ATIS STANDARD

**ATIS-0700005.v002**

ATIS Standard on -

# Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services

## Notice of Disclaimer & Limitation of Liability

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

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

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

*Published by*

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

**ATIS-0700005.v002**

ATIS Standard on

# Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services

**Alliance for Telecommunications Industry Solutions**

Approved February 2, 2017

## Abstract

This ATIS Standard defines an interface between a Telecommunications Service Provider and a Law Enforcement Agency for the reporting of Lawfully Authorized Electronic Surveillance for 3GPP IMS-based Voice-over-IP and other multimedia services.

NOTE: IMS-3GPP-VoIP-CII-Module and IMS-3GPP-VoIP-CC-Module in Annex B of this ATIS Standard has also been formatted as a separate plain text file and electronically packaged with this document.

# Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

This ATIS Standard is a revision of ATIS-0700005.2007 and its supplement ATIS-0700005a.2010, Technical Requirements document entitled *Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services*.

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

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

D. Zelmer, WTSC Chair (AT&T)

M. Younge, WTSC Vice Chair (T-Mobile)

P. Musgrove, WTSC LI Chair (AT&T)

G. Schumacher, WTSC LI Vice Chair (Sprint)

N. Rao, Technical Editor (Nokia)

The WTSC LI Subcommittee was responsible for the development of this document.

# Table of Contents

# Table of Figures

## Table of Tables

ATIS Standard

# Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services

## 1 Introduction

### 1.1 Background

*Electronic surveillance* refers to the interception and monitoring of communications – i.e., Communication-Identifying Information (CII) or CII with Communication Content (CC) – for a particular telecommunications subscriber as lawfully authorized. An *intercept subject* is a telecommunications service subscriber whose communications have been authorized by a legal instrument to be intercepted and delivered to a Law Enforcement Agency (LEA). The identification of the intercept subject is limited to subject identifiers or subject-related identifiers used by the Telecommunications Service Provider (TSP) equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

As a precondition for TSP 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 the service areas where the communications and information are to be provided. Once a 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.

The Lawful Intercept (LI) architecture, functions, and handover interface for capture and delivery of packet information (including SIP message contents) are found in the 3GPP LI specifications [107] and [108].

This ATIS Standard is provided for purposes of a “safe harbor” as specified in Section 107 of the Communications Assistance for Law Enforcement Act [CALEA]: “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.”

### 1.2 Scope & Purpose

This ATIS Standard defines an interface between a TSP and an LEA for the reporting of LAES for 3GPP IMS-based VoIP and other 3GPP IMS-based multimedia services. This ATIS Standard identifies specific United States requirements for the LI.

The main purpose of this ATIS Standard is to provide capabilities for support of LAES for VoIP. In addition, the scope also includes other IMS-based multimedia services because the media type may change in mid-session (e.g., audio to video, or video to audio). The mapping of SIP messages to [678] messages must take place from the beginning of a session because of the potential for a change to a VoIP call in the middle of a session.

The following items are defined in this ATIS Standard to support the reporting of CII and CC over an “e” interface:

- How SIP messages, as described in the 3GPP IMS specifications [228] and [229], are mapped into [678] messages;
- The CII and CC Mediation Function(s) (MF) that perform the mapping; and
- The CII and CC information delivered to the LEA(s) over an “‘e” interface.

The CII and CC MF(s) are based on the mapping functions as defined in [678], with enhancements as specified in this ATIS Standard. The CII and CC information delivered over the ”e” interface is based on [678] plus additional information.

The reporting of CII via the encapsulated SIP messages as defined in [108] is out of scope of this ATIS Standard.

Lawful interception of SMS/MMS is outside the scope of this ATIS 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. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

For a specific reference, subsequent revisions do not apply.

For a non-specific reference, the latest version applies.

## *2.1 3rd Generation Partnership Project (3GPP) Technical Specifications*

For the purpose of this ATIS Standard, the latest Release 13 version shall apply.

NOTE: Documents available at: < http://www.3gpp.org/specs/specs.htm >.

[228] 3GPP TS 23.228, *IP Multimedia Subsystem; Stage 2 (Release 13)*.

[229] 3GPP TS 24.229, *IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 13)*.

[107] 3GPP TS 33.107, *Lawful interception architecture and functions (Release 13)*.

[108] 3GPP TS 33.108, *Handover interface for Lawful Interception (Release 13)*.

## *2.2 Alliance for Telecommunications Industry Solutions (ATIS)*

NOTE: Documents available at: < https://www.atis.org/docstore/default.aspx >.

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

[025-B] ANSI/J-STD-025-B-2006, *Lawfully Authorized Electronic Surveillanc*e.

## *2.3 International Telecommunication Union, Telecommunication Standardization Sector (ITU-T)*

NOTE: Documents available at: < http://www.itu.int/ITU-T/ >.

