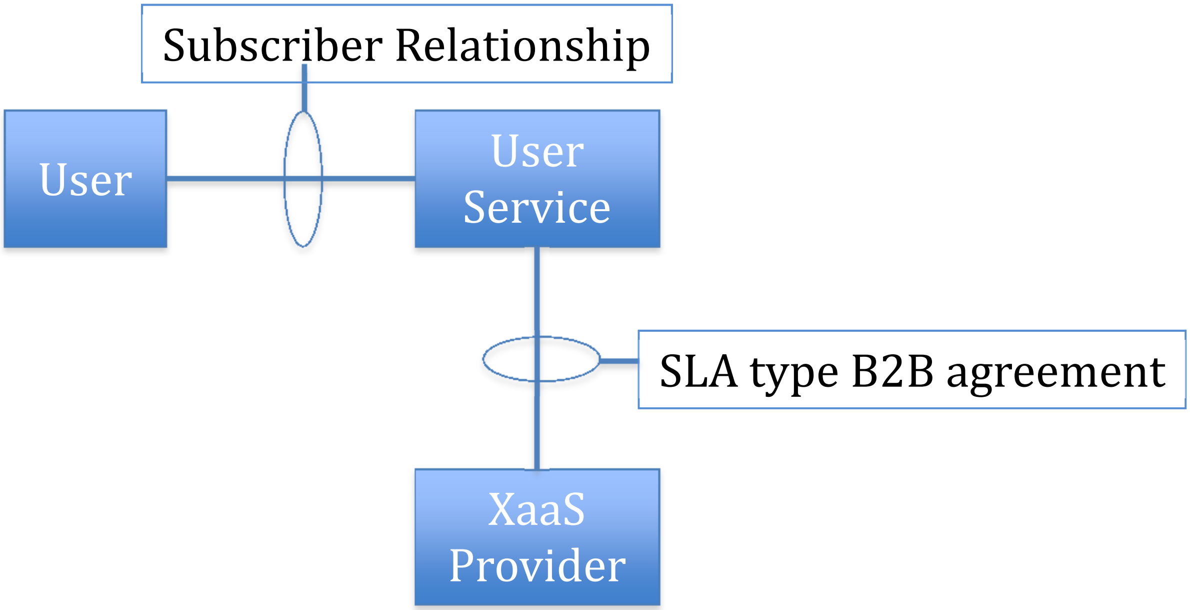


Figure 5.1 – Representation of two layer division within a cloud environment

In cloud language, the services are referred to as “Something as a Service”. For example, they can be:

- Communication as a Service (CaaS)
- Data as a Service (DaaS)
- Infrastructure as a Service (IaaS)
- Network as a Service (NaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Virtual Desktop as a Service (VaaS), etc.

.

5.2 Intercept Subject

In a non-cloud environment, an Intercept Subject is identified in a number of ways, for example:

