ATIS STANDARD

ATIS-1000678.v4.2020

Lawfully Authorized Electronic Surveillance (LAES) for Voice over Internet Protocol and Rich Communications Services Messaging in Wireline and Broadband Telecommunications Network, Version 4

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

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

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

AMERICAN NATIONAL STANDARD

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

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

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

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

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

Notice of Disclaimer & Limitation of Liability

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

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

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

ATIS-1000678.v4.2020, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Internet Protocol and Rich Communications Services Messaging in Wireline and Broadband Telecommunications Network, Version 4*

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

Published by

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

ATIS-1000678.v4.2020

ATIS Standard on

Lawfully Authorized Electronic Surveillance (LAES) for Voice over Internet Protocol and Rich Communications Services Messaging in Wireline and Broadband Telecommunications Networks, Version 4

Alliance for Telecommunications Industry Solutions

Approved: October 16, 2020

Abstract

This Standard defines the interfaces between a Telecommunication Service Provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for Voice over Internet Protocol (VoIP) and Rich Communications Services (RCS) Messaging in wireline and broadband telecommunications networks. This version of the standard extends the capabilities in ATIS-1000678.v3.2015(R2020) and also provides corrections.

This document provides the mechanisms to perform lawfully authorized electronic surveillance of VoIP subject to the appropriate legal and regulatory environment. It is not the intent of this document to imply or impact any pending Communications Assistance for Law Enforcement Act (CALEA) regulatory decisions related to VoIP.

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

Foreword

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

This document is entitled the American National Standard for Telecommunications – Lawfully Authorized Electronic Surveillance (LAES) for Voice over Internet Protocol (VoIP) and Rich Communications Services (RCS) Messaging in Wireline and Broadband Telecommunications Networks. This standard is the result of work by members of the Packet Technologies and Systems Committee (PTSC), working within the PTSC Lawfully Authorized Electronic Surveillance Subcommittee (LAES). This Standard defines the interfaces between a Telecommunication Service Provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for VoIP and RCS messaging in wireline and broadband telecommunications networks.

It is not the intent of this document to imply or impact any pending CALEA regulatory decisions related to VoIP. This document provides the mechanisms to perform lawfully authorized electronic surveillance of VoIP subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable to VoIP, it is intended that a manufacturer or service provider that is in compliance with this document will have "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001 et seq.

Suggestions for improvement of this standard will be welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, 1200 G Street NW, Suite 500, Washington, D.C. 20005.

This standard was processed and approved for submittal to ANSI by the PTSC. Committee approval of this standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, the PTSC had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Perspecta Labs)

G. Myers, PTSC LAES Chair (Counter Link)

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

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

Table of Contents

Table of Figures

Table of Tables

Introduction

1.1 Background

This Standard defines the interfaces between a Telecommunications Service Provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for Voice over Internet Protocol (VoIP) and Rich Communications Services (RCS) messaging in wireline and broadband telecommunications networks. This Standard is provided for purposes of a "safe harbor" as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [Ref 1]: "a telecommunications carrier shall be found to be in compliance with the assistance capability requirements under Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with Section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103."[1]

As used in this Standard, *electronic surveillance* refers to the interception and monitoring of communications for a particular telecommunications subscriber as lawfully authorized. The said communications may include Call Identifying Information (CII) with or without the Call Content (CC).

In this Standard, an *intercept subject*, or more simply a *subject*, is a telecommunications service subscriber whose communications have been authorized by a legal instrument to be intercepted and delivered to an LEA. The identification of the subject is limited to subject identifiers or subject-related identifiers used by the TSP's equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

As a precondition for a TSP's assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve a TSP with the necessary lawful authorization identifying the intercept subject, the communications and information to be provided, and service areas where the communications and information are to be provided. Once this lawful authorization is served on a TSP, the TSP shall perform the access and delivery of the identified communications and information to the LEA via LEA-procured equipment, facilities, or services.

1.2 Scope & Purpose

The purpose of this Standard is to facilitate a TSP's compliance with the assistance capability requirements defined in Section 103 of CALEA [Ref 1]. This Standard defines capabilities to support LAES and the interfaces to deliver intercepted communications and reasonably available CII to an LEA when authorized. This Standard also defines a protocol for delivering CC and CII to LEAs. Compliance with this Standard addresses the "safe harbor" provisions of Section 107 of CALEA [Ref 1] and helps ensure efficient and industry-wide implementation of capabilities to assist LEAs.

The scope of this Standard is the set of capabilities to support LAES for VoIP and RCS[2] (Rich Communications Services) messaging services in wireline and broadband telecommunications networks and the interface(s) between a TSP and an LEA.

J-STD-025-B [Ref 2] has been used as a basis for development of this Standard.

[1] It is not the intent of this document to imply or impact any pending CALEA regulatory decisions related to VoIP. This document provides the mechanisms to perform lawfully authorized electronic surveillance of VoIP subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable to VoIP, it is intended that a manufacturer or service provider that is in compliance with this document will have "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. 1001, et seq.

[2] The RCS services, for which interception is defined in this standard, is based on the RCS Universal Profile. RCS Voice Services (e.g., RCS enhanced voice) as defined by GSMA, and activation of an intercept of RCS communications for an already established session are not addressed in this version of this specification but may be addressed in a future version of this standard. See RCC.71 – RCS Universal Profile Service Definition Document Version 2.4, October 2019, GSM Association [Ref 29] for more information on RCS Universal Profile.

This Standard is applicable to those voice services and RCS messaging utilizing wireline and broadband connections with packet-mode technologies – e.g., voice services over Internet Protocol (IP). This standard may also be applicable to switched voice services utilizing Voice over Packet and RCS messaging accessed via non-wired connections by agreement between the LEA and TSP. This version of the standard extends the capabilities in ATIS-1000678.v3.2015(R2020) and also provides corrections.

Other Lawful Interception standards meeting CALEA requirements and providing CALEA "safe harbor" for reporting Lawful Interception of specific services (such as VoIP or RCS) also covered in this standard may exist. TSPs reporting Lawful Interception for these specific services utilizing these other standards may omit support of the corresponding Lawful Interception reporting capability or capabilities defined in this standard while supporting the remainder of this standard.

1.3 Organization

Clause 2, *Normative References*, is a list of references used in the preparation of this Standard.

Clause 3, *Definitions & Acronyms*, defines words and acronyms that are used in this Standard.

Clause 4, *Electronic Surveillance Architecture*, defines an architecture to be used in understanding the context of the specification presented in this document.

Clause 5, *User Perspective (Stage 1)*, presents the user perspective (Stage 1) requirements for LAES for VoIP technologies in wireline and broadband telecommunications networks.

Clause 6, *Network Perspective (Stage 2)*, presents the network perspective (Stage 2) requirements for LAES for VoIP technologies in wireline and broadband telecommunications networks.

Annex A, *ASN.1 Definitions (Normative)*, defines the lawfully authorized electronic surveillance protocol (LAESP) Abstract Syntax Notation One (ASN.1) and associated modules.

Annex B, *SIP Mappings (Informative)*, defines mappings from SIP messages and parameters to surveillance messages and parameters.

Annex C, *SIP Information Flows (Informative)*, provides information flows to aid in the understanding of the requirements for the mapping from user and network SIP-based signaling to surveillance messages used on the e-interface.

Annex D, *Optional Messages (Informative)*, defines optional surveillance messages for the e-interface.

Annex E, *Example VoIP CC-IAP Locations (Informative)*, contains information regarding the location of Intercept Access Points (IAP) for CC intercepts in VoIP networks.

Annex F, *Dialed Digit Extraction Scenarios (Informative)*, describes potential solutions for accomplishing dialed digit extraction.

1.4 Optional LAES Capabilities

Optional LAES Capabilities are specified in the Informative Annexes of this specification. For purposes of this Standard, an Optional LAES Capability is an LAES capability which need not be provided in order to be conformant to this Standard.

2 Normative References

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

[Ref 1] *Communications Assistance for Law Enforcement Act (CALEA)*, Public Law 103-414, October 25, 1994.[3]

[Ref 2] ANSI/J-STD-025-B-2006, *Joint Standard on Lawfully Authorized Electronic Surveillance*, February 2019.[4]

[Ref 3] *Communications Assistance for Law Enforcement Act, Order on Remand*, CC Docket No. 97-213, 17 FCC Record 6898 (2002).[2]

[Ref 4] *Communications Assistance for Law Enforcement Act, Third Report and Order,* CC Docket No. 97-213, 14 FCC Record 16794 (1999). [2]

[Ref 5] *Wire and Electronic Communications Interception and Interception of Oral Communications*, Title 18 of the United States Code, Chapter 119, Sections 2510 - 2522. [2]

[Ref 6] IETF RFC 3261, *SIP: Session Initiation Protocol*, June 2002.[5]

[Ref 7] ATIS-1000607.2014, *Integrated Services Digital Network (ISDN) - Layer 3 Signaling Specification for Circuit Switched Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)*.[3]

[Ref 8] IEEE 802.3-2018 – *IEEE Standard for Ethernet*

[Ref 9] IETF RFC 4566, *SDP: Session Description Protocol*, July 2006.[4]

[Ref 10] ITU-T Recommendation X.680, *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*, August 2015.[5]

[Ref 11] IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*, July 2003.[4]

[Ref 12] IETF RFC 793, *Transmission Control Protocol*, September 1981.[4]

[Ref 13] IETF RFC 3986, *Uniform Resource Identifiers (URI): Generic Syntax*, January 2005.[4]

[Ref 14] IETF RFC 7542, *The Network Access Identifier*, May 2015.[4]

[Ref 15] IETF RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*, April 2003.[4]

[Ref 16] IETF RFC 6665, *Session Initiation Protocol (SIP)-Specific Event Notification*, July 2012.[4]

[Ref 17] ATIS-0300260.1998(S2018), September 2018, *Operations, Administration, Maintenance, and Provisioning (OAM&P) – Extension to Generic Network Model for Interfaces between Service Provider Administrative System (Lawful Authorized Electronic Surveillance) and Network Elements.*[3]

[Ref 18] ATIS-0300276.2008(R2017), August 2008, *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security requirements for the Management Plane.*[3]

[Ref 19] *Report and Order,* CC Docket No. 97-213, FCC 99-11 (March 1999). [2]

[Ref 20] IETF RFC 3311, *The Session Initiation Protocol (SIP) UPDATE Method*, September 2002.[4]

[Ref 21] IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*, November 2002.[4]

[Ref 22] ATIS-1000067.2015, *IP NGN Enhanced Calling Name (eCNAM)*, August 2015.

[Ref 23] IETF RFC 3711, *The Secure Real-Time Transport Protocol (SRTP)*, March 2004.

[Ref 24] ATIS-1000074, Joint ATIS/SIP Forum Standard – *Signature-based Handling of Asserted information using toKENs (SHAKEN).*

[3] This document is available at < http://www.fcc.gov/calea >.

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) <http://www.atis.org> and the Telecommunications Industry Association (TIA). < http://www.tiaonline.org/standards/overview.cfm >.

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

[Ref 25] ATIS-1000085, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): SHAKEN Support of "div" PASSporT*

[Ref 26] IETF RFC 8225, PASSport: Personal Assertion Token, June 2018.

[Ref 27] IETF RFC 4975, *The Message Session Relay Protocol (MSRP)*, September 2007.

[Ref 28] RCC.07 - *Rich Communication Suite 11.0 Advanced Communications Services and Client Specifications*, October 2019, GSM Association.

[Ref 29] RCC.71 – RCS Universal Profile Service Definition Document Version 2.4, October 2019, GSM Association.

[Ref 30] ATIS-1000013.v2.2015, *Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services.*

[Ref 31] ETSI TS 102 232-2 v 3.11.1 *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP Delivery; Part 2: Service-specific details for messaging services.*

[Ref 32] OMA WSP Content Type Numbers[6]

3 Definitions & Acronyms

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

3.1 Definitions

agent: A network-based service or device that acts on behalf of a subscriber to send or receive communications (e.g., an interactive screening service, a reminder service, a delayed transmission service).

associate: A telecommunication user whose equipment, facilities, or service are communicating with a subject.

call: A sequence of events beginning with an initial connection or facility request and ending with the final release of all facilities used. A call may have one or more *legs*.

Call Content (CC): See *Content*.

Call Content Address: The Call Content Address (CC Address) value identifies the IP address(es) and port number(s) of the Call Content Channel (CCC) or pair of CCCs used for conveying call content.

Call-Identifying Information (CII): Defined in [Ref 1] 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 telecommunications carrier.” Call-identifying information is “reasonably available” to a TSP if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications.

As defined in [Ref 3]: *destination* is a party or place to which a call is being made (e.g., called party); *direction* is a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); *origin* is a party initiating a call (e.g., calling party), or a place from which a call is initiated; and *termination* is a party or place at the end of a communication path (e.g., the called or call-receiving party, or the switch of a party that has placed another party on hold).

called party: The destination party of a call.

call identity: A call identity is a value that uniquely identifies a particular call, call leg, or session.

calling party: The originating party of a call.

[6] This list is available at < https://www.openmobilealliance.org/wp/OMNA/wsp/wsp_content_type_codes.html >

Call Content Channel (CCC) Identity: The CCC Identity (CCCIdentity) value identifies the CCC or pair of CCCs used for conveying call content.

CII Mediation Function (CII-MF): A function that maps (rather than encapsulates) VoIP subject access and network signaling messages onto e-interface messages (as defined in this standard).

Collection Function (CF): Defined in [Ref 4] to be "the location where lawfully authorized intercepted communications and call-identifying information is collected by a law enforcement agency (LEA)."

communication: Any wire or electronic communication, as defined in [Ref 5].

Communication Management System (CMS): Network element that provides communication management functions for communications to and from the intercept subject.

complete: A call attempt that is answered.

connection: A relationship between two or more parties of a call to allow communication between them.

content: Defined in [Ref 5] (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."

cut-through: When an endpoint has received via call signaling the information needed to communicate with the remote endpoint and a communication path exists between the endpoint and the remote endpoint.

destination: See *call-identifying information*.

direction: See *call-identifying information*.

Direct Signal Reporting (DSR): Reporting of VoIP subject access and network signaling to LEA(s) via encapsulation (rather than mapping of parameters by a CII-MF).

electronic communications: Defined in [Ref 5] (12) to be "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."

electronic surveillance: 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. As used herein, also includes the acquisition of call-identifying information. As used herein, *surveillance* refers to a single communication intercept, pen register, or trap and trace. Its usage herein does not include administrative subpoenas for obtaining a subscriber's billing records and information about a subscriber's service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

extended name: That part of the eCNAM service [Ref 22] that replaces the traditional 15-character-maximum calling name in prior services.

feature code: The digits (0-9) or symbols (*, #) used to invoke or access a feature.

intercept: Defined in [Ref 5] (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 Access Point (IAP): A point within a telecommunication system or VoIP network where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed.

intercept subject: A telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the intercept subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

Law Enforcement Agency (LEA): A government entity with the legal authority to conduct electronic surveillance (e.g., the Federal Bureau of Investigation or a local police department).

leg: A representation of a telecommunication path towards some addressable entity.

media stream: The stream of Real Time Protocol (RTP) packets using a specific destination transport address. There is a media stream per media announcement in the SDP of a call. In RTP terminology, an RTP session is the same as a media stream.

origin: See *call-identifying information*.

origination: An outgoing call attempt.

release: Ending of a call or session as indicated by call signaling.[7]

session: When used alone (e.g., not "RTP session"), the exchange of data between participants or systems using the Session Initiation Protocol (SIP) protocol. For instance, a call is an example of a session.

SIP dialog: A peer-to-peer SIP relationship between two UAs that persists for some time. A SIP dialog is established by SIP messages. A SIP dialog is identified by a call identifier, local tag, and remote tag.

SIP Direct Signal Reporting (SIP-DSR): Reporting of SIP subject access and network signaling to LEA(s) via encapsulation (rather than mapping of parameters by a CII-MF).

subject: See *intercept subject*.

surveillance: See *electronic surveillance*.

Telecommunications Service Provider (TSP): An entity that provides telecommunication services to Customers and other users. A Telecommunications Service Provider may or may not operate a network. A Telecommunications Service Provider may or may not be a Customer of another Telecommunications Service Provider.

termination: An incoming call attempt. See also *call-identifying information*.

transmission: The act of transferring communications from one location or another by a wire, radio, electromagnetic, photo electronic, or photo optical system.

User Agent (UA): A logical entity that can act as both a user agent client and user agent server.

wireline: Refers to traditional wire-based telephone service.

3.2 Acronyms

AAA	Administration, Authorization, and Authentication
AMPS	Advanced Mobile Phone System
ANS	American National Standard
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One [Ref 10]
ATIS	Alliance for Telecommunication Industry Solutions
B2BUA	Back-to-Back User Agent
C	Conditional (parameter)
CALEA	Communications Assistance for Law Enforcement Act
CC	Call Content
CC-APDU	Call Content Delivery Application Protocol Data Unit
CC-IAP	Call Content Intercept Access Point
CCC	Call Content Channel
CF	Collection Function
CII	Call-Identifying Information
CII-IAP	Call-Identifying Information Intercept Access Point
CII-MF	CII Mediation Function
CMS	Communication Management System
CPE	Customer Premise Equipment
DDE	Dialed Digit Extraction

[7] RFC 3261 (SIP) [Ref 6] uses the term *terminate* to mean the ending or release of a session.

DF	Delivery Function
DNIC	Data Network Identification Code
DSR	Direct Signal Reporting
eCNAM	Enhanced Calling Name
FCC	Federal Communications Commission
GPS	Global Positioning System
GSM	Global System for Mobile (telecommunications)
IAP	Intercept Access Point
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LAES	Lawfully Authorized Electronic Surveillance
LAESP	LAES Protocol
LEA	Law Enforcement Agency
LI	Lawful Intercept
M	Mandatory (parameter)
MAC	Media Access Control
MF	Mediation Function
MIME	Multipurpose Internet Mail Extensions
MOC	Mandatory/Optional/Conditional
MSRP	Message Session Relay Protocol
O	Optional (parameter)
PDU	Protocol Data Unit
PTSC	Packet Technologies and Systems Committee
PSTN	Public Switched Telephone Network
RCS	Rich Communications Services
RFC	Request For Comments
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SE	Subject Equipment
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SIP-DSR	SIP Direct Signal Reporting
SMS	Short Message Service
SRTP	Secure Real-Time Transport Protocol
SSRC	Synchronization Source identifier
STI	Secure Telephone Identity
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TN	Telephone Number
TSP	Telecommunication Service Provider
UA	User Agent
UDP	User Datagram Protocol

URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

3.3 Definitions for “Mandatory,” “Optional,” & “Conditional” Parameters

The value in the Mandatory / Optional / Conditional (MOC) column in the LAESP Message Parameter tables in this document (e.g., in Clause 6, Annex B, Annex D, and Annex G) indicates whether inclusion of the indicated parameter in the indicated message is Mandatory (M), Optional (O), or Conditional (C).

- A *Mandatory (M)* value means that the sender of the message shall always include this parameter in the message.
- An *Optional (O)* value means that the sender of the message may include this parameter in the message.
- A *Conditional (C)* value means that the sender of the message shall include this parameter in the message when the conditions specified in the Usage column are met.

4 Electronic Surveillance Architecture

4.1 Electronic Surveillance Model

The functions needed to perform LAES are broadly categorized as access, delivery, collection, service provider administration, and law enforcement administration. These functions are described herein without regard to their implementation. The relationship between these functional categories is shown in **Error! Reference source not found.**. As shown, the Access Function, Delivery Function, and Service Provider Administration Function are the responsibility of the TSP, and the Collection Function and Law Enforcement Administration Function are the responsibility of the LEA. The use of these functions to perform an interception is initiated by receipt of a specific lawful authorization.

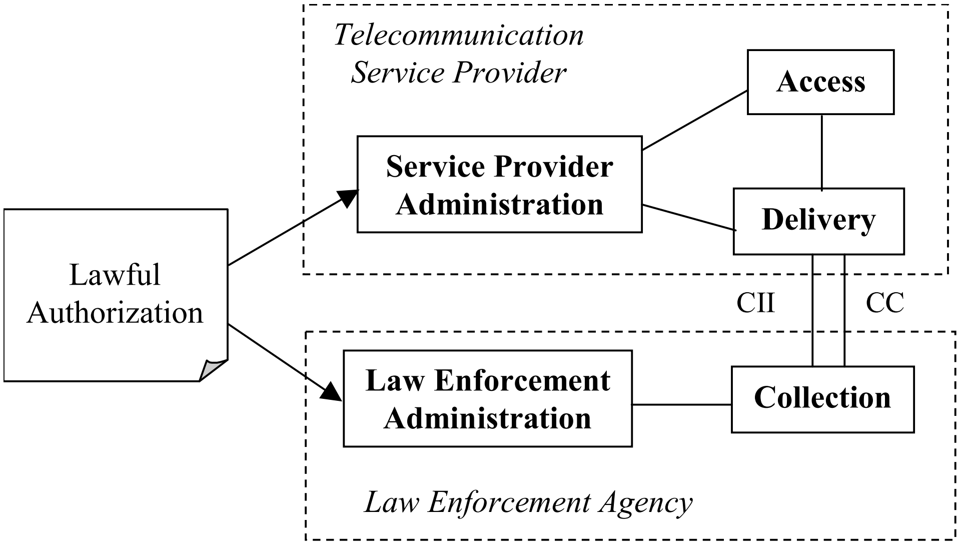


Figure 4.1: Electronic Surveillance Model

The *Access Function*, consisting of one or more Intercept Access Points (IAPs), accesses and intercepts an intercept subject’s communications and CII unobtrusively. The IAPs may vary between TSPs.

The *Delivery Function (DF)* delivers intercepted communications to one or more Collection Functions. The Delivery Function shall deliver intercepted communications in the form of *CC* (such as voice communications) and *CII* (such as calling party identities and called party identities).

The *Collection Function (CF)* collects and analyzes the CC and CII received from the Delivery Function.

The *Service Provider Administration Function* controls the TSP's Access Function and Delivery Function.

The *Law Enforcement Administration Function* controls the LEA's Collection Function.

4.2 Functional Electronic Surveillance Architecture

Error! Reference source not found. shows a general functional Lawful Intercept (LI) architecture for VoIP where both CC and CII are intercepted and delivered to LEAs. This functional architecture assumes that one TSP is providing both Call Control and packet transport. Three domains are identified[8]:

- *Subject Domain*: Consists of the subject's terminal, network access equipment-facilities, and associated functions.
- *Network Domain*: Consists of the carrier's network equipment-facilities and associated functions.
- *Law Enforcement Domain*: Consists of LEAs' LI collection equipment-facilities and associated functions.

The Network Domain includes the following functions:

- *CII Access Functions*: One or more functions in the TSP's network responsible for isolating and presenting CII to the CII Delivery Function.
- *CC Access Functions*: One or more functions in the TSP's network responsible for isolating and presenting CC to the CC Delivery Function.
- *CII Delivery Function*: A function in the TSP's network responsible for delivering the CII, which is specified in a lawful authorization, to the LEAs.
- *CC Delivery Function*: A function in the TSP's network responsible for delivering the CC, which is specified in a lawful authorization, to the LEAs.
- *CII Mediation Function (MF)*: A function in the TSP's network responsible for the presentation[9] of the CII.
- *CC Mediation Function*: A function in the TSP's network responsible for the presentation[10] of the CC. As shown in **Error! Reference source not found.**, the input to a CC Mediation Function is VoIP content and the output is either Time Division Multiplexing (TDM) or a different form of VoIP content (represented as VoIP' in **Error! Reference source not found.**).

The TDM interface shown between the CC Mediation Function and the CC Delivery Function in **Error! Reference source not found.** permits reusability of the CC Delivery Functions already implemented according to J-STD-025-B [Ref 2] and that may be embedded in a VoIP system. Such reusability is an option for the TSPs. According to this specification, TSPs will provide packetized CC to the LEA through the 'e' interface for intercepted VoIP communications.

The following physical demarcation points appear at the boundary between the Network Domain and the LEA Domain:

[8] The basic architecture and concepts of Access Function, Delivery Function, and Collection Function from J-STD-025-B [Ref 2] are assumed.

[9] *Presentation*, as used here, means the form and style of the CII information and includes the conversion or mapping of information from one form or style to another (e.g., SIP signaling [Ref 6] to J-STD-025-B call event reporting [Ref 2]).

[10] *Presentation*, as used here, means the form and style of the CC and includes the conversion of CC from one form or style to another (e.g., VoIP to Voice over TDM).

- *CII Physical Demarcation Point*: Point where CII is presented to the LEAs' procured functions and facilities for delivering CII over the 'e' interface to the LEAs' Collection Function.
- *CC Physical Demarcation Point*: Point where CC is presented to the LEAs' procured functions and facilities for delivering CC over the 'e' interface to the LEAs' Collection Function.

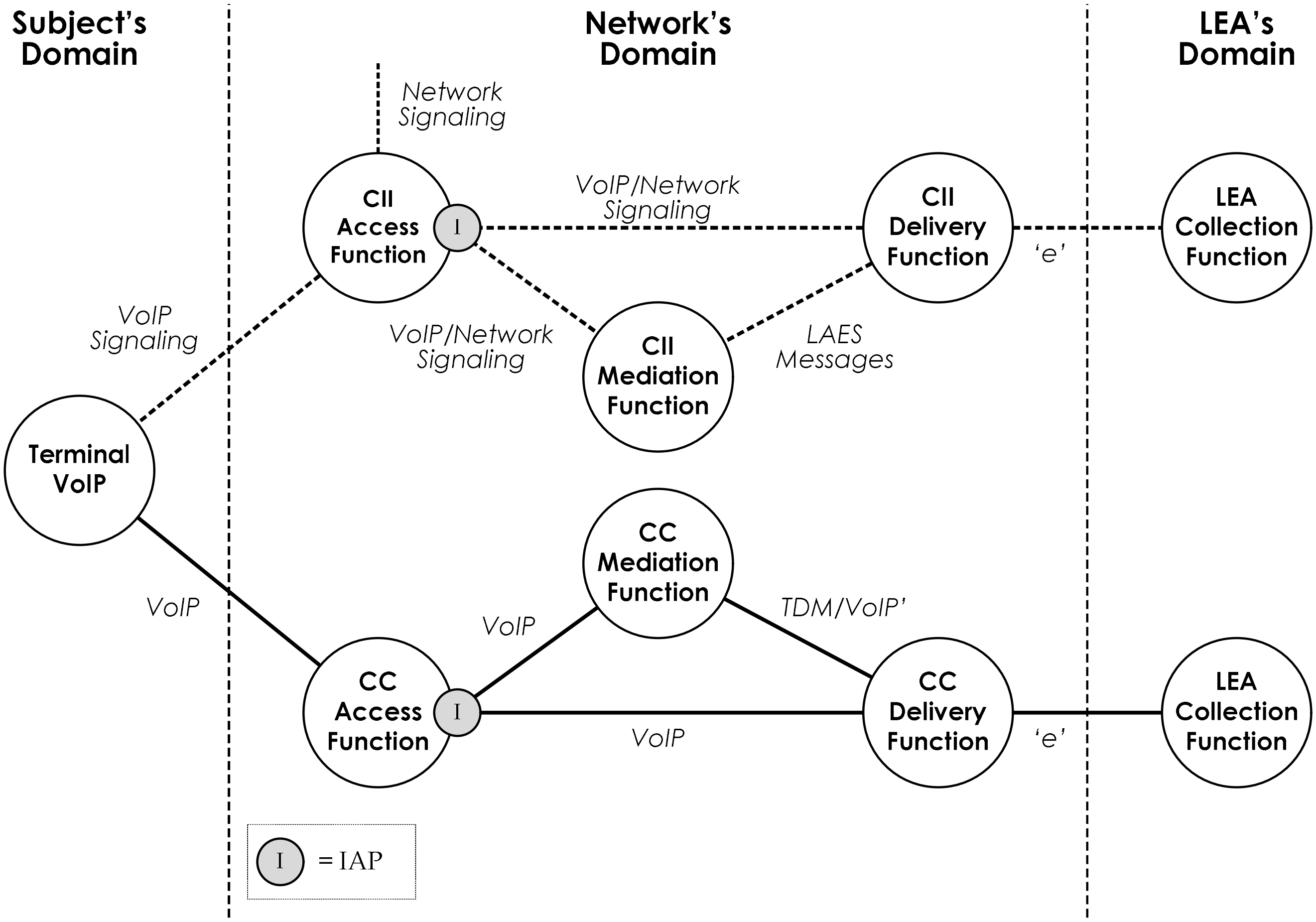


Figure 4.2: Functional LI Architecture for VoIP

Note that the LI architecture presented in **Error! Reference source not found.** is functional in nature and the functions may be distributed and grouped into various network elements and nodes.

The MF and DF are logical functions, not physical entities. They may be implemented in separate physical entities or in a single physical entity.

5 User Perspective (Stage 1)

5.1 Introduction

This Clause presents the user perspective (Stage 1) requirements for Lawfully Authorized Electronic Surveillance for VoIP technologies.

5.2 Surveillance Events

This clause presents communication-related events (termed *surveillance events*) that generate CII. The clause addresses surveillance events associated with lawful authorizations for which only CII is to be delivered to the LEA (see 5.2.1), and surveillance events associated with lawful authorizations for which CC is to be delivered to the LEA (see 5.2.2).

5.2.1 Information Events

5.2.1.1 Call Control-Related Events

The following call control-related events are defined for VoIP calls, call legs, or sessions:

- *Answer*: A VoIP call, call leg or session is answered (e.g., a party has answered the call attempt or a party has accepted a VoIP session initiation request).
- *Origination*: The subject has originated a call, the VoIP network has translated a number for the subject, or the subject sends a VoIP session initiation request.
- *Release*: A completed or attempted VoIP call, call leg, or session has been:
  - Released;
  - Requested to be released; or
  - Reported to have been released.
  - This includes when the VoIP network (e.g., SIP Redirect Server) releases a VoIP call or session to provide updated destination address information.
- *TerminationAttempt*: A VoIP call or session termination attempt to an intercept subject has been detected.

5.2.1.2 Signaling Events

The following call events associated with signaling are defined for VoIP calls:

- *DialedDigitExtraction*: The Dialed Digit Extraction (DDE) event reports digits dialed by a subject when a session is established to another TSP's service for processing and routing. However, CII DDE event reporting does not require a TSP to assure that a connection is with another TSP's service. When a subject has dialed or signaled digits in the VoIP content stream after the session is established from the perspective of the TSP, DDE reporting shall be performed on a per lawful authorization basis. The reporting shall be accomplished by the network isolating and reporting the extracted Dialed Digits as CII to the LEAs, when reasonably available. When CC delivery and DDE are required by the lawful authorization, the network shall isolate and report the Dialed Digits, when reasonably available (see 5.3.1), as CII to the LEAs. A TSP shall support the DDE capability with a toggle feature that can activate/deactivate this capability (per lawful authorization). See Annex F, *Dialed Digit Extraction Scenarios*, for information on DDE solution scenarios. A TSP may report dialed or signaled digits other than those that are call completing and has no obligation to determine which dialed or signaled digits actually complete or could complete a call.
- *DirectSignalReporting*: The VoIP network receives a SIP message from the intercept subject, sends a SIP message to the intercept subject, or sends or receives a SIP message on behalf of the intercept subject.
- *NetworkSignal*: A network signal, tone, or message that provides CII (e.g., busy, reorder, ringing, alerting, message waiting tone or visual indication, call waiting, calling or redirecting information name/number information, displayed text) is initiated, generated, or sent by a network element in the VoIP network to a subject using the facilities under surveillance, or is reported[11] to the VoIP network as having been initiated, generated, or sent toward the subject. It is also sent when a Secure Telephone Identity (STI)

[11] For example, the CMS detects that a signaling message (e.g., a SIP180 Ringing response) has been sent to a Subject by an Associate.

PASSporT signature [Ref 26] is used for authentication, verification, or Divert attestation purposes.

- *SubjectSignal*: A subject using the facilities under surveillance dials or signals to control features or services (e.g., call forwarding, call waiting, call hold, and three-way calling).

5.2.1.3 Feature Use Events

The following call events associated with use of features provided by the TSP are defined for VoIP calls, call legs, or sessions:

- *Connection*: Parties have been added to a subject-initiated conference call or one or more parties have been added to an existing call.
- *ConnectionBreak*: Parties to a subject-initiated conference call have been temporarily removed or permanently dropped from the call or one or more parties have been temporarily removed or permanently dropped from an existing call.
- *Conference Party Change*: This capability allows reporting of parties communicating in a conference, parties removed from a conference, or parties joined to a conference.
- *Redirection*: A call has been redirected by an intercept subject or an intercept subject's service (e.g., forwarded, diverted or deflected).

5.2.1.4 Registration Events

The following registration events (e.g., SIP registration) are defined for VoIP networks:

- *ServingSystem*: An intercept subject or the equipment, facilities, or service of an intercept subject provides addressing information to the VoIP network (e.g., contact information as part of registration and deregistration) to facilitate the establishment of VoIP calls or session.

In Table B.3 and B.21 a SIP REGISTER request and its response may be mapped and reported via separate ServingSystem messages, or the SIP REGISTER request and its response may be mapped and reported via a single ServingSystem message.

5.2.1.5 Media Reporting Events

The following event reports the media characteristics of a call when the characteristics are established or modified. This need not be reported if media characteristics are reported in the media information parameter of another message.

- *MediaAndAddressReporting*: Media characteristics are being established or modified.

5.2.2 Content Events

The following events associated with CC are defined for VoIP calls:

- *CCChange*: Media characteristics are being modified.
- *CCClose*: CC delivery is being disabled.
- *CCOpen*: CC delivery is being enabled.
- *CCUnavailable*: The VoIP network determines that the network does not have access to CC for a call that is under content interception.
- *UUContent*: The *UUContent Message* is a capability used to report CC sent to, or received by, the intercept subject as part of session signaling.
- *CCEncryptionInfo*: Encryption information is available relative to CC delivery.

5.3 Intercept Access Points

With respect to VoIP, IAPs are places in the network where lawful intercept VoIP CII and CC are intercepted. There are two fundamental types of VoIP IAPs:

1. VoIP Call Identifying Information IAPs (CII-IAPs); and
2. VoIP Call Content IAPs (CC-IAPs).

CII-IAPs and CC-IAPs are associated with CII and CC intercept functions that perform the actual interception of call information and content. These CII and CC intercept functions are incorporated into one or more network elements. CII and CC intercept functions may be co-located within the same network element or may be distributed among many network elements.

5.3.1 VoIP CII-IAPs

CII-IAPs intercept CII. CII may be categorized as information directly associated with a call or indirectly associated with a call.

CII is reasonably available if the information is present at the IAP for call processing purposes. With respect to the matters before the Federal Communications Commission (FCC) in [Ref 4], the commission has provided the following additional guidance: CII is “reasonably available” to a TSP if it is present at an intercept access point and can be made available without the TSP being unduly burdened with network modifications. Network protocols -- except LAES Protocol -- do not need to be modified solely for the purpose of passing CII. The specific elements of CII that are reasonably available at the IAP may vary between different technologies and may change as technology evolves.

a) *CII Directly Associated with a Call*: CII directly associated with a call is information that is directly related to the management of an existing call between an intercept subject and the associate(s) to the call (i.e., call signaling information for establishing, managing, and releasing a call). Examples of VoIP LAES information reported as a result of CII directly associated with an existing call are the Origination, TerminationAttempt, and Release surveillance messages.

b) *CII Indirectly Associated with a Call*: CII indirectly associated with a call is information related to, but not directly involved with, the management of an existing call of an intercept subject (e.g., information about where calls can be directed to an intercept subject). An example of VoIP LAES information reported as a result of CII indirectly associated with a call is the ServingSystem message.

5.3.2 VoIP CC-IAPs

VoIP CC-IAPs intercept CC between an intercept subject and the associate(s).

The VoIP CC-IAP provides the intercept capability for the VoIP CC. It intercepts the required CC and presents it to the Delivery Function or to the Mediation Function. The VoIP CC-IAP can reside in a number of places. The VoIP CC-IAP used in a particular network is a TSP design decision. See Annex E, *Example VoIP CC-IAP Locations*, for examples that provide information regarding the location of CC-IAPs in VoIP networks.

When law enforcement is legally authorized to access communications content for an intercept subject, the TSP shall access and deliver communications content, if reasonably available, for the duration of the following VoIP communications:

- Communications originated by, redirected by, and terminated to the intercept subject’s equipment, facilities, or service.
- Communications for two-party calls and multi-party calls, including when the intercept subject places a multi-party call on hold.

5.4 General Capabilities

5.4.1 Intercepted Communications Delivery

Various transport technologies can be used to support the ‘e’ interface between a TSP and law enforcement. Transmission Control Protocol (TCP) [Ref 12] is the protocol preferred by law enforcement for CII and CC delivery over the ‘e’ interface if IP-based delivery is used. If TCP is available, its use is assumed unless a different protocol is agreed to by the LEA and the TSP.

5.4.2 Timing Information

Timing information enables law enforcement agencies to associate CII with the CC. Timing information includes two elements:

a) *Event Time-stamp*: Each surveillance message shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CII triggering event was detected and the time recorded in the time-stamp).

b) *Event Timing*: Surveillance messages shall be sent to the LEA within a defined amount of time after the information pertaining to the CII triggering event is available at the IAP.

The following timing requirements shall apply to the delivery of CII:

- Each surveillance message shall be sent by the Delivery Function to the Collection Function within eight (8) seconds of receipt by the IAP of the information pertaining to the CII triggering event at least 95% of the time.
- Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CII event triggering the surveillance message was detected, and is reported to at least the thousandth of a second. The time-stamp shall report:
    - coordinated universal time; or
    - local time with the local time differential from coordinated universal time.

The following timing requirements shall apply to the delivery of VoIP CC:

- Time-stamps shall be provided with encapsulated intercepted packets delivered to the Collection Function.
- VoIP CC shall be transmitted by the IAP towards the Collection Function concurrently with its interception. The interval to commence transmission of VoIP CC from the IAP towards the Collection function after commencement of interception shall be limited to the computational delay of the IAP.

5.4.3 Performance and Quality

The quality of the ‘e’ interface is driven by the negotiation between the TSP and the LEA.

5.4.4 Security and Integrity

The FCC issued a Report and Order in March 1999 (CC Docket 97-213) [Ref 19] that “establish(ed) the systems security and integrity regulations that telecommunications carriers must follow to comply with section 105 of CALEA [Ref 1].”

To facilitate compliance with the Report and Order, the following should be considered:

a) The ability to create, review, update, or delete any aspect of a lawfully authorized surveillance shall be limited, through authorization and authentication, to users with proper authority. Surveillance related activities shall be logged to help protect from unauthorized usage and to provide an audit trail.

b) Access to any file, record, or report containing data that would compromise the ability to protect the information regarding the lawful interception of communications and access to CII shall be restricted to authorized users. Examples of such files, records, or reports are:

   - The log file of surveillance administrative activities discussed above;
   - Any file containing information about existing or past surveillances;
   - Call detail records generated due to delivery of CC or CII that would allow an association of a Telephone Number (TN) under surveillance with an LEA collection site; and
   - Billing records generated due to delivery of CC or CII that would allow an association of a TN under surveillance with an LEA collection site.

c) Messages that establish the link between the Delivery and Collection Functions shall not contain information identifying the intercept subject.

Further discussion of management plane security can be found in ATIS-0300260.1998(S2018) [Ref 17] and ATIS-0300276-2008(R2017) [Ref 18]. Further discussion of signaling plane security is beyond the scope of this document.

5.4.5 Quantitative Aspects

All capabilities described in this Standard are subject to the capacity requirements required by CALEA.

5.4.6 Encryption

If the TSP uses encryption in the network, the TSP shall deliver the intercepted communications to the LEA in unencrypted form or provide the encryption keys and specify the encryption method. If the intercepted communications are available at the IAP in both encrypted and unencrypted forms, the TSP shall provide the unencrypted form to the LEA.

Although the preference of law enforcement is to receive the intercepted communications in unencrypted form, the CCEncryptionInfo message can be used to convey the information needed to decipher encrypted communications content.

6 Network Perspective (Stage 2)

This clause identifies the triggering events and usage for the VoIP CII event messages, identifies and describes the information to be reported with each VoIP CII event message, and also describes the application level CC delivery format and associated delivery information. The LAES messages and parameters defined in Clause 6, *Network Perspective,* are delivered according to the abstract syntax notation (ASN.1) found in Annex A.

Content included in a SIP message [e.g., a Short Message Service (SMS) message, audio, video, image] shall be reported via the UUContent message only as required by a lawful authorization for content interception. With respect to SIP, ‘application/SDP’ body information shall be reported as CII with the LAES messages.

6.1 *Call Identifying Information Surveillance Messages*

The messages described in this clause emulate for a VoIP environment the LAES of Public Switched Telephone Network (PSTN) that was specified in J-STD-025-B [Ref 2]. The J-STD-025-B [Ref 2] messages have been enhanced to support VoIP.

6.1.1 Answer Message

The *Answer Message* reports when a call, call leg, or session has been answered. Transmission is usually cut-through in both directions to the intercept subject or its agent.

The Answer message shall be triggered when:

- The intercept subject answers a call, call leg, or session (including calls or sessions for which the intercept subject answers when alerted in response to a previous call or session);
- A call or session originated by the intercept subject is answered; or
- A call or session for which the intercept subject is the destination is terminated and answered at another endpoint or agent due to special call handling or redirection by the Communication Management System (CMS) -- e.g., call forwarding, voicemail.

The Answer message includes the following parameters:

Table 6.A: Answer Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system.
AnsweringPartyIdentity	C	Include, when known, to identify the answering party or agent.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of the terminal of an intercept subject with personal mobility. The level of detail of the reported location information should be commensurate with the level of detail of the location information available for use within the VoIP network.
AnsweringMediaInformation	C	Included, when the answering party's media information is known to identify the Session Description Protocol (SDP) [Ref 9] information for the answering party.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the Answer message.

6.1.2 CCChange Message

The *CCChange Message* reports a modification to the media characteristics (e.g., network addresses, media format) of an existing call or session. The CCChange message is generated for surveillances that require the delivery of packetized CC and provides the LEA collection equipment with the updated information needed to process the packetized CC. The CCChange message shall be triggered for surveillances that require the delivery of CC when CC is delivered in packetized form and an IAP determines that the media characteristics of an existing call or session involving the intercept subject's equipment, facilities, or service are being modified.

With regard to reporting media information, the CCChange message is not required if the changed media information (e.g., SDP information) is reported via other messages (e.g., MediaAndAddressReporting message, SubjectMediaInformation in the Origination message). A CCChange message may be generated individually for the subject and each associate or as a single message for the subject and all associates.

The CCChange message includes the following parameters:

Table 6.B: CCChange Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Included to identify a particular VoIP call or session for the media stream being delivered as CC.
DeliveryIdentifier Choice of: CCCIdentity or CCAddress	M	Included to uniquely identify the media stream being delivered. Use the choice CCAddress for the CC-APDU delivery of packet CC per 6.2.2 of this standard.
SubjectMediaInformation	C	Included to identify the SDP information for the intercept subject, when the intercept subject's media information is being reported.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate's media information is being reported.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the CCChange message.

When CC is not available for reporting when requested by a lawful authorization, a CCUnavailable message shall be sent as specified in 6.1.5, and a CCChange message shall not be sent.

6.1.3 CCClose Message

The *CCClose Message* reports when CC delivery is being disabled.

