

5. Call Content and Reasonably Available Call-Identifying Information Delivery

This section describes the information provided by the PSP Infrastructure Data Delivery Point for LEA(s) for use by the LEA-Provided CALEA Interface. The PSP is required to provide access to the call content and reasonably available call-identifying information for particular intercept subjects.

In cases where circumstances dictate that the call content and the reasonably available call-identifying information associated with a particular subject need to be delivered to more than one LEA simultaneously, as may occur when different LEAs are conducting independent investigations on the same subject, the delivered call content and reasonably available call-identifying information shall be made available to other LEAs as required. In the event that the LEA is conducting investigations on more than one subject, the delivered call content and reasonably available call-identifying information may be combined within the connection to the LEA. In this case, the information is uniquely identified in such a manner that the LEA is able to determine the intercept subject.

A subject's call content and reasonably available call-identifying information is transported to the LEA over a wireline connection via an HTTP shell with included MIME-encoded enclosures for content and vCard-identified reasonably available origin, destination, and, when applicable, termination information. The two types of events to be monitored within an Advanced Messaging System for an intercept subject are outbound messages and inbound messages. Call-identifying information is provided when reasonably available and is synchronized with the call content within the HTTP POST operation.

5.1 Outbound Message

An outbound message occurs when a message is delivered to the PSP radio transmission network from the subscriber's Home Node and contains the following information:

Call-Identifying Message Number is a PSP-generated message identification number that is provided to allow the LEA to coordinate related outbound and inbound messages when the latter is known to be a response to the former by the PSP;

Origin is the number or address of the party initiating the call (e.g., calling party), if reasonably available;

Destination is the radio receiving or transceiving device address to which a call is being made (e.g., called party);

Direction is the transmission path from the intercept subject's PSP Home Node to the intercept subject's radio device or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address and is inferred from the inclusion of the intercept subject's address in *Destination*;

Termination is the alternate address to which a call is being routed, if applicable (e.g., forwarded party);

Date and Time is the date and time of message delivery to the RF Network by the Home Node; and

Call Content is the actual content of the message. This may be an attached MIME-encoded file (e.g., a voice file in the case of voice paging).

5.2 Inbound Message

The Inbound Message occurs when a message is transmitted from a subscriber's radio transceiving device and delivered to the subscriber's Home Node and contains the following information:

Call-Identifying Message Number is a PSP-generated message identification number that is provided to allow the LEA to coordinate related inbound and outbound messages when the latter is known to be a response to the former by the PSP;

Origin is the address of the intercept subject's radio transceiving device sending the message (i.e., the calling party);

Destination is the number or address of the device to which the intercept subject sends a message (i.e., called party);

Direction is the transmission path from the intercept subject's radio transceiving device to the intercept subject's PSP Home Node and is inferred from the inclusion of the intercept subject's address in *Origin*;

Termination is the same as *Destination* and, as such, is not supplied;

Date and Time is the date and time of message delivery to the Home Node by the intercept subject's radio transceiving device; and

Call Content is the actual content of the message. This may be an attached MIME-encoded file (e.g., a voice file in the case of voice paging) or a simple message acknowledgment.

6. Call Content and Reasonably Available Call-Identifying Information Surveillance Service Description

This section describes the service provided by the PSP Infrastructure to deliver call content and reasonably available call-identifying information for a particular intercept subject.

The delivery mechanism specifies that identified call content and reasonably available call-identifying information which shall be expeditiously provided to LEAs (up to a total of five LEAs per intercept subject) in a common format using readily available protocols, wireline transport links, and computing equipment. The description of specific implementations for the PSP Infrastructure Data Delivery Point for LEA(s) is left flexible to handle a multitude of TCP/IP-supporting connectivity solutions. The transporting, capturing, and processing of the delivered call content and reasonably available call-identifying information is the responsibility of the Law Enforcement Administrative Function.

The communications and protocol between the PSP Infrastructure Data Delivery Point for LEA(s) and the LEA-Provided CALEA Interface allow the LEA to receive call content and reasonably available call-identifying information in an expeditious manner, regardless of the location of the intercept subject, and whether or not the subject is within RF coverage of the PSP.

The interface provides access to the messages to and from the intercept subject unobtrusively and transparently. Access to reasonably available call-identifying information and call content does not deny the availability of advanced messaging services to either the intercept subject or the calling party.

APSP shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the PSP and the PSP possesses the information necessary to decrypt the communication.⁸

If the PSP Infrastructure encodes data or voice, then the encoding algorithm will be made available to the LEA, if appropriate. Licensing issues associated with such encoding formats are beyond the scope of this Standard and must be handled between the LEA and the licensor.

If the PSP Infrastructure compresses data or voice, then the compression algorithm will be made available to the LEA, if appropriate. Licensing issues associated with such compression methods are beyond the scope of this Standard and must be handled between the LEA and the licensor.

If the PSP Infrastructure compresses a message using codes or abbreviations, then the PSP Infrastructure will decompress the message prior to sending it to the LEA.