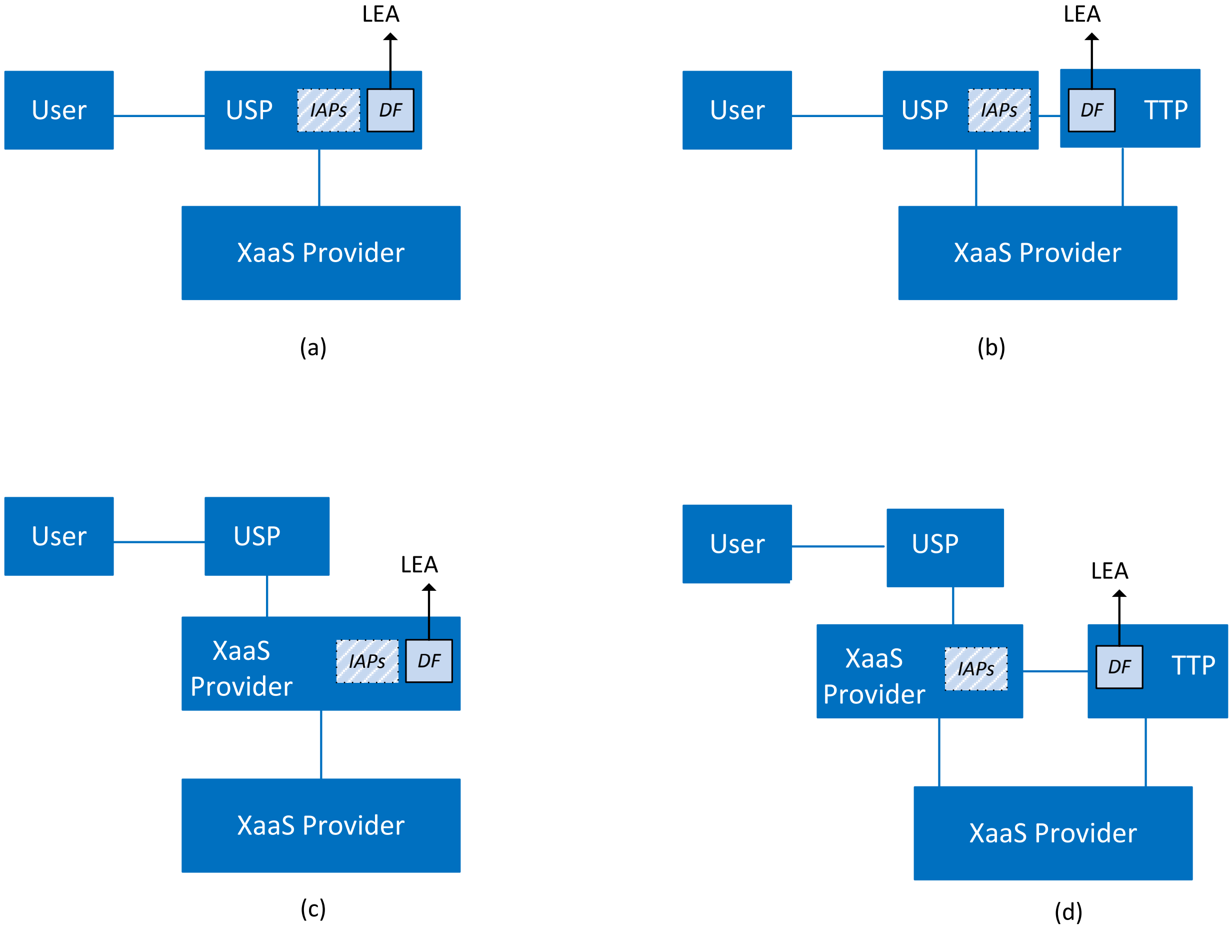
- Telephone Number.
- SIP/TEL Uniform Resource Identifier (URI).
- Media Access Control (MAC) Address, International Mobile Station Equipment Identity (IMEI).
- International Mobile Subscriber Identity (IMSI).
- Static IP Address.

For some LI cases, even a network resource may be identified as the Intercept Subject (e.g., Conference URI).

In a cloud environment, an Intercept Subject may have to be identified for lawful interception purposes through the identities used by the Intercept Subject to log in to the cloud-based service. In most situations, this could be a user ID. In some situations, it can also be the telephone number or SIP/TEL URI or even the IP address.

5.3 Distribution of LI Implementation

In a cloud environment, there is no single manner in which LI capability is provided, and in fact what is sometimes necessary is the involvement of multiple parties. This will be illustrated with four diagrams in the following Figure 5.2.



(a)

(b)

(c)

(d)

Figure 5.2 – Distribution of LI Implementation

In each of these figures, the USP is the provider of a cloud service to some user that is the potential target of a lawful intercept. The USP is therefore the entity responsible for the execution of a lawful intercept.

In Figure 5.2(a), the USP carries out the lawful intercept entirely on its own. The Delivery Function (DF) box represents the delivery function (of the interception to a law enforcement collection function). Note that in this situation there are three basic ways of implementing the interception:

1. The USP can implement, entirely in its application, the LI capability.
2. The USP can attach certain interfaces within itself to probes, and the probes implement the LI capability. Note that in a virtual environment, this requires some type of "virtual tap". These points are denoted as IAPs (intercept access points).
3. The USP can implement, in its application, proprietary LI interfaces and Application Program Interface (API) which are attached to an LI mediation system within the USP. These interfaces and API are also denoted as IAPs.

Any and all information about the presence of the intercept, the intercept's configuration data, and the actual intercepted information for a subject shall not be accessible to any provider or agent not lawfully authorized to participate in this interception and/or delivery.

In Figure 5.2(b), the USP uses a separate cloud service to provide at least part of the LI function. The most common situation is the service of a Trusted Third Party (TTP). In this model, the DF is shown within the TTP. The TTP needs interfaces into the USP (to the IAPs), and these can be of types 2 and 3 above (i.e., passive probe interfaces or active mediation APIs and interfaces).

In Figure 5.2(b), the TTP service is most likely running in the same XaaS environment as the USP. The exact relationship of their two networks is implementation and XaaS dependent. For instance, the USP and TSP could be running in the same virtual private network, or they could have special connections between their two separate networks, sometimes called peering connections.

Figure 5.2(c) shows the situation where the XaaS provider serving the USP is providing a higher-level service. For instance, this XaaS provider may be providing a VoIP switching and media service, where this USP and perhaps other USPs are providing end VoIP services to individual subscribers. For generality two levels of XaaS providers are shown, where the top one is providing service to the USP (e.g., communications as a service) and the bottom one is providing service to this one (e.g., infrastructure as a service).