The CCClose message shall be triggered when the delivery of CC is being disabled for a VoIP call, call leg or session, such as when:

- The intercepted VoIP call or session is released;
- The intercepted VoIP call leg is released;
- The intercepted VoIP call or session is merged with another intercepted VoIP call or session; or
- The intercepted VoIP call leg is merged into another intercepted VoIP call or session.

The CCClose message may be triggered when an early release of the delivery connection by the Collection Function or intervening network is detected.

A CCClose message may be generated individually for the subject and each associate or as a single message for the subject and all associates.

It is desirable that the CCClose message not be generated until after the last Call Content Delivery Application Protocol Data Unit (CC-APDU) has been sent. The CCClose message includes the following parameters:

Table 6.C: CCClose Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Included to identify a particular VoIP call or session for the media stream being delivered as CC.
DeliveryIdentifier Choice of: CCCIdentity or CCAddress	M	Included to uniquely identify the media stream being delivered. Use CCCIdentity with delivery of circuit-switch CC per J-STD-025-B [Ref 2]. Use CCAddress with CC-APDU delivery of packet CC per 6.2.2 of this standard.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the CCClose message.

When CC is not available for reporting when requested by a lawful authorization, a CCUnavailable message shall be sent as specified in 6.1.5, and a CCClose message shall not be sent.

6.1.4 CCEncryptionInfo Message

The CCEncryptionInfo message shall be sent when there is a need to pass decryption information associated with intercepted content.

> Note: This standard only defines the delivery of SRTP session key related information. Delivery of SRTP master key related information and other cryptographic protocol related information is not defined in this standard.

Table 6.D: CCEncryptionInfo Message Parameters

Parameter	MOC	Description
CaseIdentity	M	Identifies the intercept subject.
IAPSystemIdentity	C	Included to identify the system reporting the encryption information, when the underlying data carriage does not imply that system.
Timestamp	M	Identifies the date and time that the event (the creation of the encryption information) was detected.
CallIdentity	M	Uniquely identifies a VoIP call or session to which this encryption information applies.
CryptoContext	C	If further information is needed to associate the encryption information with a specific RTP session or stream, this parameter identifies the context to which this encryption message applies. This is discussed below.
Cipher	M	The name of the cipher. See further information below.
Key	M	The key needed to decipher.
Salt	C	The salt value. Include if the cipher requires a salt value.
KeyEncoding	M	Shall explicitly indicate the encoding of the key.

The cipher parameter names the cipher. The cipher names should follow the conventions for cipher names in SRTP. SRTP [Ref 23] provides for two default ciphers: AES in counter mode, and AES in f8-mode. These are denoted by placing one of the strings “AES_128_CM” or “F8_128” in the Cipher parameter. Usage of the CCEncryptionInfo Message with SRTP

This clause defines the usage of the CCEncryptionInfo for SRTP and the subparameters of the optional CryptoContext parameter. One CCEncryption is sent for each SRTP session or stream; additional CCEncryptionInfo messages may need to be sent during the session if rekeying occurs.

For SRTP, the RTP payload is encrypted with a session key, salt, and cipher algorithm, and thus can be descrypted with the same. The CryptoContext parameter contains subparameters that are specific to SRTP. With one exception, the CryptoContext parameter is needed to convey additional information needed for decryption; the one exception is where all RTP sessions of the call are encrypted with the same session key, in which case the CryptoContext parameter can be omitted. The subparameters are defined in Table 5.

Table 6.E: CryptoContext SRTP Subparameters

Subparameter	MOC	Description
destIpAddress	M	The destination IP address defining the SRTP session
destPort	M	The destination transport defining the SRTP session
sSRC	C	If session keys are unique to an SRTP stream, this shall be included and contains the Synchronization Source identifier (SSRC) identifier of the stream
sequenceNum	C	If rekeying occurs, this parameter shall be included. the sequenceNumber parameter in CyptoContext would be used to specify the lowest sequence number prior to rollover of the RTP packet to which the new information applies.
tail	M	Indicates the number of bytes (including any padding) at the end of the SRTP packet after the encrypted RTP payload.. These bytes consist of the optional Master Key Identifier (MKI) and authentication tag.

SRTP also provides the option of rekeying, meaning that rather than using one or more static session keys, new session keys can be derived during a call. If rekeying is deployed, one or more new CCEncryptionInfo messages shall be sent for each instance of rekeying. This standard does not define how the DF obtains access to the information needed for the CCEncryptionInfo message.

6.1.5 CCOpen Message

The *CCOpen Message* associates all VoIP media stream being delivered as CC with a particular call or session instance.

The CCOpen message shall be triggered when VoIP CC delivery is being enabled. This should occur after a call or session is initiated or requested (as an intercept subject origination or termination attempt), but prior to communications between the subject and associate.

A CCOpen message may be generated individually for the subject and each associate or as a single message for the subject and all associates.

Delivery of CC is dependent upon appropriate provisioning of the e-interface.

It is desirable that the commencement of CC Delivery CC-APDUs for a given VoIP call not occur until after the CCOpen message defining the content stream is generated on the delivery interface. The delivery of CC-APDUs shall continue until either the VoIP call or surveillance order for the subject terminates.

The CCOpen message includes the following parameters:

Table 6.F: CCOpen Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Included to identify a particular VoIP call or session for the media stream being delivered as CC.
DeliveryIdentifier Choice of: CCCIdentity or CCAddress	M	Included to uniquely identify the set of media streams being delivered. Use CCCIdentity with delivery of circuit-switch CC per J-STD-025-B [Ref 2]. Use CCAddress with CC-APDU delivery of packet CC per 6.2.2 of this standard.
SubjectMediaInformation	C	Included to identify the SDP information for the intercept subject, when the intercept subject’s media information is being reported.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate’s media information is being reported.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the CCOpen message.

When CC is not available for reporting as requested by a lawful authorization, a CCUnavailable message shall be sent as specified in 6.1.5, and a CCOpen message shall not be sent.

6.1.6 CCUnavailable Message

The *CCUnavailable Message* reports the unavailability of CC for a call under CC interception.

The CCUnavailable message shall be triggered if the VoIP network is aware that the network does not have access to content for a call that is under CC interception. Circumstances in which the VoIP network is not aware that the network does not have access to the content for a call that is under CC interception will not cause the CCUnavailable message to be triggered.

The CCUnavailable message includes the following parameters:

Table 6.G: CCUnavailable Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg or session within a system.
UnavailabilityReason	C	Included to indicate the reason that CC was not available to the VoIP network, when known.
EncapsulatedSignalingMessage	C	The SIP message received that stimulated the sending of the CCUnavailable message.

6.1.7 Connection Message

The *Connection Message* reports the addition of one or more parties to an existing call (i.e., a leg is connected to the call so that communications can occur). The Connection message reports the parties to a subject-initiated conference call. Added parties could be new parties or parties who were previously on hold.

The Connection message shall be triggered when:

- The intercept subject’s service changes connections to allow parties to be added to a call or to a subject-initiated conference under surveillance; or
- There are party join changes to a conference communication during a subject-initiated conference call.

The Connection message, either alone or in combination with the ConnectionBreak message, is used to satisfy the requirement to report the parties to a subject-initiated conference call. When the Connection message is used alone, it identifies all parties able to communicate with each other in a call.

The Connection message is not required when the information reported would be redundant with the information reported by other surveillance messages.

The Connection message includes the following parameters:

Table 6.H: Connection Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system (see text beneath this table).
ConnectionInformation One or more of:	M	
ConnectedParties		Identifies parties able to communicate to each other in a call -- including any added party(ies).
NewParties		Identifies one or more parties added to a call, including new parties and parties who have been retrieved from a held state.
ConnectedMediaInformation	C	*Included, when the media information is known and not previously reported, to identify the SDP information for the retrieved or added party.*
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the Connection message.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call represented by a single call identity such that a Connection message is reported, the Connection message shall include a single call identity representing the multi-party call.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call with multiple individual call identities such that a Connection message is reported, the Connection message shall include the call identities associated with the multi-party call.

6.1.8 ConnectionBreak Message

The *ConnectionBreak Message* reports when one or more parties are removed from an existing call (i.e., a leg is removed from a call so that communications cannot occur). The ConnectionBreak message reports when parties to a subject-initiated conference call are removed (e.g., temporarily or permanently).

The ConnectionBreak message shall be triggered when:

- The intercept subject's service changes connections to remove parties from a call or from a subject-initiated conference under surveillance; or
- There are party hold or drop changes to a conference communication during a subject-initiated conference call.[12]

The ConnectionBreak message, in combination with the Connection message, is used to satisfy the requirement to report the parties to a subject-initiated conference call.

The ConnectionBreak message is not required when the information reported would be redundant with the information reported by other surveillance messages.

[12] If the subject places a two-party call with associate A on hold, the subject is reported as the removed party. If the subject places a conference call with associates A and B on hold, the subject is reported as the removed party.

The ConnectionBreak message includes the following parameters:

Table 6.I: ConnectionBreak Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system (see text beneath this table).
ConnectionBreakInformation	M	
One or more of:		
RemovedParties		Identifies parties removed (e.g., due to hold service) from a call.
RemainingParties		Identifies parties remaining in a call -- excluding the removed party(ies), dropped party(ies), or both.
DroppedParties		Identifies parties permanently disconnected from a call.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the ConnectionBreak message.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call represented by a single call identity such that a ConnectionBreak message is reported, the ConnectionBreak message shall include a single call identity representing the multi-party call.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call with multiple individual call identities such that a ConnectionBreak message is reported, the ConnectionBreak message shall include the call identities associated with the multi-party call.

6.1.9 ConferencePartyChange Message

The ConferencePartyChange message reports a change to the status of the parties in a subject-initiated conference call, when this information is known at the IAP. The ConferencePartyChange message reports the following conditions:

- When the subject adds a third, or additional parties, to an existing call to form a conference call;
- When a party in a subject-initiated conference call is placed on hold, or retrieved from hold;
- When a party in a subject-initiated conference call is dropped from the conference call.

(Note that the Release message is used to indicate when a party in a subject-initiated conference call is dropped, released, or otherwise disconnects from the conference call.)

The ConferencePartyChange message shall be triggered for calls under interception when one or more of the following events are detected by an IAP:

- The subject adds a third, or additional parties, to an existing to call to form a conference call;
- A party in a subject-initiated conference call is placed on hold;[13]
- A party in a subject-initiated conference call is retrieved from hold;
- A party in a subject-initiated conference call is dropped from the conference call.

The ConferencePartyChange message includes the following parameters:

[13] If the subject places a conference call with associates A and B on hold, the subject is reported as the removed party.

Table 6.J: ConferencePartyChange Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system (see text beneath this table).
CommunicatingParties	O	Included when known, to identify all communicating party(ies) on the conference call established by the intercept subject's service. This parameter may appear independently or in combination with other parameters.
RemovedParties	O	Included when known, to identify a previously communicating party(ies) on the conference call established by the subject's service that is removed (placed on hold) from the call. This parameter may appear independently or in combination with other parameters.
JoinedParties	O	Included when known, to identify a new communicating call party(ies) on the conference call established by the intercept subject's service; the joined party(ies) has begun communicating on the call. This parameter may appear independently or in combination with other parameters.
DroppedParties	O	Include when known to identify dropped (permanently disconnected) party(ies) from the conference call. This parameter may appear independently or in combination with other parameters.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the ConferencePartyChange message.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call represented by a single call identity such that a ConferencePartyChange message is reported, the ConferencePartyChange message shall include a single call identity representing the multi-party call.

When an event (e.g., call hold, call retrieve) occurs related to a multi-party call with multiple individual call identities such that a ConferencePartyChange message is reported, the ConferencePartyChange message shall include the call identities associated with the multi-party call.

6.1.10 DialedDigitExtraction Message

The *DialedDigitExtraction Message* reports intercept subject-dialed or signaled digits in the VoIP CC stream after the session is established from the perspective of the TSP and connected to another TSP's service for processing and routing. The digits may be reported on a digit-by-digit basis, accumulated until a buffer is filled, accumulated until a timer expires, or accumulated until the call is released. The DDE capability includes a toggle feature that can activate/deactivate this capability per lawful authorization.

Subject-dialed or signaled digits that appear in SIP messages, such as INFO, after the session is established, may be reported in the DDE message.

The DialedDigitExtraction message shall be triggered when covered by the lawful authorization and:[14]

- Digit-by-digit reporting is performed and a digit is detected; or
- Digit accumulation is performed and the first of the following occurs:
  a) A maximum of 32 digits have been accumulated in the buffer;
  b) 20 seconds have elapsed since detection of the first digit in the buffer; or
  c) The call or session is released.

The DialedDigitExtraction message includes the following parameters:

[14] Note that Dialed Digit Extraction may not be possible in all situations or implementations, as it is dependent upon how the digits are included in the content stream and the capabilities available in the network to detect the digits. See Annex F for a discussion on the issues.

Table 6.K: DialedDigitExtraction Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system.
Digits	M	Identifies the post-cut-through digits dialed or signaled by the intercept subject. Examples include: “12345,” “*123,” and “#345.”

6.1.11 DirectSignalReporting Message

The *DirectSignalReporting (DSR) Message* reports when the VoIP network receives a SIP message from the intercept subject, sends a SIP message to the intercept subject, or sends or receives a SIP message on behalf of the intercept subject.

Appropriateness of the use of the DSR message for reporting CII depends on the interception architecture, as well as the service architectures and signaling protocols involved (see 6.4).

If the SIP message sent to or received from the subject is identical to the SIP message sent to or received from the associate, only the SIP message sent to or received from the subject is required to be reported.

Table 6.L: DirectSignalReporting Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Included to uniquely identify a call, call leg, or session within a system, when the encapsulated SIP signaling message is associated with a particular call.
Direction	M	Identifies whether the encapsulated SIP signaling message was sent to or received from the Intercept Subject or on behalf of the Intercept Subject.
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of the terminal of an Intercept Subject with personal mobility. The level of detail of reported location information should be commensurate with the level of detail of the location information available for use within the VoIP network.
EncapsulatedSignalingMessage	M	The SIP message that stimulated the sending of the DirectSignalReporting message.

6.1.12 MediaAndAddressReporting Message

The *MediaAndAddressReporting Message* reports the exchange (initiation or modification) of media characteristics (e.g., network addresses, media format) or a contact address, or both media characteristics and contact address, for VoIP calls or sessions involving the intercept subject’s equipment, facilities or service. The exchange or modification could be initiated by the intercept subject, an associate, or the VoIP network (e.g., CMS).

The MediaAndAddressReporting message shall be triggered when:

- Media characteristics are signaled during the establishment of media for a VoIP call or session involving the intercept subject’s equipment, facilities, or service; or
- Media characteristics or a new contact address, or both media characteristics and a new contact address, are signaled during the successful modification of media or the modification of a contact address, or both, for an existing VoIP call or session involving the intercept subject’s equipment, facilities, or service.

This message is not required when the information reported would be redundant with the information reported by other LAES messages.

A MediaAndAddressReporting message may be generated individually for subject and each associate or as a single message for the subject and all associates.

The MediaAndAddressReporting message includes the following parameters:

Table 6.M: MediaAndAddressReporting Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system.
SubjectMediaInformation	C	Included to identify the SDP information for the intercept subject, when the intercept subject's media information is being reported.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate's media information is being reported.
RedirectedToPartyMediaInformation	C	Included to identify the SDP information for a RedirectedToParty, when the MediaAndAddressReporting message is used to report media characteristics resulting from a Redirection.
SubjectContactAddresses	C	Included when one or more contact addresses (e.g., SIP Contact headers) are provided by the intercept subject, to report the intercept subject's contact address(es). The information need not be reported if reported via other messages.
AssociateContactAddresses	C	Included when one or more contact addresses (e.g., SIP Contact headers) are provided by an associate, to report the associate's contact address(es). The information need not be reported if reported via other messages.
RedirectedToPartyContactAddresses	C	Included when one or more contact addresses (e.g., SIP Contact headers) are provided by a RedirectedToParty, to report the RedirectedToParty's contact address. The information need not be reported if reported via other messages.
MediaAndAddressReportingCause	M	Identifies the reason for the generation of the MediaAndAddressReporting message (e.g., ACK, 183 Call Progress, UPDATE [Ref 20]).
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the MediaAndAddressReporting message.

6.1.13 NetworkSignal Message

The *NetworkSignal Message* reports signals, tones, or messages initiated, generated, or sent by the VoIP network toward the intercept subject; or signals, tones, or messages reported to the VoIP network as having been initiated, generated, or sent toward the intercept subject.

The NetworkSignal message shall be triggered when the VoIP network initiates, generates, sends, or receives information that indicates the initiation, generation, or sending of:

Group A: Information sent to the intercept subject:

- Alerting toward the intercept subject;
- Other network signaling toward the intercept subject, such as SIP early media and the equivalent of tones (e.g., busy, ringback);
- A call-associated display message toward the intercept subject (e.g., identifying the calling party name and number, providing a message waiting indicator, providing call progress). This includes the eCNAM Extended Name;
- A message toward the intercept subject's equipment to instruct it to remove tones or visual indicators; or

Group B: Intercept subject VoIP network receives additional information related to the call (nothing is sent to the intercept cubject).

Information or signaling is received from another endpoint (i.e., an associate's device or agent) relating to an intercept subject-initiated call;

- When an STI PASSporT is signed, verified, or attested (in the originating or terminating side).

The NetworkSignal message includes the following parameters:

Table 6.N: NetworkSignal Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Included to uniquely identify a call, call leg, or session within a system, when the network signal is associated with a particular call.
SignaledToPartyIdentity	C	Included to identify the signaled-to party, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate's media information is being reported. The information need not be reported if reported via other messages (e.g., MediaAndAddressReporting message).
Signal	M	Identifies the signal, tone or message initiated, generated or sent by the VoIP network toward the intercept subject, or the signal, tone or message reported to the VoIP network that was initiated, generated or sent toward the intercept subject. Also identifies a Secure Telephone Identity (STI) PASSporT signature, whenprovided for authentication, verification, or Divert attestation purposes.
One or more of the following:		
AlertingSignal	C	Included for an alerting signal.
SubjectAudibleSignal	C	Included for an audible tone.
TerminalDisplayInfo	C	Included for a display message, including eCNAM or SHAKEN as described below this table.
Other	C	Included for any other network signal (e.g., "call forwarding", "hold", "retrieve", "refer") that triggers this message. See also eCNAM or SHAKEN description below this table.
AssociateContactAddresses	C	Included when one or more contact addresses are provided by an associate.
EncapsulatedSignalingMessage	C	When a SIP message stimulates the sending of the NetworkSignal message, that SIP message shall be included in the EncapsulatedSignalingMessage parameter. When the use of SHAKEN causes the NetworkSignal message to be triggered, this EncapsulatedSignalingMessage will include the SIP message that contains the SIP Identity header which carries SHAKEN information.

The eCNAM Extended Name [Ref 22], if present, shall be delivered in the TerminalDisplayInfo parameter or the Other parameter based on the following considerations:

- The Extended Name that is actually sent to the intercept subject device is mapped into the callingName subparameter of the terminalDisplayInfo parameter. This would also include the values "Anonymous" and "Unavailable" when needed [Ref 22].
- If the Extended Name available at an IAP in the VoIP network is different from the Extended Name presented to the intercept subject (e.g., truncated) the Extended Name available at an IAP in the VoIP network is mapped to the Other parameter.
- eCNAM Extended Name reporting in other call scenarios, such as call forwarding, is not addressed in this scenario.

If SHAKEN (STIR) (Ref 24) is supported in the originating network the LI reporting of SHAKEN applies in the originating network and likewise if SHAKEN (Verification) is supported in the terminating network, then the LI reporting requirements apply in the terminating network. When the SP network performs SHAKEN validation with signaling resulting from analytics or SHAKEN, these results shall be delivered in the TerminalDisplayInfo parameter or the Other parameter based on the following considerations.

- When the CMS performs SHAKEN validation with signaling resulting from analytics or SHAKEN, the following shall be mapped into the generalDisplay subparameter of the terminalDisplayInfo parameter: “TN-Validation-Passed”, “TN-Validation-Failed”, or “No-TN-Validation”. In addition, the following applies:
    - For the case of TN-Validation-Failed, the Other parameter shall be included and coded with the “SHAKEN status code 4xx" or "SHAKEN status code 5xx” when validation fails in a terminating network.

- The Other parameter shall be used to indicate that SHAKEN information is present.

6.1.14 Origination Message

The *Origination Message* reports VoIP call or session origination attempts or number translations for the intercept subject. More than one Origination message is possible for a single call or session attempt when numbers are expanded or translated.

The Origination message shall be triggered when:[15]

- A call, call leg, or session originated by the intercept subject is routed toward a destination within the accessing system;
- A call, call leg, or session originated by the intercept subject is routed toward a destination on an external public or private network;
- A call session originated by the intercept subject is forked to multiple destinations;
- The destination address for a call, call leg, or session originated or provided by the intercept subject is translated from one address to another address (e.g., for speed number expansion or toll free-number translation);

The Origination message includes the following parameters:

[15] The Origination message triggers are intended to cover all cases of call originations, including successful and unsuccessful call origination attempts and calls routed within and outside of the accessing network.

Table 6.O: Origination Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system. A unique call identity may be generated for the Origination message, which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call or session (e.g., three-way calling or conference calling for some systems).
CallingPartyIdentity	C	Included when more specific than the intercept subject identity associated with the CaseIdentity, to identify the originating party. If other identities of the calling party are contained in the SIP signaling seen at the IAP (e.g., From, Contact, P-Asserted-Identity), those header fields shall be reported here using the sipHeader component.
CalledPartyIdentity	C	Included when known to identify the called party (e.g., result of final translation if any). This is not present for calls or sessions that were partially dialed. In addition to reporting the request URI, if other identities of the called party are contained in the SIP signaling seen at the IAP (e.g., To), those header fields shall be reported here using the sipHeader component.
Input One of the following:	M	Identifies specific user or translation input including when a call or session is attempted without input (e.g., hot line).
UserInput		Included to identify the input digits, address or name signaled by the calling party to originate the call, when known. Examples include: *generic*: “hot line,” “123” *specific*: “sip:UserA@here.com”
TranslationInput		Included to identify the input to an address translation process, when an address translation occurs. Examples include: *generic*: “hot line,” “123” *specific*: “sip:UserA@here.com”
Location	C	Include, when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of the terminal of an intercept subject with personal mobility. The level of detail of reported location information should be commensurate with the level of detail of the location information available for use within the VoIP network.
TransitCarrierIdentity	C	Included when the transit network selection is known, to identify the transit carrier.
SubjectMediaInformation	C	Included to identify the SDP information for the intercept subject, when the intercept subject’s media information is being reported. The information need not be reported if reported via other messages (e.g., MediaAndAddressReporting message).
OriginationCause	M	Identifies the reason for the generation of the Origination message (e.g., SIP INVITE).
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the Origination message.
ForkedCalls	O	Provide the call IDs and destinations for forked calls (e.g., forked INVITE)

6.1.15 Redirection Message

The *Redirection Message* reports the redirection of a VoIP call or session.

The Redirection message shall be triggered when:

- An incoming call or session attempt to the intercept subject is redirected by the intercept subject’s service (e.g., call forwarding, call diversion);
- An incoming call or session attempt to an intercept subject with personal mobility is redirected by the intercept subject’s mobility service to the intercept subject’s current location; or
- An incoming call or session attempt to the intercept subject is redirected by the intercept subject’s service as a result of acting on the intercept subject’s request (e.g., call deflection).

The Redirection message includes the following parameters:

Table 6.P: Redirection Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg or session within a system.
NewCallIdentity	C	Included to identify the redirected leg of the call or session when the call identity is modified at the time of redirection. The original call identity included in the CallIdentity parameter is released and shall not be reused for the lifetime of the lawful authorization.
RedirectedFromPartyIdentity	C	Included to identify the party from whom the call is redirected, when known.
RedirectedToPartyIdentity	C	Included to identify the redirected-to party, when known.
TransitCarrierIdentity	C	Included to identify the transit carrier, when a transit carrier is involved and the transit carrier identity is known.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate's media information for the redirection is being reported, if the media characteristics change. The information need not be reported if reported via other messages (e.g., MediaAndAddressReporting message).
RedirectedToSystemIdentity	C	Included to identify the system to which the call has been redirected, when a call to an intercept subject is redirected to another TSP and the system identity of that TSP is reasonably available. Examples include: "sip.provider.com" and "2025551234."
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the Redirection message.

6.1.16 Release Message

The *Release Message* reports that a VoIP call, call leg, or session has been released.

The Release message shall be triggered when:

- A VoIP call or session attempt is not completed – e.g., abandoned by the calling party, rejected by the VoIP network, released by providing updated destination address(es) to enable subsequent call or session attempts;
- A completed VoIP call or session is released.

The Release message may be triggered when a call leg is released.

The Release message includes the following parameters:

Table 6.Q: Release Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system.
Location	C	Included when the location information is reasonably available at the IAP and delivery is authorized, to identify the location of the terminal of an intercept subject with personal mobility. The level of detail of reported location information should be commensurate with the level of detail of the location information available for use within the VoIP network.
Cause	C	Included to identify the signaling type in which the release event occurred and the cause of the call or session release [e.g., busy, call rejected, called party moved temporarily (e.g., SIP 302 response)], when known.
ContactAddresses	C	Included when one or more contact addresses (e.g., SIP Contact headers) are provided to the intercept subject or associate(s) as part of the release, to report the contact address(es).[16]
EncapsulatedSignalingMessage	C	The SIP message stimulated the sending of the Release message.

6.1.17 ServingSystem Message

The *ServingSystem Message* reports a registration, a change, or an attempted change to the serving TSP, service area, or intercept subject's addressing information – e.g., for personal mobility.

The ServingSystem message shall be triggered when:

- A request to register or deregister an intercept subject's addressing information is directed or forwarded to a registrar (e.g., a SIP Proxy forwards a Register request to a SIP Registrar);
- A request to register or deregister an intercept subject's addressing information is processed, failed, or timed out by a registrar (e.g., a SIP Registrar processes a SIP Register request); or
- When the intercept subject is authorized for service by a TSP.

The ServingSystem message includes the following parameters:

[16] Contact addresses are often provided to enable subsequent call or session attempts.

Table 6.R: ServingSystem Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SystemIdentity	C	Provided to identify the serving system when the intercept subject is authorized for service by the TSP.
RequestIdentity	C	Included to identify an address registration or deregistration request within a system, when available.
AddressRegistrationType	C	Indicates whether an address registration, address deregistration, or both were detected. Provided when appropriate.
RegisteringPartyIdentity	C	Identifies the party for whom address registration, deregistration, or both, are being attempted. Provided when appropriate.
RequestingPartyIdentity	C	Included to identify the party requesting the address registration, deregistration, or both, when different from the RegisteringPartyIdentity.
RegistrarIdentity	C	Identifies the registrar to which the address registration request, deregistration request, or both, are destined. Provided when appropriate.
RequestAddressInformation	C	Address information attempted to be registered, deregistered, or both, when present.
ResponseAddressInformation	C	Address information included in the response to the attempt to register, deregister, or both register and deregister address information, when present.
FailureReason	C	Included to indicate the reason that an address registration, deregistration, or both, were unsuccessful, when the registration, deregistration, or both are unsuccessful.
ExpirationPeriod	C	Included to identify the address-independent registration lifetime applicable to the registered addresses, when known.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the ServingSystem message.

6.1.18 SubjectSignal Message

The *SubjectSignal Message* reports dialing and signaling by the intercept subject to control (including invocation and use) a feature or service (e.g., call forwarding, call waiting, call hold, three-way calling). The SubjectSignal message is also used to report call progress signaling from the subject's device to the network for VoIP networks (e.g., subject device alerting).

The signal could be call-associated or non call-associated.

The SubjectSignal message shall be triggered when:

- The intercept subject, using the facilities under surveillance, dials or signals to control (including invoke and use) a feature or service including an active call or conference (e.g., a re-INVITE).

The SubjectSignal message is not required when the information reported would be redundant with the information reported by other surveillance messages.

The SubjectSignal message includes the following parameters:

Table 6.S: SubjectSignal Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	Included to uniquely identify a call, call leg, or session within a system, when the subject signal is associated with a particular call.
SignalingPartyId	C	Included to identify the signaling party, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity.
SignaledPartyId	C	Included when known to identify the party or network resource intended to receive the associated SIP message. For example, if a REFER is sent to a party or network resource, this will identify the value present in the Request URI of the REFER message.
SubjectMediaInformation	C	Included to identify the SDP information for the intercept subject, when the intercept subject's media information is being reported. The information need not be reported if reported via other messages (e.g., MediaAndAddressReporting message).
Signal One or more of the following:	M	Identifies the dialing or signaling by the intercept subject to control a feature or service.
DialedDigits	C	Included for dialed or signaled digits or addresses that are associated with a feature or service. *Examples*: "12025551234," "UserA@here.com," "*123."
FeatureKey	C	Included for a signaled feature key. *Examples*: "KEY1," "HOLD," "CONFERENCE."
OtherSignalingInformation	C	Included for any other subject signal that triggers this message. *Examples*: "hold", "retrieve", "refer".
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the SubjectSignal message.

6.1.19 TerminationAttempt Message

The *TerminationAttempt Message* reports an incoming VoIP call attempt or session request to the intercept subject. This message shall be sent regardless of the disposition of the call or session (e.g., busy, answered, redirected).

The TerminationAttempt message shall be triggered when:

- An incoming call attempt or session request to an intercept subject is detected.

The TerminationAttempt message includes the following parameters:

Table 6.T: TerminationAttempt Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	M	Uniquely identifies a call, call leg, or session within a system. A unique call identity may be generated for the TerminationAttempt message, which is used to correlate other messages. An exception is possible when such an attempt is considered part of an on-going call or session (e.g., call waiting for some systems).
CallingPartyIdentity	M	Identifies the calling party to the extent known. For all identities of the calling party contained in the SIP signaling seen at the IAP (e.g., From, Contact, P-Asserted-Identity), those header fields shall be reported here using the sipHeader component.
CalledPartyIdentity	C	Included when more specific than the intercept subject identity associated with the CaseIdentity, to identify the called party. In addition to reporting the request URI, if other identities of the called party are contained in the SIP signaling seen at the IAP (e.g., To), those header fields shall be reported here using the sipHeader component.
AssociateMediaInformation	C	Included to identify the SDP information for an associate, when an associate's media information is being reported. The information need not be reported if reported via other messages (e.g., MediaAndAddressReporting message).
RedirectedFromInformation	C	Included when the incoming call or session has information about previous redirection.
EncapsulatedSignalingMessage	C	The SIP message that stimulated the sending of the TerminationAttempt message.

6.2 Call Content Surveillance Messages

6.2.1 General

CC delivery over the delivery interface provides packetized CC for VoIP calls under surveillance to LEA collection systems, where LEA access to CC is lawfully authorized. The CC delivery capability may be viewed as logically separated from the CII delivery from the perspective of the TSP delivery systems and LEA collection systems.

An APDU, called the CC-APDU, may be used to encapsulate CC packets for transfer over the CC delivery interface for VoIP RTP andRCS Messaging, in accordance with clauses 6.2.2 and 6.2.3 of this standard.

6.2.2 CC-APDU for VoIP RTP

The CC-APDU encapsulates an individual CC packet (called the *payload*) from the packetized media stream for a VoIP call for transfer to the LEA collection system on the delivery interface. The CC-APDU, consisting of a CCDeliveryHeader and a Payload, is sent from the DF to the CF.

The CC-APDU is generated when CC delivery is authorized and is enabled, and a VoIP call involving the intercept subject and carried by the TSP is generating media packets.

Delivery of CC via CC-APDUs is dependent upon appropriate provisioning of the CC delivery interface, and delivery over IP.

A CC-APDU shall be triggered for each VoIP CC packet in all media streams associated with the call to be delivered. Each CCDeliveryHeader contains (as necessary) a series of parameters that provides correlation to the CII, and enables the LEA collection function to properly process the encapsulated payload.

The CC-APDU contains the following parameters. All the parameters in Table 22, except Payload, are part of the CCDeliveryHeader.

Table 6.U: CC-APDU Parameters for VoIP RTP

Parameter	MOC	Usage
CorrelationInformation	M	Enables correlation of CC and CII when CII and CC are both reported.
CaseIdentity	C	Identifies the Intercept Subject, corresponding to the CaseIdentity parameter in the CCOpen message for the media stream. Include when necessary for unique correlation purposes.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system, corresponding to the IAPSystemIdentity parameter in the CCOpen message for the media stream. Include when necessary for unique correlation purposes.
CallIdentity	M	Uniquely identifies the media stream being delivered, corresponding to the CallIdentity parameter in the CCOpen message for the media stream.
TimeStamp	M	Included to identify the date and time that the VoIP media packet was intercepted, per condition listed above.
PacketDirection	C	Indicates the direction of the intercepted packet (from the intercept subject, or to/toward the intercept subject). This parameter shall be provided if the IP addresses and ports in the Payload parameter do not match those in the reported SDP of the subject and associate.
SequenceNumber	C	Included to provide the sequencing of the CC-APDUs for the media stream identified by this header. Not required when TCP [Ref 12] is used as the delivery method to the LEA.
Payload	M	Included the encapsulated intercepted CC packet. The payload shall contain the VoIP media packet's bits comprising the Protocol Data Units (PDUs) at the network layer and above [e.g., the IP/User Datagram Protocol (UDP)/RTP datagrams for a VoIP service].

6.2.2.1 Sequence Number

The SequenceNumber parameter shall be used in the following way:

- The sequence number is initialized to zero for the first CC-APDU for each call identity;
- The sequence number increases by one for each subsequent CC-APDU for the call identity.

The implementation may use a fixed size for the sequence number (e.g., 32-bit integer) and reset it to zero when it reaches its maximum positive value.

6.2.3 CC-APDU for RCS Messaging

For RCS messaging interception, the RCS Messaging CC-APDU is defined below and is generally consistent with that of clause 6.2.2. The RCS Messaging CC-APDU encapsulates an MSRP payload, part, or all of a file object. It is generated when RCS Messaging interception is authorized for the intercept subject.

One or more RCS Messaging CC-APDUs shall be triggered for each RCS Messaging File Object. The CCDeliveryHeader CC-APDU contains CorrelationInformation a series of parameters that provides correlation to the other CII associated with the same RCS Messaging session.

The RCS Messaging CC-APDU contains the parameters defined in Table 23.

Table 6.V: RCS Messaging CC-APDU Parameters

Parameter	MOC	Usage
CorrelationInformation	M	Enables correlation of CC and CII when CII and CC are both reported.
CaseIdentity	C	Identifies the Intercept Subject, corresponding to the CaseIdentity parameter in the CCOpen message for the RCS message files being exchanged. Include when necessary for unique correlation purposes.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system, corresponding to the IAPSystemIdentity parameter in the CCOpen message for the RCS message files being exchanged. Include when necessary for unique correlation purposes.
CallIdentity	M	Uniquely identifies the SIP session over which RCS message files are being exchanged, corresponding to the CallIdentity parameter in the CCOpen message for the RCS message files being exchanged.
TimeStamp	M	Included to identify the date and time that the RCS message file being exchanged was intercepted, per condition listed above.
PacketDirection	C	Indicates the direction of the contents in the APDU being exchanged (from the intercept subject, or to/toward the intercept subject). This parameter shall be provided if the IP addresses and ports in the Payload parameter do not match those in the reported SDP of the subject and associate.
SequenceNumber	C	Included to provide the sequencing of the CC-APDUs.
PayloadType	M	Specifies whether the payload contains an MSRP payload or a file object.
MsgIdentifier	C	Must be present in a CC-APDU with a file object payload, and in the associated CC-APDU with the MSRP payload. It is a unique number used to correlate files objects with the MSRP containing the file transfer message.
ChunkNumber	C	Must be present if the payload is sent in multiple CC-APDUs. Indicates the sequence number of the chunk in this CC-APDU. The first chunk shall be numbered 0.
LastChunk	C	Must be present if ChunkNumber is present. Is Boolean TRUE if this is the last chunk being sent. Otherwise is Boolean FALSE.
ContentType	C	Must be present if the CC-APDU is for part of a file object. Specifies the MIME type (e.g., imager/jpg, video/mp4).
Payload	M	The payload includes all or a chunk of the MSRP payload or of a file object being sent. See text beneath this table.

When the Payload contains an MSRP message, only MSRP headers shall be included unless content interception for RCS Messaging is lawfully authorized. If content interception is not authorized, everything in the MSRP message after the MSRP headers shall be removed or redacted.

Intercepted MSRP payloads result in a RCS Messaging CC-APDU, with the MSRP payload put in the Payload parameter and the PayloadType parameter being set to MSRP payload or file object. Additionally, if the MSRP message is a file-transfer message and a file object is to be transferred separately as a file-object CC-APDU, the MsgIdentifier is used to correlate the MSRP message with the RCS CC-APDUs containing the file object.

For the interception of a file object, the file object is sent using additional RCS Messaging CC-APDUs. In these RCS Messaging CC-APDUs, the MsgIdentifier is the same as was in the corresponding intercepted MSRP message. The DF is allowed to send large file objects as “chunks” using multiple RCS Messaging CC-APDUs. Each successive chunk has an incrementing ChunkNumber parameter value. The last chunk is denoted by the LastChunk parameter.

The RCS universal profile permits a maximum of two file objects named in a single MSRP message body, and then only if one of the files is a thumbnail of the other file. When this occurs, the DF shall first send the full first file object that appears in the MSRP body, and then send the second file object. Both will have the same MsgIdentifier. They can be distinguished, as needed, by the LEA by order of appearance, size, and possibly ContentType.

Interception of RCS includes interception of the associated SIP signaling in the same way, as described in this standard, as if the SIP signaling represented a VoIP call.

6.3 User to User Surveillance Messages

6.3.1 UUContent Message

The *UUContent Message* is a capability used to report content sent to, or received by, the intercept subject in the SIP MESSAGE method. The sending and receiving of the SIP MESSAGE method may or may not be related to a VoIP call.

When user-to-user content is part of a VoIP session, the UUContent message shall be reported only under a lawful authorization for content. If the user-to-user content is outside of a VoIP session, reporting of user-to-user content under a lawful authorization for content, is optional.

The UUContent message includes the following parameters:

Table 6.W: UUContent Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
CallIdentity	C	For a VoIP session, CallIdentity uniquely identifies a call, call leg, or session within a system.
EncapsulatedSignalingMessage	M	The SIP message that stimulated the sending of the UUContent message.

6.4 Use of DSR and Mapped VoIP Surveillance Messages

Two methods of reporting VoIP CII are provided in this standard:

1. Mapped Signaling Information or Mapped; or
2. DSR.

'Mapped' is a method characterized by mapping signaling CII information onto J-STD-025-B [Ref 2] messages modified to carry VoIP CII. Examples of mapping include the mapping of SIP signaling information onto the enhanced J-STD-025-B messages (e.g., a SIP INVITE message mapped onto an Origination message). The following J-STD-025-B messages have been enhanced for mapping VoIP signaling**:**

- *Answer*: see 6.1.1
- *Connection*: see 6.1.6
- *ConnectionBreak*: see 6.1.7
- *ConferencePartyChange*: see6.1.8
- *DialedDigitExtraction*: see 6.1.9
- *NetworkSignal*: see 6.1.12
- *Origination*: see 6.1.13
- *Redirection*: see 6.1.14
- *Release*: see 6.1.15
- *ServingSystem*: see 6.1.16
- *SubjectSignal*: see 6.1.17
- *TerminationAttempt*: see 6.1.18

The following ‘mapped’ messages not found in J-STD-025-B [Ref 2] have been developed for this standard:

- MediaAndAddressReporting: see 6.1.11
- UUContent: see 6.3.1

The Direct Signal Reporting method is characterized by reporting appropriate VoIP SIP messages as CII. A DSR CII message for VoIP has been developed to carry the signaling:

- *DSR*: see 6.1.10

The following messages are used with both the mapped and DSR methods when there is CC interception and delivery:

- *CCOpen*: see 6.1.5
- *CCEncryptionInfo:* see 6.1.4
- *CCClose*: see 6.1.3
- *CCChange*: see 6.1.2
- *CCUnavailable*: see 6.1.6

The CCOpen and CCClose close messages are J-STD-025-B [Ref 2] messages modified for VoIP. CCChange and CCUnavailable have been developed for this standard to support VoIP CC delivery.

With respect to SIP, SIP Proxy Servers, SIP redirect Servers, and many others, SIP servers can achieve redundancy and scale by processing SIP methods individually without maintaining state for the duration of the call. Although some call management systems may chose to maintain state to offer SIP services, it is not required by the SIP architecture.

The interpretation of SIP messages used to invoke supplementary services (e.g., conferencing, transfer, hold, retrieve) into the appropriate LAES messages (e.g., Connection, ConnectionBreak) requires the CMS to have knowledge of events that previously occurred. In other words, only a CMS that maintains call state for the entire duration of the call and all parties to the call for the supplementary service being performed can map the SIP messages to the LAES messages.

Only a CMS that maintains state in these call setups and manipulations may be able to perform the mapped message reporting.

A CMS that does not maintain call state may be limited to the DSR method of reporting. In addition, a CMS that does maintain call state may optionally choose the DSR method.

6.4.1 Use of DSR Messaging

The DSR method may be appropriate for CMS implementations not based on or migrated from J-STD-025-B [Ref 2] circuit-switch intercept concepts and events [e.g., based on Internet Engineering Task Force (IETF) Request For Comments (RFC) 3261 [Ref 6] multi-media session concepts]. These implementations may have different event concepts based on multi-media sessions and not calls. Reporting their native CMS event concepts based on industry standardized signaling (e.g., reporting a SIP INVITE to mean ‘invitation to a session’) may be more logical and efficient than creating and maintaining a second pseudo event model based on J-STD-025-B event reporting (i.e., acting as a SIP to J-STD-025-B gateway and reporting Call Origination).

The following messages may be used with the DSR reporting method to supplement the reporting of signaling information sent-to or received-from the intercept subject:

- DialedDigitExtraction Message: see 6.1.9;
- Subject Signal Message: see 6.1.17; or

- Network Signal Message: see 6.1.12.

6.4.2 Use of Mapped Messaging

The ‘mapped’ method may be appropriate and logical for implementations with circuit-switch CMS(s) that have been modified or migrated from a circuit-switch intercept implementation based on J-STD-025-B [Ref 2] messages to VoIP CMS(s). In these cases, the ‘mapped’ method may be logical and appropriate since the CMS may have J-STD-025-B message event concepts and reporting (e.g., Call Origination, Call Termination Attempt, Call Release). Note that DSR may still be required with the ‘mapped’ method to report CII signaling information which cannot be mapped onto the modified J-STD-025-B VoIP messages (e.g., for new SIP methods or responses or extensions) and when a CMS merely forwards signaling without processing or interpreting (e.g., forwards a SIP ACK).

6.4.3 Use of the EncapsulatedSignalingMessage Parameter

In those LAES messages that contain the EncapsulatedSignalingMessage as a parameter, the SIP message present at the IAP, if any, that triggered the LAES message shall be provided, excepting:

a. Location-information headers and message bodies recognized by the TSP (e.g., P-Access-Network-Info headers, Geolocation headers and associated message bodies) shall be removed or redacted (e.g., by overwriting), unless lawfully authorized;[17]

b. If CC reporting is not lawfully authorized, all other message bodies other than MIME type application/SDP shall be removed or redacted.

6.5 Use of Call Identity

A Call Identity is used to correlate all of the reported LI messages associated with a specific call, call leg, or session and shall be unique per a subject’s communications during the lifetime of a lawful authorization. A unique call identity may be achieved by using a SIP Call ID as defined in RFC 3261 [Ref 6].