If the PSP Infrastructure compresses a message using a lossless or lossy compression algorithm, then the compression algorithm will be made available to the LEA. If a lossy compression algorithm is used on the call content, no translations of content will be provided as part of the Delivery process to the LEA so as to protect the integrity of information content of the message. Licensing issues associated with such algorithms are beyond the scope of this Standard and must be handled between the LEA and the licensor.

⁸ CALEA, § 103(b)(3).

7. Advanced Messaging Interface (AMI) Protocol

The Advanced Messaging Interface (AMI) protocol deals with only the transfer of application layer information from the Data Delivery Point for LEA(s) as shown in Figure 4. The delivery network is based on the computer industry standard TCP/IP protocols, but the specification of the lower layers of this stack are beyond the scope of this document.

The AMI protocol is defined to supply the LEA-Provided CALEA Interface with:

- Lawful Authorization identifying information,
- PSP identifying information,
- Date and time of outbound or inbound message delivery to or from the Intercept Subject identified by the Lawful Authorization,
- Origin information, if reasonably available,
- Destination information,
- Termination information, if applicable, and
- Call Content.

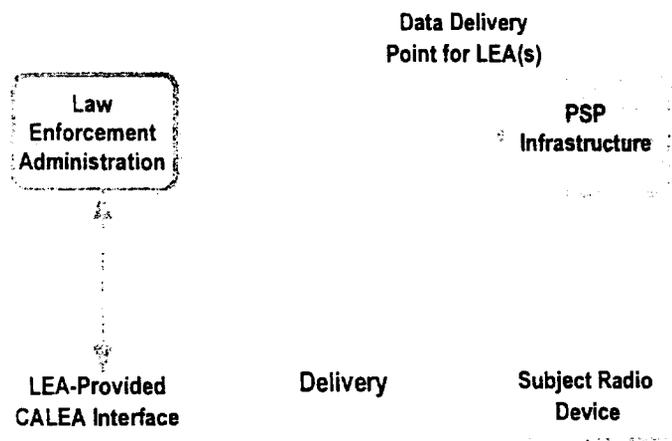


Figure 4: Data Delivery Point for LEA(s)

The AMI protocol is designed to the following criteria:

- Use standard and open protocols where possible,
- Use protocols which may be supported by the widest range of equipment,
- Use protocols which allow the use of readily available software applications by LEAs,
- Use protocols which are scalable for platform requirements, and
- Use protocols which allow inclusion of new formats when necessary.

The protocol delivery method is HTTP v1.1's POST operation. Lawful authorization information, call content and reasonably available call-identifying information is supplied as a single file that consists of MIME-encoded concatenated vCards and Call Content as shown in the stack diagram in Figure 5.

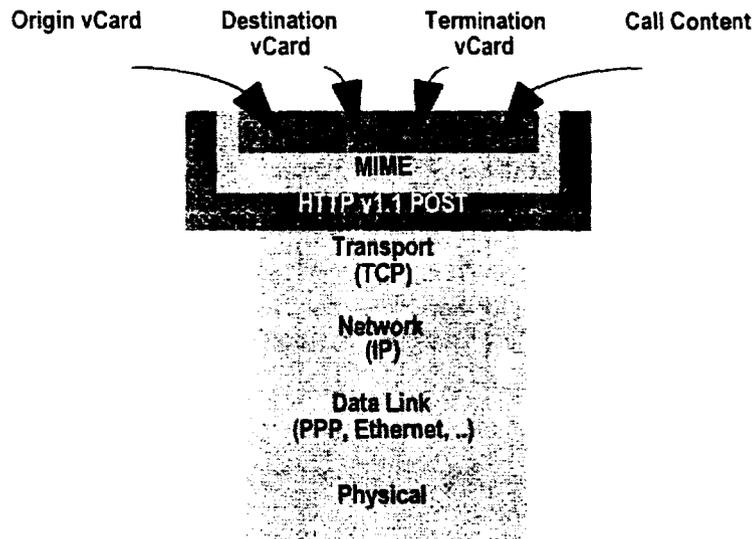


Figure 5: AMI Stack Diagram

7.1 HTTP v1.1 POST

HTTP v1.1 POST provides the ability to direct messages to specific server targets by specifying the specific server target's address for the interpreting application needed to process the operation.

The POST format for an AMI Protocol transaction has the following mandatory fields:

```
POST /cgi-bin/process_ami HTTP/1.1
Host: [domain name or IP of destination LEA-Provided CALEA Interface]
From: [lawful_authorization_identification]@[node].[carrier_identifier].[com]
Date: [date of call completion]
MIME-Version: 1.0
Content-Type: [type of content]
Content-Length: [length of POST Content in octets]
[POST Content]
```

where

- **/cgi-bin/process_ami** identifies the path ('cgi-bin' - mandatory) to the 'process_ami' application (e.g., 'process_ami.asp', 'process_ami_joe_n_pete_paging.asp') needed to interpret the AMI protocol,
- **Host:** identifies the domain name or IP address of the destination LEA-Provided CALEA Interface,
- **From:** identifies the associated Lawful Authorization and the originating carrier information where
 - **[lawful authorization identification]** is the information needed to uniquely identify the Lawful Authorization obtained to receive this information,
 - **[node]** is the identifying information for the PSP's originating Home Node of the Intercept,
 - **[carrier_identifier]** is the identifying information for the originating PSP, and
 - **[com]** or org, gov, edu .. is the extension of the carrier's domain name.
- **Date:** identifies the date and time (uses RFC 822 Date and Time format as modified by RFC 1123) of call completion,
- **MIME-Version:** identifies what version of the MIME protocol was used to construct the message,
- **Content-Type:** identifies the type of content,
- **Content-Length:** identifies the length of the POST Content data file in octets, followed by
- **[POST Content]** the actual POST Content data file.