In this situation, the higher-level XaaS provider may need to provide most or all of the LI functionality. For instance, in the example where this XaaS is providing VoIP capabilities, it is conceivable that this XaaS might need to provide *all* of the LI functionality. In fact, LI functions might be part of the business agreement between XaaS and USP. Since the USP is still the party responsible for lawful interception orders on its subscribers, the USP needs some means to "trigger" these LI services. There are several ways in which this might be provided. For instance, the XaaS provider might define an API or user interface through which the USP can automatically invoke the LI functionality. Alternatively, the invocation of the LI functionality might require human interaction between the two companies.

Note that the three approaches outlined earlier for LI implementation now apply to the XaaS provider. For instance, it might embody the LI functions within its application, use passive probes, or use an API and interfaces to a mediation system. But in all cases, the actual delivery of the interception to law enforcement is carried out by the XaaS provider as a service to the USP.

Figure 5.2(d) adds the independent LI service provider, typically a TTP, to the previous case, making three organizations or companies involved in the intercept. Here, the LI service is provided to the USP by the TTP, and thus the TTP has automated or manual interfaces from the USP to invoke an intercept. The TTP carries out the intercept via interfaces to the XaaS provider (again, probe-type or mediation-system-type interfaces).

6 Approaches to Interception of Cloud Services

6.1 Overview

The principal type of intercept today is voice – a legacy Public Switched Telephone Network (PSTN) or VoIP phone call. A phone call has well-defined properties that can be clearly expressed in an LI handover standard (e.g., [025-B], [678]). A phone call has the act of calling and answering, a caller and callee, an audio media stream, dialed-digit signaling, and other properties. Thus it is a relatively straightforward to define an LI handover standard.

For instance, Figure 6.1 below illustrates LI interception of a cloud-based VoIP service. Attached somehow to the VoIP service is intercept logic, and this logic drives the delivery function, which sends VoIP-specific information to the collection function. The Communications Identifying Information (CII) expresses specific information relative to the voice service, such as the Origination, Answer, and Bye messages in [678], and clearly identifies the calling and called parties, etc. For a content intercept, the Communications Content (CC) format is specific to this type of (voice) service.

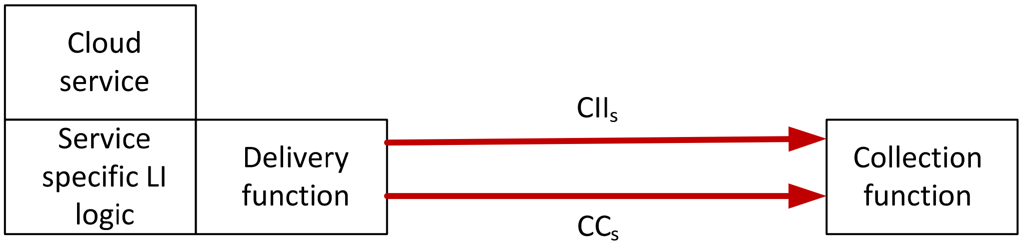


Figure 6.1 – LI interception of a cloud-based VoIP service

In this type of approach, all of the heavy lifting is done on the left side, and the collection system has little more to do than store the intercept information and display and replay it. This is considered the traditional service-specific approach.

The problem with this approach is that the handover interface (the LI standard) is specific to the service (voice calls in this case). It doesn't cover the myriad ways that people can communicate using cloud services, e.g., messaging, email, social networking, online meetings, bulletin boards, blogs, file sharing, photo sharing, multiplayer games, presence, etc. Trying to develop service-specific LI standards for each of these services is very difficult because, unlike the well-standardized public telephone service, each service provider's rendition of a particular service can be quite different than that of another service provider.

6.2 Approaches

In the search for different strategies that could be used for cloud services, three different approaches are explored below.

6.2.1 The Black-Box Approach

An alternative approach is shown in the next diagram. Here the handover uses a generic LI interface with communications identifying information and content labeled C_{bb}. C_{bb} is part of a new "black box" LI standard. Messages in this standard contain a few standardized elements, such as case identity and time stamp, but the rest of the message cannot be interpreted out of context.