6.6 Location Information

Location information identifies the location of the subject’s terminal. When reasonably available and covered by the lawful authorization, location type (e.g., “SIP INVITE P-header,” “SIP location header,” “SIP location message body,” “GPS Data,” “Cell Tower”) and actual content of the location field shall be delivered to Law Enforcement.

To support the reporting of the target location at the end of call, when the location is lawfully authorized, when the associate sends a BYE first (thus triggering Release of the call), an operator may delay the sending of the Release to include the final target location or alternatively, use DSR of the target 200 OK (BYE) with final target location.

6.7 Party Identity

This clause lists possible values for the Party Identity type, which is used with numerous LAES messages (e.g., Origination, TerminationAttempt, MediaAndAddressReporting) and message parameters (e.g., CallingPartyID, CalledPartyID, SubjectMediaInformation, AssociateMediaInformation). For parameters (e.g., CallingPartyID) that are specified as Party Identity type, all reasonably available party identifiers shall be reported. Redundant

[17] Location information for the Intercept Subject, if lawfully authorized, will be mapped into the Location parameter.

information need not be reported. For example, if a SIP header is reported, URI included in that header need not be reported separately.

The following party identifiers are defined as part of this Standard:

esn	Advanced Mobile Phone System (AMPS)-based Electronic Serial Number, a hexadecimal string -- e.g., “82ABCDEF”
imei	Global System for Mobile (GSM)-based International Mobile Equipment Identity
tei	Integrated Services Digital Network (ISDN)-based Terminal Equipment Identity
spid	ISDN-based Service Profile Identifier
imsi	International Mobile Station Identity E.212 number beginning with Mobile Country Code
min	AMPS-based Mobile Identification Number
dn	e.g., called directory number or network provided calling number.
userProvided	user provided calling number as supplied
callingCardNum	
ipAddress ipV4 ipV6	
x121	begin with Data Network Identification Code (DNIC)
trunkId	indicate trunk group, trunk number or both. This is usually used to identify an associate when other identifying information is not available. This may also identify a subject’s agent (e.g., screening service).
subaddress	encoded according to ATIS-1000607.2014 [Ref 7] Subaddress information element starting with octet 3.
genericAddress	indicate use of the generic address
genericDigits	indicate use of the generic digits
genericName	indicate use of the generic name
port	identifies a particular equipment port. This is used to identify an associate when other identifying information is not available.
context	when none of the other identities are known or to identify the context and special considerations of the supplied identifier(s), especially when the identifier(s) is(are) abnormal (e.g., international, private, restricted, operator, no address, hotel/motel, coin, etc.)
isdnHighLayer	encoded according to ATIS-1000607.2014 [Ref 7] High Layer Compatibility information element starting with octet 3
isdnLowLayer	encoded according to ATIS-1000607.2014 [Ref 7] Low Layer Compatibility information element starting with octet 3
uri	uniform resource identifier (see RFC 2396 [Ref 13])
sipHeader	e.g., To, From, and Contact SIP header fields
nai	The Network Access Identifier (e.g., foo@bar.com) as defined in RFC 2486 [Ref 14]. For example, this could be the username passed to the Administration, Authorization, and Authentication (AAA) server for authentication (e.g., RADIUS attribute 1)
mac802	Institute of Electrical and Electronic Engineers (IEEE) 802 Media Access Control (MAC) address [Ref 8]
fqdn	Fully Qualified Domain Name (e.g., foo.bar.com)

6.8 Cause

This clause lists the defined values for the Cause type, which is used with individual LAES messages (Release and ServingSystem) and message parameters (Cause and Failure Reason). The following elements of the Cause type are defined as part of this Standard:

signalingType	Indicates the signaling type and message by which the release or failure event occurred (e.g., SIP 302, SIP 401 Unauthorized). Examples include: “busy,” “user not registered,” “SIP WWW-Authenticate,” “SIP

	Proxy-Authenticate," entire SIP Error-Info header, and entire SIP Warning header. SIP/2.0 404 The number you have dialed is not in service; Error-Info: <sip:not-in-service-recording@atlanta.com>
cause	Included to identify the specific cause of the release or failure, when available.

6.9 CCC Identity

Each CCC is identified with a VisibleString which may contain a directory number (e.g., "202-555-1111"), a trunk identity (e.g., "FBITG-001" or "LAES-999"), an IP network address (e.g., "IP: 10.12.103.104:100") or an X.25 network address (e.g., "X121: 1234-5678901234").

6.10 CC Address

The CC Address is a null value indicating that the CC is delivered over a pre-arranged IP data stream.

6.11 RCS Messaging

RCS (Rich Communications Services) [Ref 28] messaging interception involves the following types of information:

1. CII:
   The SIP signaling messages such as INVITE, 200 OK, ACK, and BYE are reported.
   Header part of the MSRP in the CC-APDU.
2. CC:
   MSRP that contain the textual information and the metadata of a file object being transferred along with the optional identifier. Transferred file objects, for instance, photos, videos, files of any type and size.

If the lawful interception is limited to CII, then only the SIP signaling messages and the header part of MSRP (as shown under CII above) shall be reported.

The TSP shall be able to intercept and deliver signaling and content for RCS Messaging to the exclusion of VoIP. Likewise, the TSP shall be able to intercept and deliver CII and CC for VoIP to the exclusion of RCS Messaging. For each service, the TSP shall be able to provision whether content (e.g. CC) is to be delivered for a given intercept.

One example solution is if the SDP in the SIP INVITE includes a RCS specific service extension or service tag that corresponds to those specified in [Ref 29] clause 2.6.1.1, enabling the ability to isolate RCS specific signaling.

As part of reporting CII, the reporting shall include information that includes:

1) The establishment, modification, and release of an RCS Messaging Session via SIP signaling.
2) All of the MSRP messages to and from or on behalf of the intercept subject (e.g., SENDs, REPORTs, replies); any other MSRP is beyond the scope of this standard.
3) Everything in the MSRP message beyond the MSRP headers and URI, if present, shall be removed or redacted (e.g., by overwriting) if RCS content interception is not lawfully authorized.

If the lawful interception requires CII + CC delivery, then DF shall retrieve and deliver the file object represented by the URI of the file object. Otherwise, the DF delivers the URI of the file object.

The RCS Messaging CC-APDU encapsulates an MSRP payload or file object in the Payload parameter for a RCS session for transfer to the LEA collection system on the delivery interface. The RCS CC-APDU, consisting of a CCDeliveryHeader and a Payload, is sent from the DF to the CF.

When RCS Messaging content interception is lawfully authorized, an intercepted MSRP payload shall result in reporting of a RCS CC-APDU (as defined in 6.2.3), with the MSRP payload residing in the payload parameter. If the MSRP message defines one or more file objects being transferred according to the definition in [Ref 28], one or more CC-APDUs shall be sent containing the contents of each file object.

It is advisable for RCS implementations to have the capability to provision with options to indicate whether or not to report the file objects, and the maximum size of the file object that can be sent to the LEA collection function.

Any TSP's limits on the transmission file objects or maximum size of file objects to transmit is based on operator policy and agreement with the LEA.

As an alternative to sending the file object as a file-object RCS CC-APDU under this standard, other LI standards that have the means to send bulk data, such as ATIS-1000013 ("IAS") [Ref 30] and ETSI 102 232-2 [Ref 31], may be used. However, when this is done, the TSP is responsible for providing correlation of CII and the CC. Such correlation is not defined in this specification.

RCS Messaging, for which interception is defined in this standard, is based on the RCS universal profile [Ref 29]. RCS Voice Services (e.g., RCS enhanced voice) as defined by GSMA [Ref 29], and activation of an intercept of RCS communications for an already established session are not addressed in this version of this standard but may be addressed in a future version of this document.

For an RCS messaging session, the SDP offer is always included in a SIP INVITE and SDP answer is always included in a 200 OK. CCOpen and CCClose are sent even if the content interception is not authorized.

Annex A ASN.1 Definitions

(normative)

This annex is normative and is considered part of this Standard.

NOTE - This Annex has also been formatted as a separate plaintext file and electronically packaged with this standard.

```
ATIS-LAES-VoIP-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-678(0) cii(0) common (0) version-5(4)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CCCIdentity, CaseIdentity, Timestamp, AlertingSignal, AudibleSignal,
TransitCarrierIdentity, RedirectedFromInformation
FROM Laesp-j-std-025-b {iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-
b(2) version-1(0)};

aTIS-LAES-VoIP-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
tia(113737) laes(2) t1(1) t1-678(0) cii(0) common (0) version-5(4)}
    -- OID for ATIS-LAES-VoIP-Abstract-Syntax-Module

LAESProtocol ::= SEQUENCE {
    aTIS-LAES-VoIP-Abstract-Syntax-Module-OID    [0] OBJECT IDENTIFIER,
    laesMessage                                  [1] LaesMessage
}

LaesMessage ::= CHOICE {
    answer                   [1] Answer,
    ccClose                  [2] CCClose,
    ccOpen                   [3] CCOpen,
    null-4                   [4] NULL,
    origination              [5] Origination,
    null-6                   [6] NULL,                 -- reserved by J-STD-025-B [Ref 2]
    redirection              [7] Redirection,
    release                  [8] Release,
    servingSystem            [9] ServingSystem,
    termAttempt              [10] TerminationAttempt,
-- null-11                   [11] NULL,
    confPartyChange      [12] ConferencePartyChange,
    connection               [13] Connection,
    connectBreak             [14] ConnectionBreak,
    dialedDgtExtrn           [15] DialedDigitExtraction,
    networkSignal            [16] NetworkSignal,
    subjectSignal            [17] SubjectSignal,
    directSignalReporting    [18] DirectSignalReporting,
    mediaAndAddressReporting [19] MediaAndAddressReporting,
    ccChange                 [20] CCChange,
    ccUnavailable            [21] CCUnavailable,
 surveillanceStatus          [22] SurveillanceStatus,          -- see Annex D of this Standard
 featureManagement       [23] FeatureManagement,           -- see Annex D of this Standard
    uuContent                [24] UUContent,
    ccEncryptionInfo         [25] CCEncryptionInfo,

    ...
}

-- Message Definitions

Answer ::= SEQUENCE {
    caseId                   [0] CaseIdentity,
    iAPSystemId              [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                [2] TimeStamp,
    callId                   [3] CallIdentity,
    answering                [4] PartyIdentity                            OPTIONAL,
    location                  [5] Location                                 OPTIONAL,
    answeringMedia            [6] SDP                                      OPTIONAL,
    signalingMsg              [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

CCChange ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callID                    [3] CallIdentity,
    deliveryIdentifier        [4] DeliveryIdentifier,

                              -- Include at least one of the two following parameters:
    subjectMedia              [5] SDP                                      OPTIONAL,
    associateMedia            [6] SDP                                      OPTIONAL,

    signalingMsg              [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

CCClose ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callID                    [3] CallIdentity,
    deliveryIdentifier        [4] DeliveryIdentifier,
    signalingMsg              [5] SET OF EncapsulatedSignalingMessage      OPTIONAL
}
CCEncryptionInfo ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    cryptoContext             [4] CryptoContext                            OPTIONAL,
    key                       [5] OCTET STRING,
    salt                      [6] OCTET STRING                             OPTIONAL,
    keyEncoding               [7] ENUMERATED {
                                  binary  (0),
                                  base64  (1),
                                  ...
                              }          OPTIONAL,  ...
}

CryptoContext ::= CHOICE {
    sRTP                      [0] SEQUENCE {
               destIpAddress      [0] IpAddress,
               destPort       [1] OCTET STRING(SIZE(2)),
               sSRC           [2] OCTET STRING(SIZE(4))                OPTIONAL,
               sequenceNum        [3] INTEGER                              OPTIONAL,
               tail               [4] INTEGER                              OPTIONAL
                          },
    ...
}


CCOpen ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callID                    [3] CallIdentity,
    deliveryIdentifier        [4] DeliveryIdentifier,

                              -- Include at least one of the two following parameters:
    subjectMedia              [5] SDP                                      OPTIONAL,
    associateMedia            [6] SDP                                      OPTIONAL,

    signalingMsg              [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

CCUnavailable ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    unavailabilityReason      [4] VisibleString                            OPTIONAL,
    signalingMsg               [5] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

Connection ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callId                     [3] SEQUENCE OF CallIdentity,

                               -- Include at least one of the following two parameters:
    connectedParties           [4] SEQUENCE OF PartyIdentity                OPTIONAL,
    newParties                 [5] SEQUENCE OF PartyIdentity                OPTIONAL,

    connectedMedia             [6] SDP                                      OPTIONAL,
    signalingMsg               [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

ConnectionBreak ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callId                     [3] SEQUENCE OF CallIdentity,

                               -- Include at least one of the following three parameters:
    removedParties             [4] SEQUENCE OF PartyIdentity                OPTIONAL,
    remainingParties           [5] SEQUENCE OF PartyIdentity                OPTIONAL,
    droppedParties             [6] SEQUENCE OF PartyIdentity                OPTIONAL,

    signalingMsg               [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

ConfPartyChange ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callId                     [3] SEQUENCE OF CallIdentity,

                               -- Include at least one of the following four parameters:
    communicatingParties       [4] SEQUENCE OF PartyIdentity                OPTIONAL,
    removedParties             [5] SEQUENCE OF PartyIdentity                OPTIONAL,
    joinedParties              [6] SEQUENCE OF PartyIdentity                OPTIONAL,
    droppedParties             [7] SEQUENCE OF PartyIdentity                OPTIONAL,

    signalingMsg               [8] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

DialedDigitExtraction ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callId                     [3] CallIdentity,
    digits                     [4] VisibleString (SIZE (1..32))
}

DirectSignalReporting ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callID                     [3] CallIdentity                             OPTIONAL,
    direction                  [4] MessageDirection,
    location                   [5] Location                                 OPTIONAL,
    signalingMsg               [6] EncapsulatedSignalingMessage
}


MediaAndAddressReporting ::= SEQUENCE {
    caseId                     [0] CaseIdentity,
    iAPSystemId                [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                  [2] TimeStamp,
    callId                     [3] CallIdentity,

                               -- Include at least one of the following three parameters:
    subjectMedia               [4] SDP                                      OPTIONAL,
    associateMedia             [5] SDP                                      OPTIONAL,
    redirectedToPartyMedia    [6] SDP                                      OPTIONAL,

    subjectContactAddresses   [7] PartyIdentity                            OPTIONAL,
    associateContactAddresses [8] PartyIdentity                            OPTIONAL,
    redirectedToPartyContactAddresses [9] PartyIdentity                    OPTIONAL,
    mediaAndAddressReportingCause [10] VisibleString,
    signalingMsg              [11] SET OF EncapsulatedSignalingMessage     OPTIONAL
}

NetworkSignal ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity                             OPTIONAL,
    signaledToPartyId         [4] PartyIdentity                            OPTIONAL,
    associateContactAddresses [5] PartyIdentity                            OPTIONAL,
    associateMedia            [6] SDP                                      OPTIONAL,

                              -- Include at least one of the following five parameters:
    alertingSignal            [7] AlertingSignal                           OPTIONAL,
    subjectAudibleSignal      [8] AudibleSignal                            OPTIONAL,
    terminalDisplayInfo       [9] TerminalDisplayInfo                      OPTIONAL,
    other                     [10] UTF8String                          OPTIONAL,
    signalingMsg              [11] SET OF EncapsulatedSignalingMessage     OPTIONAL
}

Origination ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    calling                   [4] PartyIdentity                            OPTIONAL,
    called                    [5] PartyIdentity                            OPTIONAL,
    input                     [6]CHOICE {
                                  userInput          [0] CHOICE {
                                         generic        [0] VisibleString,
                                         specific       [1] PartyIdentity},
                                  translationInput   [1] CHOICE {
                                         generic        [0] VisibleString,
                                         specific       [1] PartyIdentity}
                                  },
    location                  [7] Location                                 OPTIONAL,
    transitCarrierId          [8] TransitCarrierIdentity                   OPTIONAL,
    subjectMedia              [9] SDP                                      OPTIONAL,
    originationCause          [10] VisibleString,
    signalingMsg              [11] SET OF EncapsulatedSignalingMessage     OPTIONAL,
    forkedCalls               [12] SET OF ForkedCallInformation            OPTIONAL
}

Redirection ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    newCallId                 [4] CallIdentity                             OPTIONAL,
    redirectedFrom            [5] PartyIdentity                            OPTIONAL,
    redirectedTo              [6] PartyIdentity                            OPTIONAL,
    transitCarrierId          [7] TransitCarrierIdentity                   OPTIONAL,
    associateMedia            [8] SDP                                      OPTIONAL,
    redirectedToSystemIdentity[9] SystemIdentity                           OPTIONAL,
    signalingMsg              [10] SET OF EncapsulatedSignalingMessage     OPTIONAL
}

Release ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    location                  [4] Location                                 OPTIONAL,
    cause                     [5] Cause                                    OPTIONAL,
    contactAddresses          [6] PartyIdentity                            OPTIONAL,
    signalingMsg              [7] SET OF EncapsulatedSignalingMessage      OPTIONAL
}
```

```
ServingSystem ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    systemIdentity            [3] SystemIdentity                           OPTIONAL,
    requestId                 [4] CallIdentity                             OPTIONAL,
    registrationType          [5] AddressRegistrationType                  OPTIONAL,
    registering               [6] PartyIdentity                            OPTIONAL,
    requesting                [7] PartyIdentity                            OPTIONAL,
    registrar                 [8] PartyIdentity                            OPTIONAL,

    requestAddressInfo        [9] CHOICE {
               generic                [0] SEQUENCE OF SEQUENCE {
                                             address            [0] PartyIdentity,
                                             expirationPeriod   [1] INTEGER},  -- in seconds
               sip                    [1] SET OF SipHeader}                OPTIONAL,

    responseAddressInfo       [10] CHOICE {
               generic                [0] SEQUENCE OF SEQUENCE {
                                             address            [0] PartyIdentity,
                                             expirationPeriod   [1] INTEGER},  -- in seconds
               sip                    [1] SET OF SipHeader}                OPTIONAL,

    failureReason             [11] Cause                                   OPTIONAL,

    expirationPeriod          [12] CHOICE {
               generic                [0] INTEGER,                  -- for all addresses, in seconds,
               sip                    [1] SipHeader}            OPTIONAL, -- maps SIP Expires header

    signalingMsg              [13] SET OF EncapsulatedSignalingMessage     OPTIONAL
}

SubjectSignal ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity                             OPTIONAL,
    signalingPartyId          [4] PartyIdentity                            OPTIONAL,
    signaledPartyId       [5] PartyIdentity                            OPTIONAL,
    subjectMedia              [6] SDP                                      OPTIONAL,

    signal                    [7] SEQUENCE {
           -- Include at least one of the following three parameters:
           dialedDigits               [0] VisibleString (SIZE (1..128))    OPTIONAL,
           featureKey                 [1] VisibleString (SIZE (1..128))    OPTIONAL,
           otherSignalingInformation  [2] VisibleString (SIZE (1..128))    OPTIONAL},
    signalingMsg              [8] SET OF EncapsulatedSignalingMessage      OPTIONAL
}

TerminationAttempt ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity,
    calling                   [4] PartyIdentity,
    called                    [5] PartyIdentity                            OPTIONAL,
    associateMedia            [6] SDP                                      OPTIONAL,
    redirectedFromInfo        [7] RedirectedFromInformation                OPTIONAL,
    signalingMsg              [8] SET OF EncapsulatedSignalingMessage      OPTIONAL
}


UUContent ::= SEQUENCE {
    caseId                    [0] CaseIdentity,
    iAPSystemId               [1] IAPSystemIdentity                        OPTIONAL,
    timestamp                 [2] TimeStamp,
    callId                    [3] CallIdentity                             OPTIONAL,
    signalingMsg              [4] SET OF EncapsulatedSignalingMessage
}


-- Parameter Definitions

AddressRegistrationType ::= ENUMERATED {
    unknown                           (0),
    registration                      (1),
    deregistration                    (2),
    registrationAndDeregistration     (3)
}

CallIdentity ::= SEQUENCE {
    main               [0] UTF8String,
    leg                [1] UTF8String                                   OPTIONAL
}

Cause ::= SEQUENCE {
    signalingType      [0] UTF8String,
    cause              [1] ParameterFormat                              OPTIONAL
}

DeliveryIdentifier ::= CHOICE {
    cccId              [0] CCCIdentity,
    ccAddress          [1] NULL
}

ForkedCallInformation ::= SEQUENCE {
    forkedCallID       [0] CallIdentity,
    calledParty        [1] PartyIdentity
}

EncapsulatedSignalingMessage ::= OCTET STRING

IpAddress ::= CHOICE {
    ipV4               [1] OCTET STRING(SIZE(4)),
    ipV6               [2] OCTET STRING(SIZE(16))
}

Location ::= SET OF SEQUENCE {
    locationType       [0] UTF8String,
    location           [1] UTF8String
}


MessageDirection ::= ENUMERATED {
    fromSubject        (0),
    toSubject          (1),
    unknown            (2),
    ...
}

ParameterFormat ::= CHOICE {
    generic            [0] UTF8String,               -- generic parameter representation
    sip                [1] SET OF SipHeader          -- SIP header representation
}

-- Include those PartyIdentity identification elements necessary to uniquely identify the party
-- known at the point in call or session and are authorized.
-- At least one of the PartyIdentity parameters is required.

PartyIdentity ::= SEQUENCE {
    esn                [0] VisibleString (SIZE (8))                     OPTIONAL,
    imei               [1] VisibleString (SIZE (1..15))                 OPTIONAL,
    tei                [2] VisibleString (SIZE (1..15))                 OPTIONAL,
    spid               [3] VisibleString (SIZE (3..20))                 OPTIONAL,
    imsi               [4] VisibleString (SIZE (1..15))                 OPTIONAL,
    min                [5] VisibleString (SIZE (10))                    OPTIONAL,
    dn                 [6] VisibleString (SIZE (1..15))                 OPTIONAL,
    userProvided       [7] VisibleString (SIZE (1..15))                 OPTIONAL,
    appearanceId       [8] VisibleString (SIZE (1..15))                 OPTIONAL,
    callingCardNum     [9] VisibleString (SIZE (1..20))                 OPTIONAL,
    ipAddress          [10] IpAddress                                   OPTIONAL,
    x121               [11] VisibleString (SIZE (1..15))                OPTIONAL,
    trunkId            [12] VisibleString (SIZE (1..32))                OPTIONAL,
    subaddress         [13] OCTET STRING (SIZE (2..21))                 OPTIONAL,
    genericAddress     [14] SEQUENCE OF VisibleString (SIZE (1..32))OPTIONAL,
    genericDigits      [15] SEQUENCE OF VisibleString (SIZE (1..32))OPTIONAL,
    genericName        [16] SEQUENCE OF UTF8String                      OPTIONAL,
    port               [17] VisibleString (SIZE (1..32))                OPTIONAL,
    context             [18] VisibleString (SIZE (1..64))                OPTIONAL,
    isdnHighLayer       [19] OCTET STRING (SIZE (2..14))                 OPTIONAL,
    isdnLowLayer        [20] OCTET STRING (SIZE (2..14))                 OPTIONAL,
    uri                 [21] SET OF UTF8String                           OPTIONAL,
    sipHeader           [22] SET OF SipHeader                            OPTIONAL,
    nai                 [27] UTF8String                              OPTIONAL,
    mac802              [28] VisibleString                               OPTIONAL,
    fqdn                [29] UTF8String                              OPTIONAL
}

PortNumber ::= INTEGER

SDP ::= UTF8String

SipHeader ::= UTF8String


-- The following are optional messages:

SurveillanceStatus ::= SEQUENCE {
    caseId              [0] CaseIdentity,
    reportingSystemId  [1] IAPSystemIdentity                             OPTIONAL,
                                -- include to identify the system reporting the surveillance status,
                                -- when the underlying data carriage does not imply that system.
    timestamp           [2] TimeStamp,
    statusEventType[3] SurveillanceStatusEventType,
    currentStatus       [4] CurrentSurveillanceStatus
}

CurrentSurveillanceStatus ::= ENUMERATED {
    fullyActive         (0),
    partiallyActive(1),
    inactive            (2)
}

SurveillanceStatusEventType ::= ENUMERATED {
    activation          (0),
    deactivation        (1),
    change              (2),
    scheduledReport(3)
}

FeatureManagement ::= SEQUENCE {
    caseId              [0] CaseIdentity,
    iAPSystemId         [1] IAPSystemIdentity                             OPTIONAL,
                            -- include to identify the system containing the Intercept Access Function,
                            -- when the underlying data carriage does not imply that system.
    timestamp           [2] TimeStamp,
    subscriberId        [3] PartyIdentity                                 OPTIONAL,
                            -- Include to identify the subscriber to the service, when the identifier is
                            -- more specific than the intercept subject identity associated with the
                            -- CaseIdentity.
    featureId           [4] UTF8String,
    managementType      [5] FeatureManagementType,
    activationInfo      [6] UTF8String                                    OPTIONAL,
                            -- include to identity information provided for use by a feature
                            -- (e.g., forward-to number for call forwarding), when feature activation
                            -- was attempted and information was provided for use by the feature.
    failureReason       [7] UTF8String                                    OPTIONAL
                            -- include to indicate the reason for an unsuccessful feature activation or
                            -- deactivation, when the feature activation or deactivation was unsuccessful.
}

FeatureManagementType ::= ENUMERATED {
    activation      (0),
    deactivation    (1)
}

IAPSystemIdentity ::= CHOICE {
    string                  [1] VisibleString (SIZE (1..15)),
                        -- Used for backwards compatibility with J-STD-025-B.
    iAPSystemIdentityType  [2] IAPSystemIdentityType
                        -- Used for reporting IP address formats and reporting multiple identity types.
}
```

```
IAPSystemIdentityType ::= SEQUENCE {
    ipV4              [1] OCTET STRING (SIZE(4))                      OPTIONAL,
    ipV6              [2] OCTET STRING (SIZE(16))                     OPTIONAL,
    fqdn              [3] OCTET STRING                                OPTIONAL,
                          -- Fully Qualified Domain Name and the trailing “.” may not be included.
    other             [4] OCTET STRING                                OPTIONAL
}

SystemIdentity ::= IAPSystemIdentity

TerminalDisplayInfo ::= SEQUENCE {
   generalDisplay         [0] VisibleString (SIZE(1..80))          OPTIONAL,
   calledNumber           [1] VisibleString (SIZE(1..40))          OPTIONAL,
   callingNumber              [2] VisibleString (SIZE(1..40))          OPTIONAL,
   callingName            [3] VisibleString                        OPTIONAL,
   originalcalledNumber       [4] VisibleString (SIZE(1..40))          OPTIONAL,
   lastRedirectNumber     [5] VisibleString (SIZE(1..40))          OPTIONAL,
   redirectingName        [6] VisibleString (SIZE(1..40))          OPTIONAL,
   redirectingReason          [7] VisibleString (SIZE(1..40))          OPTIONAL,
   messageWaitingNotif    [8] VisibleString (SIZE(1..40))          OPTIONAL
}


END -- of ATIS-LAES-VoIP-Abstract-Syntax-Module



CCDeliveryHeaderModule
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-678(0) ccdeliveryheader(1) version-5(4)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

TimeStamp, CaseIdentity
FROM Laesp-j-std-025-b {iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-
b(2) version-1(0)}

CallIdentity, IAPSystemIdentity
FROM ATIS-LAES-VoIP-Abstract-Syntax-Module{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-
678(0) cii(0) common (0) version-5(4)};

cCDeliveryHeaderModuleOID OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1)
t1-678(0) ccdeliveryheader(1) version-5(4)}
               -- OID for CCDeliveryHeaderModule

CCProtocol ::= SEQUENCE {
    cCDeliveryHeaderModuleOID  [0] OBJECT IDENTIFIER,
    ccapdu                     [1] CC-APDU
}

CC-APDU ::= SEQUENCE {
    ccDeliveryHeader   [0] CCDeliveryHeader,
    payload            [1] OCTET STRING
}

CCDeliveryHeader ::= SEQUENCE {
    correlationInfo[0] SEQUENCE {
            caseId             [0] CaseIdentity                           OPTIONAL,
            iapId              [1] IAPSystemIdentity                      OPTIONAL,
            callID             [2] CallIdentity},
    timeStamp          [1] TimeStamp,
    packetDirection    [2] PacketDirection                                OPTIONAL,
    sequenceNumber     [3] INTEGER                                        OPTIONAL,
    payloadType        [4] PayloadType          OPTIONAL,
    -- Required for RCS Messaging Services


    -- The following are used primarily for payloadType fileObject
    msgIdentifier      [5] INTEGER          OPTIONAL,
    chunkNumber        [6] INTEGER (0..2147483647)      OPTIONAL,
    lastChunk          [7] BOOLEAN            OPTIONAL,
    contentType        [8] RCSContentType            OPTIONAL,

    ...

}


-- For the following, refer to the OMA WSP Content Type Registry [Ref 32]
RCSContentType ::= CHOICE {
    wellKnownMedia [0] INTEGER (0..127),
    mediaType    [1] UTF8String
}
PacketDirection ::= ENUMERATED {
    fromSubject    (0),
    toSubject      (1)
}
PayloadType ::= ENUMERATED {
    msrpNoTCP          (0), -- MSRP payload without layer 3 or layer 4 headers
    msrpTCP        (1), -- MSRP payload with TCP layer
    fileObject     (2), -- Body of a file object
    ...
}


END -- of CCDeliveryHeaderModule
```

Annex B SIP Mappings

(informative)

This annex is informative and is not considered part of this Standard.

This annex provides the message and parameter mappings from SIP standard signaling to the surveillance messages reported to the LEA by the TSP. Vendors who develop vendor-specific implementations that utilize non-standard SIP messages, parameters, or parameter values must specify how they map such messages, parameters, or parameter values to the VoIP surveillance messages specified in this standard, in order to be compliant to this Standard.

When VoIP Surveillance information reporting is triggered by SIP signaling, the messages described in Clause 6 are generated and sent from the DF to the CF, or, in the case of DSR, the DirectSignalReporting message and the encapsulated SIP message are sent to the CF. The message mappings in this annex are described from the perspective of the 'e' interface (the interface between the DF and the CF). A SIP protocol-specific trigger encountered at the IAP shall cause the SIP mapped message to be sent to the CF, or in the case of DSR (the DirectSignalReporting message), to be sent to the CF.

The following note is referenced in several tables in this Annex:

> NOTE B1 - This information is not necessarily mapped from the triggering SIP message, but may be derived from other available information.

B.1 Message Mappings

This clause defines the mapping of SIP messages to surveillance messages defined in this Standard. Table B.1 identifies SIP message mappings when the Subject originates a session. Table B.2 identifies SIP message mappings when a session is terminated to the Subject.

Mappings for the SIP protocol occur when the network's call processing equipment is in the path of the SIP message exchange. These mappings do not apply when the network's call processing equipment is not in the path of the SIP message exchange.

> NOTE: The SIP response "100 Trying" may be present in SIP call flows, depending upon the implementation in the CMS, the User Agent, and the placement of the IAP. Reporting of the "100 Trying" to law enforcement is not required.

Table B.1: SIP Message Mapping - Subject Origination

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
INVITE		Origination	Indication that a call has been initiated by the Subject.
	180 Ringing	NetworkSignal (subjectAudibleSignal (ringbackTone))	Indication that an Associate's device has been alerted.
	181 Call Is Being Forwarded	NetworkSignal ("call forwarding" as other)	Indication that the call has been forwarded by or on behalf of the Associate.
	182 Queued	NetworkSignal ("queued" as other)	Indication that the call has been queued.
	183 Session Progress	MediaAndAddressReporting	Used to pass SDP information, if present in the 183 Session Progress.
	200 OK (to INVITE)	Answer	Indication that the call has been answered.
	200 OK (to PRACK or UPDATE	MediaAndAddressReporting	Used to pass SDP information, if present in the 200 OK.
	3xx, 4xx, 5xx, 6xx	Release (with release reason/code)	Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 3xx, 4xx, 5xx, or 6xx). For 3xx redirection, the redirection information is also provided with the Release message. A 487 response to a CANCEL message maps to Release.
ACK (for 200 OK to INVITE) PRACK		MediaAndAddressReporting	Used to report the SDP information, if present in the ACK or PRACK.
BYE	BYE	Release (with release reason/code)	Indication that the call has been or is being released.
UPDATE	UPDATE	MediaAndAddressReporting	Used to pass SDP information, if present in the UPDATE.
CANCEL		SubjectSignal	Used to indicate that Subject has abandoned a call origination before the call is answered.

Table B.2: SIP Message Mapping - Subject Termination

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
	INVITE	TerminationAttempt	Indication there has been an attempt to terminate a call to the Subject.
180 Ringing		SubjectSignal (“alerting” as the otherSignalingInformation)	Indication that the Subject’s device has been alerted.
183 Session Progress		MediaAndAddressReporting	Used to pass SDP information, if present in the 183 Session Progress.
200 OK (to INVITE)		Answer	Call is answered (by Subject or agent).
200 OK (to PRACK or UPDATE)		MediaAndAddressReporting	Used to send SDP information, if present in the 200 OK..
4xx, 5xx, 6xx		Release (with release reason/code)	Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 4xx, 5xx, or 6xx). Note that the Release message is not sent if the call is not released (e.g., a 486 Busy may result in call forwarding rather than a release).
3xx		Release	The original session is released. The redirection information is provided in the Contact field of the Release message.
	ACK (for 200 OK to INVITE) PRACK	MediaAndAddressReporting	Used to send SDP information, if present in the ACK or PRACK.
BYE	BYE	Release (with release reason/code)	Indication the call has been or is being released.
UPDATE	UPDATE	MediaAndAddressReporting	Used to pass SDP information, if present in the UPDATE.

Table B.3: SIP Message Mapping – Subject Registration

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
REGISTER		ServingSystem	The Subject requests registration of contact information.
	200 OK	ServingSystem	Include registration information.
	4xx, 5xx	ServingSystem	Include failure reason.

Table B.4: SIP Message Mapping – REFER

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
REFER (per RFC 3515 [Ref 15])		SubjectSignal (“REFER” as otherSignalingInformation)	The Subject sends a REFER message.
	REFER (per RFC 3515 [Ref 15])	NetworkSignal (“REFER” as other)	The Associate sends a REFER message.

Table B.5: SIP Message Mapping – NOTIFY

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
NOTIFY (per RFC 3265 [Ref 16])		SubjectSignal (“NOTIFY” as otherSignalingInformation)	The Subject sends a NOTIFY message.
	NOTIFY (per RFC 3265 [Ref 16])	NetworkSignal (“NOTIFY” as other)	The Associate sends a NOTIFY message.

Table B.6: SIP Message Mapping – Hold and Retrieve

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
re-INVITE (hold) or UPDATE (hold)		SubjectSignal (“hold” as otherSignalingInformation)	Indication the Subject has requested the media stream to be suspended (i.e., hold).
	re-INVITE (hold) or UPDATE (hold)	NetworkSignal (“hold” as other)	Indication the Associate has requested the media stream to be suspended (i.e., hold).
200 OK (to re-INVITE (hold) or to UPDATE (hold))	200 OK (to re-INVITE (hold) or to UPDATE (hold))	ConnectionBreak	Indication that the party has accepted the hold.
re-INVITE (retrieve) or UPDATE (retrieve)		SubjectSignal (“retrieve” as otherSignalingInformation)	Indication the Subject has requested the media to be re-established.
	re-INVITE (retrieve) or UPDATE (retrieve)	NetworkSignal (“retrieve” as other)	Indication the Associate has requested the media to be re-established.
200 OK (to re-INVITE (retrieve) or to UPDATE (retrieve))	200 OK (to re-INVITE (retrieve) or to UPDATE (retrieve))	Connection	Indication that the party has accepted the retrieve.

Table B.7: SIP Message Mapping – Subject Initiated Conferences

SIP Message				LAES Message	Description
From Subject	To Subject	From Associate	To Associate		
INVITE				Origination	Indication that Subject has sent an invitation to a Conference.
INVITE UPDATE				SubjectSignal ("hold" as otherSignalingInformation)	Indication that Subject has sent a re-INVITE/UPDATE to place a Conference on hold.
INVITE UPDATE				SubjectSignal ("retrieve" as otherSignalingInformation)	Indication that Subject has sent a re-INVITE/UPDATE to retrieve a Conference from hold.
	200 OK (INVITE)			Answer	Indication that Subject's invitation to a Conference is answered.
	200 OK (INVITE) 200 OK (UPDATE)			ConferencePartyChange or Connection	Indication that Subject has retrieved a Conference from hold.
	200 OK (INVITE) 200 OK (UPDATE)			ConferencePartyChange or ConnectionBreak	Indication that Subject has placed a Conference on hold.
REFER				SubjectSignal ("refer" as otherSignalingInformation)	Indication that Subject has sent a REFER message to add an Associate to a Conference or to drop an Associate from a Conference.
		200 OK (INVITE)		ConferencePartyChange or Connection	Indication that an Associate has joined a Conference.
			BYE	ConferencePartyChange or ConnectionBreak	Indication that an Associate has been dropped from a Conference.
		BYE		ConferencePartyChange or ConnectionBreak	Indication that an Associate has dropped out of a Conference.
	BYE			Release	Indication that Subject's call leg has been released.
BYE				Release	Indication that Subject's call leg has been released.

Note 1: When the conference bridge used for the Conference resides within the Subject's device, the reported CII messages are not correlated between the call legs.

Note 2: The mapping shown in this table is based on the assumption that the conferencing function is provided by the CMS.

Table B.8: SIP Message Mapping – Attended Transfer

SIP Message sent by Subject	SIP Message received by Subject	Surveillance Message	Description
re-INVITE(hold)		SubjectSignal (“hold” as otherSignalingInformation)	Indicates the Subject places an Associate on hold.
	200 OK	ConnectionBreak	Indicates the Associate accepts the hold request.
INVITE		Origination	Indicates the Subject originates a call to another Associate.
	180 Ringing	NetworkSignal (subjectAudibleSignal (ringbackTone))	Indicates Associate is alerted.
	200 OK (to INVITE)	Answer	Indicates Associate answered the call.
REFER		SubjectSignal (“REFER” as otherSignalingInformation)	Indicates Subject requests an Associate to transfer the call to another Associate.
	202 Accepted	NetworkSignal (“accepted” as other)	Indicates transfer accepted.
	NOTIFY	NetworkSignal (“NOTIFY” as other)	Indicates the result of the transfer request, i.e., Transfer Complete (indicated by placing the result in the “Other” field of the NetworkSignal message).
BYE	BYE	Release	Indicates release of the call between the Subject and an Associate.

Table B.9: SIP Message Mapping – Call Forwarding

SIP Message sent towards the calling party	SIP Message sent towards the forwarded-to party	Surveillance Message	Description
181 Call is Forwarded	INVITE	Redirection	Indication that the call attempt has been forwarded by or on behalf of the Subject. At this time, a 181 Call is Forwarded is sent towards the calling party. Note that no Redirection message is sent if one of the two indicated SIP messages are not sent.
180 Ringing		MediaAndAddressReporting	Used to pass SDP information, if present in 180 Ringing.
183 Session Progress		MediaAndAddressReporting	Used to pass SDP information, if present in 183 Session Progress.
200 OK (to INVITE)		Answer	Call is answered (by forwarded-to party or agent).
200 OK (to PRACK or UPDATE)		MediaAndAddressReporting	Used to send SDP information, if present in 200 OK.
4xx, 5xx, 6xx		Release (with release reason/code)	Indication that the call has been or is being released. The Release message indicates the reason for release (i.e., the SIP response code of 4xx, 5xx, or 6xx). A 487 response to a CANCEL message maps to Release.
3xx		Release	The original session is released. The redirection information is provided in the Contact field of the Release message.
	ACK (for 200 OK to INVITE) PRACK	MediaAndAddressReporting	Used to send SDP information, if present in ACK or PRACK.
BYE	BYE	Release (with release reason/code)	Indication the call has been or is being released.
UPDATE	UPDATE	MediaAndAddressReporting	Used to pass SDP information, if present in UPDATE.

B.2 Message Parameter Mappings

The following tables show what information is mapped from SIP messages to VoIP LAES messages in this Standard. When a table specifies mapping of a SIP header to a parameter whose ASN.1 type is SipHeader, the whole header, including its name (e.g., “To: ...”), is included in the parameter.

The following parameters are not shown in the subsequent tables, but shall be included in VoIP LAES messages per the requirements of this Standard:

- Case Identity
- IAPSystemIdentity
- TimeStamp

The following table shows the mapping of SIP message parameters from a SIP INVITE message to the LAES Origination message when a call is originated from the Subject.

Table B.10: INVITE to Origination Message Parameter Mapping (Subject Origination)

INVITE Message Parameter	Origination Message Parameter	Description
Call-ID	callId	Identifies the call or session.
From	calling	See Note 1.
To	called	See Note 2.
Request-URI	called	See Note 3.
Request-URI	input userInput	Input Request-URI received.
Contact	calling	Contact information present in the INVITE sent by the Subject.
Application: SDP information	subjectMedia	Identifies SDP information when present.
see note B1 at the beginning of annex B	originationCause	Include ‘SIP INVITE.’
see note B1 at the beginning of annex B	transitCarrierId	Provide if known.
P-Access-Network-Info, or see note B1 at the beginning of annex B	location	Provide if known.
P-Asserted-Identity	calling	See Note 4.

Note 1: The FROM field does not necessarily provide the identity of the calling party. For example, it won’t be the calling party identity if the FROM field has the value “anonymous@invalid.com” (and it can be that way in some cases).

Note 2: The TO field does not necessarily provide the identity of the real destination. When a subject-initiated call does not encounter any redirections, the TO field may correctly identify the called party. However, when a subject-initiated call encounters one or more redirections (i.e., network initiated call forwarding), the TO field contains the identity of the original called party instead of the real destination. For example, if Subject calls party A, and if the network detects a call forwarding from party A to the party B, then the TO field points to party A rather than to party B who is the real destination of the call.

Note 3: The REQUEST URI field does not necessarily provide the identity of the real destination. When a subject-initiated call does not encounter any redirections, the REQUEST URI field may correctly identify the called party. However, when a subject-initiated call encounters one or more redirections (i.e., network initiated call forwarding), the REQUEST URI field contains the identity of the original called party instead of the real destination. For example, if the Subject calls party A, and if the network detects a call forwarding from party A to the party B, then the REQUEST URI field points to party A rather than to party B who is the real destination of the call.

Note 4: The SIP From field does not contain reliable calling party information since it comes from the user agent and is generally not validated by a TSP. The P-Asserted-Identity [Ref 21] contains calling party identity that is validated by the TSP and is trustworthy.

The following table shows the mapping of SIP message parameters from a SIP INVITE message to the LAES TerminationAttempt message when an incoming call arrives at the Subject.

Table B.11: INVITE to TerminationAttempt Message Parameter Mapping Table (Subject Termination)

INVITE Message Parameter	TerminationAttempt Message Parameter	Description
Call-ID	callId	Identifies the call or session.
From	calling	See Note 1.
To	called	See Note 2.
Request-URI	called	See Note 3.
Application: SDP information	associateMedia	Identifies SDP information when present.
History-Info	redirectedFromInfo	Provides information, if known, about redirection when the incoming call was previously redirected.
P-Asserted-Identity	calling	See Note 4.