An example of such a POST header for a POST Content data file consisting of a multipart MIME message of 3819 octets in length is:

```

POST /cgi-bin/process_ami.asp HTTP/1.1
Host: www.LEA1.gov
From: 1T234G78@st_louis.joe_n_pete_paging.com
Date: Sun, 15 Jun 1998 14:49:37 GMT
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=--content
Content-Length: 3819
--content
Content-Type: text/x-vcard; charset=us-ascii; name="destination.vcf"
(mandatory blank line)
[actual content of destination.vcf]
(mandatory blank line)
--content
Content-Type: text/plain; charset=us-ascii
(mandatory blank line)
[actual text content]
(mandatory blank line)
--content--

```

All fields use the definitions given in the HTTP v1.1 RFC 2068 and the MIME protocol RFCs 2045 through 2049.

7.2 HTTP v1.1 POST Content

The content of the POST operation is a single file consisting of MIME-encoded concatenated vCards followed by the Call Content as shown in the stack diagram in Figure 5. All vCard fields use the definitions given in the vCard 2.1 specification or the vCard v2.1-IrDA extension specification except as noted in Section 7.5. All MIME fields use the definitions given in RFC 2045 through RFC 2049.

7.3 vCards

The concatenated vCards includes at least one of the following:

- 'origin.vcf' vCard used to identify the origin of the message,
- 'destination.vcf' vCard used to identify the destination of the message, or
- 'termination.vcf' vCard used to identify the termination of the message.

Support for all AMI-identified vCard properties and parameters is mandatory for AMI server applications conforming to this specification. However, all vCard 2.1 and vCard 2.1-IrDA properties and parameters (e.g., other TEL and EMAIL parameters) are applicable and may be used. However, if such a non-supported property or parameter is encountered, then the server application must provide the field in the delivered format as a COMMENT.

7.3.1 Origin vCard

The 'origin.vcf' vCard contains the relevant identification information for the origination of the message.

If the origination is the Intercept Subject, then this vCard is mandatory with format as follows:

```
BEGIN:VCARD
VERSION:2.1-IrDA
N:[Intercept Subject's Name]
TEL;PAGER:[PIN]
X-PCIA-CAPCODE:[CapCode]
END:VCARD
```

where the [Intercept Subject's Name] is the Intercept Subject's name, if reasonably available, or simply the name 'intercept subject', if not reasonably available. Use of the TEL or X-PCIA-CAPCODE properties will depend on the type of Lawful Authorization supplied.

If the origination is not the Intercept Subject, then this vCard is supplied only if reasonably available with format as follows:

```
BEGIN:VCARD
VERSION:2.1
N:not available
TEL:[Phone Number]
EMAIL;INTERNET:[name@domain]
TEL;PAGER:[PIN]
END:VCARD
```

where the name is a choice of the names 'not available', if not reasonably available, 'PIN Name', or 'System' depending on the nature of the origination point and reasonably available origination information. Use of the TEL or EMAIL properties is mutually exclusive in this context and will depend on the nature of the origination.

7.3.2 Destination vCard

The 'destination.vcf' vCard contains the relevant identification information for the destination of the message.

If the destination is the Intercept Subject, then this vCard is mandatory with format as follows:

```
BEGIN:VCARD
VERSION:2.1-IrDA
N:[Intercept Subject's Name]
TEL;PAGER:[PIN]
X-PCIA-CAPCODE:[CapCode]
UID:[Message Number]
END:VCARD
```

where the [Intercept Subject's Name] is the Intercept Subject's name, if reasonably available, or simply the name 'intercept subject', if not reasonably available. Use of the TEL or X-PCIA-CAPCODE parameters will depend on the type of Lawful Authorization supplied.

If the destination is not the Intercept Subject, then this vCard is mandatory with format as follows:

```
BEGIN:VCARD
VERSION:2.1-IrDA
N:not available
TEL:[Phone Number]
TEL;PAGER:[PIN]
EMAIL;INTERNET:[name@domain]
X-PCIA-CAPCODE:[CapCode]
UID:[Message Number]
END:VCARD
```

where the name is a choice of the names 'not available', if not reasonably available, 'PIN Name', or 'System' depending on the nature of the destination point and reasonably available destination information. Use of the TEL, EMAIL, or X-PCIA-CAPCODE parameters is mutually exclusive in this context and will depend on the nature of the destination.