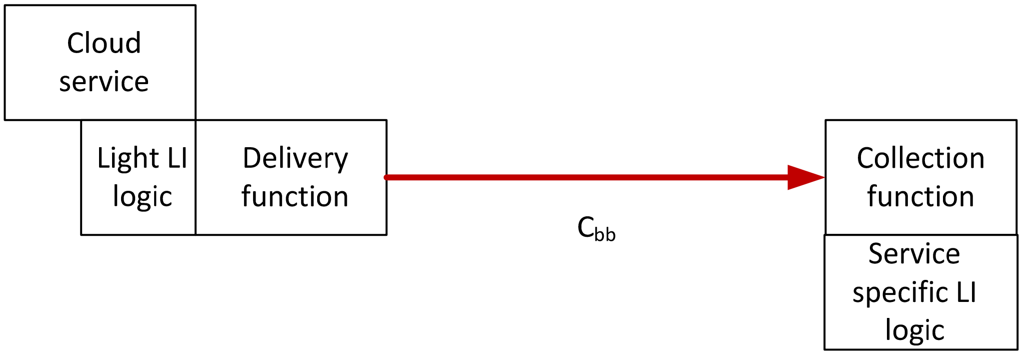


Figure 6.2 – The Black-Box Approach

Rather than place the service-specific LI logic on the left, there is just a modest amount of logic that grabs events and traffic relative to an intercept subject. Instead, the service provider provides a module to the collection function that decodes and displays the CII and CC. In many situations, this module can be very similar to the "app" that the service provider provides to its customers. Because the C_{bb} is only known to the service-specific logic, there is no definition at the handover-standard level of CII versus CC, but the distinction would exist (as known to the service-specific LI logic) for the purposes of pen registers when there is no probable cause to warrant receiving content.

To explain further, there is something a bit similar to this that goes on in collection systems today. Many collection systems contain add-on functions for interpreting broadband intercepts. The most common one looks for port 80 HTTP traffic and attempts to recreate the browser session seen by the intercept subject. The dissimilarity is that HTTP traffic to browsers is reasonably standardized so that this can be done independent of the specific web server being browsed.

The collection system still receives, correlates, and records the intercept information, but then it needs to interact with the service-specific LI module provided by the service provider to interpret and display the information (in one way, not unlike how a collection system needs the right codec to play audio for a VoIP call, but on a much grander scale here).

So the above model requires the development of an LI standard with the C_{bb} interface, and then requires each cloud service to develop the "light" logic on the left and the heavy-duty code/display module on the right. The standard would be highly generic, with almost no discernable information without the service-provider's "decoding module"; i.e., the LI message would consist of a case identifier, timestamp (preferably in binary epoch form as discussed in a separate PTSC LAES contribution), service identifier, and then a body as an octet stream. Conventional ways of transport to the collection system still apply (e.g., Transmission Control Protocol [TCP]).

6.2.2 The Metadata & Black-Content Approach

An alternative to the above approach is to leave some CII-related service specific logic on the "left" and leave the CC (content)-related specific logic on the "right". Here we will label the CII as CII_m, where the m denotes metadata. The CII_m standard would be a highly flexible metadata format into which the service provider would map its equivalent of signaling and "pen-register-level" information. Thus a collection system would have a way of interpreting the CII, but it would still need a service-specific module to interpret the CC.

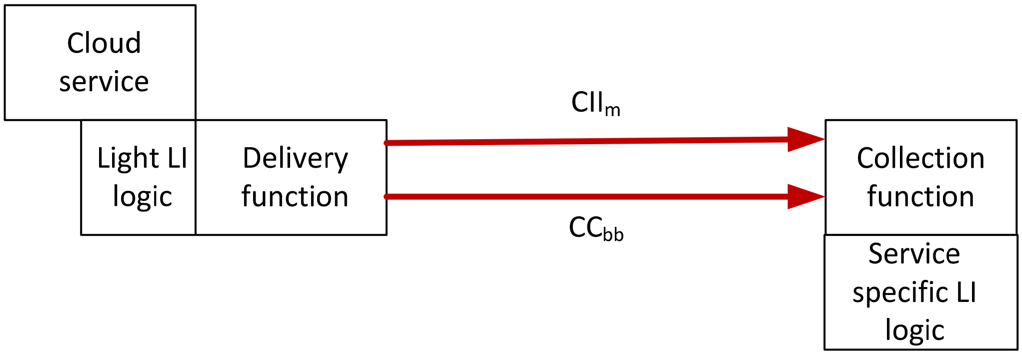


Figure 6.3 – The Metadata & Black-Content Approach

To a certain degree, this approach is not unlike VoIP intercepts, where the CII is spelled out in the standard but the CC is undecipherable unless the appropriate module (in this case, a codec) is obtained. However, this analogy is only a general one, because in a VoIP intercept the CII format is very specific to a voice call, and the majority of codecs are not service specific.

The CII$_m$ metadata needs to be very generic and flexible in order to cover all possible cloud services. Thus the risk in this approach is whether such metadata could be successfully defined. One might have Metadata-Start, Metadata-Update, and Metadata-End messages so that the concept of a session can be described, and within these messages one might expect parameters such as case identifier, timestamp, service identifier, location, initiating party id, contacted party ids, possibly service-specific parameters, and others. The party identifiers would have to be very flexible themselves, because they would have to express a wide range of identifiers, e.g., email addresses, phone numbers, arbitrary textual names, IP addresses, MAC addresses, IMSIs, MEIs, etc. The content message would be similar to the message in the first approach, i.e., black boxes, meaningful only to the service's decode module in the collection system.