Note 1: The FROM field does not necessarily provide the identity of the calling party. For example, the FROM field won't be the calling party identity if the FROM field has the value "anonymous@invalid.com" (and it can be that way in some cases).

Note 2: The TO field does not necessarily provide the identity of the called party. When a terminating call arrives at the Subject without any prior redirections, the TO field may correctly identify the called party. However, when a terminating call arrives at the Subject with one or more prior redirections (i.e., network initiated call forwarding), the TO field contains the identity of the original called party instead of the Subject. For example, if party A calls party B, and if the network detects a call forwarding from party B to the Subject, then the TO field points to party B rather than the Subject.

Note 3: The Request URI of the SIP INVITE message points to the identity of the Subject.

Note 4: The SIP FROM field does not contain reliable calling party information since it comes from the user agent and is generally not validated by a TSP. The P-Asserted-Identity [Ref 21] contains calling party identity that is validated by the TSP and is trustworthy.

General note: The calledPartyIdentity present within a TerminationAttempt message may contain the identity of one or more parties.

The following table shows the mapping of SIP message parameters from a SIP 180-RINGING message to the LAES SubjectSignal message when an incoming call arrives at the Subject.

Table B.12: 180-RINGING to SubjectSignal Message Parameter Mapping (Subject Termination)

180-RINGING Message Parameter	SubjectSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
see note B1 at the beginning of annex B	signal	Provide "SIP 180-RINGING"
Application: SDP information	subjectMedia	Identifies SDP information when present.

The following table shows the mapping of SIP message parameters from a SIP 180-RINGING message to the LAES NetworkSignal message when a call is originated from the Subject.

Table B.13: 180-RINGING to NetworkSignal Message Parameter Mapping (Subject Origination)

180-RINGING Message Parameter	NetworkSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Contact	associateContactAddresses	Contact information when present in a 180 response.
see note B1 at the beginning of annex B	subjectAudibleSignal	Provide 'ringback' tone.
Application: SDP information	associateMedia	Identifies SDP information when present.

Note 1: The CONTACT field present within the SIP 180-RINGING message may point to the identity of the Associate.

The following table shows the mapping of SIP message parameters from a SIP 200 OK (INVITE) message to the LAES Answer message when a call is originated from the Subject or when an incoming call arrives at the Subject.

Table B.14: 200-OK (INVITE) to Answer Message Parameter Mapping (Subject Origination and Termination)

200-OK Message Parameter	Answer Message Parameter	Description
Call-ID	callId	Identifies the call or session.
see note B1 at the beginning of annex B	answering	Included if known to identify the answering party. May be derived from: (1) the Request-URI present in the SIP INVITE sent to the terminating user (who is an Associate in the Subject Origination case or to the Subject in the Subject Termination case); or (2) from other means. Not present in the SIP 200 OK message.
Contact	answering	Identifies Contact header content. Usually, it is the IP address of the party sending the SIP 200-OK message. See Note 1.
P-Access-Network-Info.	location	Only included if present in the SIP 200 response for the Subject termination case.
Application: SDP information	answeringMedia	Identifies SDP information when present.

Note 1: Used only for Subject Terminating call. For a Subject Originating call, this field may not be pointing to the IP address of the answering party due to the possibility of a back-to-back user agent (B2BUA) changing the Contact header field value.

General Note: The answeringPartyIdentity present within an Answer message may contain the identity of one or more parties.

Table B.15: BYE to Release Message Parameter Mapping (Subject Origination and Termination)

BYE Message Parameter	Release Message Parameter	Description
Call-ID	callId	Identifies the call or session.
P-Access-Network-Info, or see note B1 at the beginning of annex B	location	Provide if known.
see note B1 at the beginning of annex B	cause	Provide "SIP BYE".

Table B.16: ACK or PRACK to MediaAndAddressReporting Message Parameter Mapping (Subject Origination and Termination)

ACK or PRACK Message Parameter	MediaAndAddressReporting Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Application: SDP information	subjectMedia associateMedia	Identifies SDP information.
Contact	subjectContactAddresses	Contact information when present in an ACK or PRACK response (sent by a Subject).
Contact	associateContactAddresses	Contact information when present in an ACK or PRACK response received by the Subject.
See note B1 at the beginning of annex B	mediaAndAddressReportingCause	“ACK” or “PRACK”

Table B.17: 183 Session Progress to MediaAndAddressReporting Message Parameter Mapping (Subject Origination and Termination)

183 Session Progress Message Parameter	MediaAndAddressReporting Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Application: SDP information	subjectMedia associateMedia	Identifies SDP information.
Contact	subjectContactAddresses	Contact information when present in a 183 Session Progress response sent by the Subject.
Contact	associateContactAddresses	Contact information when present in a 183 Session Progress received by the Subject.
See note B1 at the beginning of annex B	mediaAndAddressReportingCause	“183 Session Progress”

Table B.18: UPDATE to MediaAndAddressReporting Message Parameter Mapping (Subject Origination and Termination)

UPDATE Message Parameter	MediaAndAddressReporting Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Application: SDP information	subjectMedia associateMedia	Identifies SDP information.
Contact	subjectContactAddresses	Contact information when present in an UPDATE sent by the Subject.
Contact	associateContactAddresses	Contact information when present in an UPDATE response received by the Subject.
See note B1 at the beginning of annex B	mediaAndAddressReportingCause	“UPDATE”

Table B.19: 4xx, 5xx, 6xx to Release Message Parameter Mapping (Subject Origination and Termination)

4xx/5xx/6xx Message Parameter	Release Message Parameter	Description
Call-ID	callId	Identifies the call or session.
P-Access-Network-Info, or see note B1 at the beginning of annex B	location	Provide if known.
Response Code	cause	Provide the 4xx, 5xx, 6xx failure reason code (e.g., 'SIP 400').
Contact	contactAddresses	Provide if known.

Table B.20: 3xx to Release Message Parameter Mapping (Subject Origination and Termination)

3xx Message Parameter	Release Message Parameter	Description
Call-ID	callId	Identifies the call or session.
P-Access-Network-Info, or see note B1 at the beginning of annex B	location	Provide if known.
Response Code	cause	Provide the 3xx redirection reason code (e.g., 'SIP 301').
Contact	contactAddresses	Provide if known.

Table B.21: REGISTER and 200-OK/4xx/5xx/6xx to ServingSystem Parameter Mapping

REGISTER Request Message Parameter	200-OK /4xx/5xx/6xx Response Message Parameter	ServingSystem Message Parameter	Description
see note B1 at the beginning of annex B		systemIdentity	Provide the identity of the serving system.
Call-ID		requestId	Identifies a register request.
see note B1 at the beginning of annex B		registrationType	Identifies the type of registration.
To		registering	Identifies the party associated with the address information.
From		requesting	Identifies the party making the request.
Request-URI		registrar	Identifies the registrar.
Contact(s)		requestAddressInfo	Contact information present in the REGISTER sent by the Subject.
Expires		expirationPeriod	Identifies SIP Expires information when present.
	Contact(s)	responseAddressInfo	Address information in the response.
	Response Code	failureReason	Included by registrar when request fails (e.g., SIP 4xx, 5xx, 6xx).
	Expires	expirationPeriod	Identifies SIP Expires information when present.

The following table shows the mapping of SIP message parameters from a SIP REFER message to the LAES NetworkSignal message when the Subject's device receives a SIP REFER message

Table B.22: REFER to NetworkSignal Message Parameter Mapping

REFER Message Parameter	NetworkSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Request-URI	signaledToPartyId	Identifies the signaled-to party (i.e., Subject).
Contact	associateContactAddresses	Contact information when present in a REFER received by the Subject.

Table B.23: REFER to SubjectSignal Message Parameter Mapping

REFER Message Parameter	SubjectSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Request-URI	signaledPartyId	Identifies the signaled-to party or network resource of the SIP REFER.

The following table shows the mapping of SIP messages to the parameters of the LAES DSR message. With mapped messaging, only those SIP messages that are not mapped are reported as DSR messages.

Table B.24: SIP Messages to DSR Message Parameter Mapping

SIP Message	DSR Message Parameter	Description
	callId	Uniquely identifies a series of encapsulated signaling messages (e.g., for a SIP session).
Any SIP message	signalingMsg	The SIP message received from the Intercept Subject, sent to the Intercept Subject, or sent or received on behalf of the Intercept Subject. If the CMS modifies a received message and then sends the modified message, both the message received and sent should be reported by the CMS.

The following table shows the mapping of SIP message parameters from a SIP 181 Call Is Being Forwarded (Subject Origination) message to the LAES NetworkSignal message.

Table B.25: 181 Call Is Being Forwarded to NetworkSignal Message Parameter Mapping (Subject Origination)

181 Call Is Being Forwarded Message Parameter	NetworkSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
see note B1 at the beginning of annex B	other	Provide “call forwarding”.

The following table shows the mapping of SIP message parameters from a SIP 200 OK (re-INVITE or UPDATE) message to the LAES ConnectionBreak message when a party is placed on hold.

Table B.26: 200-OK (re-INVITE-hold or UPDATE-hold) to ConnectionBreak Parameter Mapping (the media stream has been suspended)

200-OK Message Parameter	ConnectionBreak Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Application: SDP information	suspendedMedia	Identifies SDP information when present.
see note B1 at the beginning of annex B	removedParties	None of the SIP headers in the SIP 200 OK can confidently point to the removed party. Therefore, this is derived using the P-Asserted-Identity if present or the request URI in the SIP INVITE or the SIP UPDATE to which this SIP 200 OK is returned.

The following table shows the mapping of SIP message parameters from a SIP 200 OK (re-INVITE or UPDATE) message to the LAES Connection message when a party is retrieved from hold.

Table B.27: 200-OK (re-INVITE-retrieve or UPDATE-retrieve) to Connection Parameter Mapping (indicates the media stream has been re-established)

200-OK Message Parameter	Connection Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Application: SDP information	connectedMedia	Identifies SDP information when present.
see note B1 at the beginning of annex B	newParties	None of the SIP headers in the SIP 200 OK can confidently point to the new party. Therefore, this is derived using the P-Asserted-Identity if present or request URI in the SIP INVITE or SIP UPDATE to which this SIP 200 OK is returned.

The following table shows the mapping of SIP message parameters from a SIP 200 OK (UPDATE or PRACK) message to the LAES MediaAndAddressReporting message.

Table B.28: 200-OK (UPDATE or PRACK) to MediaAndAddressReporting Parameter Mapping

200-OK Message Parameter	MediaAndAddressReporting Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Contact	subjectContactAddresses	Contact information when present in a 200 response sent by the Subject.
Contact	associateContactAddresses	Contact information when present in a 200 response received by the Subject.
Application: SDP information	subjectMedia associateMedia	Identifies SDP information when present.

The following table shows the mapping of SIP message parameters from a re-INVITE or SIP UPDATE message to the LAES SubjectSignal message when the Subject’s device sends one of those messages.

Table B.29: re-INVITE (hold) or UPDATE (hold) to SubjectSignal Parameter Mapping (request media stream be suspended)

re-INVITE or UPDATE Message Parameter	SubjectSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Contact	signalingPartyId	Contact information when present in the INVITE or UPDATE sent by the Subject.
Application: SDP information	subjectMedia	Identifies SDP information when present.
see note B1 at the beginning of annex B	signal	Include “hold”.

The following table shows the mapping of SIP message parameters from a re-INVITE or SIP UPDATE message to the LAES NetworkSignal message when the Subject’s device receives one of those messages.

Table B.30: re-INVITE (hold) or UPDATE (hold) to NetworkSignal Parameter Mapping (request media stream be suspended)

re-INVITE or UPDATE Message Parameter	NetworkSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Request-URI	signaledToPartyId	
Contact	associateContactAddresses	Contact information when present in an INVITE or UPDATE received by the Subject.
Application: SDP information	associateMedia	Identifies SDP information when present.

The following table shows the mapping of SIP message parameters from a re-INVITE or SIP UPDATE message to the LAES SubjectSignal message when the Subject’s device sends one of those messages.

Table B.31: re-INVITE (Retrieve) or UPDATE (Retrieve) to SubjectSignal Parameter Mapping

re-INVITE or UPDATE Message Parameter	SubjectSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Contact	signalingPartyId	Contact information present in the INVITE or UPDATE sent by the Subject.
Application: SDP information	subjectMedia	Identifies SDP information when present.
see note B1 at the beginning of annex B	signal	Include “retrieve”.

General Note: The signalingPartyIdentity present in the SubjectSignal message may contain the identity of one or more parties.

The following table shows the mapping of SIP message parameters from a re-INVITE or SIP UPDATE message to the LAES NetworkSignal message when the Subject’s device receives one of those messages.

Table B.32: re-INVITE (Retrieve) or UPDATE (retrieve) to NetworkSignal Parameter Mapping

re-INVITE or UPDATE Message Parameter	NetworkSignal Message Parameter	Description
Call-ID	callId	Identifies the call or session.
Request-URI	signaledToPartyId	
Contact	associateContactAddresses	Contact information when present in an INVITE or UPDATE received by the Subject.
Application: SDP information	associateMedia	Identifies SDP information when present.

The following table shows the mapping of a SIP 200-OK to an LAES Connection message when a new party is added to a subject initiated conference call. There are two cases where a Connection message is sent to indicate the addition of a party to the conference: 1) when the Subject retrieves a held conference call; and 2) when a new party joins the subject initiated conference call. The following table handles the second case.

Table B.33: 200-OK (conference-joined) to Connection Parameter Mapping (a party has been added to a conference)

200-OK Message Parameter	Connection Message Parameter	Description
Call-ID	callId	Identifies the call or session.
see note B1 at the beginning of annex B	newParties	When the network adds a new party to the conference call, the party added is determined from the SIP INVITE sent to the new party. When a new party adds himself to the conference call, the party added is determined from the P-Asserted-Identity present in the SIP INVITE received from that new party.
Contact	newParties	Contact information when present in the 200 response.

Table B.34: BYE (party drop) to ConnectionBreak Parameter Mapping (a party drops from a conference)

BYE Message Parameter	ConnectionBreak Message Parameter	Description
Call-ID	callId	Identifies the call or session.
see note B1 at the beginning of annex B	droppedParties	Assuming this BYE is received from a party dropping from the conference, the party dropped out of the conference is determined based on the call leg information. The network may also use the FROM header of the BYE, even though the FROM header cannot be trusted to reveal to true party identity.
Contact	dropped	Contact information when present in the BYE.

B.3 SIP Forking

Table B.35: INVITE (Forked Call) to Origination Parameter Mapping

INVITE Message Parameters	ORIGINATION Message Parameters	Description
derived from Forked INVITE	forkedCalls	SET OF forked call information. Provide when Intercept Subject's INVITE is forked.
CallID	forkedCallId	Call ID of the forked call
REQUEST-URI	calledParty	Identify of the destination party of the forked call

Annex C SIP Information Flows

(informative)

This annex is informative and is not considered part of this Standard.

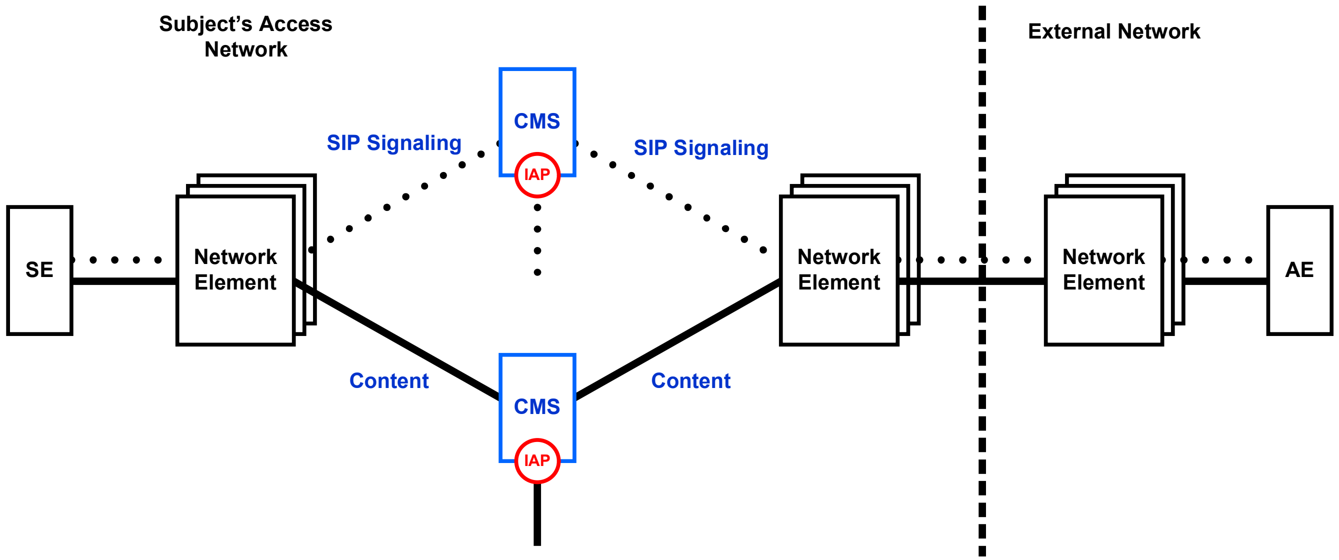
This annex is divided into two clauses. The scenarios in the first clause (C.1) illustrate the mapped method of reporting with SIP signaling. In this clause, it is assumed the CMS maintains call state for the duration of the call. The scenarios in the second clause (C.2) illustrate the Direct Signal Reporting method with SIP signaling. In this clause, it is assumed the CMS call state is not used to generate DSR messages. The best common practices for CCOpen are applicable to both mapped and direct signal methods of event reporting.

The information flows contained in this annex presume a particular network architecture and are provided to assist in the understanding and development of the VoIP LAES events, their triggers, and the associated surveillance messages with respect to SIP. The primary focus of the information flows is SIP signaling and the surveillance messages triggered by detection or processing of SIP signaling by a CMS function in a network element. A CC network element is also shown to assist with the understanding and relationship between the signaling controlling the communication and the actual communication content (i.e., call content).

The information flow examples are based on the premise that the SIP signaling is separated in time and place from the actual CC. Accordingly, a CMS function is shown in a separate network element from the network element processing the CC. In the case of mapping, the assumption is the CMS is call-stateful and has access to all necessary SIP signaling to enable the CMS to manage the communication. CII-IAPs and CC-IAPs are respectively present at the CMS and CC network elements.

Circled numbers (e.g., ①) in the flows indicate where surveillance messages may be triggered by the signaling.

The following figure depicts a network architecture for the scenarios. The information flows also support other possible configurations of network elements.



SE - Intercept Subject's Equipment
AE - Associate's Equipment
CMS - a network element with a CMS function (transaction stateful)
CC - a network element with access to call content
IAP - Intercept Access Point

Figure C.1: An Architecture for the SIP LAES Information Flows

All possible scenarios and signaling combinations for SIP messaging are not shown in the information flows, and surveillance messages may be triggered at different times based on different SIP information flows.

The following are the best common practices for reporting SIP Lawful Intercepts:

- CCOpen

The CCOpen message is applicable to CC intercepts. It is sent from the DF to CF to indicate media is enabled between the Subject and Associate, and correlate CC delivery to law enforcement with CII.

The trigger for media enablement, and therefore the trigger for the CCOpen message in a SIP signaling environment may be unidirectional or bidirectional.

In theory, when the SIP UA originating an INVITE includes SDP information in the INVITE method, the SIP UA receiving the INVITE may immediately begin sending media using any of the parameters in the originating UA's SDP.

In practice, the SDP information provides the receiving user agent (UA) the ability to negotiate the optimal parameters for media transmission. The receiving UA would respond with the optimal settings with SDP in the 1xx Ringing, 200 OK, or other response message.

While it is permissible to send a CCOpen message when the originating UA sends an INVITE with SDP, and a second CCOpen when the receiving UA responds with SDP indicating the optimal media parameters, it is not recommended. The first CCOpen does not serve a valid purpose as it would require the CF to enable all codecs indicated in the originating UA's codec list, and if the INVITE is rejected, requires a subsequent CCClose to be sent to tear down the binding set up by the CCOpen.

The best common practice recommendation is to send a single CCOpen when the receiving UA responds, and media negotiation is completed.

Note that the labeled messages (e.g., ①) in the information flows designate triggers for LAES reporting events.

C.1 Mapped Reporting of Call Related Events

For all information flows illustrated in Clause C.1, wherever a SIP request or response is shown without an associated LAES message being generated, a DSR message may be generated to report that SIP request or response.

C.1.1 Sessions Originated by Subject

C.1.1.1 Successful Session Completions

The information flow in Figure C.2 depicts a scenario where the intercept subject initiates a session with an associate and the associate accepts the invitation. In this scenario, media flow is begun by the intercept subject after acknowledging the session acceptance by the associate.

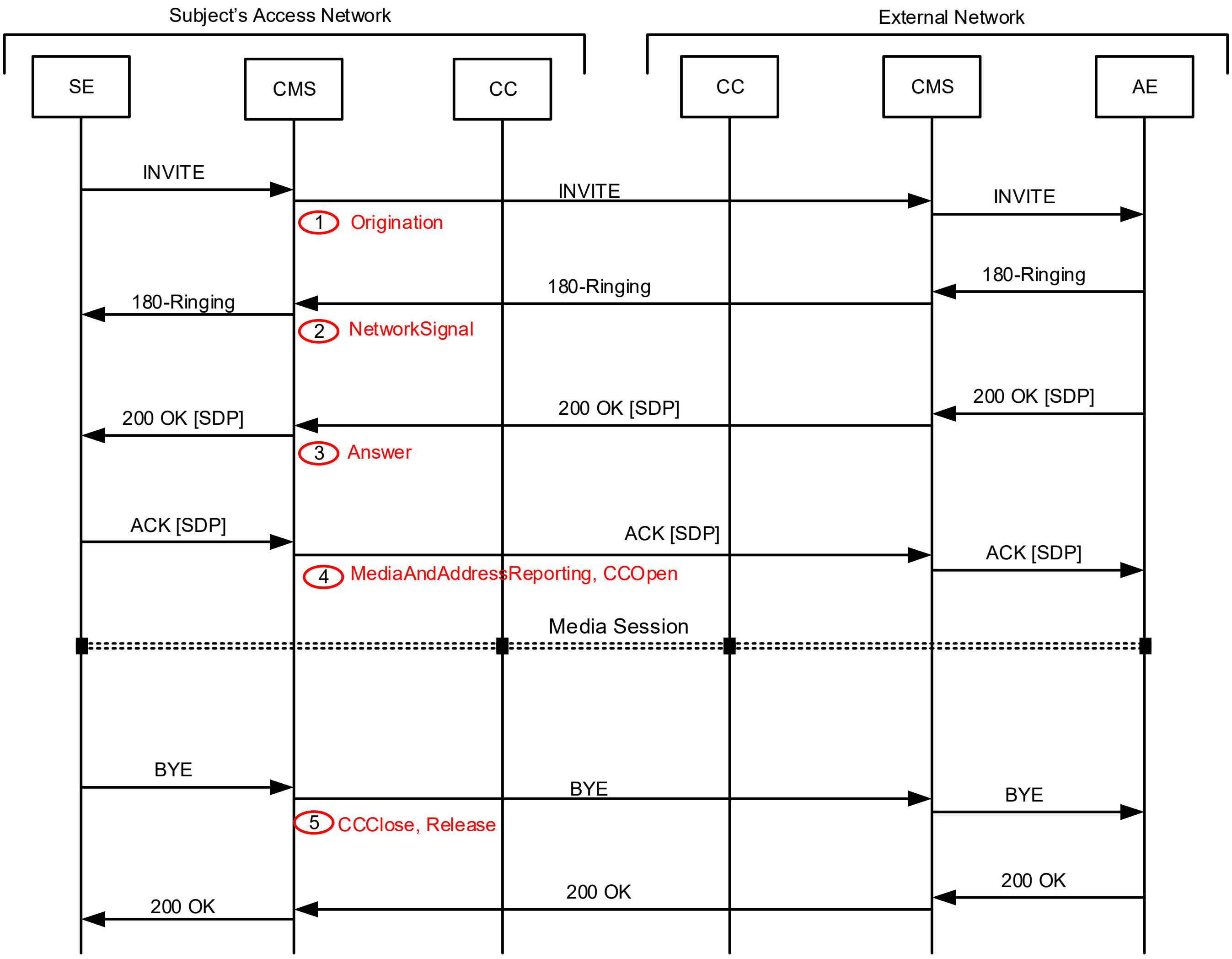


Figure C.2: Session Originated by Subject (Successful)

Notes:

Trigger Point 4: In this information flow, the SIP ACK contains the SDP information and hence, a MediaAndAddressReporting message is sent.

Trigger Point 5: The order of the CCClose and Release messages is not implied.

C.1.1.2 Unsuccessful Session Completions

C.1.1.2.1 Unsuccessful Session Completion with 4xx/5xx/6xx Release

The information flow in Figure C.3 depicts a scenario where the intercept subject initiates a session with an associate, and the associate or CMS on behalf of the associate rejects the invitation. In this scenario, media flow is not begun.

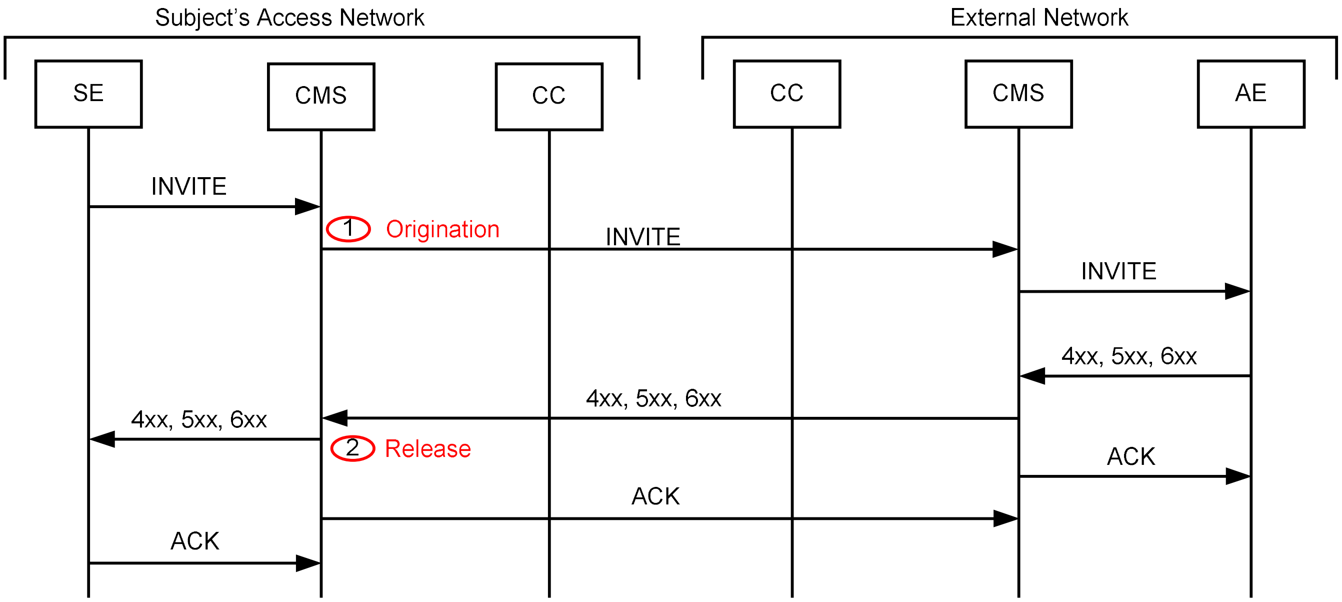


Figure C.3: Session Originated by the Subject with 4xx/5xx/6xx Release

C.1.1.2.2 Unsuccessful Session Completion with 3xx Redirection

The information flow in Figure C.4 depicts a scenario where the intercept subject initiates a session with an associate and the associate or CMS on behalf of the associate rejects the invitation. In this scenario, media flow is not begun.

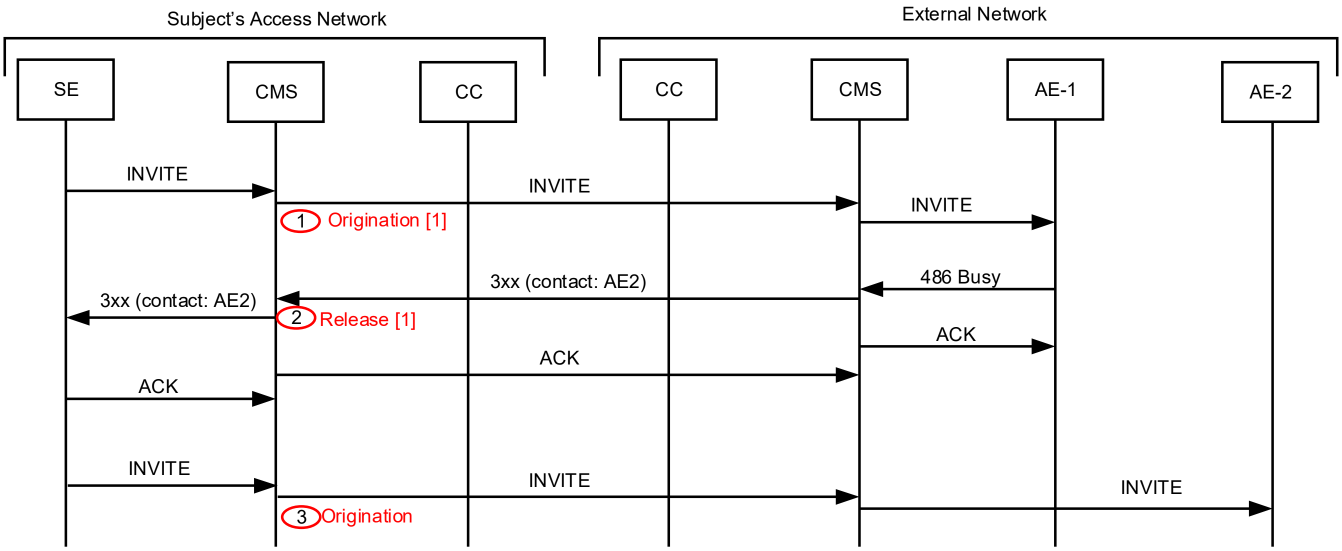


Figure C.4: Session Originated by the Subject with 3xx Redirection

Notes:

In this information flow, the Subject makes a call to Associate-1. The Associate-1's Equipment (AE-1) returns a 486 Busy. The AE-1's CMS determines that the call has to be redirected to AE-2 and returns a SIP 3xx with AE-2 information in the Contact header field. The Subject's equipment (SE), upon receiving the SIP 3xx, sends a new SIP INVITE to AE-2.

Trigger Points 1 and 2: In this scenario, the Origination and Release messages have Call Identity 1. The redirect information from the Contact header of the SIP 3xx message is reported in the "Contact" field of Release message.

Trigger Point 3: The Origination message will have the same Call identity as the Origination Message on trigger point 1 if the two INVITEs have the same SIP Call-ID.

C.1.1.3 Subject Cancels INVITE Request

Figure C.5 depicts a scenario where the intercept subject initiates a session with an associate and subsequently decides to cancel the invitation. In this scenario, media flow is not begun.

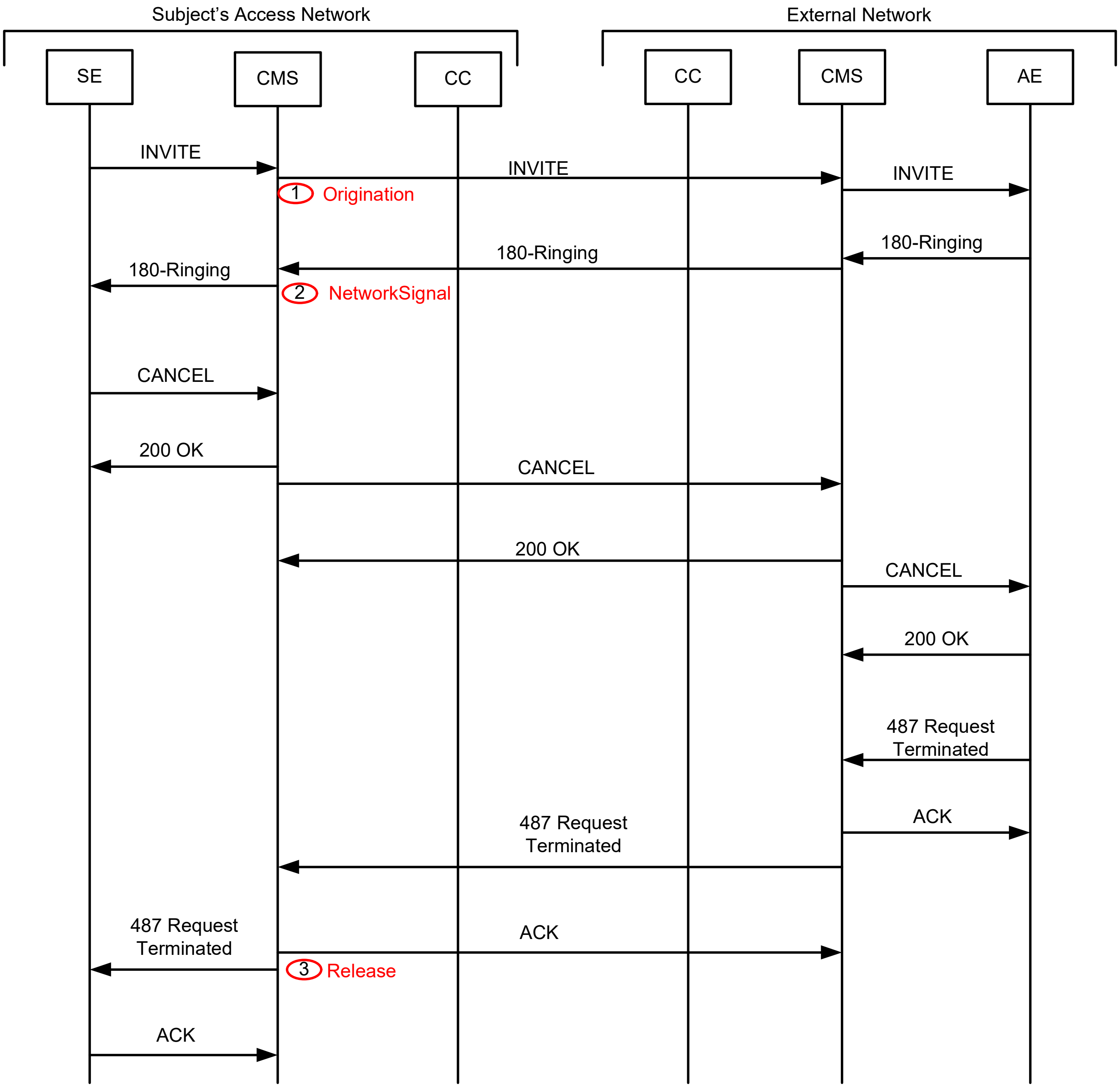


Figure C.5: Subject Cancels INVITE Request

Note:

The 200 OK is to the CANCEL request.

C.1.1.4 Forwarding by Associate

The information flow in Figure C.6 depicts a scenario where the intercept subject invites associate-1 to participate in a session and the session is then forwarded by associate-1's CMS to associate-2, due to associate-1's busy condition.

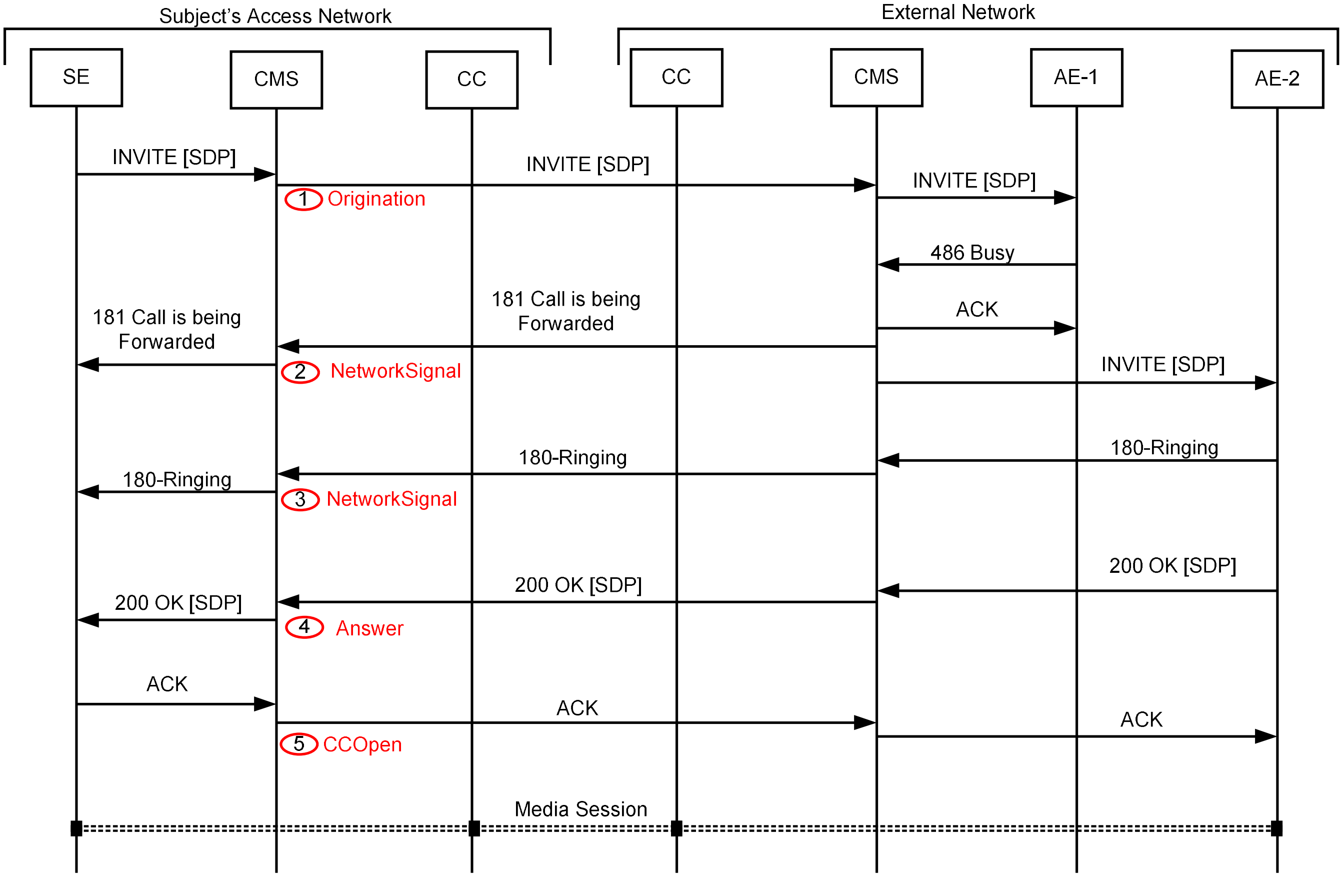


Figure C.6: Forwarding by Associate's CMS

C.1.1.5 Call Forking by Subject

The information flow in Figure C.7 depicts a scenario in which the intercept subject initiates a session with an associate and the intercept subject's CMS forks the session to three different destinations associated with the provided associate identity. The third associate's destination accepts the invitation. Sessions to other two destinations are not established.

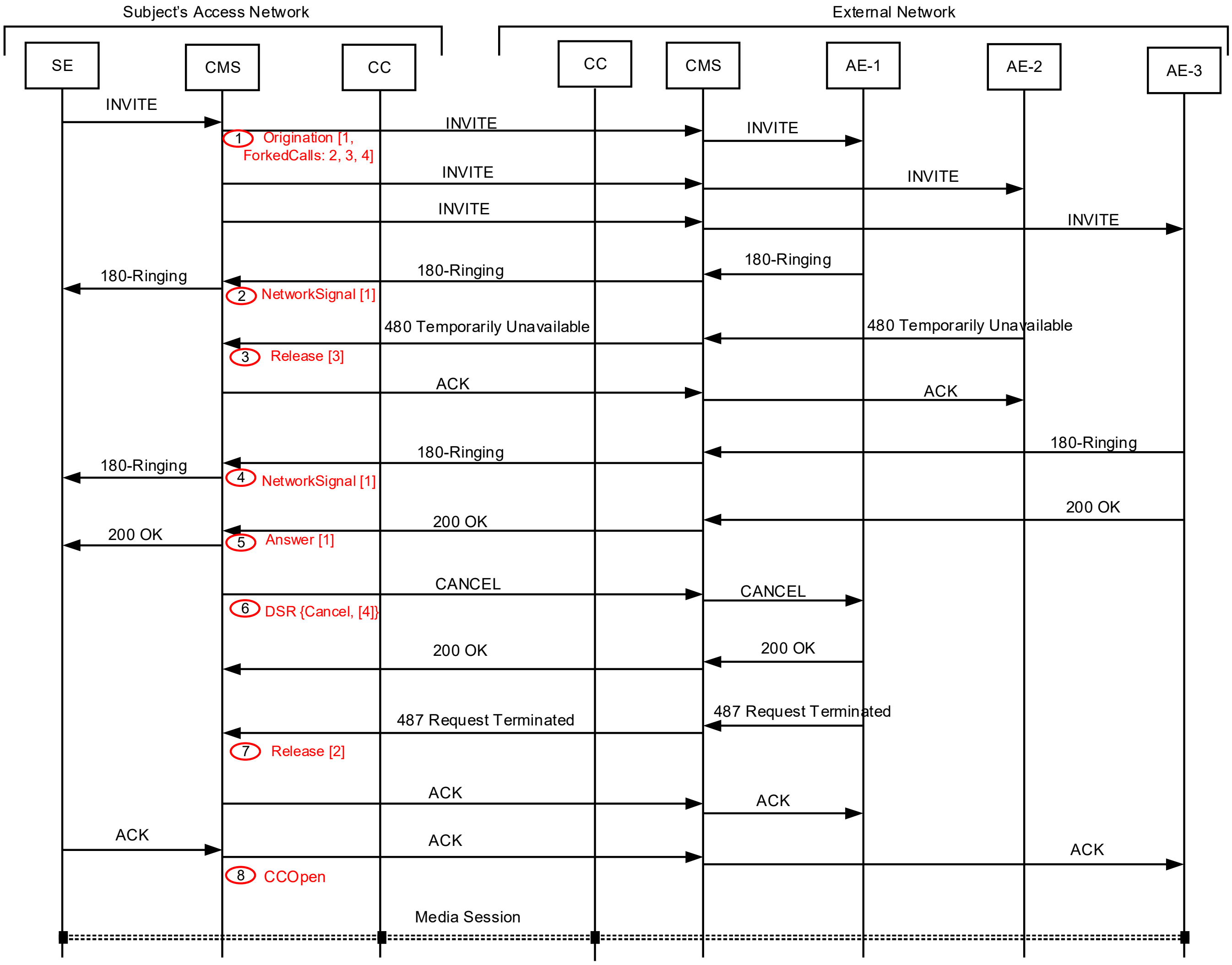


Figure C.7: Forking by Subject

Notes:

The numbers in the parenthesis indicate the Call Identity values associated with each of the LAES messages.

Trigger Point 1: The Subject's CMS forks the INVITE to three destinations (Call Identity 2, 3 and 4). An Origination message is reported containing the Call Identity related to the Subject's INVITE, and the Call Identities and destinations of the forked INVITEs.

Trigger Point 6: A DSR message encapsulating the Cancel message with Call Identity 4 is sent indicating that the Call Identity 4 is no longer in use.