Since the 'destination.vcf' vCard is always present, the Call-Identifying Message Number is carried in the Destination vCard as the UID. Use of the Call-Identifying Message Number is optional in one-way transactions and mandatory in two-way transactions to allow tying of related outbound and inbound messages when the latter is known to be a response to the former by the PSP.

Lists of addressees (e.g., terminal group call) are to be treated as individual transactions.

7.3.3 Termination vCard

The 'termination.vcf' vCard contains the relevant identification information for the termination of the message.

If the Intercept Subject has forwarded messaging to another destination, then this vCard is mandatory with format as follows:

```
BEGIN:VCARD
VERSION:2.1
N:[Termination Subject's Name]
TEL;PAGER:[PIN]
TEL;FAX:[fax number]
EMAIL;INTERNET:[name@domain]
X-PCIA-CAPCODE:[CapCode]
END:VCARD
```

where the [Termination Subject's Name] is the Termination Subject's name, or is a choice of the names 'not available', if not reasonably available, 'PIN Name', or 'System' depending on the nature of the termination point and reasonably available termination information. Use of the TEL, EMAIL, or X-PCIA-CAPCODE parameters is mutually exclusive in this context and will depend on the nature of the termination.

Lists of addressees (e.g., terminal group call) are to be treated as individual transactions.

7.4 Call Content

The nature and interpretation of the Call Content is defined by the MIME type identifier(s) associated with the Call Content.

It is beyond the scope of this Standard to identify and define all MIME types currently in existence. The determination of how to interpret new or custom MIME types is the responsibility of the LEA and is also beyond the scope of this Standard.

If a custom MIME type is developed by the PSP, then the custom MIME type's encoding format(s) and algorithm(s) will be made available to the LEA, if appropriate. Licensing issues associated with such custom MIME type's encoding format(s) and algorithm(s) are beyond the scope of this Standard and must be handled between the LEA and the licensor.

Call Content must be omitted in those instances where the Lawful Authorization does not specify collecting the Call Content.

7.5 New vCard Protocol Property - CapCode

This property specifies the CapCode of the vCard-identified radio device as an 'X-' extension to vCard v2.1 as defined by the Miscellaneous Properties' Extensions section of vCard v2.1.

The property is identified by the property name **X-PCIA-CAPCODE**. The CapCode is to be indicated as follows:

```
CapCode          X-PCIA-CAPCODE
```

where X-PCIA-CAPCODE is defined by an ASCII string representation.

The following are examples of this parameter:

```
X-PCIA-CAPCODE:1234567
X-PCIA-CAPCODE:1T467B59
```

X-PCIA-CAPCODE:F13ACD23
X-PCIA-CAPCODE:199.3.38.10

Support for this property is mandatory for AMI protocol implementations conforming to this specification.

The following modified Backus-Naur Notation (BNF) extension to the formal definition in section 3.9 of vCard is provided to assist developers in building parsers for AMI vCards.

name = / "X-PCIA-CAPCODE"

7.6 Custom MIME Types and vCard Properties and Parameters

'X-' type custom MIME and vCard properties and parameters must be registered with the PCIA for use with this specification. Contact the PCIA for further information.

References

- CALEA Suite of Standards for Traditional Paging, Advanced Messaging, and Ancillary Services, v1.0, 04 May, 1998 (http://www.pcia.com/calea_specs_v1p0.zip)
- Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414
- IrDA® Telecom Extensions to the IMC vCard Format, v1.0, 15 October, 1997 (<http://www.irda.org/>)
- Hypertext Transfer Protocol - HTTP/1.1, RFC 2068, January, 1997 (<ftp://ds.internic.net/rfc/rfc2068.txt>)
- Lawfully Authorized Electronic Surveillance, TIA/ATIS, Interim/Trial Use Standard (J-STD-025)
- Standard for the Format of ARPA Internet Text Messages, RFC 822, 13 August, 1982 (<ftp://ds.internic.net/rfc/rfc822.txt>)
- Requirements for Internet Hosts - Application and Support, RFC 1123, October, 1989 (<ftp://ds.internic.net/rfc/rfc1123.txt>)
- Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, RFC 2045, November, 1996 (<ftp://ds.internic.net/rfc/rfc2045.txt>)
- Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, RFC 2046, November, 1996 (<ftp://ds.internic.net/rfc/rfc2046.txt>)
- Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text, RFC 2047, November, 1996 (<ftp://ds.internic.net/rfc/rfc2047.txt>)
- Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures, RFC 2048, November, 1996 (<ftp://ds.internic.net/rfc/rfc2048.txt>)
- Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples, RFC 2049, November, 1996 (<ftp://ds.internic.net/rfc/rfc2049.txt>)
- Telecommunications Carrier Assistance to the Government, H. Rep. No. 103-827
- vCard - The Electronic Business Card Exchange Format, v2.1, The Internet Mail Consortium (IMC), 18 September, 1996, (<http://www.imc.org/pdi/vcard-21.doc>)

Glossary

Advanced Messaging

Advanced Messaging services include such services as subscriber defined on-demand roaming, forwarding and redirection, two-way and acknowledged voice paging, and wireless packet data services.