6.2.3 The Classes Approach

This alternative is the closest to today's approach. However, rather than developing very narrowly focused standards (e.g., SIP-based VoIP, IMS-based conferencing), standards would be developed for broader classes of communications. Thus there is a set of standards, one per broad class.

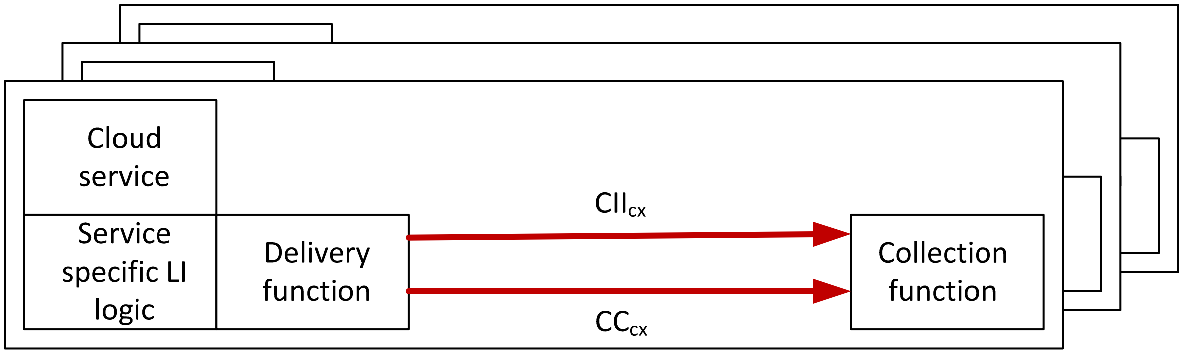


Figure 6.4 – The Classes Approach

As an example, there might be a standard developed for "non-real-time addressed information", meaning communications that have a sender and a set of recipients. Email and the hundreds of forms of instant messaging would fit into this category. CII would include case identity, timestamp, service, sender, recipients, and event. CC would need to cover numerous classes of data, such as textual, Real-time Transport Protocol (RTP), HTTP, Multipurpose Internet Mail Extensions (MIME), and file.

There could be another standard for “non-real-time posted information”, meaning creation or retrieval of stored information. Services falling in this category might include cloud file storage (e.g., Dropbox), Facebook news feeds, Twitter, blogs, and bulletin boards. Events are the obvious things like the creation or posting of information and the retrieval of information.

The challenge of this alternative is similar to that of the second alternative, the Metadata & Black-Content Approach, but magnified – showing that a limited set of standards can cover the majority of cloud services.

7 Case Studies

Case studies of several widely used cloud services are explained in the following sections.

7.1 VoIP as a Cloud Service

7.1.1 Overview

Voice over IP (VoIP) provided as a cloud service is of obvious interest from a Lawful Intercept (LI) perspective. Not only is it a growing replacement for traditional phone service, but also some of the capabilities of VoIP make it a better hiding place. Because these VoIP services operate independently of the access networks, they are often called over-the-top (OTT).

The number of companies providing such services is large, and the services cover a wide range of capabilities. What is covered here is the set of services that are most like traditional phone services.

Some VoIP services are “fully interconnected”, meaning that they can initiate calls to outside networks (e.g., PSTN) and receive calls originating from outside networks. Such VoIP services are subject to CALEA today in the U.S. Most VoIP services that aren’t fully interconnected are interconnected on the outbound side (i.e., can initiate calls to outside networks) but can’t receive calls. However, since this study is independent of CALEA, the above is basically moot.

Some VoIP services are focused more on residential customers, some on business customers, and some on mobile customers. Also note that some of these are what we could call “soft VoIP”, where the user interface is a software application residing in a smartphone, tablet, or PC, and others are “hard VoIP”, where the user interface is a traditional phone, and the service uses a special hardware device to connect to the Internet.

Generally, the same LI considerations apply to both the “soft” and “hard” approaches, although the soft approach is perhaps more interesting because it breaks the usual tie between an intercept subject as a person, and a device. The soft approach generally relies on a softphone application. Sometimes the app is provided by the VoIP provider, but more often the app is not necessarily tied to the VoIP provider but sourced from a third party.

7.1.2 What’s Excluded

A certain number of services have been purposely excluded from this discussion, not that they aren’t of equal interest, but because they warrant separate analysis. These include:

- Voice communications services that depart significantly from the traditional model,
- Services that are principally video-based services,
- Services that are principally messaging atop mobile phones, and
- Services that are principally conferencing.

7.1.3 LI Considerations

7.1.3.1 Ability to Force Route Certain Peer-Peer Calls

Some VoIP implementations, once the call is set up, have the RTP streams go directly between the two parties. This can be done even if the parties are NAT'd. This makes the interception of the call content virtually impossible. Thus the VoIP implementation needs to have the capability of routing certain calls (those subject to a content intercept) to a point in the network containing the appropriate IAP.