[Y-101] Y.101, *Global Information Infrastructure Terminology: Terms and definitions*, March 2000.

[X-680] X.680, *Abstract Syntax Notation One (ASN.1): Specification of basic notation*, July 2002.

## *2.4 Internet Engineering Task Force (IETF)*

NOTE: Documents available at: < http://www.ietf.org >.

[SDP] RFC 2327, *SDP: Session Description Protocol*, April 1998.

[SIP] RFC 3261, *SIP: Session Initiation Protocol*, June 2002.

## 2.5 Federal Communications Commission (FCC)

NOTE: Documents available at: < https://www.fcc.gov/ >.

[99-230] FCC 99-230, CC Docket No. 97-213, *Third Report and Order*, Released August 31, 1999.

[05-153] FCC 05-153, ET Docket No. 04-295, *First Report and Order and Further Notice of Proposed Rulemaking (NPRM)*, September 23, 2005, which concludes that CALEA applies to facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP).

[06-56] FCC 06-56, ET Docket No. 04-295, *Second Report and Order and Memorandum Opinion and Order*, Released May 12, 2006, which addresses the assistance capabilities required, pursuant to section 103 of the Communications Assistance for Law Enforcement Act (CALEA), for facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP).

## 2.6 103rd Congress

NOTE: The following document is available at: < https://www.fcc.gov/ >.

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

NOTE: The following document is available at: < http://uscode.house.gov/ >.

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

# 3 Definitions, Acronyms, & Abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in [107] and [108] and the following terms listed below apply.

**3.1.1 Access Function (AF):** Consists of one or more *Intercept Access Point(s)* (*IAPs*), which isolate an intercept subject’s communication-identifying information unobtrusively [678].

**3.1.2 Associate:** A communication user whose equipment, facilities, or services are communicating with an intercept subject.

**3.1.3 Call Management Server (CMS):** A core network function that includes sending and receiving signaling and call control information (e.g., SIP messages) for the management of a call to and from endpoints (e.g., Mobile Station).

**3.1.4 Collection Function (CF):** Where the intercepted communications and communication-identifying information is collected by a Law Enforcement Agency (LEA).

**3.1.5 Communication Content (CC):** see *Content*.

**3.1.6 Communication Content Delivery Function (CC DF):** The CC DF delivers the mapped CC to the LEA CF.

**3.1.7 Communication Content Mediation Function (CC MF):** The CC MF maps the CC from the TSP network to the CC delivered to the LEA CF.

**3.1.8 Content:** Defined in [Title 18] to be: “when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication.”

**3.1.9 Communication-Identifying Information (CII):** 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 TSP.

**3.1.10 Communication-Identifying Information Mediation Function (CII MF):** The CII MF maps the CII from the TSP network to the CII delivered to the LEA CF.

**3.1.11 Core Network:** Defined in [Y-101] to be "a portion of the delivery system composed of networks, system equipment, and infrastructures connecting the TSP to the access network".

**3.1.12 "d" interface:** The interface between the Access Function and the Delivery Function, and is outside the scope of this document.

**3.1.13 Delivery Function (DF):** A logical entity in the TSP network that delivers intercepted CC and CII toward one or more CF(s) for each LEA requesting an intercept.

**3.1.14 Delivery Function 2 (DF2):** Defined in [107].

**3.1.15 Delivery Function 3 (DF3):** Defined in [107].

**3.1.16 "e" interface:** The interface between a Delivery Function and a Collection Function as defined in [025-B].

**3.1.17 Electronic Surveillance:** The statutory-based legal authorization, process, and associated technical capabilities and activities of LEA(s) related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of communication-identifying information. As used in this ATIS Standard, surveillance refers to a single communication intercept, pen register, or trap and trace. Its usage in this ATIS Standard does not include administrative subpoenas for obtaining a subscriber's toll 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. For the purposes of this document, LI and LAES are synonymous with electronic surveillance.

**3.1.18 Handover Interface (HI):** As defined in [108], the physical and logical interface across which the interception measures are requested from a network operator, access provider, or service provider, and the results of interception are delivered from a network operator, access provider, or service provider to a law enforcement monitoring facility.

**3.1.19 Handover Interface 2 Intercept Related Information (HI2 IRI):** HI delivers *Intercept Related Information (IRI)*.

**3.1.20 Handover Interface 3 Communication Content (HI 3 CC):** HI delivers *Communication Content*.

**3.1.21 Intercept Access Point (IAP):** A point within a communication system where some of the communications or communication-identifying information of an intercept subject's equipment, facilities, and services are accessed.

**3.1.22 Intercept Related Information (IRI):** See also *CII*. As defined in [108], collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (e.g., unsuccessful communication attempts), service associated information or data, and location information.

**3.1.23 Interception Subject:** As defined in [108], person(s) specified in a lawful authorization whose telecommunications are intercepted.