C.1.2 Sessions Terminated to Subject

C.1.2.1 Successful Session Completions

The information flow in Figure C.8 depicts a scenario where the intercept subject receives and accepts an invitation to a session initiated by an associate. In this scenario, media flow is begun by the associate after acknowledging the session acceptance by the subject.

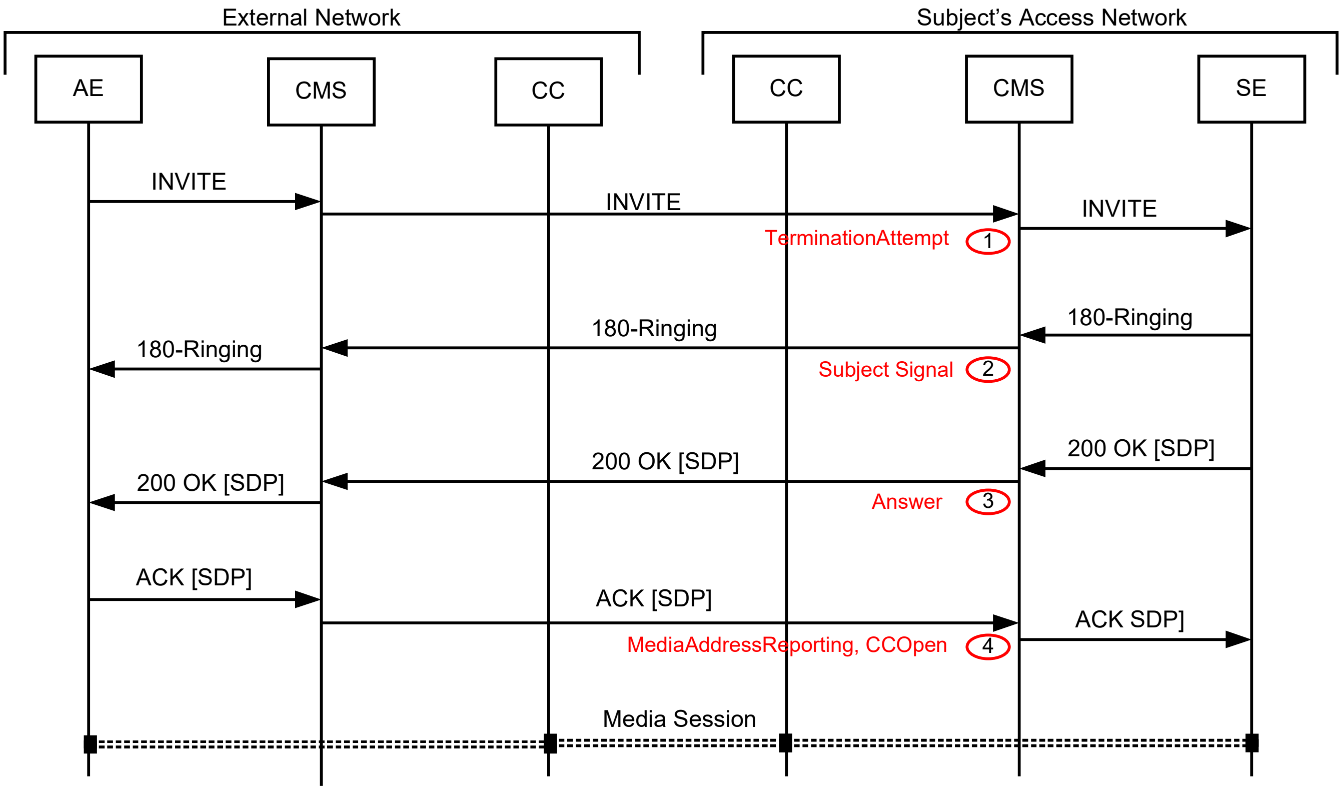


Figure C.8: Session Terminated to Subject (Successful)

Notes:

Trigger Point 4: In this call flow, the SIP ACK contains the SDP information and hence, a MediaAndAddressReporting message is sent.

Trigger Point 5: The order of the CCClose and Release messages is not implied.

C.1.2.2 Associate Cancels INVITE Request

The information flow in Figure C.9 depicts a scenario where an associate initiates a session with the intercept subject and the associate subsequently decides to cancel the invitation. In this scenario, media flow is not begun.

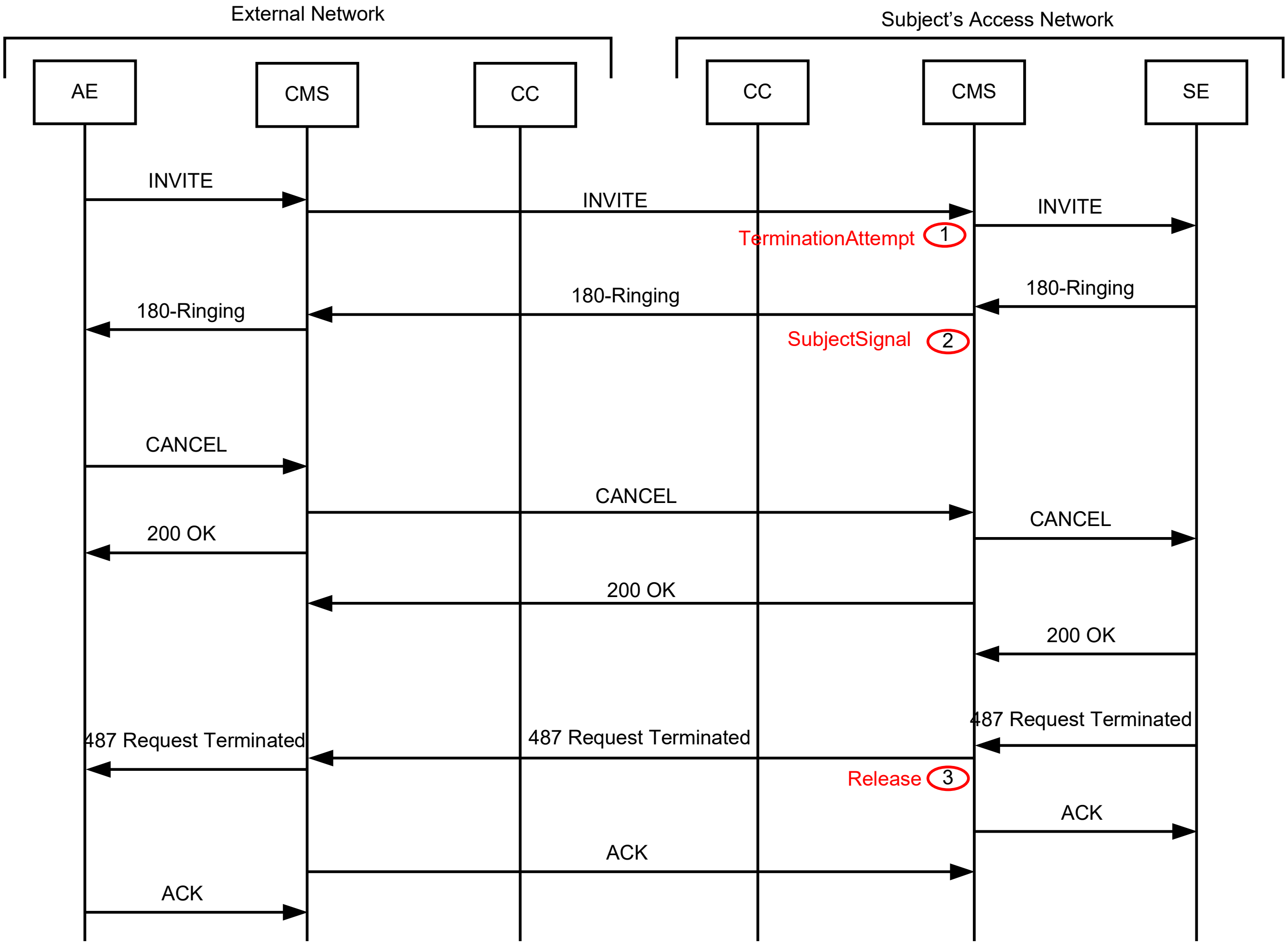


Figure C.9: Associate Cancels INVITE Request

C.1.2.3 Forwarding by Subject

The information flow in Figure C.10 depicts a scenario where an incoming call to an Intercept Subject (SE) is forwarded due to the Call Forwarding Busy feature invoked within the CMS serving the Intercept Subject. An associate (shown as AE-1) calls the Intercept Subject. The SE sends a SIP 486 Busy to the CMS serving the SE and the call is forwarded to another associate (shown as AE-2).

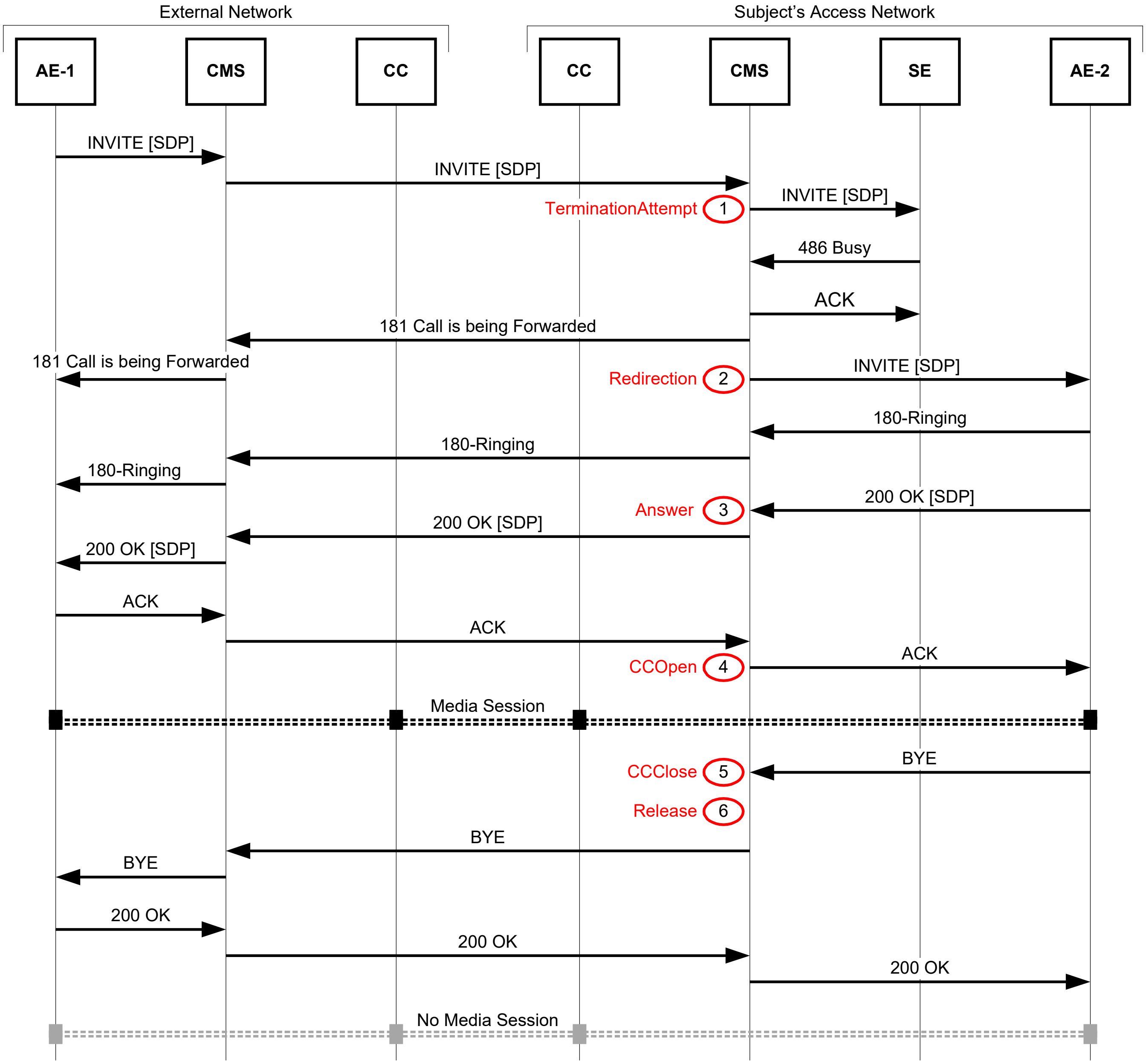


Figure C.10: Forwarding by Subject

C.1.3 Subject Manipulation of Established Calls

The call flows in this clause deal with manipulation of established calls (e.g., Hold-Retrieve, Transfer, establishment of a 3-Way Conference). Call states for the CMS are assumed.

- The call states noted in these flows are for modeling purposes and example only and do not necessarily reflect actual implemented CMS call states for these supplementary services. Accordingly, these call states, as examples, are not being proposed as call states to support the SIP Mapped method.

C.1.3.1 Hold & Retrieve

The information flow in Figure C.11 depicts a scenario where the intercept subject has an established session with an associate. The subject then places the call with the associate on hold. The subject then retrieves the held call.

For the SIP Mapped method, the CMS treats the re-INVITE request as a Hold/Retrieve service and maintains call states to support Hold and Retrieve.

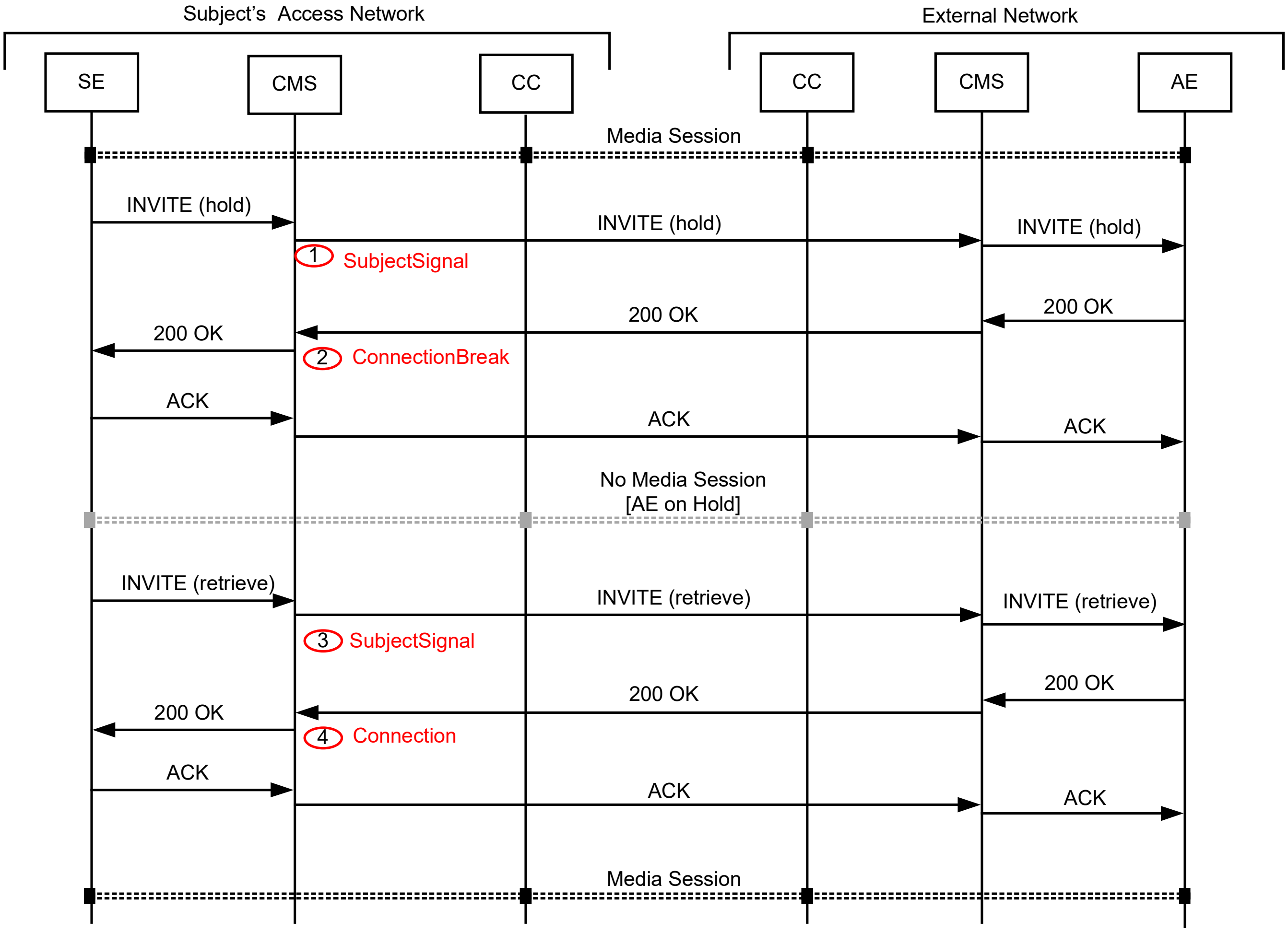


Figure C.11: Subject Holds and Retrieves an Established Call

C.1.3.2 Subject REFERs Associate 1 to Associate 2 (Case 1 – One Call)

The information flow in Figure C.12 depicts a scenario where the intercept subject has an established session with associate 1 (AE-1). The subject then sends information to associate 1 (via a SIP REFER message) to contact associate 2 and hangs up the call. Associate 1 then establishes a call with associate 2 using the information received from the subject. The subject subsequently receives information (via a SIP NOTIFY message) on the establishment of a call between associate 1 and associate 2.

The CMS treats the SIP REFER as a subject Transfer request and treats the first SIP NOTIFY as a confirmation to the subject request by associate 1. No state is maintained to indicate transfer completed by associate 1 (i.e., the 2nd NOTIFY is not treated as a change of state for the service).

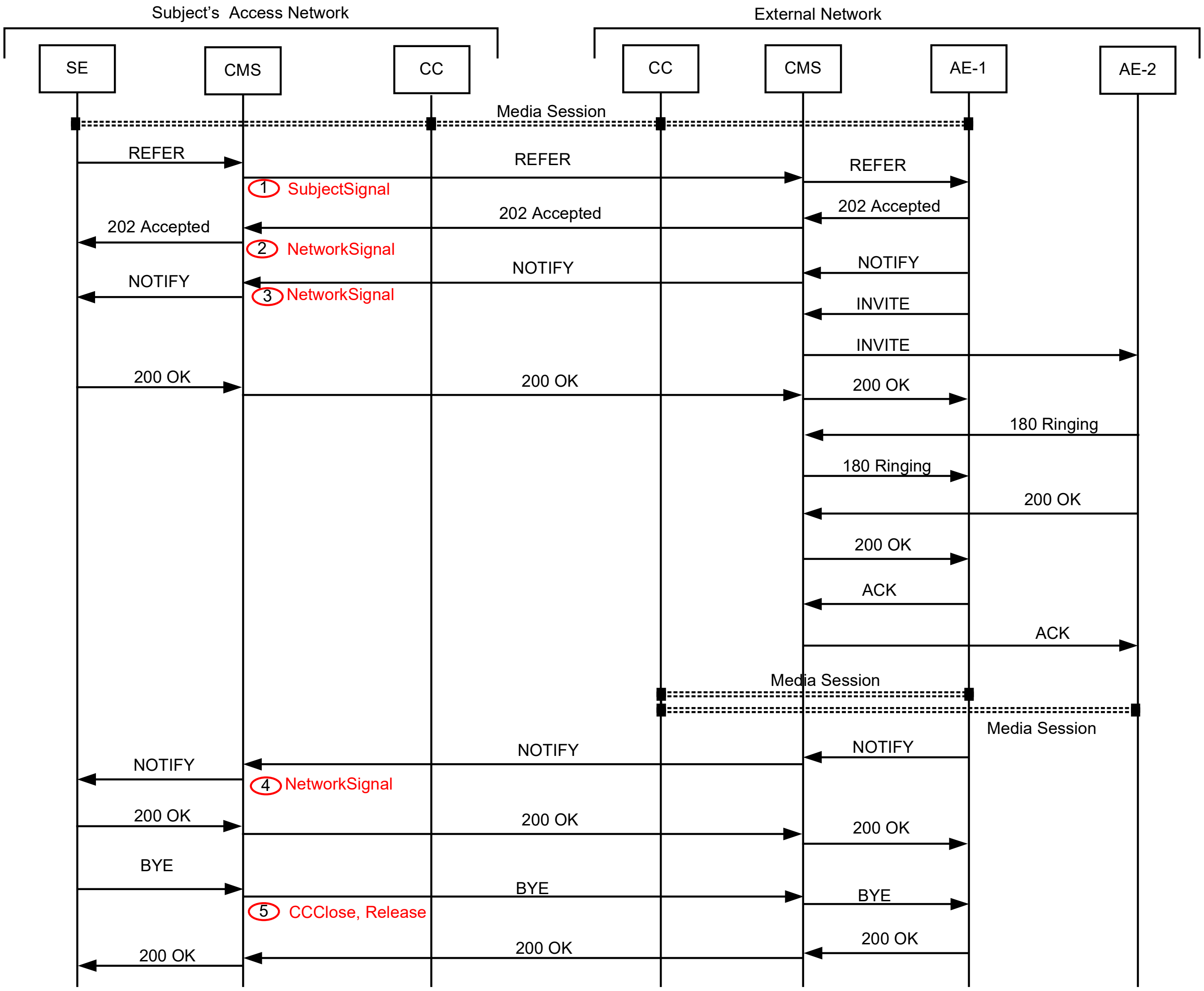


Figure C.12: Subject Blind Transfer

C.1.3.3 Subject REFERs Associate 1 to Associate 2 (Case 2 – Two Calls)

The information flows in Figure C.13 and Figure C.14 depict a scenario where the intercept subject has an established call session with associate 1 (AE-1). The subject places associate 1 on Hold and establishes a call with associate 2 (AE-2). The subject then places associate 2 on Hold. The subject refers associate 1 to associate 2 and associate 1 then establishes a call with associate 2. Associate 2 disconnects from the subject. The subject then disconnects from associate 1 leaving a call established between associate 1 and associate 2.

The CMS treats the SIP re-INVITE request as a Hold/Retrieve service request and maintains call states to support Hold and Retrieve. The CMS treats the SIP REFER as a subject Transfer request and the 1st SIP NOTIFY as a confirmation by the associate to the Transfer request. No state is maintained to indicate transfer complete and call establishment between associate 1 and associate 2.

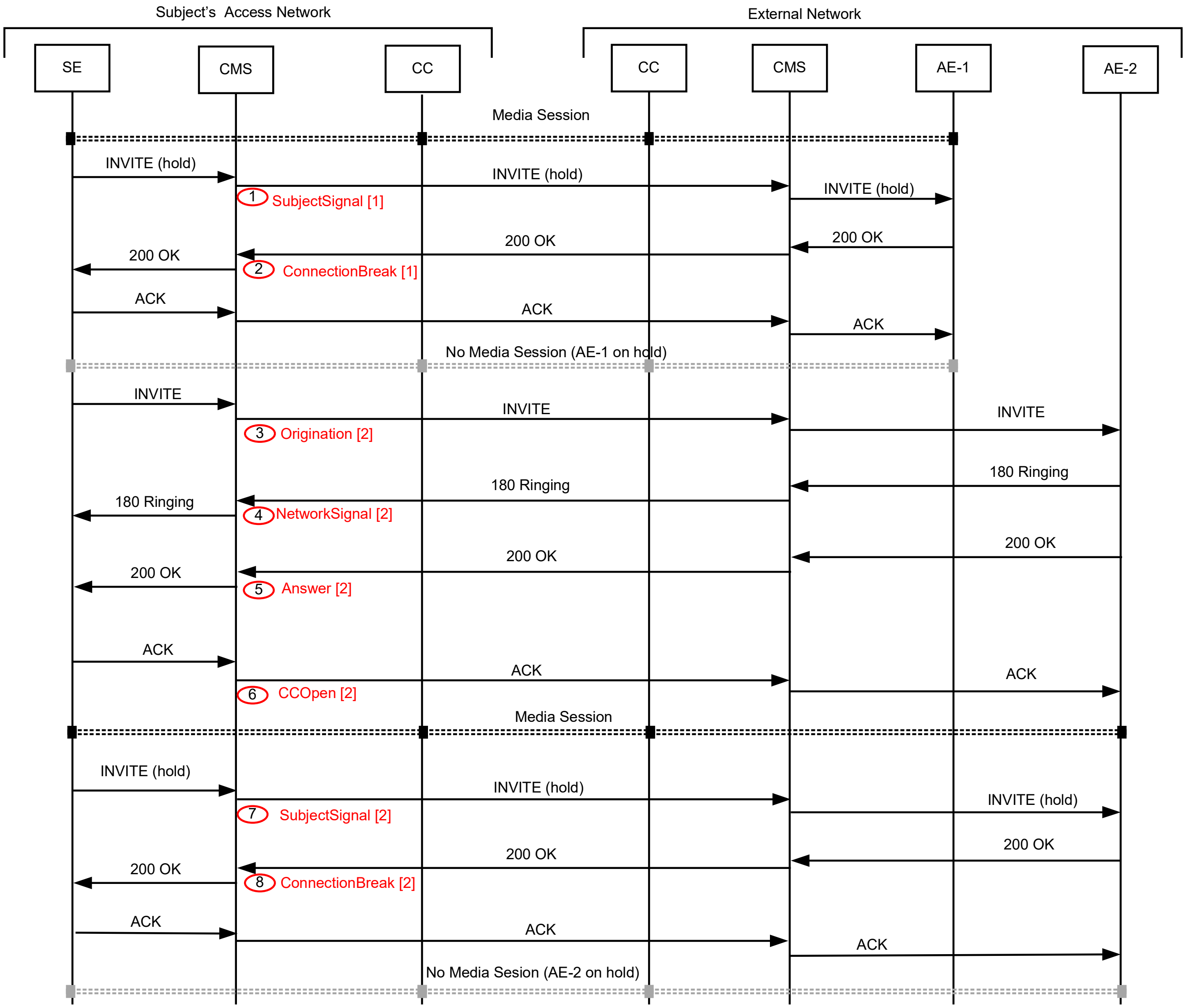


Figure C.13: Attended Transfer (1 of 2)

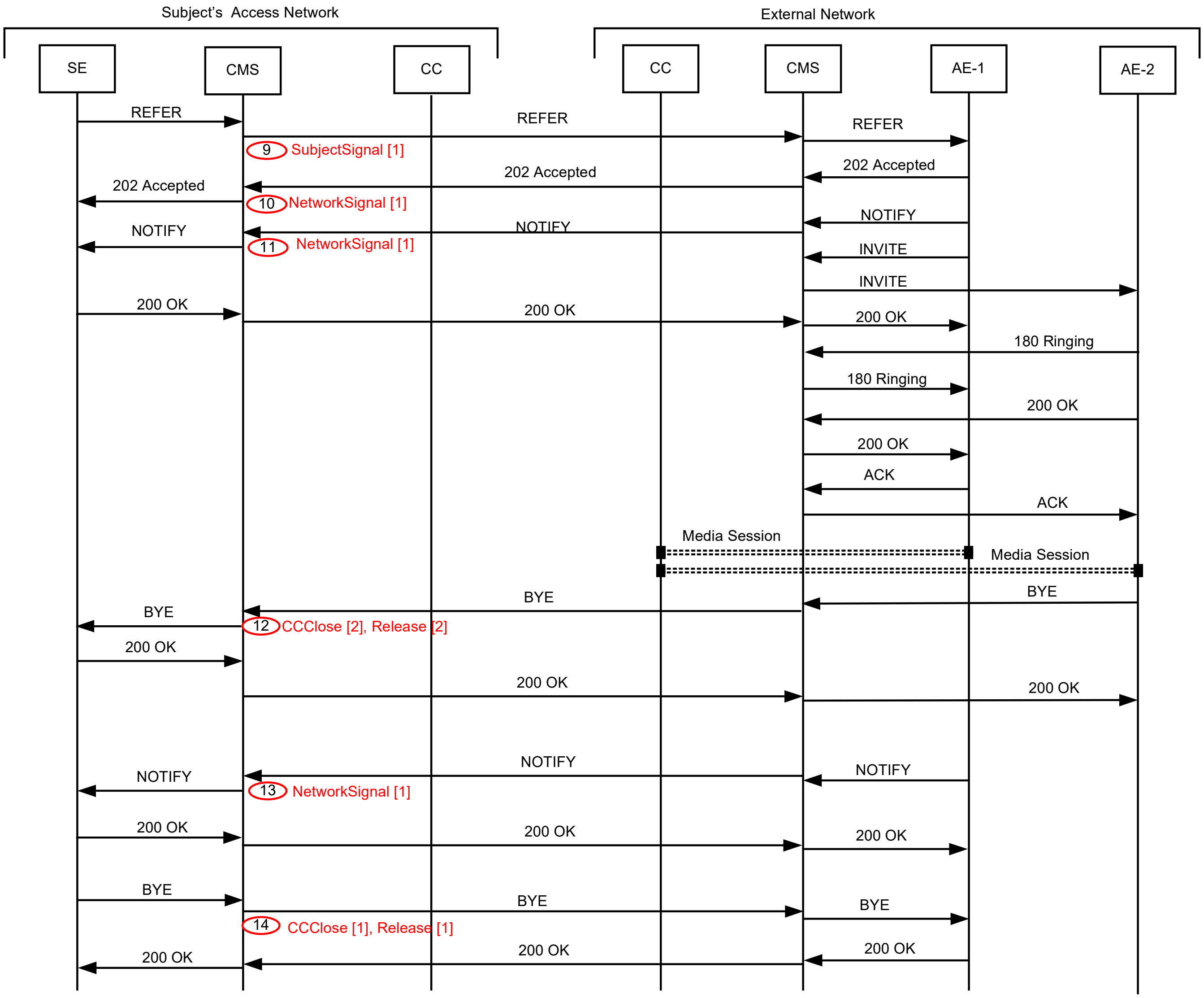


Figure C.14: Attended Transfer (2 of 2)

C.1.3.4 Subject Initiated Conference Call (Network-based Conferencing)

The call flows in the following two figures depict the Intercept Subject (shown as SE) engaged in a call with one Associate (shown as AE-1) before creating a Conference and calling a second Associate (shown as AE-2) through the Conference. The SE (with AE-1 on hold) creates a Conference, invites AE-2 through the Conference, and joins AE-1 to the Conference. At the end, AE-2 drops out of the Conference.

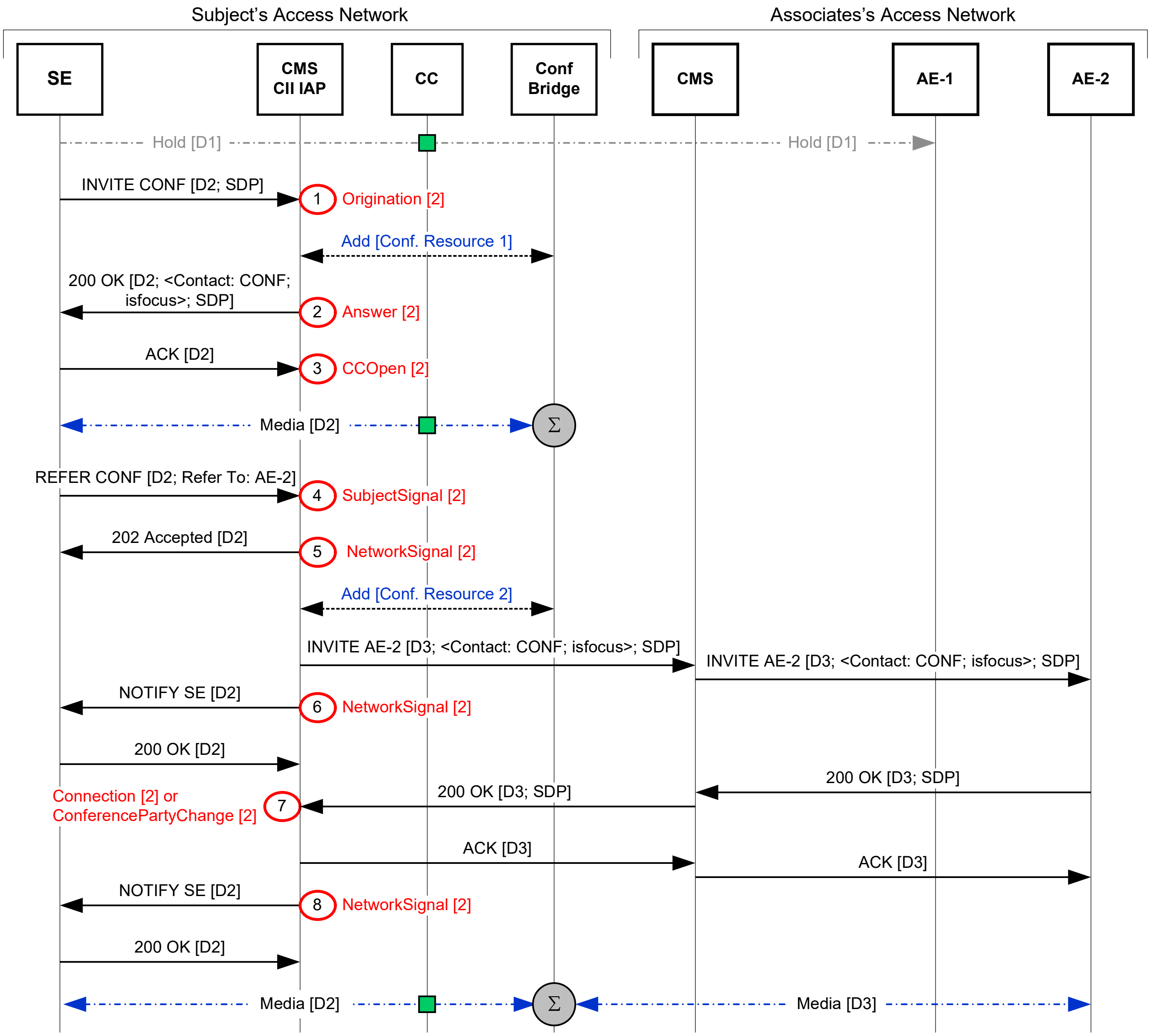


Figure C.15: Subject Initiated Conference Call (network-based conferencing) (1 of 2)

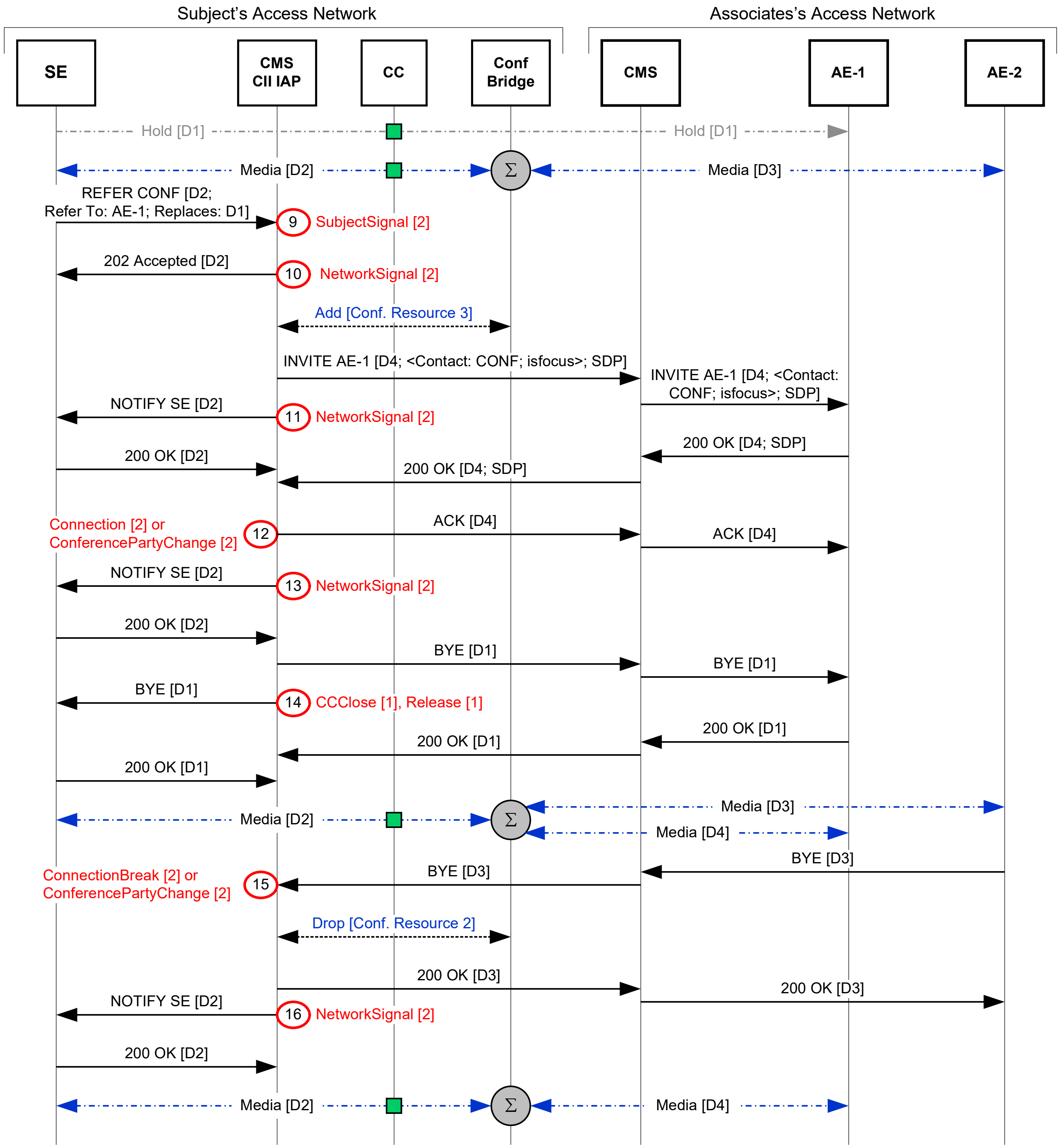


Figure C.16: Subject Initiated Conference Call (network-based conferencing) (2 of 2)

Note: To join AE-1 (party on hold) to the Conference, the CMS may send either a re-INVITE (as shown) or an INVITE with a new dialogue ID. In the latter case, the call with the earlier dialogue ID is released.

C.1.4 PRACK & UPDATE

C.1.4.1 Mapped Reporting of a SIP PRACK & SIP UPDATE

The following information flow depicts a scenario where the intercept subject initiates a session with an associate and then sends a SIP PRACK and SIP UPDATE with SDP and Contact information.

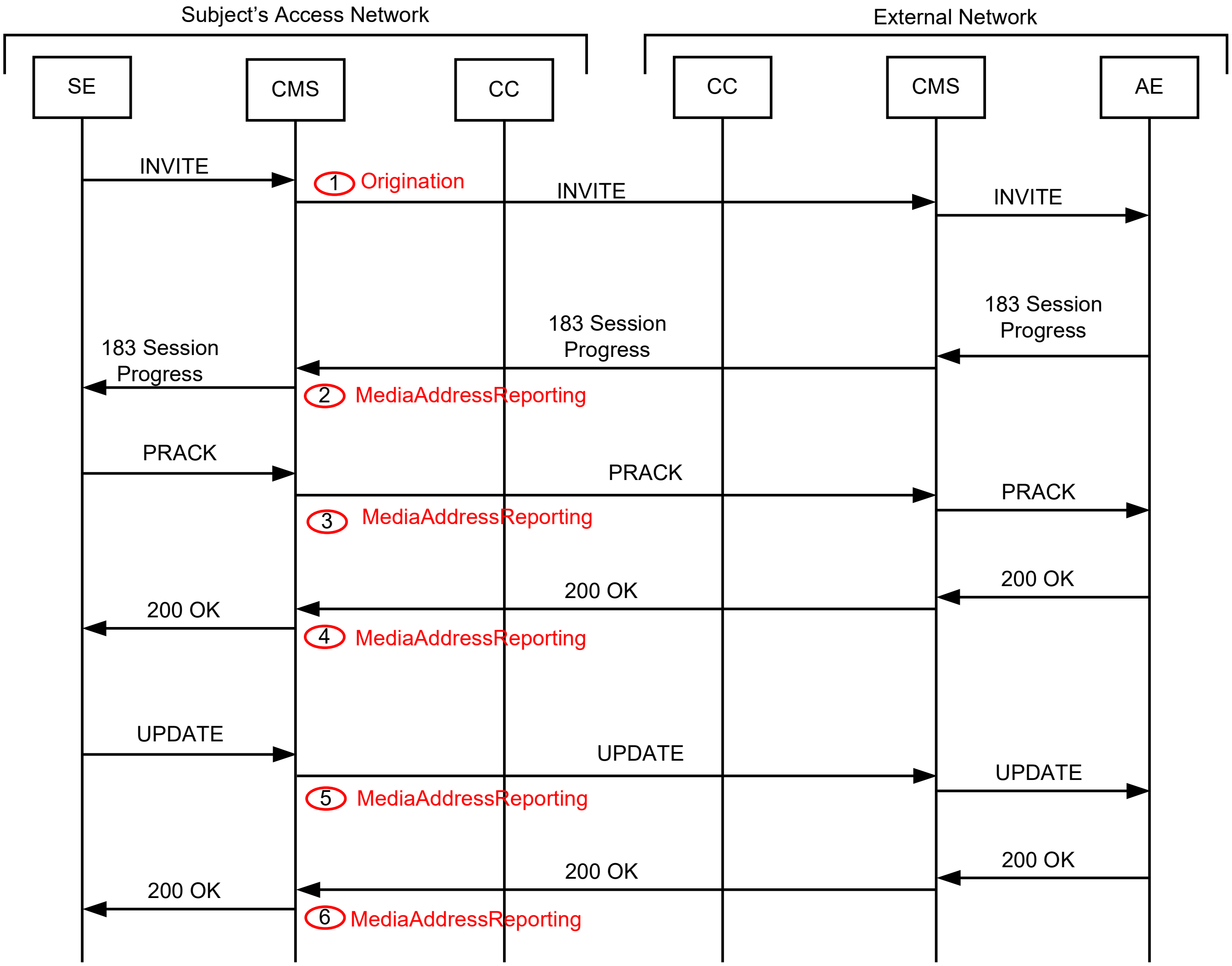


Figure C.17: Subject Sends a SIP PRACK and SIP UPDATE

C.1.4.2 Mapped Reporting of a SIP UPDATE (hold-retrieve)

The following information flow depicts a scenario where the intercept subject has an established a session with an associate. The subject then places the call with the associate on hold. The subject then retrieves the held call.

For the SIP Mapped method, the CMS treats the SIP UPDATE request as a Hold/Retrieve service and maintains call states to support Hold and Retrieve.