In theory this is detectable by an intercept subject, but the likelihood of detection is very small, and the consequences of not doing this are large (not being able to do the intercept). Ultimately, it is the law enforcement agency that needs to make the determination on the routing decisions at intercept-provisioning time.

7.1.3.2 Potential Need for a Significant Number of IAPs & for IAP Interaction

A large VoIP implementation might centralize the SIP processing but decentralize the RTP switching to multiple gateways in multiple geographies. Unless, similar to the point made in section 7.1.3.1 above, the RTP associated with an active intercept subject can be routed to a specific gateway, multiple IAPs will be needed. In this event the SIP processing is likely to be separated from the RTP processing, and thus IAPs associated with the call handling will need the ability to interact with the IAPs associated with the call content.

This interaction among IAPs could motivate a project to develop a standard for such interaction.

7.1.3.3 Ephemeral Phone Numbers

Because the phone number is just a unique identifier, it can be readily changed. In many VoIP services, a subscriber can change his phone number in real time. In the extreme, where an intercept subject was just making outgoing calls, the intercept subject could change his phone number between every call.

This has major implications on how intercepts are provisioned. Obviously, human provisioning based on a phone number is easily defeated. Instead, provisioning might need to be based on something that is more permanent, such as the identity of the subscriber, with then some type of "dynamic triggering" of the current phone number(s).[10]

7.1.3.4 Multiple Phone Numbers

Another consequence of the loss of significance of a phone number is that it is easy for a subscriber to obtain a set of phone numbers instead of one.

The obvious implication is that the ability to provision a case with just a single phone number is insufficient.

7.1.3.5 Filtering of Extraneous Traffic

Depending on the implementation, VoIP systems may generate extraneous traffic that, at the least, would be confusing to the LEA and should be filtered out (e.g., only sent if changed, only sent at provisioned period).

One example is registrations for the purposes of being able to receive incoming calls (and for other purposes, such as 9-1-1). Because a phone number can move from device to device, from hot spot to hot spot, from a wired network to a wireless network, the VoIP system needs to know how to locate the client. This is generally done by having the client "report in" periodically, typically with a SIP REGISTER. In some actual systems, VoIP clients actually report in every few seconds. Currently, strict compliance with [678] requires that each of these be reported. An extension that didn't require each of these to be reported would be of some value.

[10] This can also be defeated, although it takes a bit more work. Many VoIP services provide a free trial period. Thus a target could sign up, make a call, sign up with a different name, make a call, etc.

Another example is that every call on some systems starts with an INVITE, then a 407 Proxy Authenticated Required, then the "real" INVITE, etc. Strict compliance with ATIS-10000678 requires that this be reported as two calls, which is confusing. An extension that removed this requirement would be of use.

7.1.4 Adequacy of Current Standards

ATIS-10000678 [678] fulfills the needs of intercepting cloud-based VoIP.

Cloud-based VoIP often involves multiple media streams (e.g., audio and video), and there are some instances where some but not all of the content streams can be made available. The 678 CCUnavailable message is inadequate for reporting this because CCUnavailable is an "all or nothing" message (i.e., because it is specified as an alternative to a CCOpen, its presence means no content is available and its absence means all content is available). A more general error and exception reporting mechanism over the "e" interface is desirable.

Similarly, because a large VoIP service may have many IAPs to capture RTP, in certain situations some but not all of the RTP might be available and having the means to report this is important.

7.2 Conferencing/Meetings as a Cloud Service

7.2.1 Overview

Cloud-based, or web, conferencing or meeting services are of obvious interest from an LI perspective. There are upward of 100 such services, although the best known are GoToMeeting, WebEx, Lync, and Adobe Connect.[11] The services offer generally the same functions, namely:

- The ability for a subscriber to schedule a meeting and notify (invite) participants. This can be a reservation for a future meeting or a "meet now" request.
- The ability to share (such that all participants can see) a desktop or application. In some services, this can include streaming media.
- The mixing of audio from all (non-muted) participants, with a real-time display of the participants currently speaking (the loudest).
- The ability to show real-time video of some or all participants to some or all other participants.
- The ability for participants to direct text messages during the meeting to all participants or a particular participant.
- The ability to record the entire meeting or parts thereof (e.g., record with video).
- The ability to transfer control of the meeting among participants.

7.2.2 What's Excluded

A certain number of services or extensions have been purposely excluded from this discussion, not that they aren't of equal interest, but because they warrant separate analysis. These include:

- File-sharing capabilities.
- Video communications services that are primarily non-reservation-based or one-to-one (e.g., face-face "phone calls").