CALEA

CALEA is the acronym for Communications Assistance for Law Enforcement Act.

call completion

As interpreted by this Standard for advanced messaging, call completion is interpreted as follows: delivery of the tone-only, numeric, alphanumeric, binary data, and/or voice messages to the RF network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address in advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services, and arrival, at the Home Node, of the tone-only, numeric, alphanumeric, binary data, and/or voice messages transmitted from a subject's radio transceiving device in advanced two-way, acknowledged voice, and wireless packet data inbound message services. Any transmissions attempted by a subjects' radio transceiving device which do not arrive at the Home Node are not considered to be "completed".

call content

see *content*.

call-identifying information

Call-identifying information is defined in CALEA Section 102 (2) to be "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a [PSP]." As interpreted for advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services by this Standard for advanced messaging: *destination* is the radio receiving or transceiving device address to which a call is being made (e.g., called party); *direction* is the outbound transmission path from the PSP Home Node to the RF network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address; *origin* is the number or address of the party initiating the call (e.g., calling party); and *termination* is the alternate address to which a call is being routed, if applicable (e.g., forwarded party). As interpreted for advanced two-way, acknowledged voice, and wireless packet data inbound message services by this Standard for advanced messaging: *destination* is the number or address of the device to which the intercept subject sends a message (i.e., called party), *direction* is the transmission path from the intercept subject's radio transceiving device to the intercept subject's PSP Home Node, *origin* is the address of the intercept subject's radio transceiving device sending the message (i.e., the calling party), and *termination* is the same as *Destination*. For these outbound message services, reasonably available call-identifying information is that information used in the Home Node for call processing. Reasonably available call-identifying information generally consists of the address of the subject's radio receiving or transceiving device(s) and, if appropriate, the address to which the message has been forwarded or redirected. The call origin is not reasonably available in most PSP installations but may be obtained through the originating service provider (e.g., EC, ISP). For these inbound message services, both *Origin* and *Destination* information are available.

calling party

The calling party is the originating party of an advanced messaging message regardless of destination.

capcode

Capcode is the radio address decoder element in each radio device that permits the radio device to be selectively identified and signaled over a common radio channel. Colloquially, this term is used to generically identify the radio device's radio signaling scheme address in this Specification for advanced messaging even though different radio signaling scheme technologies may use similar but different names for the same function.

channel

Channel is an independent path for communicating between two points.

clone radio receiving device

A clone radio receiving device is a radio receiving device, provided by the LEA, that is pre-programmed by the PSP as authorized by a lawful authorization with the intercept subject's radio receiving address and set to monitor the subject's radio receiving frequency with the express purpose of decoding and capturing the subject's call content when used within the subject's fixed geographical broadcast area. A clone radio receiving device has the same characteristics and call content reception and processing features as the intercept subject's radio receiving device.

Commission

Commission is defined in CALEA Section 102 (3) to be "the Federal Communications Commission".

communication

Communication, in this Standard, refers to any wire or electronic communication, as defined in 18 USC 2510.

communication intercept

see *intercept*.

compression

Compression is a method or methods for reducing the bandwidth or number of bits needed to encode information or encode a signal. Algorithms used may be 'lossless' which allows recovery of all information content or 'lossy' which does not allow recovery of all information content.

connection

Connection is a relationship between two or more parties of a call to allow communication between them.

content

Content is defined in 18 USC 2510 (8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication." As interpreted by this Standard for advanced messaging, call content covers tone-only, numeric, alphanumeric, binary data, and voice messages delivered to the PSP RF Network or to the appropriate External Messaging source or Input Node when termination is applicable and the alternate address is an external wireline address from the subscriber's Home Node in the PSP Infrastructure in advanced one-way, two-way, acknowledged voice, and wireless packet data outbound message services, or transmitted from a subscriber's radio transceiving device and delivered to the subscriber's Home Node in the PSP Infrastructure in advanced two-way, acknowledged voice, and wireless packet data inbound message services.

coverage area

Coverage area is the geographic region throughout which radio receiving and/or transceiving devices can be expected to reliably send communication to and/or receive communication from the PSP Infrastructure

Data Delivery Point for LEA(s)

The Data Delivery Point for LEA(s) is the PSP-maintained AMI protocol interface between the PSP Infrastructure and the LEA-provided transport function to the LEA-provided CALEA Interface.

Delivery Action

For advanced messaging, the Delivery Action is responsible for delivering intercepted communications expeditiously from the PSP Infrastructure Data Delivery Point for LEA(s) for use by one or more LEA-Provided CALEA Interfaces (up to a total of five per intercept subject) using the Advanced Messaging Interface (AMI) Protocol.

destination

see *call-identifying information*

Destination.vcf

Destination.vcf is a vCard-formatted file containing identification information pertaining to the destination of a message.

direction

see *call-identifying information*

EC

see *Exchange Carrier*.

electronic surveillance

Electronic surveillance is the statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission.

encoding

Encoding is the process of converting data or voice signals into a format suitable for transmission.

encryption

Encryption is the process of changing the format of the information content of a message or message routing information such that external observers will not be able to interpret correctly the content or routing information.