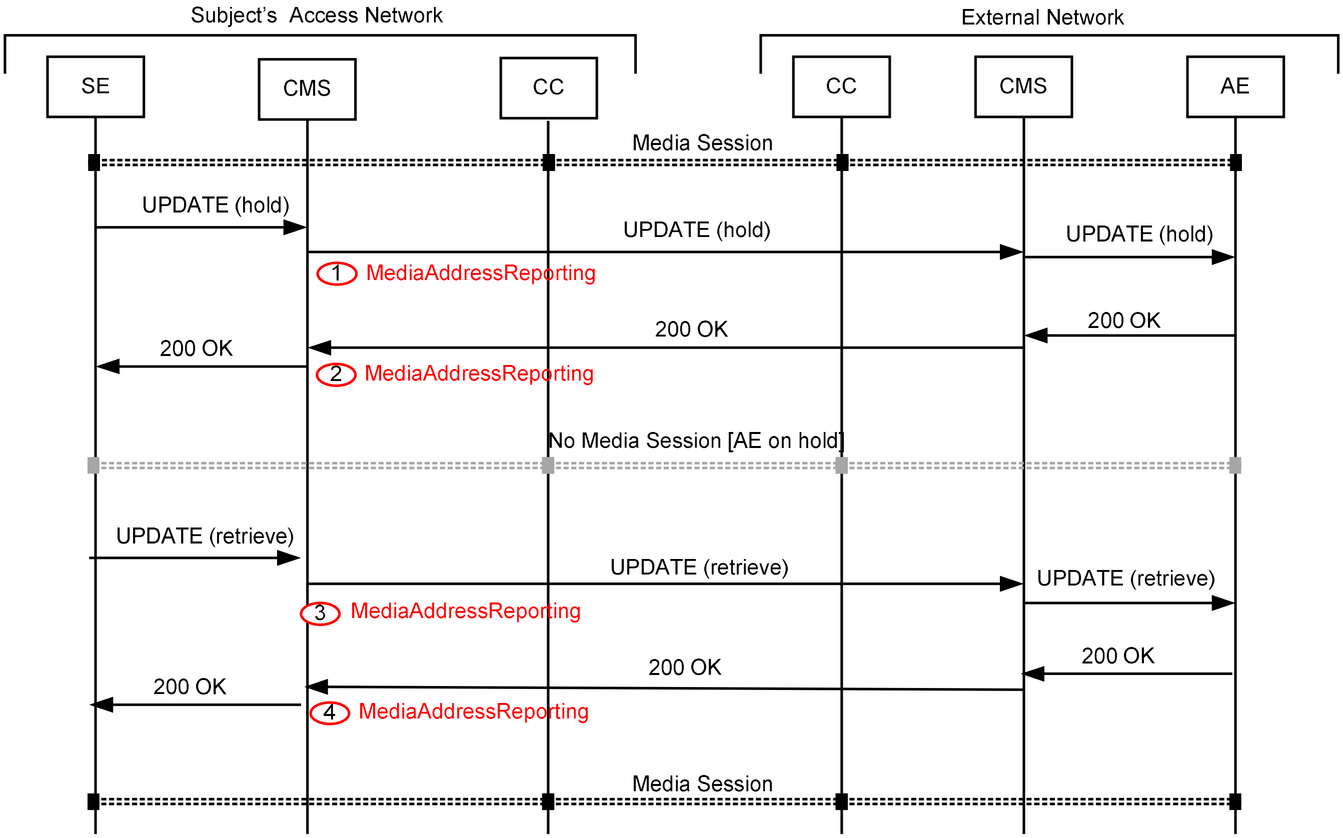


Figure C.18: Subject Holds and Retrieves an Established Call Using A SIP UPDATE

C.1.5 C1.5 STI PASSporT Signature

C.1.5.1 STI PASSporT signature handling in the originating VoIP network

The information flow in Figure C.19 depicts a scenario where the intercept subject initiates a session with an associate and the associate accepts the invitation.

In this flow, the originating VoIP network (shown as subject's access network) uses the STI PASSporT signature for the calling party identity for authentication, verification, or Divert attestation purposes.

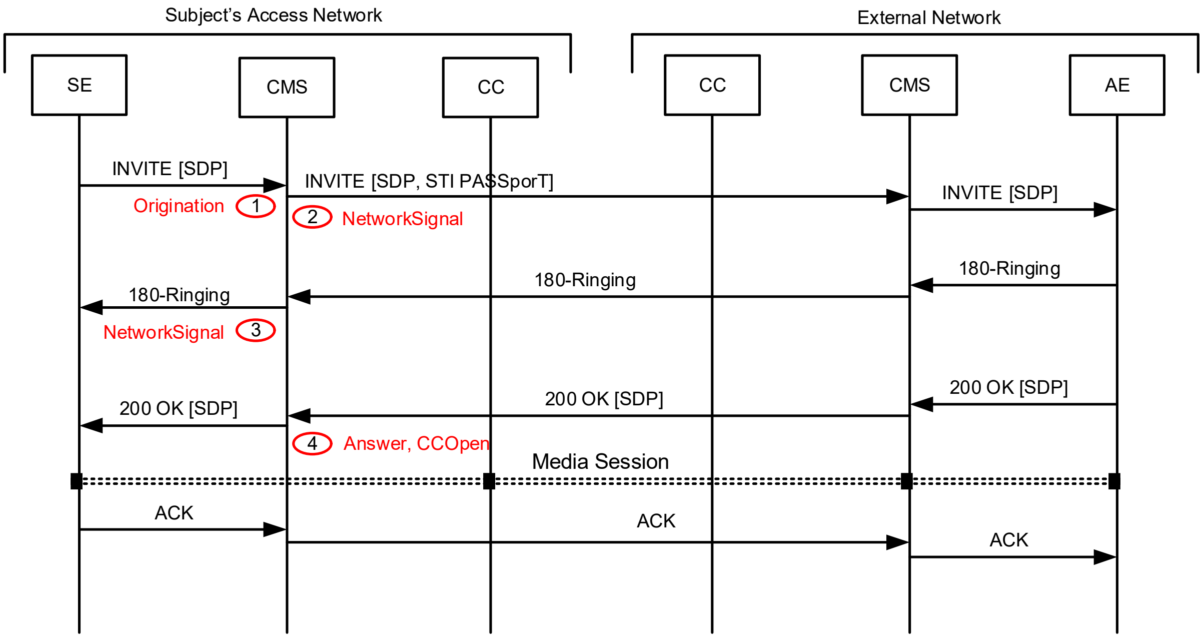


Figure C.19: STI PASSporT signature handling in the originating subject's access network

Note:

Trigger Point 2: When the identity header containing the STI PASSporT signature is included in the outgoing SIP INVITE, a NetworkSignal message that contains the STI PASSpoRT signature is sent.

C.1.5.2 STI PASSporT signature handling in the terminating VoIP network

The information flow in Figure C.20 depicts a scenario where the intercept subject accepts an invitation from an associate.

In this flow, the terminating VoIP network (shown as subject's access network) receives the STI PASSporT signature of the calling party identity and verifies the same before handling the call.

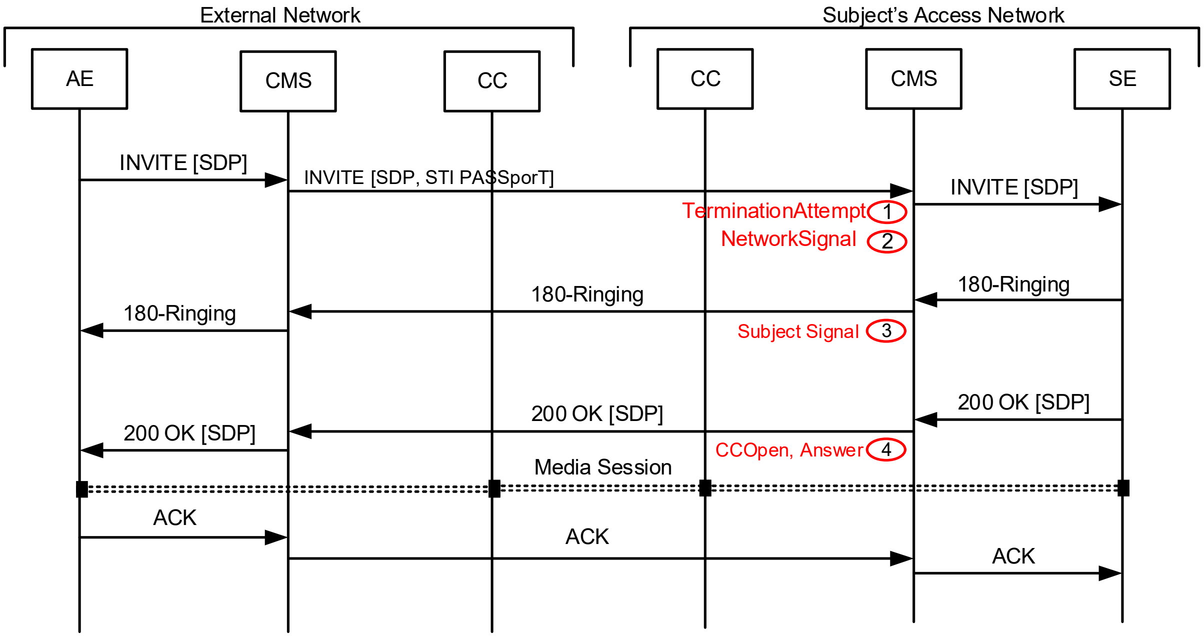


Figure C.20: STI PASSporT signature handling in the terminating subject's access network

Note:

Trigger Point 2: When the identity header containing the STI PASSporT signature received in the SIP INVITE from the originating external network and verified within this terminating subject's access network, a NetworkSignal message that contains the STI PASSpoRT signature is sent.

C.1.5.3 STI PASSporT signature handling in the intermediate VoIP network

The information flow in Figure C.21 depicts a scenario where an incoming call to an intercept subject is redirected and then accepted by a remote forwarded-to user.

In this flow, the intermediate VoIP network (shown as Subject's Access Network) receives the STI PASSporT signature of the calling party identity and verifies the same before handling the call.

In addition, that intermediate VoIP network includes the STI PASSporT signature within the PASSporT identity header of the SIP INVITE sent toward the terminating external network that serves the forwarded-to user.

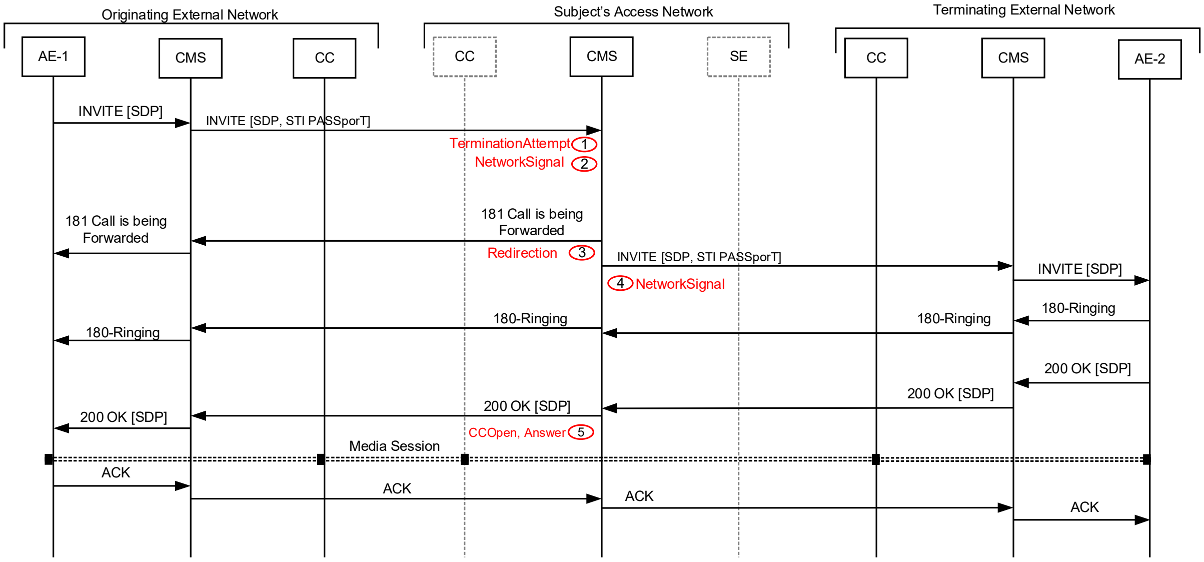


Figure C.21: STI PASSporT signature handling in the intermediate subject's access network

Note:

Trigger Point 2: When the identity header containing the STI PASSporT signature received in the SIP INVITE from the originating external network and verified within this intermediate subject's access network, a NetworkSignal message that contains the STI PASSporT signature is sent.

Trigger Point 4: When the intermediate subject access network redirects the call and includes the STI PASSporT signature within the PASSporT identity header of the outgoing SIP INVITE sent toward the terminating external network, a NetworkSignal message that contains the STI PASSporT signature is sent.

C.1.6 eCNAM

C.1.6.1 eCNAM Extended Name handling in the terminating VoIP network

The information flow in Figure C.22 depicts a scenario where the intercept subject accepts an invitation from an associate.

In this flow, the terminating VoIP network (shown as Subject's Access Network) delivers the eCNAM Extended Name to the intercept subject when the call is offered.

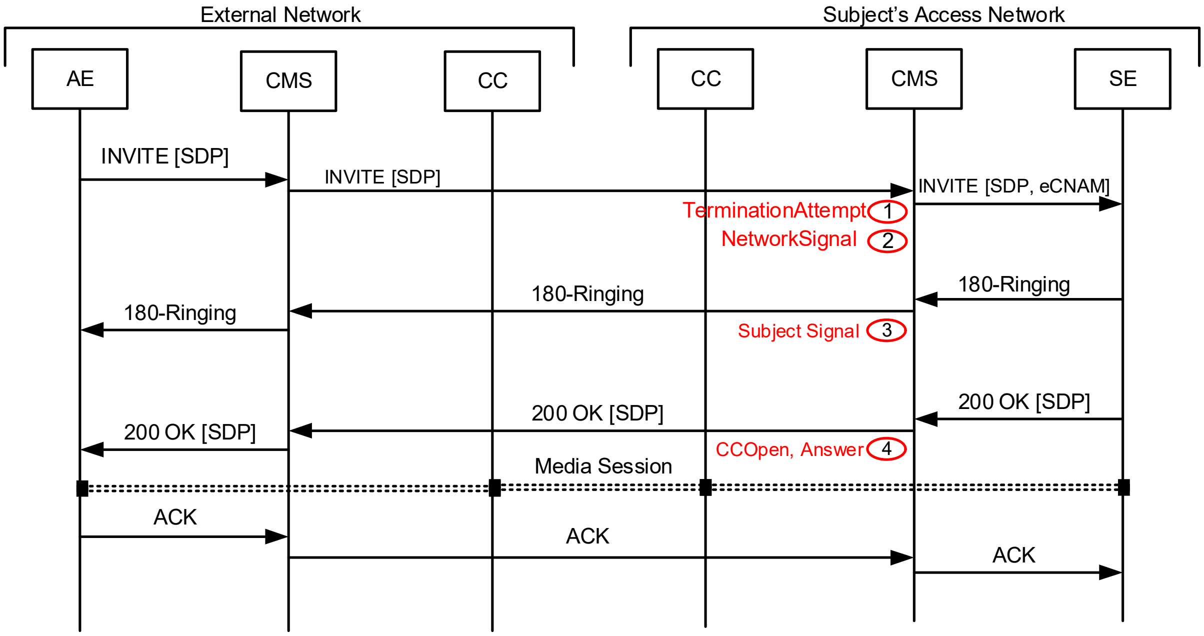


Figure C.22: eCNAM extended name handling in the terminating subject's access network

Note:

Trigger Point 2: When the eCNAM Extended Name is delivered to the called intercept subject, a NetworkSignal message that contains the eCNAM Extended Name in the Terminal Display or Other field is sent.

C.2 DSR Reporting of Call Related Events

The information flows in this clause demonstrate the use of DSR for reporting SIP call event or call related information. DSR can be used to report SIP call event or call-related information when the reporting of the actual SIP message(s) provides CII information about a subject's call or session. The following flows depict content interception and the use of CCOpen and CCClose. Note that the represented DSR Reporting is also valid for non-content interceptions.

Note that the labeled messages (e.g., ①) in the following DSR information flows highlight particular events that are reported by the mapping method. However, with the DSR method all SIP messages are reported.

C.2.1 Sessions Originated by Subject

C.2.1.1 Successful Session Origination by the Subject

The following information flow depicts a scenario where the intercept subject initiates a session with an associate and the associate accepts the invitation. In this scenario, media flow is enabled in both directions after the subject acknowledges the session acceptance by the associate. The Call-ID in the initial SIP "INVITE" and subsequent SIP signaling uniquely identifies this call from all other subject calls.

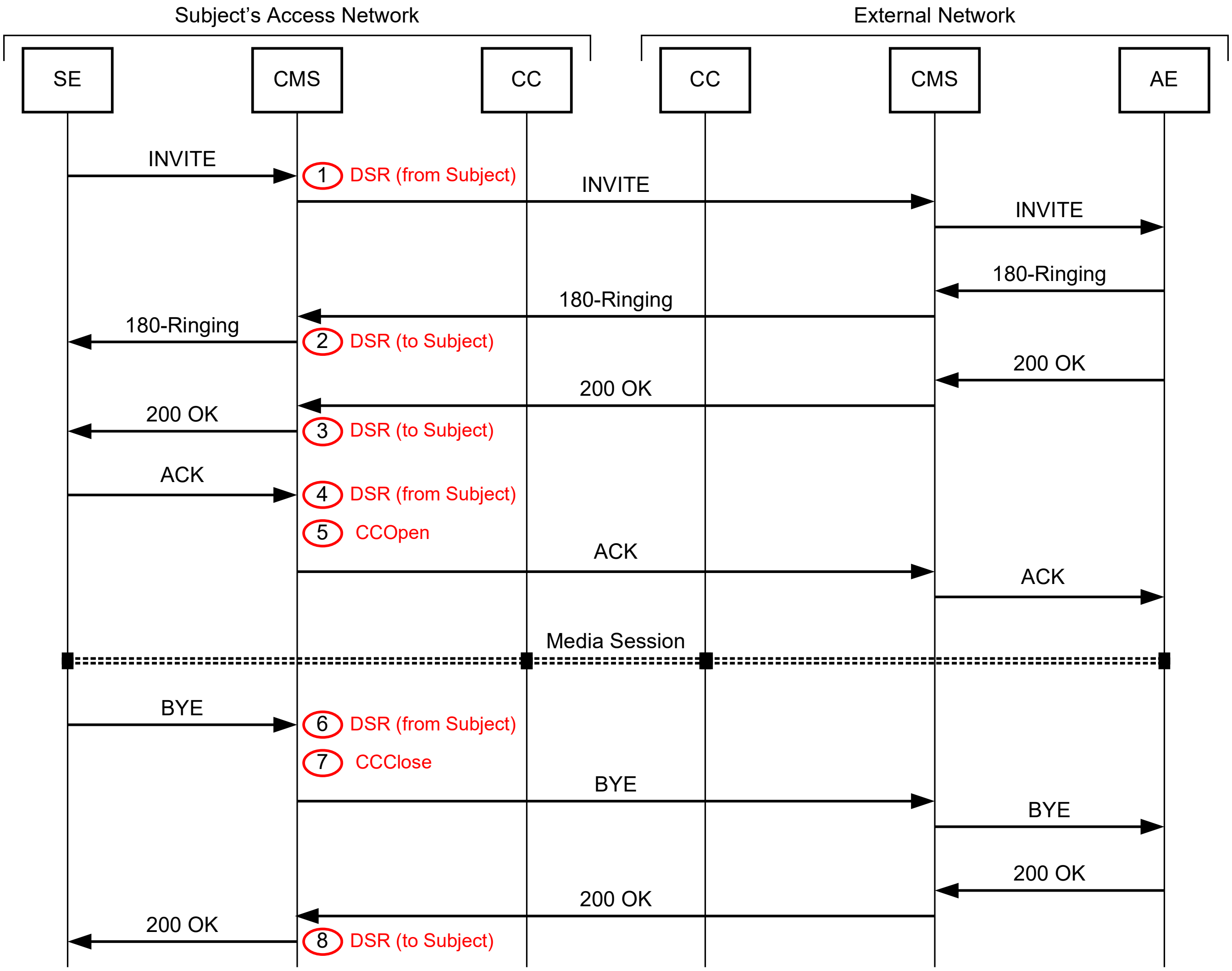


Figure C.23: Session Originated by Subject (Successful)

C.2.2 Sessions Terminated to Subject

C.2.2.1 Successful Session Termination to Subject

The following information flow depicts a scenario where the intercept subject receives an incoming session request from an associate. In this scenario, media flow is enabled in both directions after the associate acknowledges the session acceptance. The Call-ID in the initial SIP "INVITE" and subsequent SIP signaling uniquely identifies this call from all other subject calls.

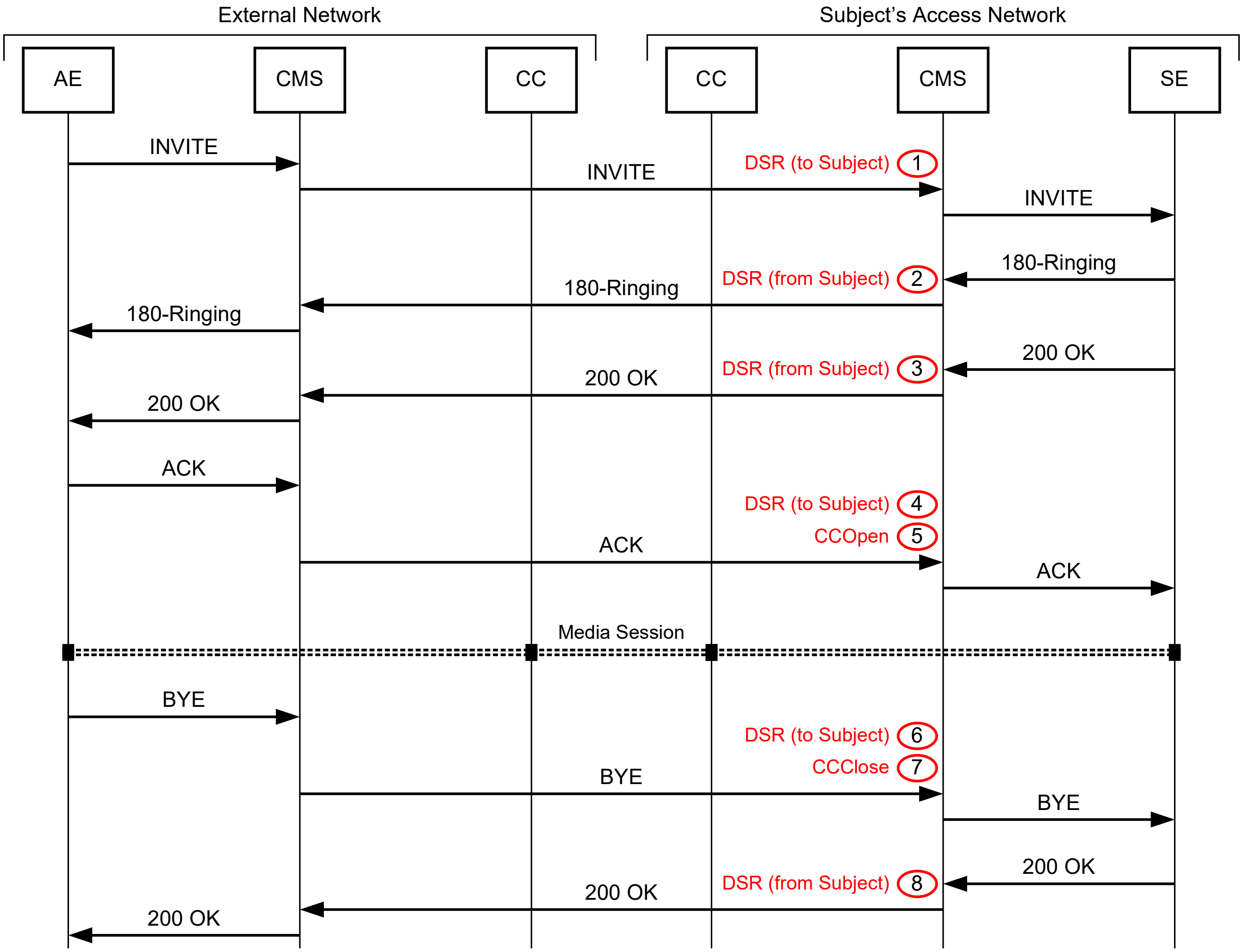


Figure C.24: Session Terminated to Subject (Successful)

C.2.2.2 Successful Call Forwarding

The following information flow depicts a scenario where the intercept subject receives an incoming session request from an associate, and the session is forwarded to due a call forwarding variable service of the intercept subject. The direction of the DSR messages is populated according to clause 6.1.10.

In this scenario, media flow is enabled in both directions after the calling associate acknowledges the session acceptance by the forwarded-to party.

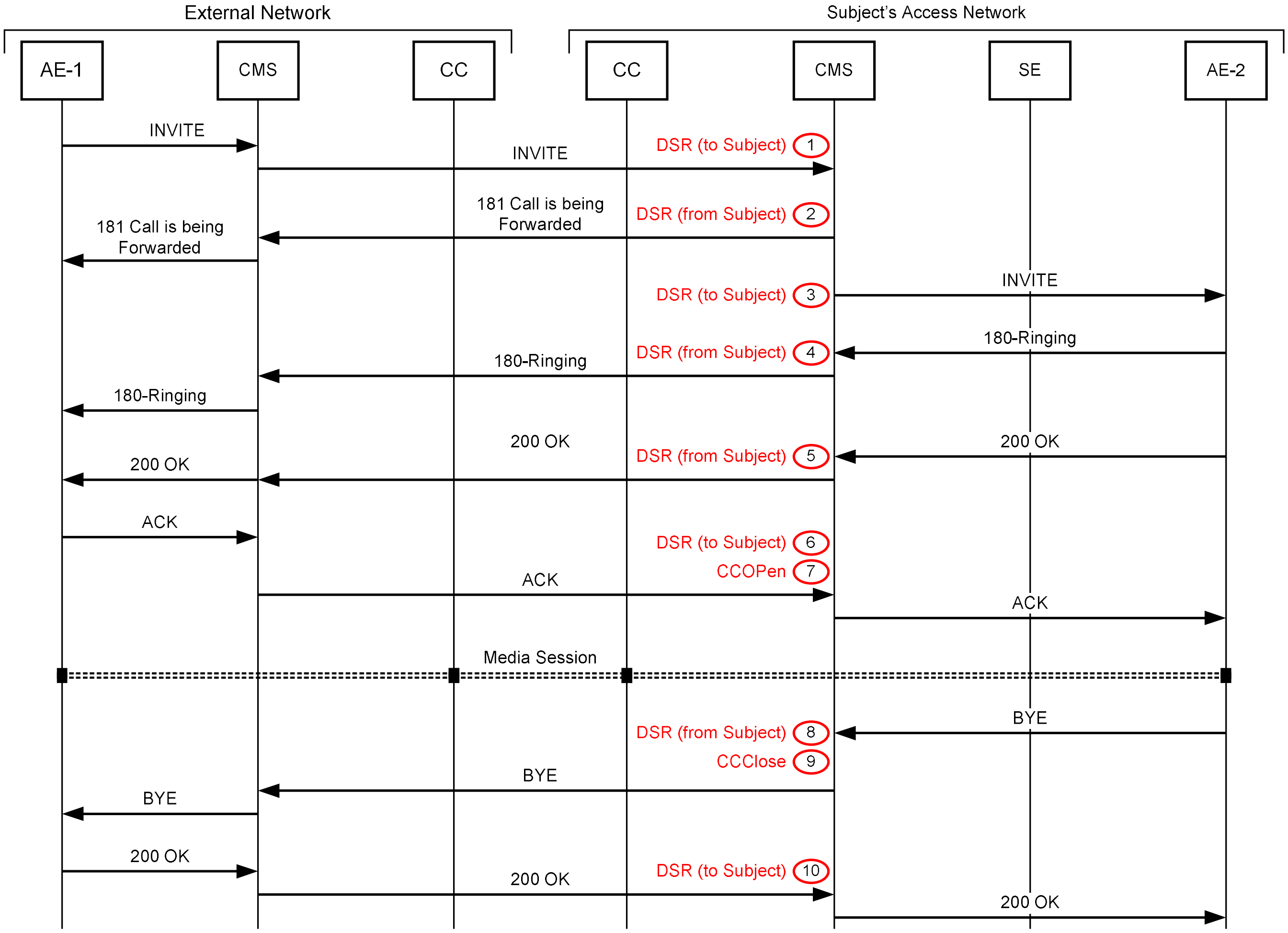


Figure C.25: Successful Call Forwarding

C.3 Call Scenarios Relative to Annex B Mapped Reporting Corrections

This clause provides information flows that illustrate various scenarios in reference to the SIP-to-LAES Message and Parameter Mapping Tables shown in Annex B.

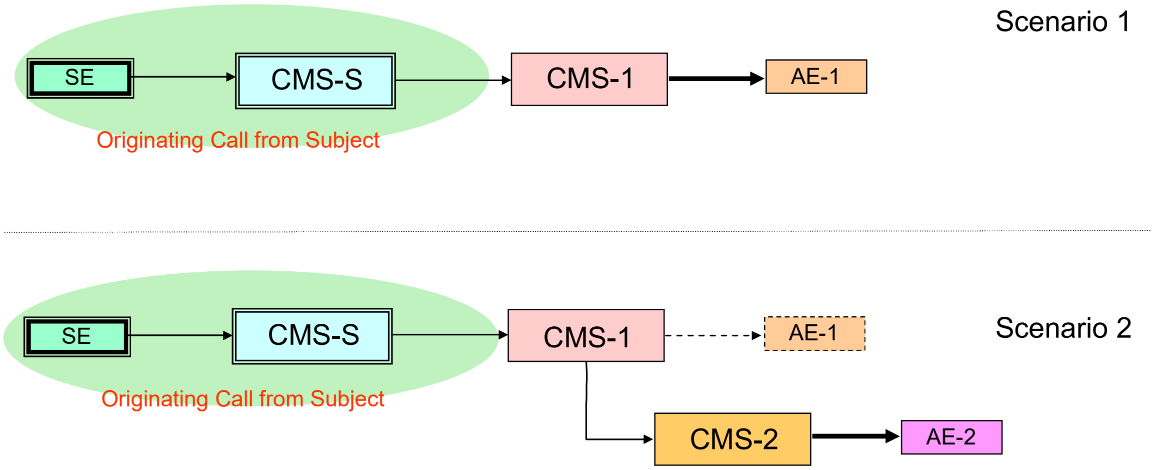
C.3.1 FROM and TO Mapping for Originating Calls

The following information flows illustrate calls originated by an Intercept Subject:

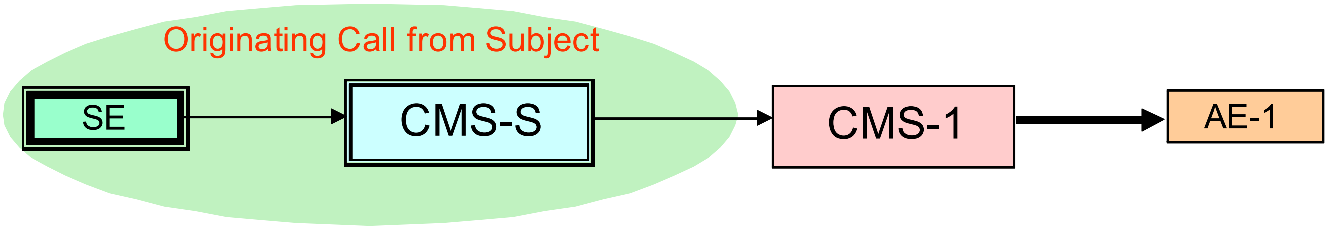
- Intercept Subject SE makes a call to AE-1. The call does not encounter any redirection.
- Intercept Subject SE makes a call to AE-1. AE-1 has a call forwarding active to AE-2.

The CMS-S that serves the Intercept Subject provides the IAP functions for the intercepted call. The SIP-to-LAES Message and Parameter mapping tables in clauses B.15, B.18, and B.19 are related to these information flows.

Call Origination from a Subject



Call Origination from a Subject – Scenario 1



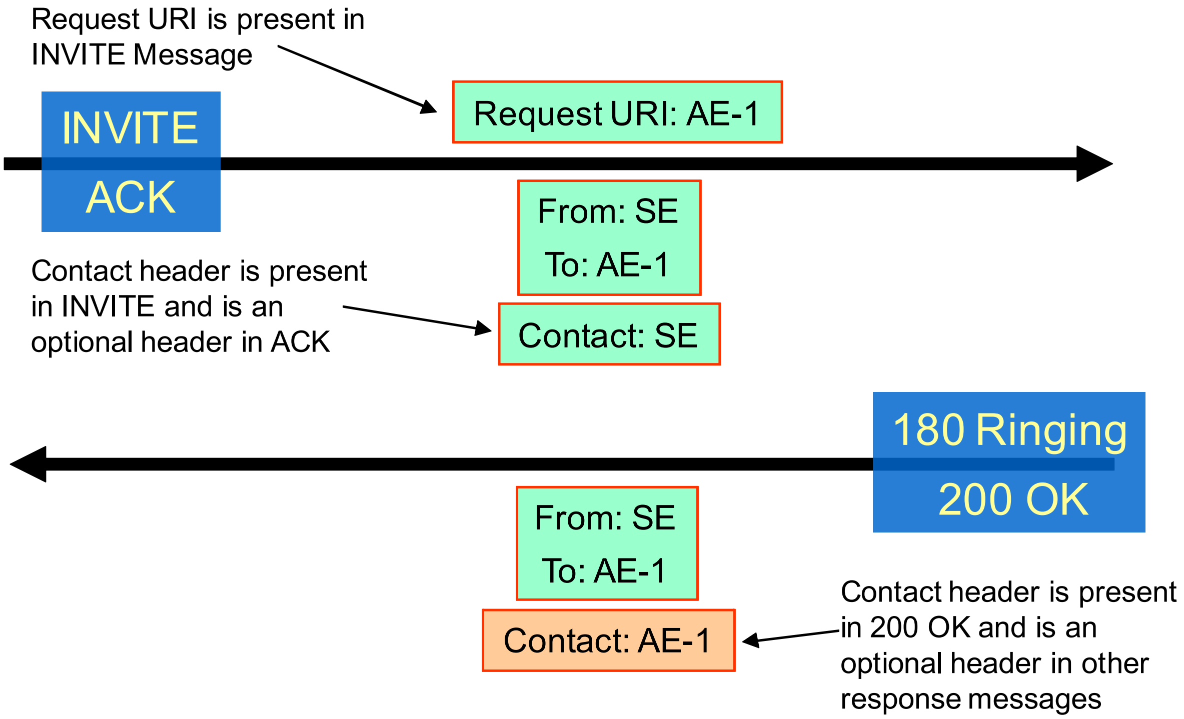
Originating Call from Subject

SE

CMS-S

CMS-1

AE-1



Request URI is present in INVITE Message

Request URI: AE-1

INVITE

ACK

From: SE

To: AE-1

Contact header is present in INVITE and is an optional header in ACK

Contact: SE

180 Ringing

200 OK

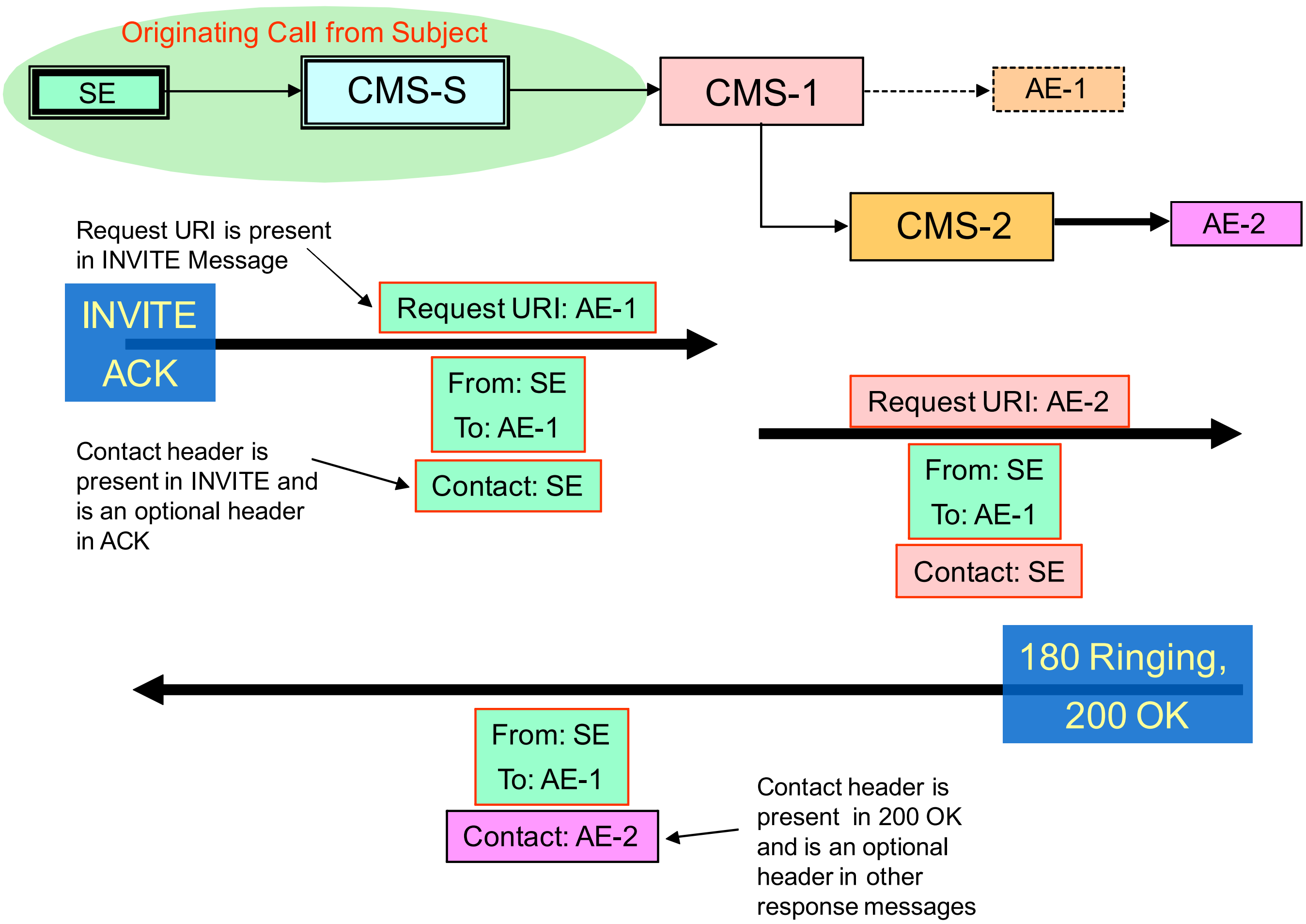
From: SE

To: AE-1

Contact: AE-1

Contact header is present in 200 OK and is an optional header in other response messages

Call Origination from a Subject Scenario 2



Request URI is present in INVITE Message

Contact header is present in INVITE and is an optional header in ACK

Contact header is present in 200 OK and is an optional header in other response messages

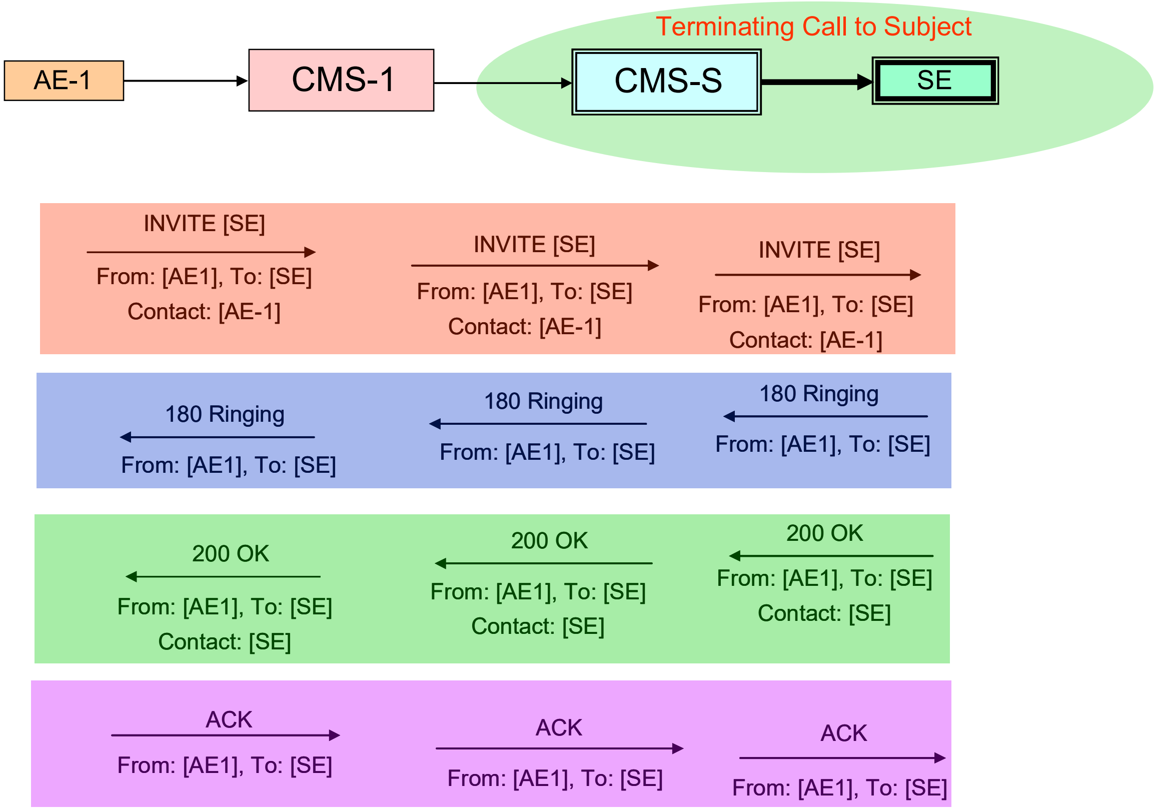
C.3.2 FROM & TO Mapping for Terminating Calls

The following information flows illustrate calls terminated to an Intercept Subject:

- AE-1 calls the Intercept Subject SE. The terminating call to the SE has no prior redirection.
- AE-1 calls AE-2 and AE-2 has a call forwarding active to the Intercept Subject SE. The call from AE-1 to AE-2 is redirected to the SE. The terminating call to the SE has one prior redirection.
- AE-1 calls AE-2 and AE-2 has a call forwarding active to AE-3 and AE-3 has a call forwarding active to the Intercept Subject SE. The call from AE-1 to AE-2 is redirected to AE-3 and in turn is redirected to the SE. The terminating call to the SE has two prior redirections.

The CMS-S that serves the Intercept Subject provides the IAP functions for the intercepted call. The SIP-to-LAES Message and Parameter mapping tables in clauses B.16, B.17, and B.19 are related to these information flows.