7.2.3 LI Considerations

7.2.3.1 Applicability of Current LI Standards

ATIS-1000042 [042] (Support for Lawfully Authorized Electronic Surveillance [LAES] of Advanced Voice over Packet (VoP) Conferencing) is closest to being applicable, but it is insufficient in many significant ways. Most significant is that it provides the means to intercept just an audio stream. Some of the ideas in this standard can be used as a starting point, but the standard itself is completely inadequate as a handover standard for the conferencing services described herein.

[11] Trademarks, respectively, of Citrix, Cisco, Microsoft, and Adobe.

7.2.3.2 Approaches to the Intercept

There are three distinct ways that a conference or meeting can be intercepted for law enforcement:

1. The meeting, or a designated subset of it as specified by the LEA (e.g., exclude video), is intercepted at the point of the service provider, encapsulated into an LI handover standard, and transmitted over the “e” interface in real time.
2. The service provider provides for a “stealth participant” – a participant that is muted and is not identified in any way to any and all other participants. The stealth participant could be an LEA person, an LEA recording system, or both.
3. The service provider provides for surreptitious recording that is later sent to the LEA.

7.2.3.3 Target of the Interception

The provisioning capability of the intercept needs to be flexible enough to allow any of the following to trigger the interception:

1. A subscriber of the service scheduling a meeting.
2. A specific meeting (e.g., intercept is identified by a meeting identifier).
3. A specific participant attending a meeting.

7.2.3.4 Scheduling Information

Similar to that in ATIS-1000042 [042], CII should be created in the event that a subscriber who is the intercept subject schedules a meeting. This would contain the meeting identifier, the scheduled time, and the invited participants.

Even in the approaches where instead of using an LI handover standard for the actual meeting a stealth participant or surreptitious recording is done, this scheduling information would still need to be handed over in advance. In this case, where only the scheduling information is needed, [042] could actually be used as is for this purpose.

7.2.3.5 Intra-Meeting CII

In the approach where an LI standard is being used for the handover, CII should be generated and sent upon certain events occurring. This CII should be such that it can be sent without probable cause and thus used in a pen-register intercept. The events, not necessarily a complete list, are:

1. Meeting has started (and also identifying the participant who has initial control).
2. Meeting has ended.
3. Specific participant has entered or left the meeting.
4. Change of control.
5. Current speaker.
6. To and from identifiers of a text message.

7.2.3.6 Media Interception

There are at least four types of media common in these services:

1. The audio mix.
2. The visual image of the shared desktop or application.
3. Live video of some or all participants.
4. Intra-meeting text/chat content.

Ideally, the LEA would have the ability to opt out of certain information (e.g., opt out of receiving the video images)

7.2.3.7 Distributed IAPs

As is the case for over-the-top VoIP, a large conferencing service might decentralize processing to multiple gateways in multiple geographies, requiring the use of multiple IAPs. Conceivably there might be situations where part of the service logic might be within an enterprise and part in the cloud.

The need for interaction among IAPs could motivate a project to develop a standard for such interaction.

7.2.3.8 Use Case Implications on an LI Standard

If a standard were to be developed to encompass the reporting as described above, a major attribute the standard would need is a high degree of flexibility, because conferencing services differ in the details, and new capabilities are added over time. The competitive nature of these services and the limited or nonexistent need for interoperability among them mean that common service models do not exist.

One set of reporting messages, as noted in section 3.4, is related to scheduling of meetings. The related messages of ATIS-1000042 [042] are a good starting point. Another set of reporting messages, as noted in section 3.5, are for reporting intra-meeting events. These should be defined to be devoid of communications content so that they can be received in a pen-register type of intercept.

Information elements such as meeting identifiers and participant identifiers need to be open-ended. Because specific services may have critical information to report that do not fit a stylized reporting message in a new standard, an open-ended informational message is an important part of such a standard.

Although SIP may be used as some part of the meeting protocol, reporting of SIP is not relevant here.

7.2.3.9 Media Reporting

Reporting the media is more complicated than in existing standards because of the different types of media and because their representations inside the service providers may vary significantly. Although some of the media may or may not be encapsulated in RTP, a media-reporting message containing RTP (as an option) is warranted because RTP payloads can already be defined as audio, video, and text. Because SIP and Session Description Protocol (SDP) is not being captured (and may not in fact exist), some way of defining each RTP payload type used is needed, somewhat along the lines of the CCOpen message in [678]. Rather than containing SDP, it would contain one or more items; something like: “when a media message contains RTP and the RTP payload type is …, then the media is … and codec is …”.

Alternatively, it might be possible to have the media-reporting message contain HTTP, because often everything is delivered over HTTP (e.g., audio and video is RTP over HTTP). If audio and video and text are already separated as implied above, a media reporting message containing HTTP is still necessary to contain the display images denoting the shared desktop or application.

It is also conceivable, particularly when a specific application is used by the participants rather than a web browser, that the media is delivered to the application with a proprietary protocol. To cover this possibility, the media-reporting message needs to be able to contain proprietary protocols. In these cases, the service provider might then provide the LEA with a decoding application.