Exchange Carrier

Exchange Carrier is the wireline PSTN carrier interface provider. Exchange carriers may take the form of a local exchange carrier or an interexchange carrier.

External Messaging Function

External Messaging Function is the delivery of messages to and from wireline carrier sources (e.g., EC, ISP) to the PSP Infrastructure.

functional entity

Functional entity is a system or subsystem capable of providing a defined service.

government

Government is defined in CALEA Section 102 (5) to be "the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance."

Home Node

Home Node is the PSP Infrastructure network node that encompasses subscriber database records and those functions needed to route messages between the appropriate Input Node(s) and the RF Network.

HTTP

HyperText Transfer Protocol is a set of protocols used to transfer information on the WWW.

IETF

Internet Engineering Task Force is the technical body responsible for developing and maintaining protocols related to the Internet.

IMC

Internet Mail Consortium (<http://www.imc.org/>) is the standards development organization responsible for developing and maintaining many mail and identification formats and protocols (e.g., vCard®).

inbound message

Inbound messages are transmitted by the radio transceiving device to the radio transceiving device's Home Node within the PSP network. These messages may be destined for external wireline addresses, other wireless devices, or the PSP system.

Information Service

Information Service is defined in CALEA Section 102 (6) to be "(A) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunication; and (B) includes -- (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services; but (C) does not include any capability for a [PSP's] internal management, control, or operation of its telecommunication network."

Input Node

Input Node is the PSP Infrastructure network node that encompasses those functions needed to deliver messages to and from wireline carrier sources (e.g., EC, ISP).

intercept

Intercept is defined in 18 USC 2510 (4) to be "the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

intercept subject

Intercept subject is a paging or wireless packet data service subscriber whose reasonably available call-identifying information and call content have been authorized by a court to be intercepted and delivered to an LEA.

Internet Service Provider

Internet Service Provider is the wireline Internet carrier interface provider.

IrDA®

InfraRed Data Association (<http://www.irda.org/>) is the standards development organization responsible for developing and maintaining many infrared-based communications protocols and for extending the IMC's identification formats and protocols (e.g., vCard®) to cover RF technologies.

ISP

see *Internet Service Provider*.

LAES

LAES is an initialism for Lawfully Authorized Electronic Surveillance.

Law Enforcement Administrative Function

Law Enforcement Administrative Function is responsible for controlling LEA electronic surveillance functions, for providing the LEA-Provided CALEA Interface and the associated Delivery Function link to the PSP Infrastructure for receiving the messaging traffic of the subject of a lawful authorization, and for capturing and processing of the delivered call content and reasonably available call-identifying information. The Law Enforcement Administrative Function is the responsibility of the LEA. Other functions of the Law Enforcement Administrative Function are beyond the scope of this standard.

Law Enforcement Agency

Law Enforcement Agency is a government entity with the legal authority to conduct electronic surveillance.

Lawful Authorization

Lawful Authorization is the legal entity required to authorize a CALEA intercept. No intercepts shall take place without specific lawful authorization. One Lawful Authorization may encompass multiple devices and/or multiple geographic locations.

Lawful Authorization Action

Lawful Authorization Action is the serving of the Lawful Authorization to the PSP by the LEA.

LEA

see *Law Enforcement Agency*.

MIME

MIME is an acronym for Multipurpose Internet Mail Extensions which is a set of specifications designed to extend the usefulness of Internet mail.

Origin

see *call-identifying information*.

Origin.vcf

Origin.vcf is a vCard-formatted file containing identification information pertaining to the origin of a message.

outbound messages

Outbound messages are transmitted to the radio transceiving device from the radio transceiving device's Home Node within the PSP Infrastructure. These messages may originate from external wireline sources, other wireless devices, or the PSP Infrastructure.

Output Node

Output Node is that portion of the PSP Infrastructure RF Network node that encompasses those functions needed to encode and deliver messages to and from wireless carrier sources (e.g., radio transceiving devices) using RF transmitters and, in two-way advanced messaging systems, RF receivers.

Paging or Wireless Packet Data Service Provider⁹

Paging or Wireless Packet Data Service Provider is defined from CALEA Section 102 (8) to be, "a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, and includes 1) a person or entity engaged in providing commercial mobile service, or 2) a person or entity engaged in providing wire or electronic communications switching or transmission service to the extent that the Commission finds such service is a replacement for a substantial portion of local telephone exchange service and that it is in the public interest to deem such a person or entity to be a [PSP] for purposes of this title. This does not include 1) persons or entities insofar as they are engaged in providing information services, and 2) any class or category of [PSPs] that the Commission exempts by rule after consultation with the U. S. Attorney General."

⁹ This Standard uses the term *paging or wireless packet data service provider* instead of the CALEA term *telecommunication carrier*.