Call Terminating to a Subject



Terminating Call to Subject

AE-1 → CMS-1 → CMS-S → SE

INVITE [SE]
From: [AE1], To: [SE]
Contact: [AE-1]

INVITE [SE]
From: [AE1], To: [SE]
Contact: [AE-1]

INVITE [SE]
From: [AE1], To: [SE]
Contact: [AE-1]

180 Ringing
From: [AE1], To: [SE]

180 Ringing
From: [AE1], To: [SE]

180 Ringing
From: [AE1], To: [SE]

200 OK
From: [AE1], To: [SE]
Contact: [SE]

200 OK
From: [AE1], To: [SE]
Contact: [SE]

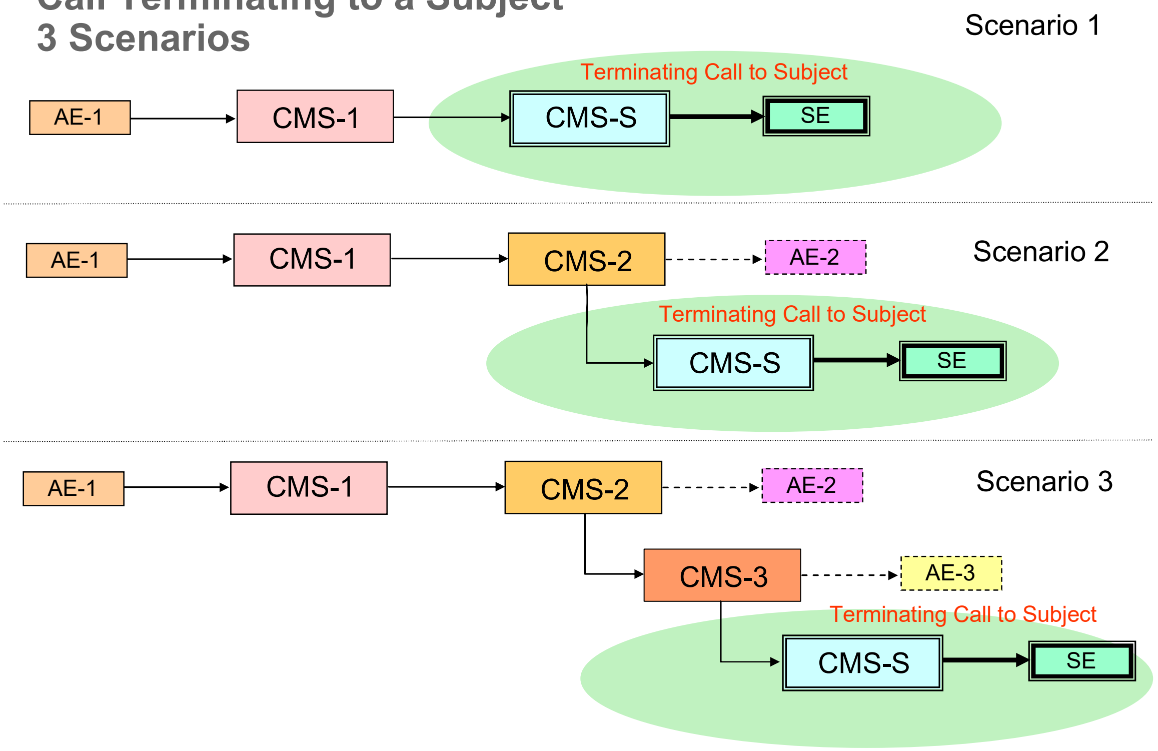
200 OK
From: [AE1], To: [SE]
Contact: [SE]

ACK
From: [AE1], To: [SE]

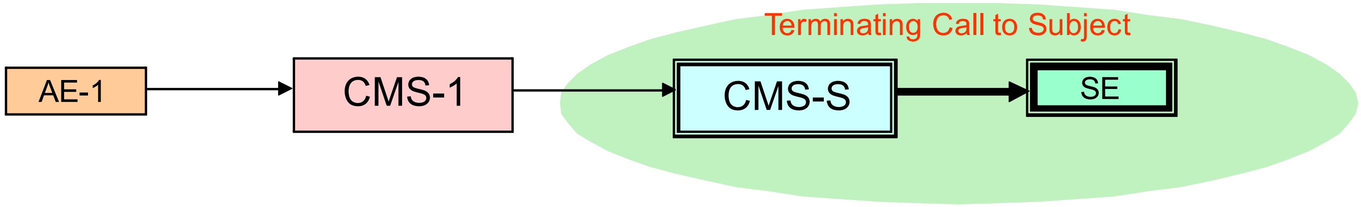
ACK
From: [AE1], To: [SE]

ACK
From: [AE1], To: [SE]

Call Terminating to a Subject
3 Scenarios



Scenario 1: Terminating Call to Subject w/o prior redirections



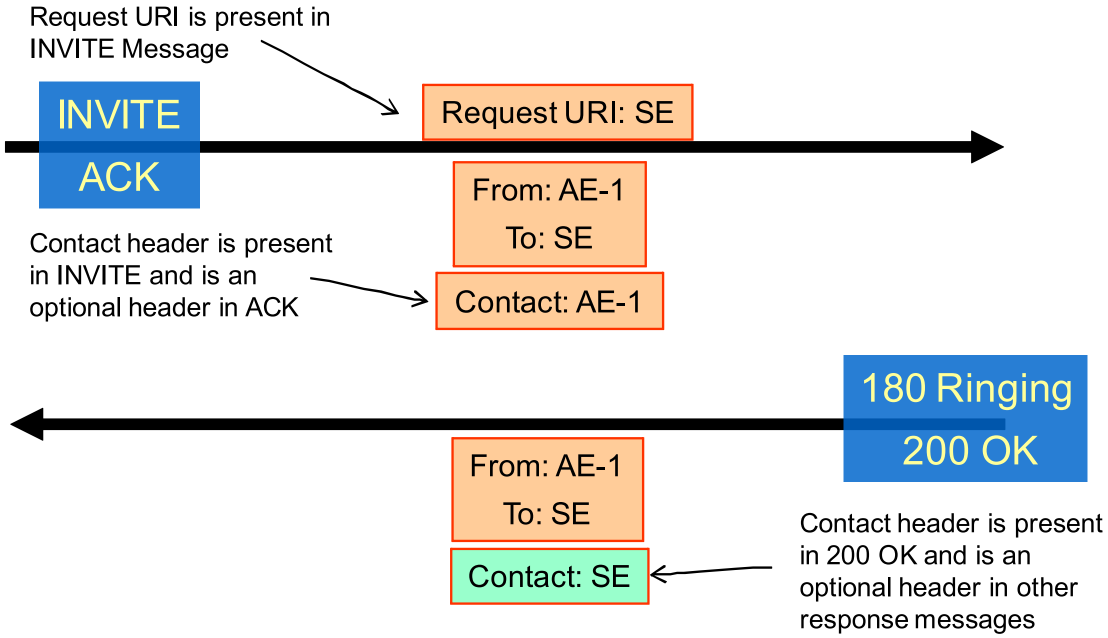
Terminating Call to Subject

AE-1

CMS-1

CMS-S

SE



Request URI is present in INVITE Message

INVITE

ACK

Request URI: SE

From: AE-1

To: SE

Contact header is present in INVITE and is an optional header in ACK

Contact: AE-1

180 Ringing

200 OK

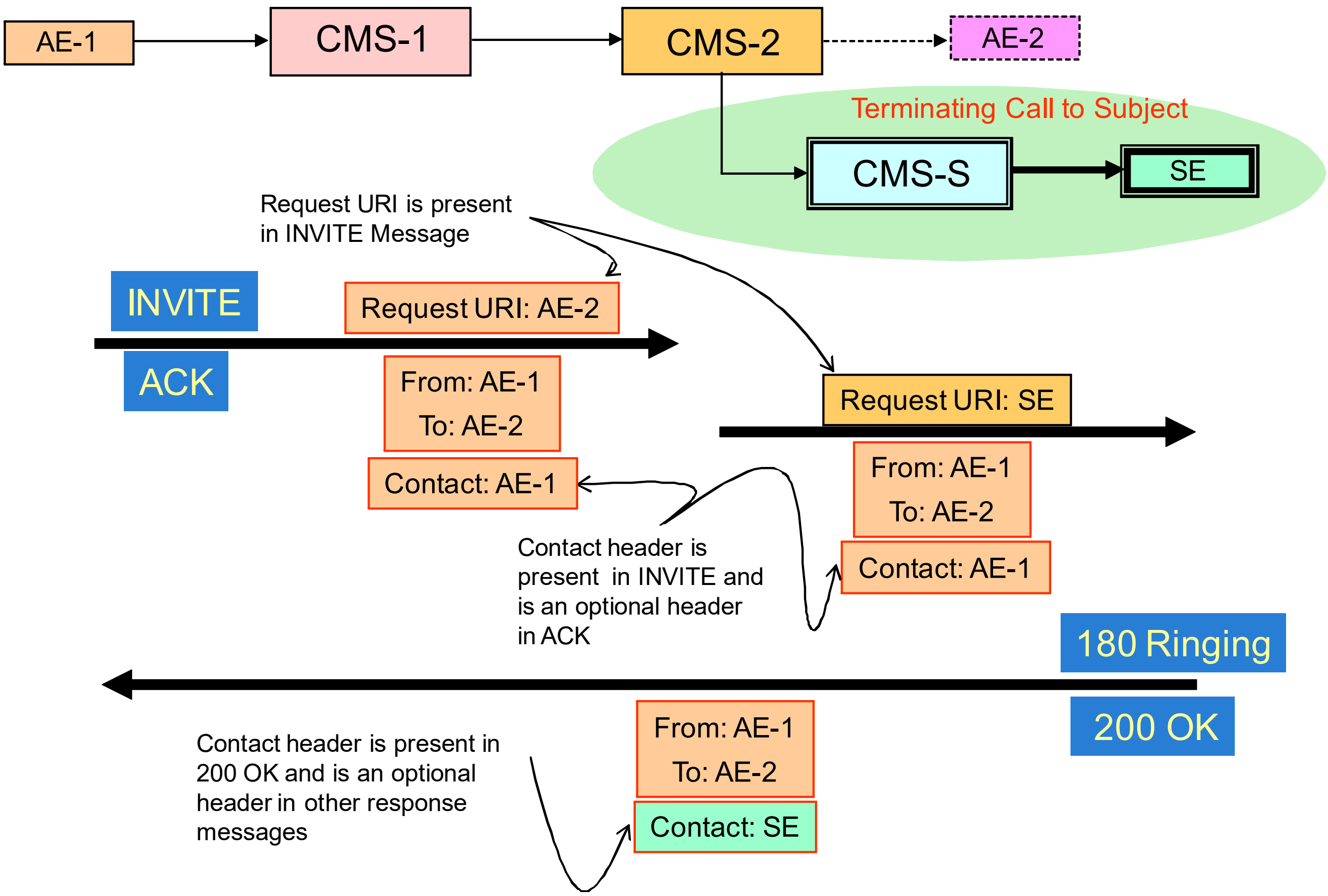
From: AE-1

To: SE

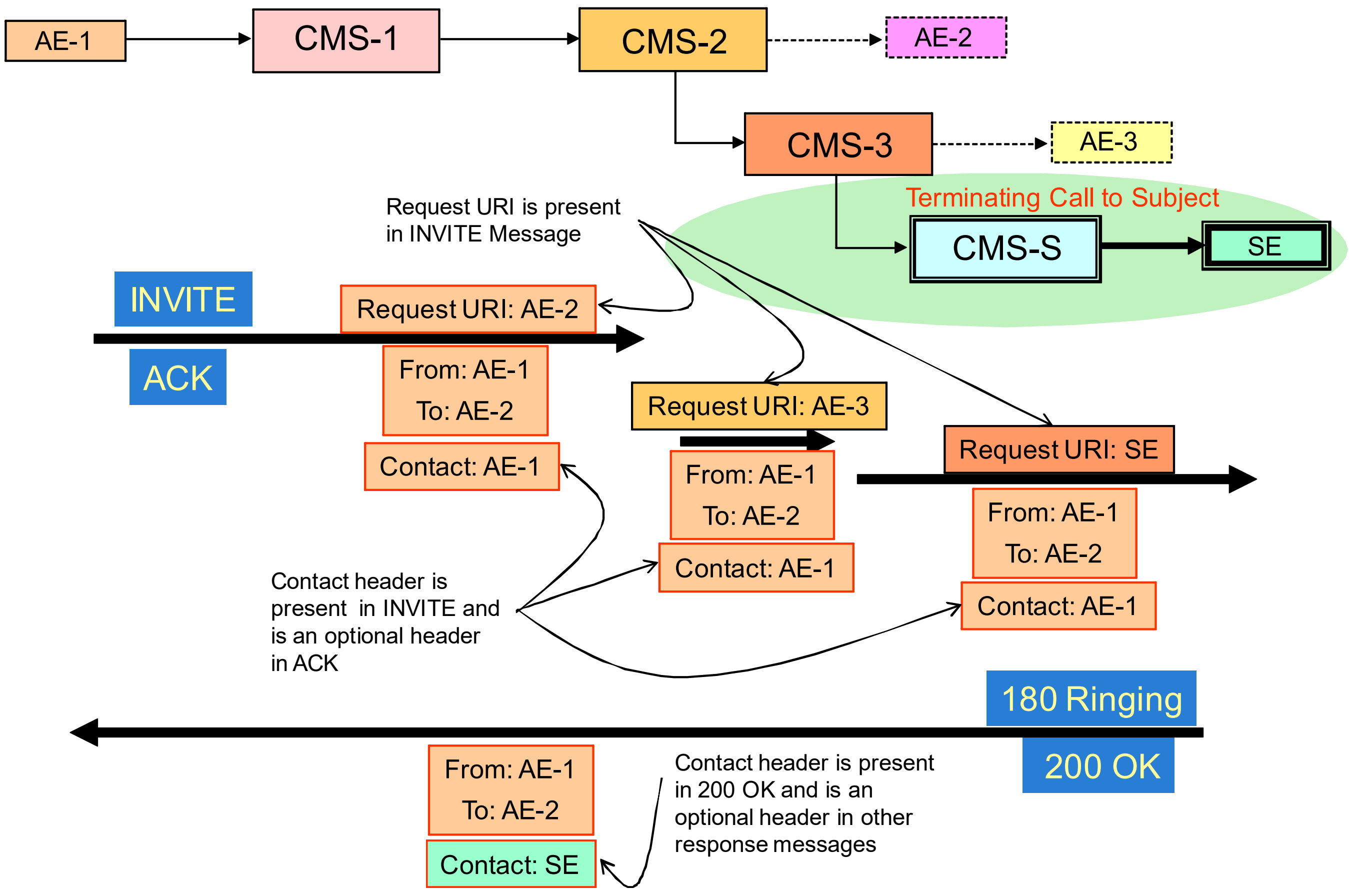
Contact: SE

Contact header is present in 200 OK and is an optional header in other response messages

Scenario 2: A terminating call to a subject with a prior redirection


AE-1
CMS-1
CMS-2
AE-2
Terminating Call to Subject
CMS-S
SE
Request URI is present in INVITE Message
INVITE
ACK
Request URI: AE-2
From: AE-1
To: AE-2
Contact: AE-1
Request URI: SE
From: AE-1
To: AE-2
Contact: AE-1
Contact header is present in INVITE and is an optional header in ACK
180 Ringing
200 OK
From: AE-1
To: AE-2
Contact: SE
Contact header is present in 200 OK and is an optional header in other response messages

Scenario 3: A terminating call to a subject with multiple prior redirections



C.3.3 FROM & TO Mapping for REFER Method

The following information flows illustrate the use of the REFER method:

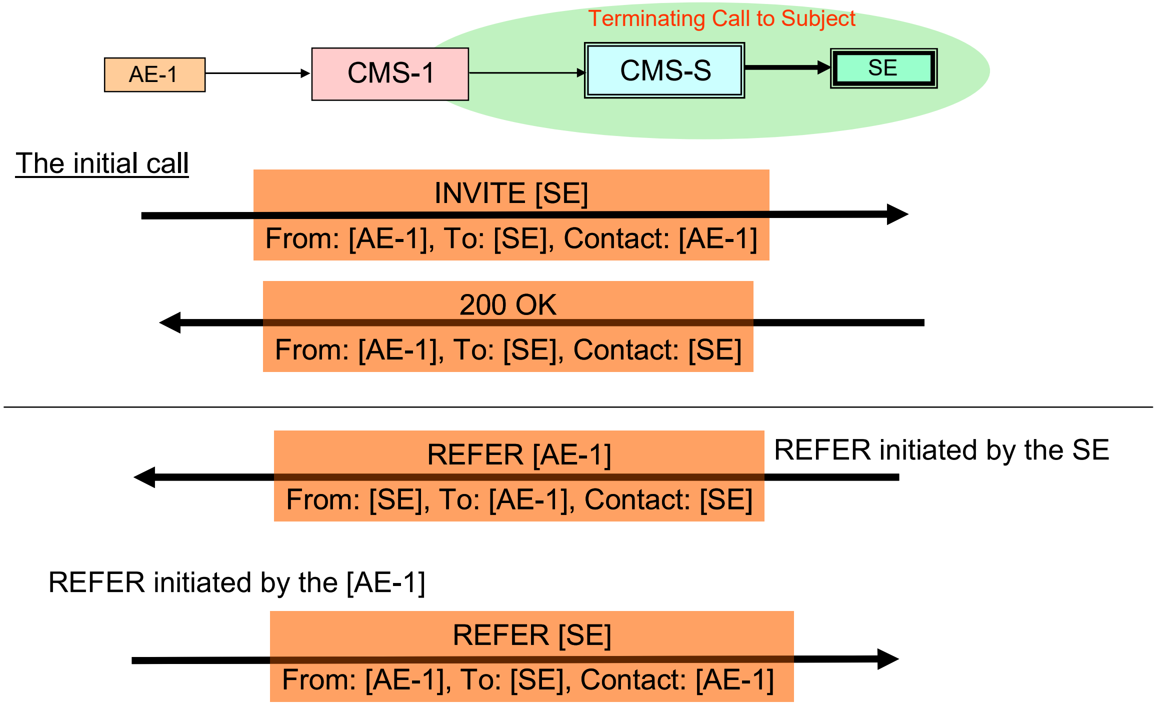
- The initial call is originated from an Intercept Subject SE. The call may or may not encounter redirection.
- The initial call is terminated to an Intercept Subject. The call may or may not have prior redirection.

Each of these scenarios has two applications for the REFER method:

- The REFER method is initiated by the Intercept Subject SE;
- The REFER method is initiated by the current associate of the call (i.e., the Intercept Subject SE receives the REFER message).

The CMS-S that serves the Intercept Subject provides the IAP functions for the intercepted call. The SIP-to-LAES Message and Parameter mapping tables in clauses B.28 and B.29 are related to these information flows.

REFER Method



Terminating Call to Subject

AE-1 → CMS-1 → CMS-S → SE

The initial call

INVITE [SE]
From: [AE-1], To: [SE], Contact: [AE-1]

200 OK
From: [AE-1], To: [SE], Contact: [SE]

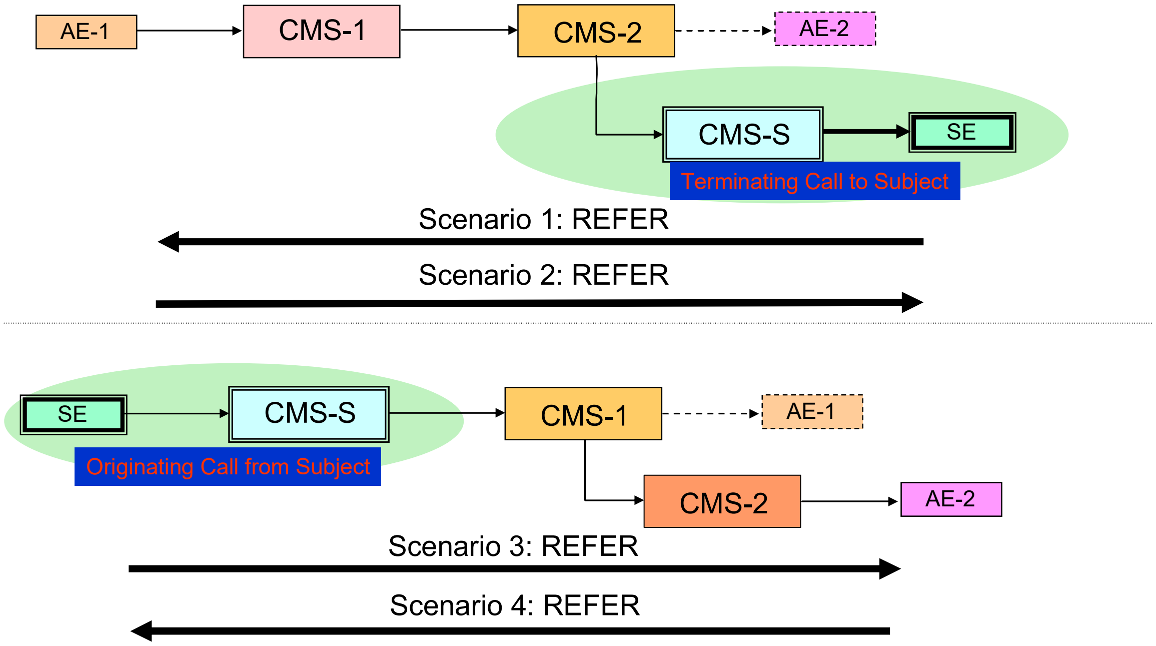
REFER [AE-1]
From: [SE], To: [AE-1], Contact: [SE]

REFER initiated by the SE

REFER initiated by the [AE-1]

REFER [SE]
From: [AE-1], To: [SE], Contact: [AE-1]

REFER Method – More Scenarios



AE-1 → CMS-1 → CMS-2 → AE-2

CMS-2 → CMS-S → SE

Terminating Call to Subject

Scenario 1: REFER

Scenario 2: REFER

SE → CMS-S → CMS-1 → AE-1

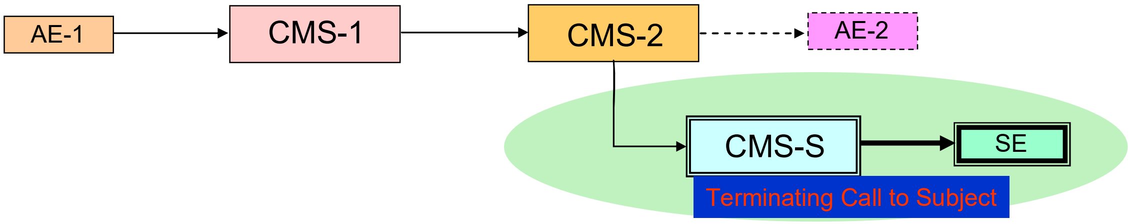
Originating Call from Subject

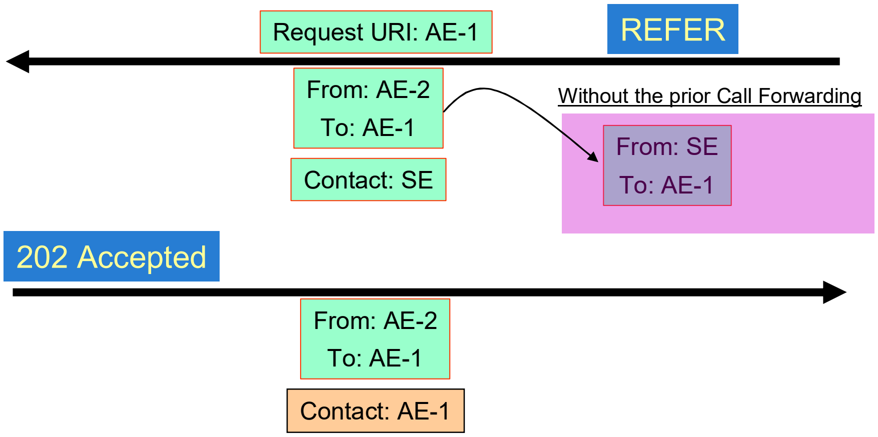
CMS-1 → CMS-2 → AE-2

Scenario 3: REFER

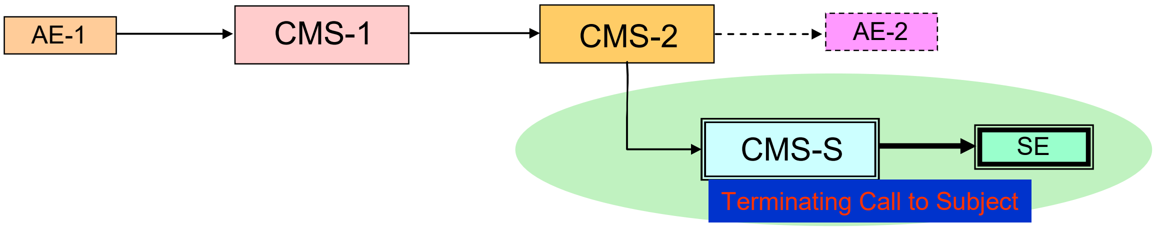
Scenario 4: REFER

REFER Method Scenario 1





REFER Method Scenario 2



AE-1

CMS-1

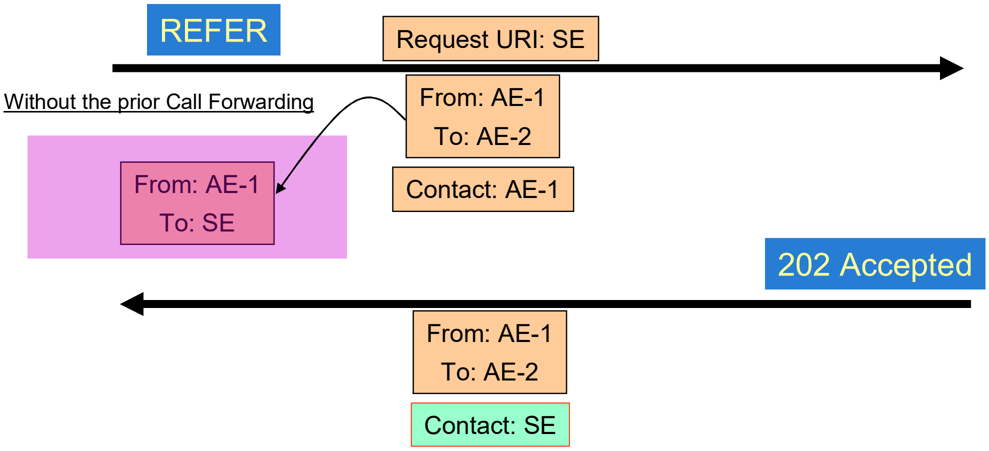
CMS-2

AE-2

CMS-S

SE

Terminating Call to Subject



REFER

Request URI: SE

From: AE-1
To: AE-2

Contact: AE-1

Without the prior Call Forwarding

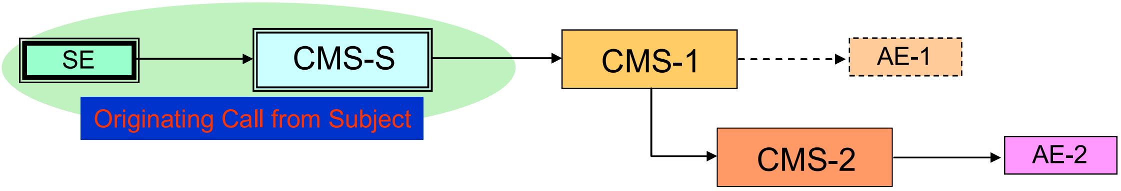
From: AE-1
To: SE

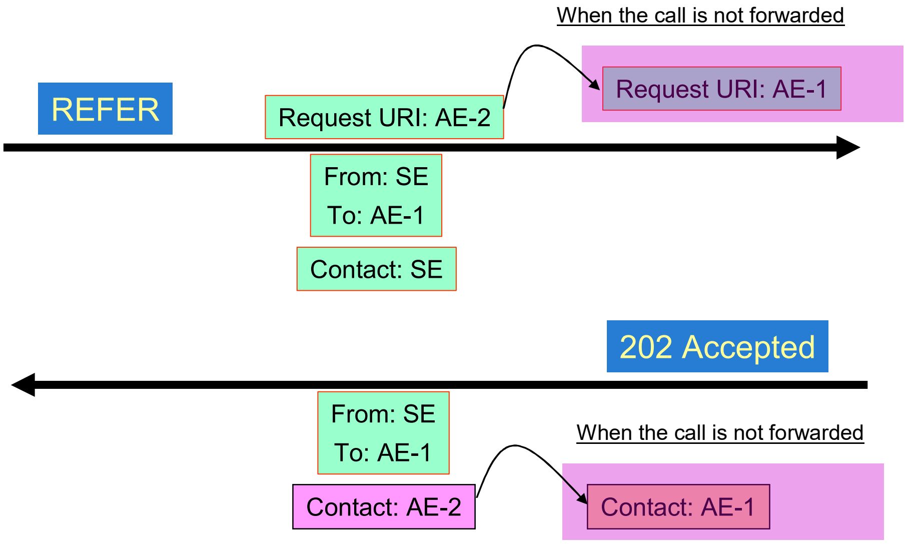
202 Accepted

From: AE-1
To: AE-2

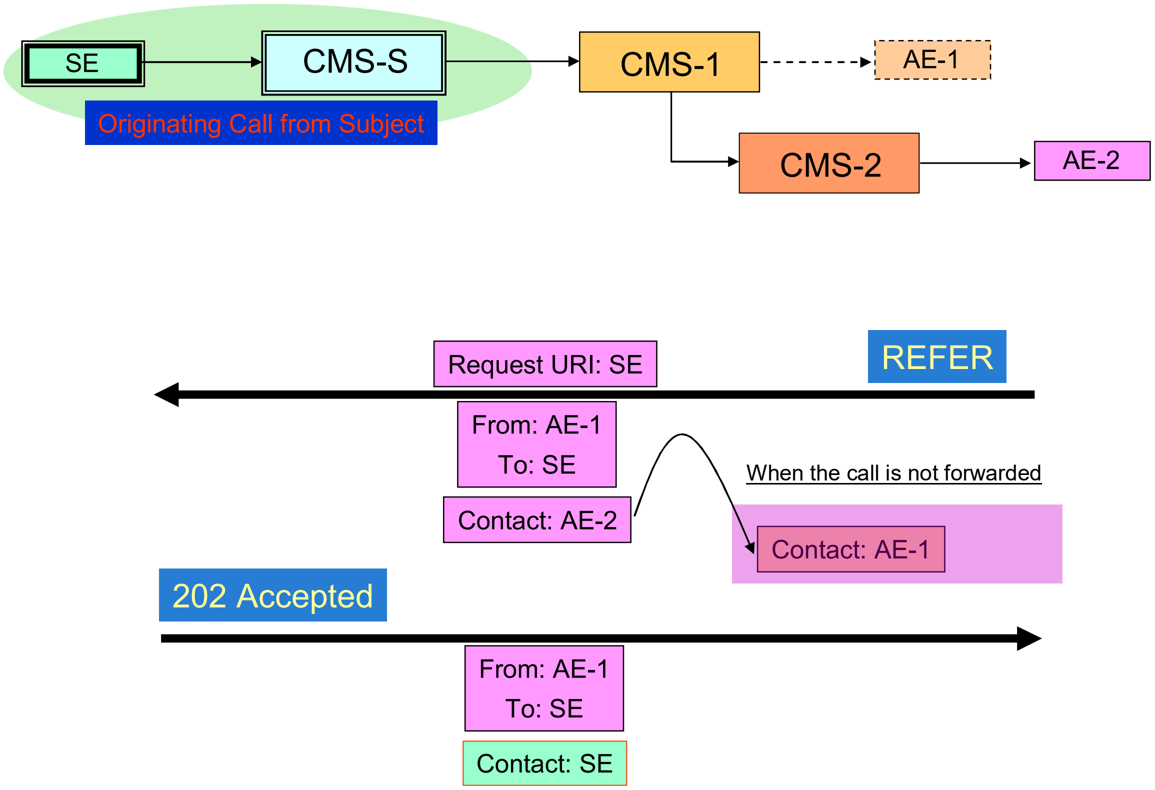
Contact: SE

REFER Method Scenario 3





REFER Method Scenario 4



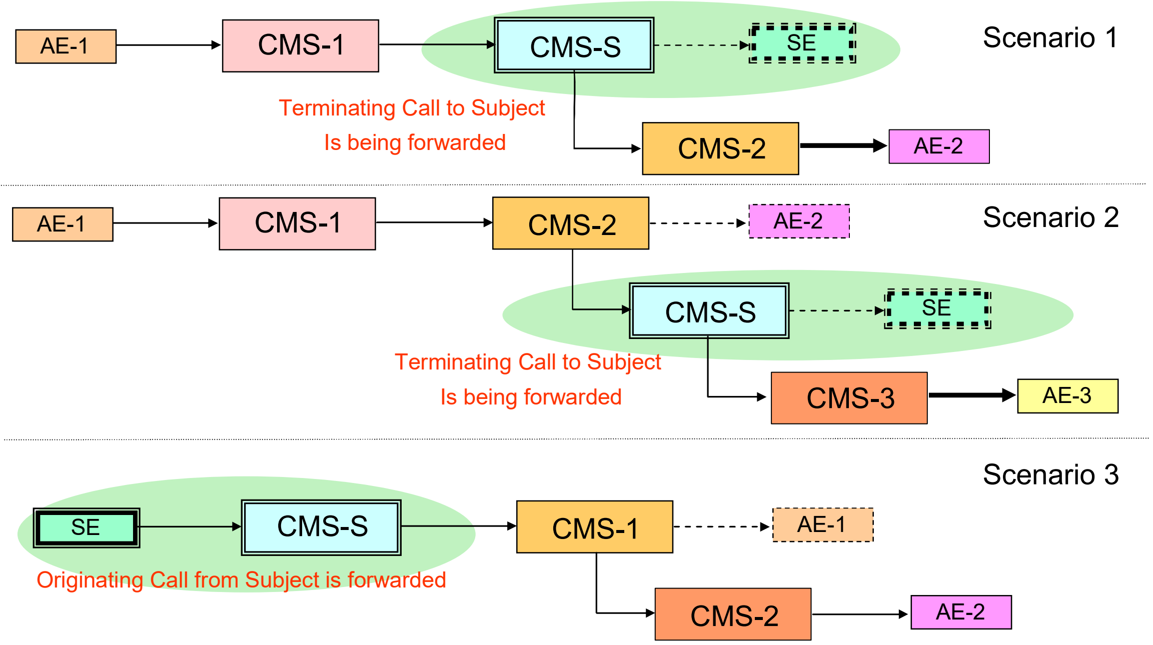
C.3.4 FROM & TO Mapping for Call Forwarding

The following information flows illustrate various call forwarding scenarios:

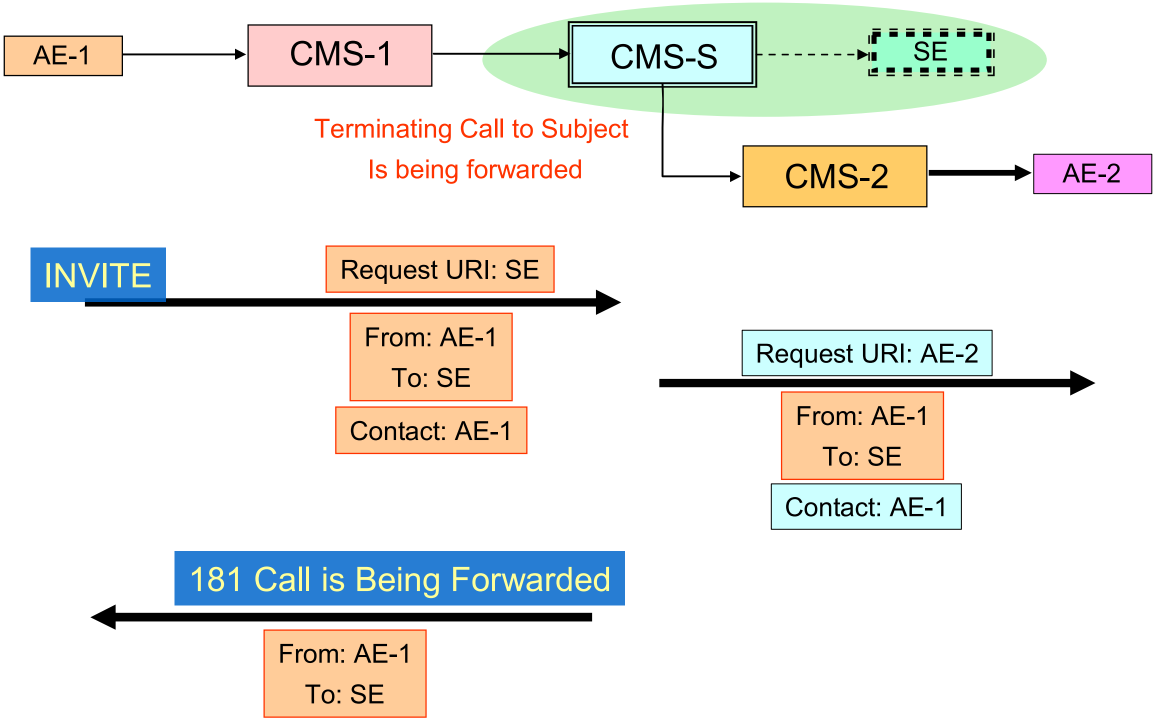
- AE-1 calls the Intercept Subject SE and the SE has a call forwarding active to AE-2. From an intercept perspective, forwarding occurs on a call to the Intercept Subject SE without any prior redirection.
- AE-1 calls AE-2 and AE-2 has call forwarding active to the Intercept Subject SE. The SE has call forwarding active to AE-3. From an intercept perspective, forwarding occurs on the call to the Intercept Subject SE that had prior redirection.
- Intercept Subject SE makes a call to AE-1 and AE-1 has a call forwarding active to AE-2.

The CMS-S that serves the Intercept Subject provides the IAP functions for the intercepted call. The SIP-to-LAES Message and Parameter mapping tables in clauses B.31 and B.32 are related to these information flows.

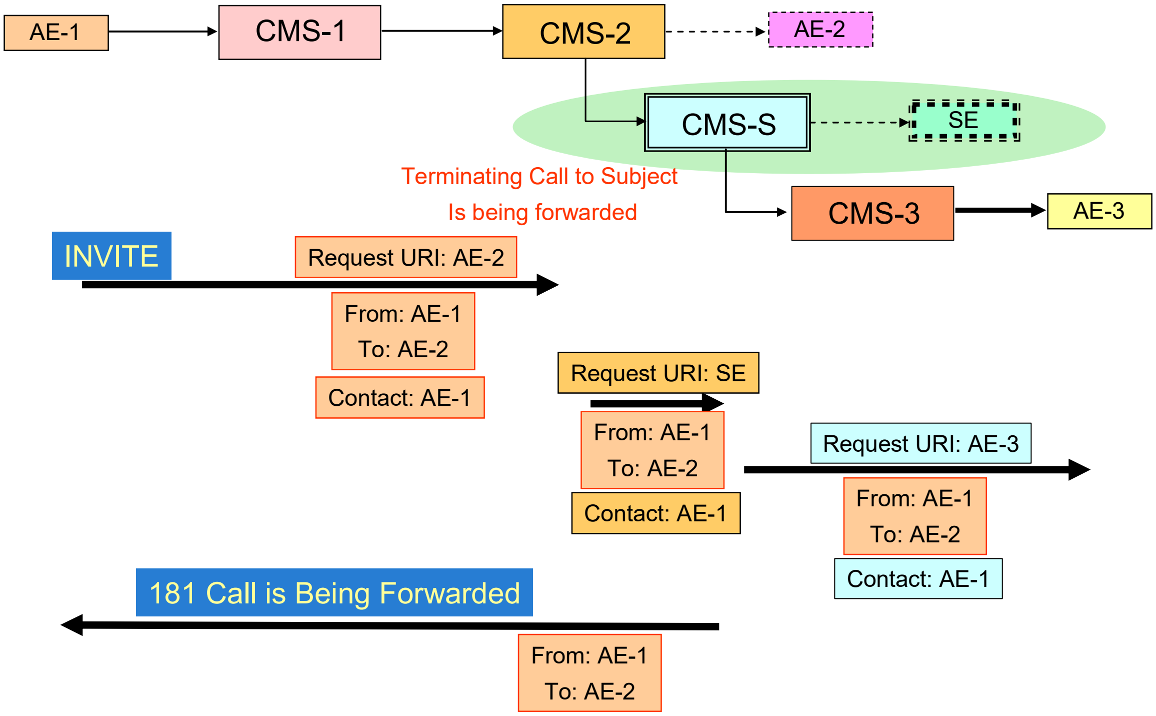
Signaling Flows
Terminating and Originating Calls



Call Terminating to a Subject – Scenario 1



Call Terminating to a Subject – Scenario 2



AE-1

CMS-1

CMS-2

AE-2

CMS-S

SE

Terminating Call to Subject
Is being forwarded

CMS-3

AE-3

INVITE

Request URI: AE-2

From: AE-1
To: AE-2

Contact: AE-1

Request URI: SE

From: AE-1
To: AE-2

Contact: AE-1

Request URI: AE-3

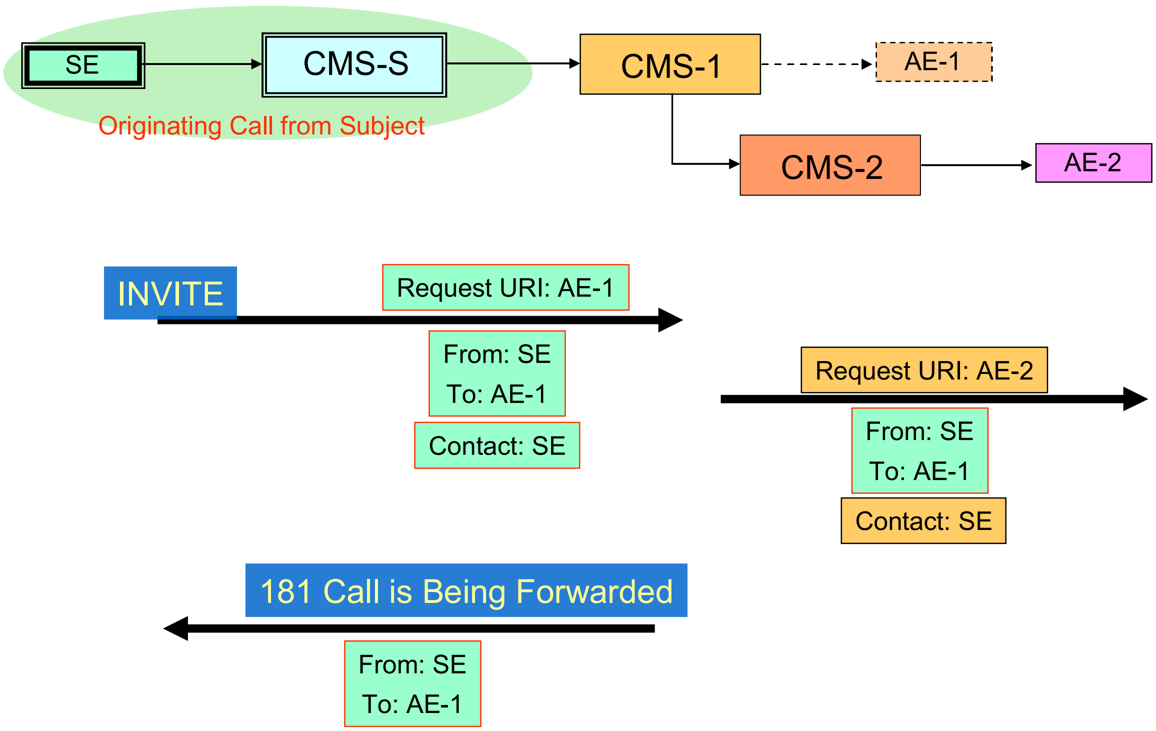
From: AE-1
To: AE-2

Contact: AE-1

181 Call is Being Forwarded

From: AE-1
To: AE-2

Call Originated from a Subject - Scenario 3



SE

CMS-S

Originating Call from Subject

CMS-1

AE-1

CMS-2

AE-2

INVITE

Request URI: AE-1

From: SE
To: AE-1

Contact: SE

Request URI: AE-2

From: SE
To: AE-1

Contact: SE

181 Call is Being Forwarded

From: SE
To: AE-1

C.3.5 FROM & TO Mapping for Call Hold and Retrieval

The following information flows illustrate Call Hold and Retrieval. The Hold and Retrieval of a call can be done by SIP users either using an UPDATE Method or using a re-INVITE Method. These information flows assume that the re-INVITE Method is used.