7.2.3.10 Participant Identities

Commercial conferencing/meeting services generally have identity information for the subscriber to the service, but generally do not know the real identities of meeting participants. Thus it is important to understand that participants have been anonymous or have spoofed identities.

8 Relationship to ETSI TR 101 567

A related study has recently been published by ETSI [101 567]. Its scope is similar to the scope herein, but its treatment of the subject is considerably different, and the reader is encouraged to study both documents.

A major difference of the two reports is in the definition of cloud service. This ATIS report is principally focused on services that are provided to people, principally for the communication of private information, over the public Internet. The ETSI report takes more of a cloud-computing focus, defining a cloud service as one where (1) consumers can provision the computing capabilities, (2) resources are pooled physically and virtually, and (3) capabilities can be elastically provisioned and released. Fundamentally then, this ATIS report treats a cloud service more as a black box where the question of interest is how to intercept communications between users of such service, and the ETSI report is more focused on the "insides" of the services.

Both reports identify a number of challenges in common, such as user identities, physical distribution of services, and location information.

This ATIS report outlines some significantly different potential approaches to interception of cloud services.

There is also a significant difference in the case studies. In this ATIS report, two case studies are presented: phone-call-like voice communications, and conferencing/meeting services. In the ETSI report, the majority of the case studies are consumer file-sharing services, and several others such as telepresence, virtual-machine usage, and distributed applications.

9 Conclusion

Historically, lawful interception has been focused on and placed within the access network, for instance through the cable network to which a residential subscriber is attached, through a commercial Wi-Fi access point to which a user is attached, or through an LTE network to which a phone is connected. Interception of a user of a cloud service changes this model in several fundamental ways:

1. The access network becomes irrelevant, because the user of a cloud service can access that service from a varied and unknown number of access paths.
2. Whereas the architecture of access networks is fairly well understood with a lot of commonality among service providers, cloud services are more like "black boxes" where the architecture and implementation is generally unknown and probably widely varying.
3. Historical identifiers of the subject of an intercept, such as phone number, cable modem MAC address, IMSI, etc. are generally access-network identifiers, where cloud services use different types of identifiers.

The above imply that the traditional way of doing lawful intercept, and perhaps the existing standards for lawful interception, need to be rethought. Considerations along those lines discussed in this report are:

Scope of services
The scope of services is far broader than voice and Internet access. The scope of cloud services pertinent to interception includes online meetings, email, file sharing, social networking, and others.

Distributed implementation
Because of possible layering of services that might exist in a cloud environment (e.g., a VoIP cloud service running atop a VoIP-communications-as-a-service provider running atop an infrastructure-as-a-service provider), the implementation of an LI solution might cross several organizations.

Radical model changes
Because many or most cloud services involve protocols and data formats that are proprietary to the service provider, significantly different approaches to LI and to the structure of handover standards may need to be deployed.

Limitations of current standards
Several case studies show where current LI handover standards can be applied to some cloud services, and how those standards might need to change. However, the bigger challenge is with the services not covered by case studies. This is discussed in more detail below.

Section 7 of this report discusses in more detail the case study of VoIP as a cloud service, and it concludes that the ATIS-1000678 standard [678] serves this application reasonably well, one reason being that ATIS-1000678 is largely implementation independent, that is, it focuses on the handover interface. However, this analysis also shows ways that ATIS-1000678 can be extended to support cloud VoIP environments better.

Another case study is of online conferences and meetings. Here there is another applicable solution – ATIS-1000042 [042] – but it has significant shortcomings. One major shortcoming is that it provides for communications content that is only RTP based, but today's online meetings also include media such as desktop sharing, files, and chat. As a starting point, some ideas are discussed that could be used to extend the capabilities of ATIS-1000042.

Left for future case study is the rest of communications-oriented cloud services – email, social networking, file sharing, intra-application user communications, and more. One might think that the ATIS-1000013 [013] standard might have some role here, because it provides for generic IP packet intercept, but its CII is specific to access networks, and its layer-3 orientation of captured traffic is too crude to convey the semantics of a cloud-service interaction.

9.1 Directions for Further Consideration

The following are offered as opportunities for further consideration:

1. Because voice is likely to continue as a major communications form, ATIS-1000678 [678] could be enhanced further with the observations from section 7.
2. Because online conferences and meetings are important cloud services, ATIS-1000042 [042] could be studied in light of its significant shortcomings, and perhaps a major enhancement could result.
3. Cloud services that could fit into an implementation-independent model should be identified and studied. The foremost example is email. Because by nature email is intended to be conveyed among widely different implementations of email products, it seems better suited to this approach than other types of cloud services.
4. Approaches to handle the widely different and implementation-specific cloud services can be studied in further detail. For instance, section 6 summarizes a variety of approaches, from somewhat different than tradition to wildly different.