Provision Action

Provision Action is responsible for enabling and disabling activation of the interface to the LEA-Provided CALEA Interface Function as required to receive the reasonably available call-identifying information and call content described in the Lawful Authorization. For advanced messaging, the Provision Action includes the ability to unobtrusively make the call content and reasonably available call-identifying information available to the delivery action and to protect (i.e., prevent unauthorized access, manipulation, and disclosure) intercept controls and intercepted call content and reasonably available call-identifying information consistent with PSP security policies and practices. The Provision Action establishes the interface and controls between the LEA and the PSP for the purpose of intercepting messaging traffic as specified by a Lawful Authorization.

PSDN

PSDN is an initialism for Public Switched Data Network.

PSP

see *Paging or Wireless Packet Data Service Provider*.

PSP Administration Function

PSP Administration Function is responsible for controlling the Provision, enabling the Delivery Actions, and maintaining the Data Delivery Point for LEA(s). Other functions of the PSP Administrative Function are beyond the scope of this standard.

PSP Infrastructure

PSP Infrastructure embodies the Home Node central control switch(es), RF Network of Output Node(s), RF transmitter(s), and RF receiver(s), and Input Node wireline interconnect(s) that tie the radio network to the PSTN, PSDN, the World Wide Web, and other land-based facilities to allow advanced messaging calls to be initiated and transmitted to or transmitted from the intended subscriber.

PSP Infrastructure Function

PSP Infrastructure Function is the switching and radio transmission network of the PSP. For this Standard, the PSP Infrastructure is responsible for the collection and delivery of call content and reasonably available call-identifying information of one or more lawfully authorized intercept subject(s).

PSTN

PSTN is an initialism for Public Switched Telephone Network.

RF

RF is an initialism for Radio Frequency.

RF Network

RF Network is the PSP Infrastructure network node that encompasses those functions needed to deliver messages to and from wireless carrier sources (e.g., radio transceiving devices). The RF Network includes RF transmitters and Output Node encoders and, in two-way advanced messaging systems, RF receivers.

RF receiver

RF receiver is a component in the PSP Infrastructure's RF Network which receives and translates radio-based communications from the subject radio device to wireline-based communications.

RF transmitter

RF transmitter is a component in the PSP Infrastructure's RF Network which receives and translates wireline-based communications to radio-based communications and transmits the radio-based communications to the subject radio device.

RFC

RFC is an initialism for Request For Comment and represents the protocol specifications produced by the IETF.

signaling scheme

Signaling scheme is the radio signaling protocol used to deliver messages to specific radio receiving devices. Radio signals radiated by base station transmitters are encoded with radio receiving device capcode and message content information. These signaling schemes may utilize analog (e.g., 2-tone, 5/6-tone) or digital (e.g., POCSAG, Golay Sequential Code®, FLEX™, ERMES, ReFLEX™, InFLEXion™, DataTAC™) modulating techniques with the transmitted information organized in accordance with any of several formats which specify such parameters as transmission rate, structure of the information, and error control mechanisms.

SMTP

SMTP is an initialism for Simple Mail Transport Protocol and represents the protocol specifications produced by the IETF for simple internet email.

Subject Radio Device Function

Subject Radio Device Function is responsible for collecting and interpreting and, where applicable, encoding and disbursing communications for the intercept subject.

subscriber

Subscriber is the entity subscribing to the services provided by the PSP.

Termination.vcf

Termination.vcf is a vCard-formatted file containing identification information pertaining to the termination of a message.

traditional paging

Traditional paging supports the one-way wireless transmission of tone-only, numeric, alphanumeric, and voice messages from a PSP to one or more radio receiving devices within a stipulated, predefined geographic radio coverage area of the PSP Infrastructure.

termination

see *Call-Identifying Information*.

transmission

Transmission is the act of transferring communications from one location or another by wire, radio, electromagnetic, photoelectronic, or photo-optical system.

unobtrusive

Unobtrusive in this context is not undesirably noticeable or blatant; inconspicuous; within normal call variances.

USC

USC is an initialism for United States Code.

vCard®

vCard® is an IMC-defined file format containing identification information.

wire communications

Wire communications is defined in 18, USC 2510 (1) to be "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication."

wireless

Wireless, in this Standard, refers to traditional paging and advanced messaging services.

wireline

Wireline, in this Standard, refers to traditional wire-based telephone and packet data services.

World Wide Web

World Wide Web is an application running on an ad hoc global network that has been defined to provide communications between a wide range of people, places, and things.

WWW

see World Wide Web.

Annex 1 Examples

The following annex is informative only and is not a part of this standard.

Several basic messaging scenarios are described in this annex. The intent of the annex is to provide representative examples of how such communications *might* be intercepted and the appropriate information conveyed to the LEA under this standard. This annex is not intended as an exhaustive set of examples. The scenarios contained in this annex are informative only. PSPs may provide access using configurations and accesses not shown. PSPs are not obligated to implement particular services or features in the way illustrated in these exemplary scenarios.

For the purposes of illustrating the following examples, the PSP referenced will be known as "USA Wireless Messaging" with a home node in "Slippery Rock, SD". The LEA will be known as "LEA1" and the Lawful Authorization identification number will be "PI314159265".