A call hold/retrieval scenario may apply for the following two scenarios:

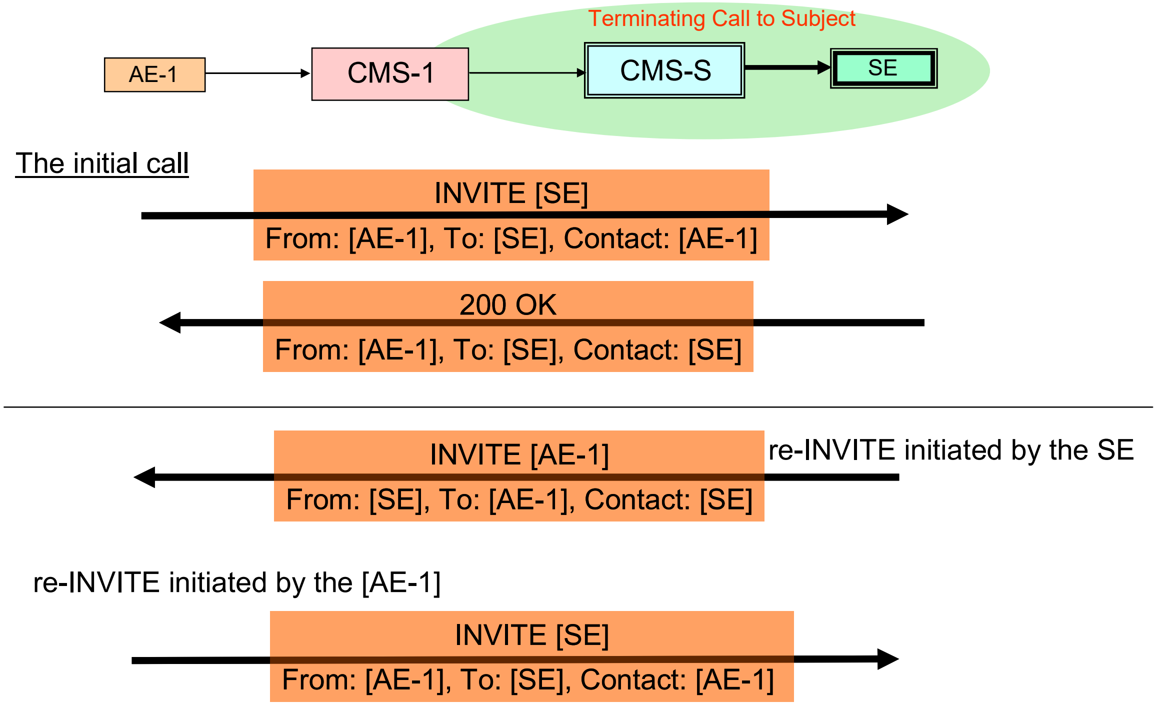
- The initial call is originated from an Intercept Subject SE. The call may or may not encounter redirection.
- The initial call is terminated to an Intercept Subject. The call may or may not have prior redirection.

Each of these scenarios has the following two scenarios for the hold/retrieval (i.e., re-INVITE method):

- The re-INVITE method is initiated by the Intercept Subject SE;
- The re-INVITE method is initiated by the current associate of the call (in other words, the Intercept Subject receives the re-INVITE message).

The CMS-S that serves the Intercept Subject provides the IAP functions for the intercepted call. The SIP-to-LAES Message and Parameter mapping tables in clauses B.33, B.34, B.35, B.36, B.37, and B.38 are related to these information flows.

re-INVITE Method



The initial call

INVITE [SE]
From: [AE-1], To: [SE], Contact: [AE-1]

200 OK
From: [AE-1], To: [SE], Contact: [SE]

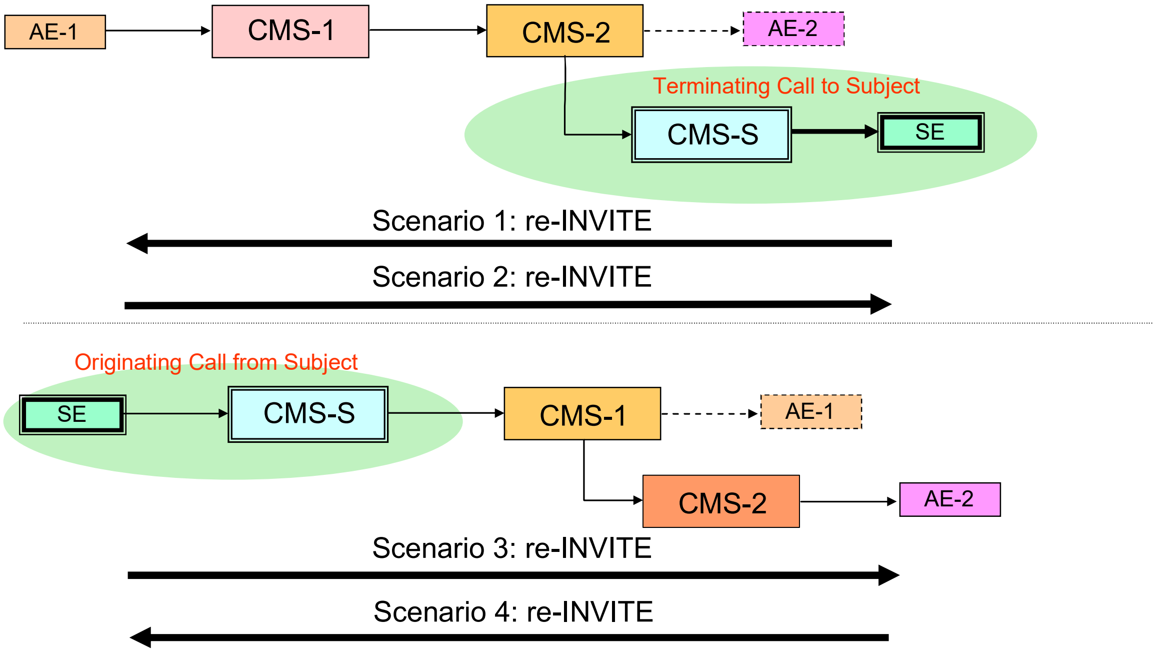
INVITE [AE-1]
From: [SE], To: [AE-1], Contact: [SE]

re-INVITE initiated by the SE

re-INVITE initiated by the [AE-1]

INVITE [SE]
From: [AE-1], To: [SE], Contact: [AE-1]

re-INVITE Method – More Scenarios



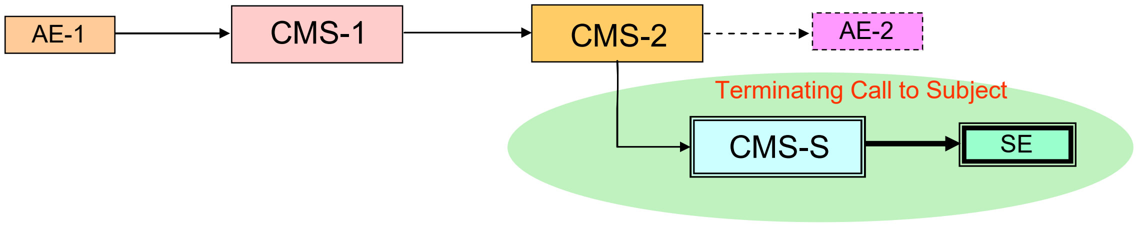
Scenario 1: re-INVITE

Scenario 2: re-INVITE

Scenario 3: re-INVITE

Scenario 4: re-INVITE

re-INVITE Method – Scenario 1



AE-1

CMS-1

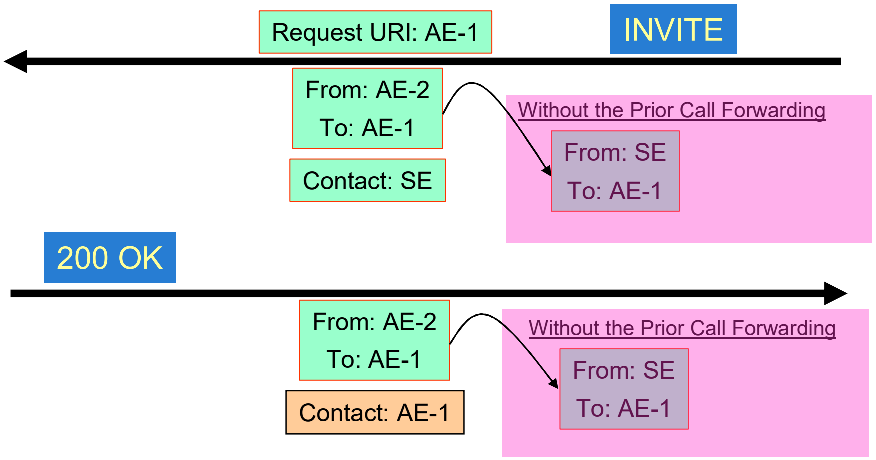
CMS-2

AE-2

Terminating Call to Subject

CMS-S

SE



INVITE

Request URI: AE-1

From: AE-2
To: AE-1

Contact: SE

Without the Prior Call Forwarding

From: SE
To: AE-1

200 OK

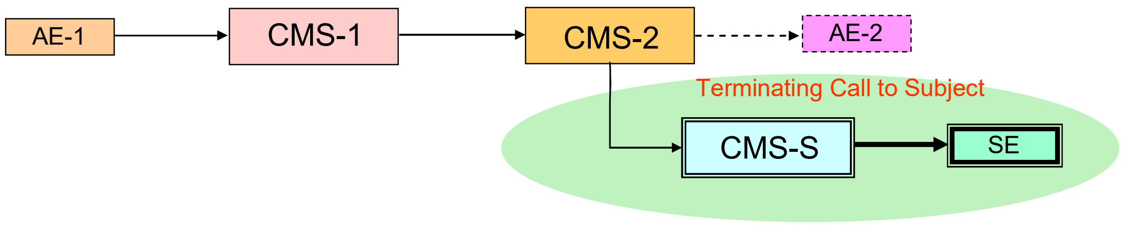
From: AE-2
To: AE-1

Contact: AE-1

Without the Prior Call Forwarding

From: SE
To: AE-1

re-INVITE Method – Scenario 2



AE-1

CMS-1

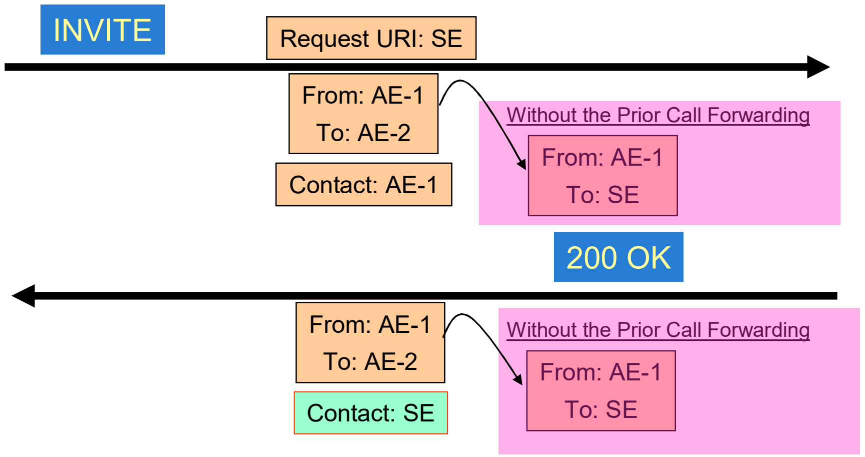
CMS-2

AE-2

Terminating Call to Subject

CMS-S

SE



INVITE

Request URI: SE

From: AE-1
To: AE-2

Contact: AE-1

Without the Prior Call Forwarding

From: AE-1
To: SE

200 OK

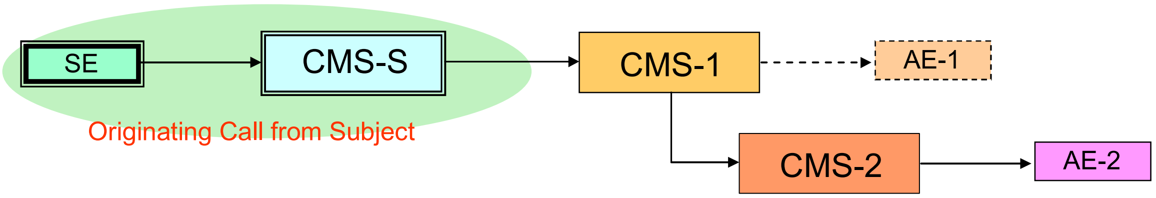
From: AE-1
To: AE-2

Contact: SE

Without the Prior Call Forwarding

From: AE-1
To: SE

Re-INVITE Method – Scenario 3



SE

CMS-S

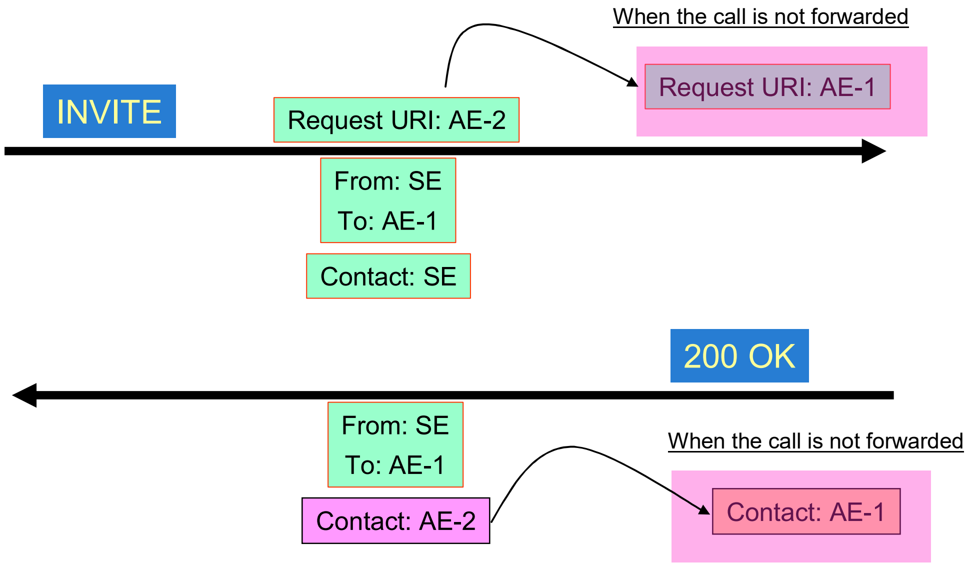
Originating Call from Subject

CMS-1

AE-1

CMS-2

AE-2



When the call is not forwarded

Request URI: AE-1

INVITE

Request URI: AE-2

From: SE

To: AE-1

Contact: SE

200 OK

From: SE

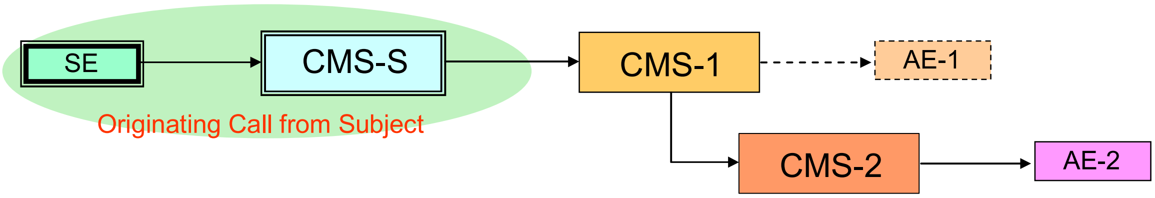
To: AE-1

Contact: AE-2

When the call is not forwarded

Contact: AE-1

re-INVITE Method – Scenario 4



SE

CMS-S

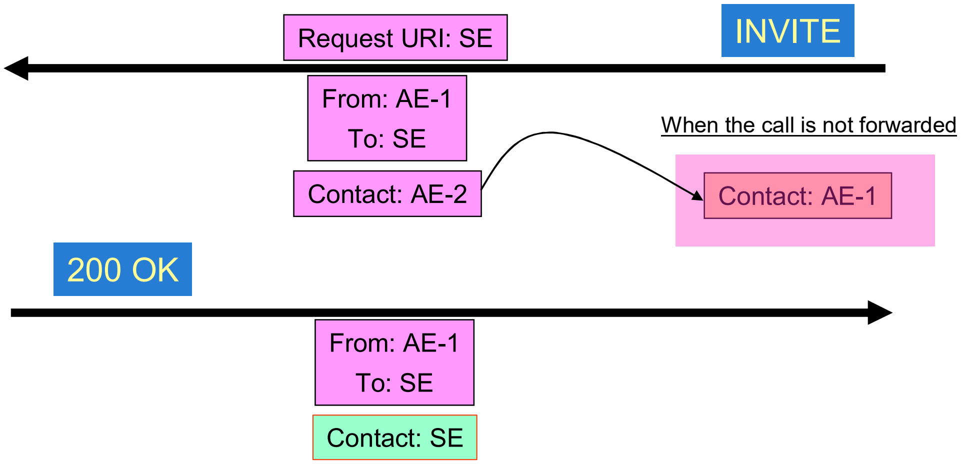
CMS-1

AE-1

CMS-2

AE-2

Originating Call from Subject



INVITE

Request URI: SE

From: AE-1

To: SE

Contact: AE-2

When the call is not forwarded

Contact: AE-1

200 OK

From: AE-1

To: SE

Contact: SE

Annex D Optional Messages

(informative)

This annex is informative and is not considered part of this Standard.

D.1 SurveillanceStatus Message

The *SurveillanceStatus Message* is an optional message that may be used to report the status of a lawfully authorized electronic surveillance. The optional message may be used to report that a surveillance has been activated, deactivated or changed status, or the current status of an active surveillance (based on a schedule).

The following are the possible surveillance statuses:

- *Inactive*: Surveillance is not being performed.
- *Active*: Surveillance is being performed. A surveillance is active between the activation and deactivation of the surveillance. The following are the two possible specific surveillance statuses for an active surveillance:
    1. *Partially active*: Not all of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.
    2. *Fully active*: All of the functionality (e.g., IAPs) needed to fully perform surveillance on an intercept subject is performing surveillance.

The SurveillanceStatus message may be triggered when:

- The VoIP network activates a lawfully authorized electronic surveillance (with a status of *fully active* or *partially active*);
- The VoIP network deactivates a lawfully authorized electronic surveillance (with a status of *inactive*);
- The VoIP network determines that the current status of an active lawfully authorized electronic surveillance has changed from *partially active* to *fully active* or from *fully active* to *partially active*; or
- The VoIP network determines that the current status (*fully active* or *partially active*) of an *active* lawfully authorized electronic surveillance is to be reported to the corresponding LEA (based on a schedule).

The SurveillanceStatus message includes the following parameters:

Table D.1: SurveillanceStatus Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
ReportingSystemIdentity	C	Included to identify the system reporting the surveillance status, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
StatusEventType	M	Indicates which surveillance status event occurred.
CurrentStatus	M	Indicates the current surveillance status.

```
SurveillanceStatus ::= SEQUENCE {
    caseId                  [0] CaseIdentity,
    reportingSystemId       [1] IAPSystemIdentity                            OPTIONAL,
                            -- include to identify the system reporting the surveillance status
```

```
                          -- when the underlying data carriage does not imply that system.
    timestamp             [2] TimeStamp,
    statusEventType       [3] SurveillanceStatusEventType,
    currentStatus         [4] CurrentSurveillanceStatus
}

CurrentSurveillanceStatus ::= ENUMERATED {
    fullyActive        (0),
    partiallyActive    (1),
    inactive           (2)
}

SurveillanceStatusEventType ::= ENUMERATED {
    activation         (0),
    deactivation       (1),
    change             (2),
    scheduledReport    (3)
}
```

D.2 FeatureManagement Message

The *FeatureManagement Message* is an optional message that may be used to report the activation and deactivation of service features in the VoIP network for an intercept subject performed through an indirect mechanism (e.g., VoIP network updates prompted by filling in a Web page form). Direct activations and deactivations (e.g., dialing a vertical feature code, pressing a feature key) of service features are reported through the Origination message (see 6.1.13) or SubjectSignal message (see 6.1.17).

The FeatureManagement message only addresses feature activations and deactivations that result in attempts to update the VoIP network. Any feature activations or deactivations that *only* result in attempts to update a TSP's operations support systems (e.g., Billing System) are not addressed.

The FeatureManagement message may be triggered when an attempt is made to update the VoIP network to activate or deactivate a service feature for the intercept subject through an indirect mechanism (whether or not the activation or deactivation is successful).

The FeatureManagement message includes the following parameters:

Table D.2: FeatureManagement Message Parameters

Parameter	MOC	Usage
CaseIdentity	M	Identifies the Intercept Subject.
IAPSystemIdentity	C	Included to identify the system containing the IAP, when the underlying data carriage does not imply that system.
TimeStamp	M	Identifies the date and time that the event was detected.
SubscriberIdentity	C	Include to identify the subscriber to the service, when the identifier is more specific than the intercept subject identity associated with the CaseIdentity.
FeatureIdentity	M	Identifies the feature for which the activation or deactivation is attempted.
FeatureManagementType	M	Indicates whether the feature was attempted to be activated or deactivated.
FeatureActivationInformation	C	Include to identify information provided for use by a feature (e.g., forward-to number for call forwarding), when feature activation was attempted and information was provided for use by the feature.
FailureReason	C	Include to indicate the reason for an unsuccessful feature activation or deactivation, when the feature activation or deactivation was unsuccessful.

```
FeatureManagement ::= SEQUENCE {
    caseId                  [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity                        OPTIONAL,
                            -- include to identify the system containing the Intercept Access Point,
                            -- when the underlying data carriage does not imply that system.
    timestamp               [2] TimeStamp,
    subscriberId            [3] PartyIdentity                            OPTIONAL,
                            -- Include to identify the subscriber to the service, when the identifier
```

```
                              -- is more specific than the intercept subject identity associated with
                              -- the CaseIdentity.
    featureId                 [4] UTF8String,
    managementType            [5] FeatureManagementType,
    activationInfo            [6] UTF8String                              OPTIONAL,
                              -- include to identity information provided for use by a feature
                              -- (e.g., forward-to number for call forwarding), when feature activation
                              -- was attempted and information was provided for use by the feature.
    failureReason             [7] UTF8String                              OPTIONAL
                              -- include to indicate the reason for an unsuccessful feature activation
                              -- or deactivation, when the feature activation or deactivation was
                              -- unsuccessful.
}

FeatureManagementType ::= ENUMERATED {
    activation     (0),
    deactivation   (1)
}
```

Annex E Example VoIP CC-IAP Locations

(informative)

This annex is informative and is not considered part of this Standard.

A TSP may use several different types of VoIP CC-IAPs depending on the network design and the type of call. Figure E.1 and Figure E.2 illustrate some of the options. In Figure E.1 and Figure E.2, the Access Router is the first router in the TSP's network that the subject's traffic passes.

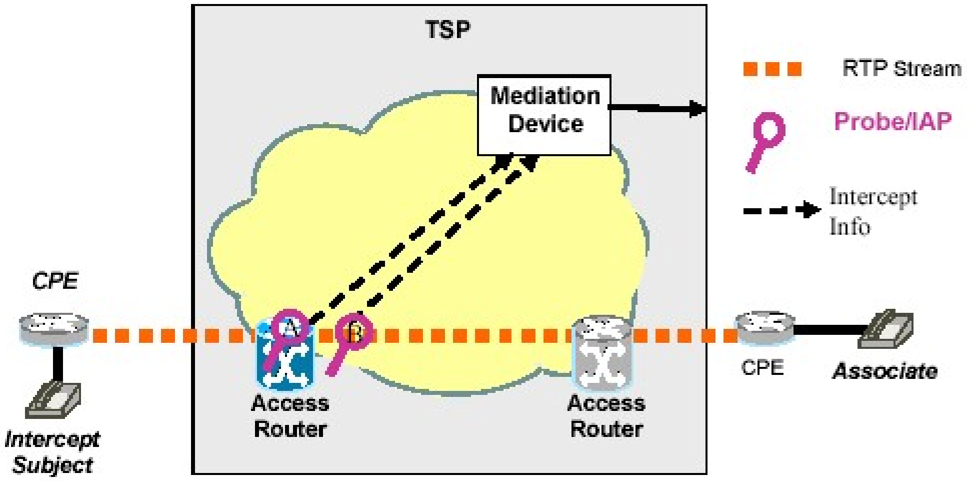


Figure E.1: VoIP CC-IAP At or Near Access Router

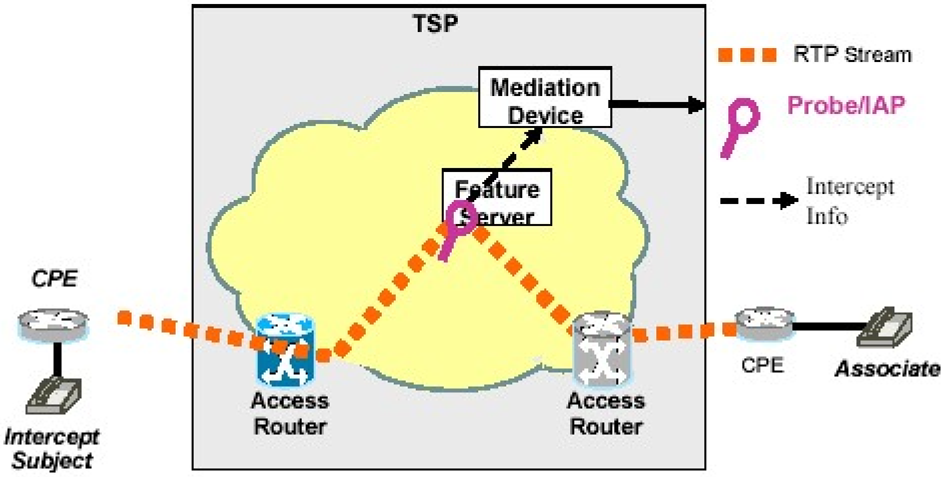


Figure E.2: VoIP CC-IAP At Feature Server

One of the key requirements is to ensure that the intercept subject is unable to detect the intercept. This places some constraints on the location of the IAP. This standard assumes a sophisticated subject or a subject with sophisticated tools:

- Able to check IP addresses, use traceroute, etc.
- Able to check if any unusual signaling is occurring on their customer premises equipment (CPE).
- Able to detect degradation or interruptions in service.

This implies that the intercept mechanism should not involve:

- *Requests to the CPE*: In this case, the intercept subject could detect the extra signaling occurring on the CPE and the traffic replication.
- *Re-routing of packets or end-to-end changes in IP addresses specifically for the intercept*: In this case, the user could use traceroute to determine the path the packets are taking. This could allow the subject to detect that there is a network device in the voice path. In addition, if the IP address of the associate is different from the IP address signaled for the call, the subject could infer that a network device is terminating the voice packet stream.

This in turn implies that the CC intercept should be done on a device along the normal network path between the two endpoints (i.e., no re-routing has occurred) that is within the service provider (rather than the customer's) network.

As shown in Figure E.1, the CC-IAP can be located in the access router or in an external probe located near the network access point. In either case, the access router or probe is configured with the appropriate filters. Traffic that matches the filters is replicated and sent to the Mediation Device. For VoIP, the filter information is acquired from the call control signaling at the IAP.

The IAP at point A is embedded in the Access Router. In this case, the IAP has access to the traffic crossing the Access Router.

The IAP at point B is located in equipment external to the Access Router. This could be specialized equipment or embedded in other network equipment. In this case, the IAP has to be placed such that it has access to the packet stream containing the CC.

For special features such as TSP-provided conference services, voice mail, etc., a feature server may be required. For these types of features, an IAP may need to be in place in the Feature Server or in a probe adjacent to the Feature Server to access the CC. Again, the CC-IAP will have to be controlled based on call control information.

In VoIP, packets are routed via the IP address. In the case in which the intercept subject uses features like Call Forwarding, Call Transfer, etc., to redirect calls to other endpoints, the packets containing the voice stream may not pass through the Access Router or even through the network local to the intercept subject. In those cases, the IAP may have to change in order to follow the call.

Annex F Dialed Digit Extraction Scenarios

(informative)

This annex is informative and is not considered part of this Standard.

The following Dialed Digit Extraction (DDE) scenarios are presented for information purposes. Possible issues with the various solutions are identified. Ultimately, each network implementation will determine the issues and feasibility of its DDE solution.

A requirement for each scenario is access to and availability of the characteristics of the packet CC stream in order to provide the means to isolate the embedded dialed digits. This means providing the DDE Function with at least the SDP information in the SIP messages along with the packet stream. In addition, the DDE Function must support the codec being used between the endpoints and must support and have knowledge of how the dialed digits are encoded (i.e., IETF RFCs used to encode the digits). End-to-end CC or SDP information encryption will also prevent the isolation of any Dialed Digits in the packet stream.

Considerations for the scenarios are:

a) DDE is done on a per lawful authorization basis; and

b) Intercepted CC for purposes of DDE is considered to be part of the network engineered capacity allocated for lawful intercept (e.g., maximum number of active intercepts required for CC access, handling, and delivery).

F.1 Scenario 1 – DDE with Internal Delivery Function

F.1.1 Case 1 – Signaling & Content are Accessible on a Single Network Access Node

Architecture: Both the signaling and CC are present and accessible to the DDE-IAP function on a single network element. This eliminates the need for an internal network interface to send the SIP-SDP information to the DDE-IAP function in a separate node.

Description: The network element receives both SIP signaling and CC streams and has a CMS function. CII and CC-IAPs are present. The network element has internal Delivery Functions for reporting CII and CC to the LEAs.

A DDE-IAP is added to isolate the dialed digits in the CC stream. The DDE-IAP, having access to the SIP-SDP information at the CMS and access to the CC, isolates the dialed digits and presents the results to the CII-IAP for reporting to the LEA.

Issues: The following issues can be identified:

a) The requirement to investigate every packet in the CC stream is resource intensive and may require additional resources (e.g., processing power and memory), which may impact the marketability of a product.

b) Interrogation of the CC stream may introduce a detectable delay and thus visibility of the intercept to the subject or associate. This may be overcome by adding additional resources as noted.

c) The network element performing DDE may be required to support the codec used for the CC stream (i.e., RFC 2833 is not used to carry digits), which it may not otherwise need to do, depending on its functions. With end-to-end codec negotiation, the user may select a codec not supported by the network element. Which codes to support then becomes an issue. Adding codec support for DDE to network elements, which inherently by their normal network functions (e.g., routing) have no need for such codec support, may impact the marketability of a product.

d) DDE may not be applicable to all user media streams (e.g., video) and unless the network element is able to distinguish the media on a service basis (e.g., audio vs. video), all media streams would have to be investigated for dialed digits. This exacerbates the resource issue. Adding the ability to distinguish media streams may impact the network design, interfaces, and architecture, and may not be possible for all networks.

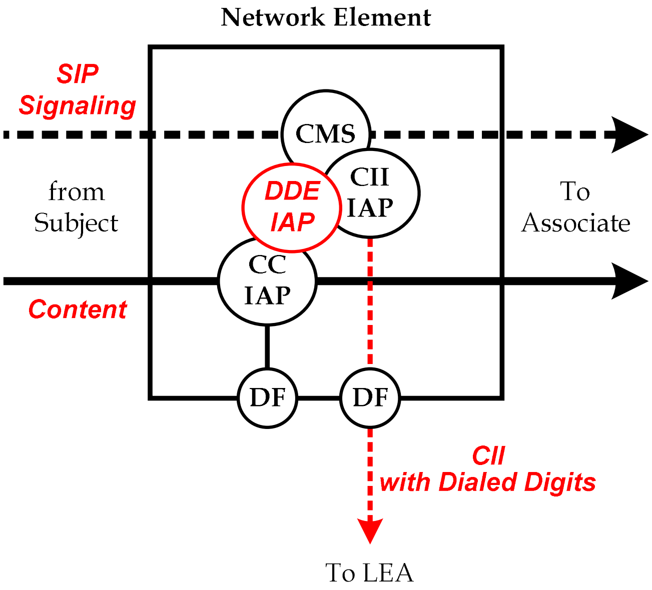


Figure F.1: Dialed Digit Extraction with Single Network Element

F.1.2 Case 2 – Signaling & CC are Present on Multiple Network Elements

Architecture: The signaling and CC are present on separate network elements, requiring new network interfaces to send the SIP signaling to the DDE-IAP function and to return the Dialed Digit CII back to the CII IAP.

Description: Network Element A receives the SIP signaling, has a CMS, and has a CII IAP. Network Element B receives the CC streams and has a CC-IAP. The network elements have internal Delivery Functions for reporting CII and CC to the LEAs.

A DDE-IAP is added to Network Element B to isolate the dialed digits in the CC stream. This requires receiving the SIP-SDP information from the CMS in Network Element A. The DDE-IAP isolates and sends the dialed digits to the CII-IAP in Network Element A for delivery to the LEAs.

Issues: The following issues can be identified:

a) Scenario 1, Case 1, issues apply.

b) The development and maintenance of internal network interfaces for lawful intercept of DDE will be impacting on the network.

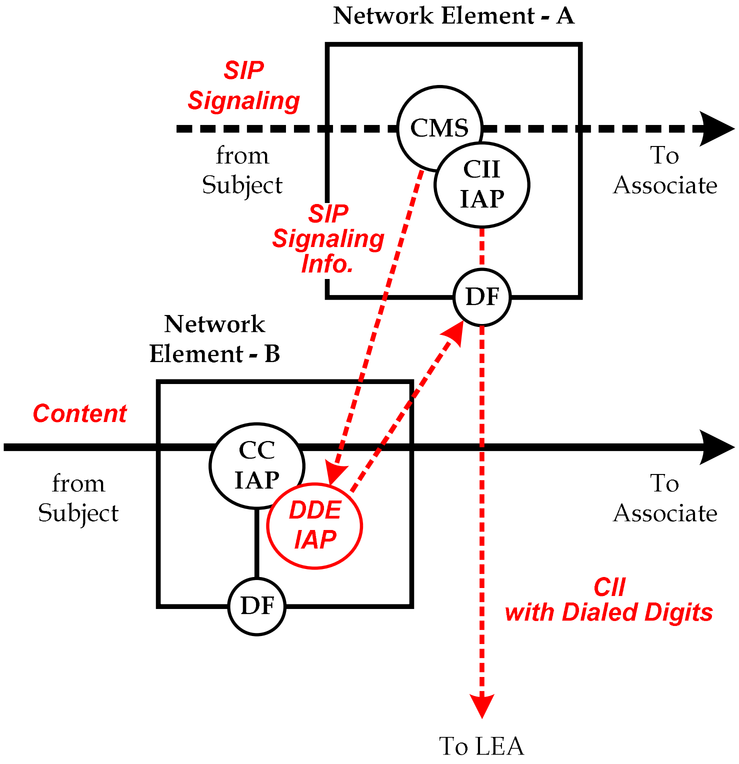


Figure F.2: Dialed Digit Extraction with Multiple Network Elements

F.2 Scenario 2 – DDE with Delivery Function Network Element

Architecture: The signaling and CC are present on separate network elements. A separate network element is used as the Delivery Function. The DDE-IAP is implemented in the Delivery Function network element. A signaling interface is developed from the CMS in Network Element A to the DDE-IAP in the Delivery Function network element to send the SIP-SDP information needed for isolation of the dialed digits.

Description: Network Element A receives the SIP signaling, has a CMS, and has a CII-IAP. Network Element B receives the CC streams and has a CC-IAP. The CII is extracted at Network Element A from the SIP signaling stream and sent to the Delivery Function network element for delivery to the LEA. The CC is intercepted at Network Element B and sent to the Delivery Function network element for delivery to the LEA.[18]

A DDE-IAP is added to the Delivery Function network element B to isolate the dialed digits in the CC stream. This requires receiving the SIP-SDP information from the CMS in Network Element A. The DDE-IAP isolates and presents the dialed digits to the CII DF in the Delivery Function for integrating into the CII stream for law enforcement.

Issues: The following issues can be identified:

a) Scenario 1, Case 1, issues apply to the Delivery Function with the exception of a detectable delay.

b) An additional impact of developing and maintaining a new network interface for sending the SIP-SDP information from the CMS node to the DDE-IAP node. (Note that it may be possible to extract the necessary signaling information -- e.g., SIP SDP -- from the CII-IAP-to-CII-DF interface.)

[18] Note that CC is normally intercepted and delivered to the Delivery Function network element only when content interception is required by the warrant. With DDE, CC will be delivered for every intercept and lawful authorization, unless conditional by the lawful authorization.

c) Adding DDE to a Delivery Function results in a larger, more complex, and more resource intensive Delivery Function.

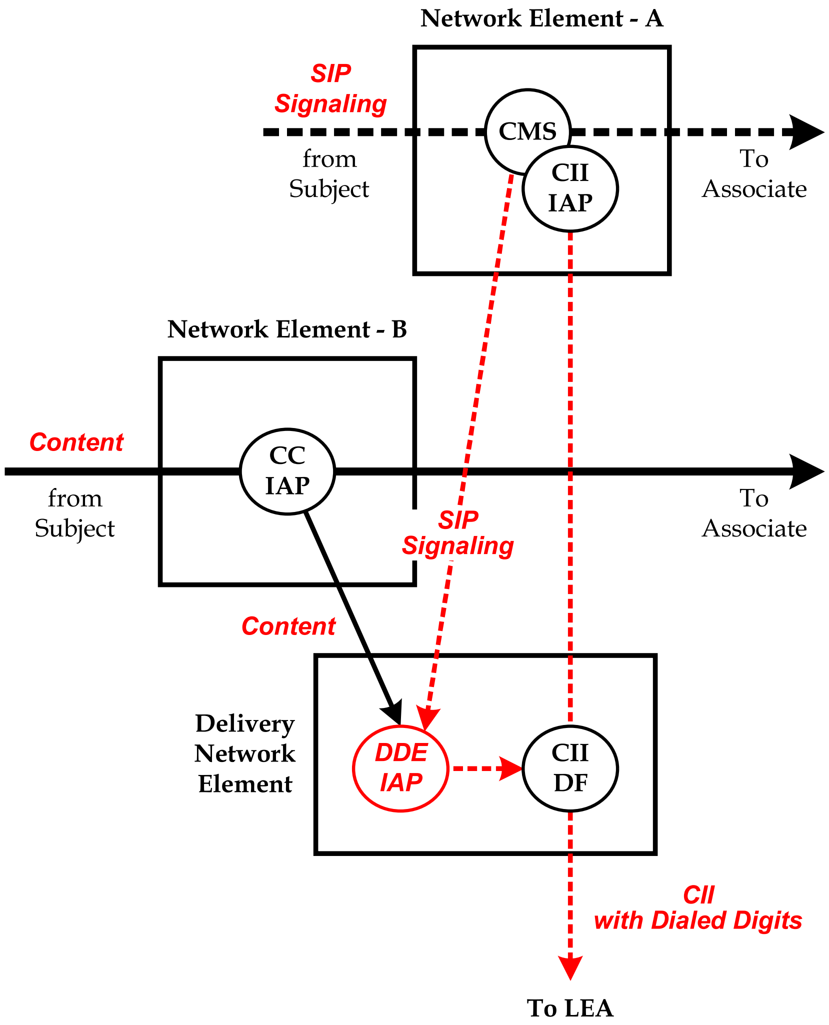


Figure F.3: Dialed Digit Extraction with Delivery Function Network Element

F.3 Scenario 3 – DDE at the LEA's Collection Function

Architecture: The signaling and CC are present on separate network elements. A separate network element is used as the Delivery Function. The DDE-IAP is implemented in the LEA's Collection Function.

Description: Network Element A receives the SIP signaling, has a CMS, and has a CII-IAP. Network Element B receives the CC streams and has a CC-IAP. The CII is extracted at Network Element A from the SIP signaling stream and sent to the Delivery Function network element for delivery to the LEA. The CC is intercepted at Network Element B and sent to the Delivery Function network element for delivery to the LEA. This is the normal processing for current Delivery Functions and no new functionality is required on the network for VoIP DDE.

Issues: The following issues can be identified:

a) Scenario 1, Case 1, issues are eliminated.

b) The impact on adding a DDE-IAP to the Delivery Function as identified in Scenario 2 is eliminated.

c) The impact of DDE is isolated to the LEA's Collection Function as opposed to the network's Delivery Function(s). In addition, the collection function must already have codec support to process the VoIP CC.

Thus, codec support does not need to be added to the collection equipment for an LEA equipment-based DDE solution as would be required with a network-based solution. Given that there are more likely Delivery Function Network Elements than Collection Function elements, economies of scale are also achieved by a LEA based solution as opposed to a network based solution

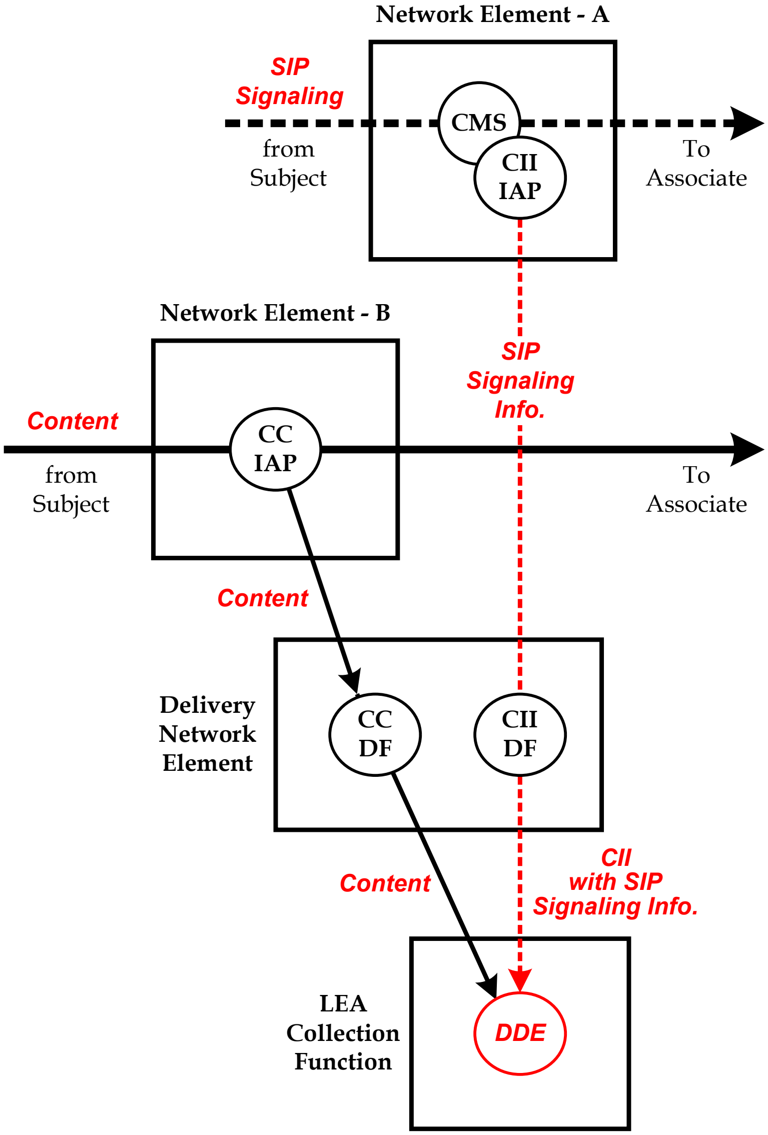


Figure F.4: Dialed Digit Extraction at LEA's Collection Function