A1. Message Examples Sent To Radio Receiving Devices

The following examples are provided to illustrate typical messaging sent to radio receiving devices.

A1.1 Intercept Subject using Traditional Paging's Predefined Geographical Coverage

This is a simple paging example using techniques covered by Standard 1 - CALEA Specification for Traditional Paging.

A1.1.1 Transaction Flow:

- LEA (LEA1) presents a Lawful Authorization for a capcode or PIN intercept to the PSP (USA Wireless Messaging).
- PSP determines that the intercept subject has traditional paging features and programs the LEA-provided clone radio receiving device with the intercept subject's capcode.
- PSP receives a message for the intercept subject.
- PSP sends the message to the PSP's RF infrastructure.
- The RF infrastructure broadcasts the message in the intercept subject's predefined geographical coverage area.
- Both the subject and the clone radio receiving device receive the call content of the message at the same time.

A1.1.2 AMI-Delivered Information

Since this is an example of a traditional paging application, there is no AMI Data Transfer.

A1.2 Intercept Subject Using Advanced Messaging's Subscriber Defined On-Demand Roaming

This example illustrates the transaction flow and AMI-delivered information for a message sent to an intercept subject who has redefined the available coverage area in which messages shall be sent.

A1.2.1 Transaction Flow:

- LEA (LEA1) presents a Lawful Authorization for a capcode intercept to the PSP (USA Wireless Messaging).
- PSP determines that the intercept subject has advanced messaging features and sets up monitoring within the PSP Infrastructure.
- PSP does not receive *origin* call-identifying information.
- PSP receives a message for the intercept subject.
- PSP sends the message as call content to the PSP Infrastructure's RF Network.
- PSP sends an AMI protocol message with this call content from the PSP's Data Delivery Point for LEA(s) for reception by the LEA-Provided CALEA Interface.
- PSP RF Network broadcasts the message in the intercept subject's current geographical coverage area.

A1.2.2 AMI-Delivered Information

The following data transfer is sent via the AMI protocol from the PSP's Data Delivery Point for LEA(s).

AMI Data Transfer - Outbound Message from the PSP to the Radio Transceiving Device:

```

POST /cgi-bin/process_ami.asp HTTP/1.1
Host: www.LEA1.gov
From: PI314159265@Slippery_Rock.USA_Wireless_Messaging.com
Date: Sun, 15 Jun 1998 18:13:23 GMT
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=--content
Content-Length: 225
(mandatory blank line)
--content
Content-Type: text/x-vcard; charset=us-ascii; name="destination.vcf"
(mandatory blank line)
BEGIN:VCARD
VERSION:2.1
N:John Q. Public
X-PCIA-CAPCODE:987654321
END:VCARD
(mandatory blank line)
--content
Content-Type: text/plain; charset=us-ascii
(mandatory blank line)
[actual text content]

```

(mandatory blank line)

--content--

A1.3 Intercept Subject Forwards to Alternate Radio Receiving Device

This example illustrates the transaction flow and AMI-delivered information for a message sent to an intercept subject who has defined an alternate destination to which messages shall be sent.

A1.3.1 Transaction Flow:

- LEA (LEA1) presents a Lawful Authorization for a capcode intercept to the PSP (USA Wireless Messaging).
- PSP determines that the intercept subject has advanced messaging features and sets up monitoring within the PSP Infrastructure.
- PSP does not receive *origin* call-identifying information.
- Intercept subject has implemented forwarding to an alternate radio receiving device PIN.
- PSP receives a message for the intercept subject and forwards to alternate radio receiving device PIN.
- PSP sends the message as call content to the PSP Infrastructure's RF Network for delivery to the alternate radio receiving device.
- PSP sends an AMI protocol message with this call content and alternate address from the PSP's Data Delivery Point for LEA(s) for reception by the LEA-Provided CALEA Interface.

A1.3.2 AMI-Delivered Information

The following data transfer is sent via the AMI protocol from the PSP's Data Delivery Point for LEA(s).

AMI Data Transfer - Outbound Message from the PSP to the Radio Transceiving Device:

```

POST /cgi-bin/process_ami.asp HTTP/1.1
Host: www.LEA1.gov
From: PI314159265@Slippery_Rock.USA_Wireless_Messaging.com
Date: Sun, 15 Jun 1998 18:13:23 GMT
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=--content
Content-Length: 225
(mandatory blank line)
--content
Content-Type: text/x-vcard; charset=us-ascii; name="destination.vcf"
(mandatory blank line)
BEGIN:VCARD
VERSION:2.1
N:John Q. Public
X-PCIA-CAPCODE:987654556
END:VCARD
(mandatory blank line)
--content

```

Content-Type: text/x-vcard; charset=us-ascii; name="termination.vcf"

(mandatory blank line)

BEGIN:VCARD

VERSION:2.1

N:not available

TEL;PAGER:5553535

END:VCARD

(mandatory blank line)

--content

Content-Type: text/plain; charset=us-ascii

(mandatory blank line)

[actual text content]*(mandatory blank line)*

--content--