**3.1.24 Intercept Subject:** See *Interception Subject*.

**3.1.25 Mediation Function (MF):** A logical entity used to convert IRI and CC information as specified in 3GPP LI specifications to message format and contents as described in this ATIS Standard. The mediation function may be part of the delivery function or any other network element.

**3.1.26 Mobile Station (MS):** A wireless terminal used by subscribers to access network services over a radio interface.

**3.1.27 Pen Register:** Defined in [Title 18] section USC 3127 to be "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business".

**3.1.28 Subject:** See *Interception Subject*.

**3.1.29 Surveillance:** See *Electronic Surveillance*.

**3.1.30 Trap and Trace:** Defined in [Title 18] section USC 3127 to be "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".

**3.1.31 X2 Intercept Related Information interface (X2 IRI):** As defined in [107], this interface delivers IRI from the Access Function to the DF ( "d" interface).

**3.1.32 X3 Communication Content (X3 CC):** As defined in [107], this interface delivers CC from the Access Function to the DF ( "d" interface).

## *3.2 Abbreviations*

For the purposes of the present document, the terms and definitions given in [108] and the following terms listed below apply.

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| ANS | American National Standard |
| ANSI | American National Standards Institute |
| APDU | Application Protocol Data Unit |
| AS | Application Server |
| ASN.1 | Abstract Syntax Notation One |
| ATIS | Alliance for Telecommunications Industry Solutions |
| BGCF | Breakout Gateway Control Function |
| CC | Communication Content |
| CC MF | Communication Content Mediation Function |
| CC DF | Communication Content Delivery Function |
| CC ITF | Communication Content Intercept Triggering Function |
| CF | Collection Function |
| CII | Communication-Identifying Information |
| CII MF | Communication-Identifying Information Mediation Function |
| CMS | Call Management Server |
| CS | Circuit Switched |
| CSCF | Call Session Control Function |
| DDE | Dialed Digit Extraction |
| DF | Delivery Function |
| DF2 | Delivery Function 2 |
| DF3 | Delivery Function 3 |
| DSR | Direct Signal Reporting |
| GGSN | Gateway GPRS Serving Node |
| GMT | Greenwich Mean Time |
| GPRS | General Packet Radio Service |
| FCC | Federal Communications Commission |
| HI | Handover Interface |

| | |
|---|---|
| HI2 IRI | Handover Interface 2 Intercept Related Information |
| HI3 CC | Handover Interface 3 Communication Content |
| HPLMN | Home PLMN |
| HSS | Home Subscriber System |
| IBCF | Interconnection Border Control Function |
| IAP | Intercept Access Point |
| IETF | Internet Engineering Task Force |
| I-CSCF | Interrogating CSCF |
| IM-MGW | IMS Media Gateway |
| IMS | IP Multimedia core network Subsystem |
| IMS-AGW | IMS Access Gateway |
| IP | Internet Protocol |
| IP-CAN | IP-Connectivity Access Network |
| IRI | Intercept Related Information |
| ITU-T | International Telecommunication Union, Telecommunication Standardization Sector |
| LAES | Lawfully Authorized Electronic Surveillance |
| LAESP | LAES Protocol |
| LBO | Local Breakout |
| LEA | Law Enforcement Agency |
| LI | Lawful Intercept |
| MF | Mediation Function |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MRFC | Media Resource Function Control |
| MRFP | Media Resource Function Processor |
| MS | Mobile Station |
| OID | Object Identifier |
| P-CSCF | Proxy CSCF |
| PCRF | Policy and Charging Rules Function |
| PoC | Push to talk over Cellular |
| PDN-GW | Packet Data Network Gateway |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switching Telephone Network |
| RAS | Registration, Admission and Status |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SDES | Session Description Protocol Security Descriptions |
| SIP | Session Initiation Protocol |
| TCP | Transaction Control Protocol |
| TrGW | Transit Gateway |
| TSP | Telecommunications Service Provider |
| UDP | User Datagram Protocol |
| USC | United States Code |
| VoIP | Voice over IP |

| | |
|---|---|
| VPLMN | Visited PLMN |
| X2 IRI | X2 Intercept Related Information |
| X3 CC | X3 Communication Content |

# 4 Stage 1 Description: User Perspective

## 4.1 Introduction

This section presents the law enforcement user perspective requirements for LAES for  IMS-based VoIP and other multimedia services as defined in 3GPP telecommunications networks; communication-related events that represent or generate CII; and general capabilities needed for LAES for 3GPP VoIP and other multimedia services  based on IMS ([228], [229]).

## 4.2 Electronic Surveillance Model

LI is comprised of five major functions: access, delivery, collection, service provider administration, and law enforcement administration.  These functions are discussed without regard to their implementation. The relationships between these functions are shown in Figure 4.1.

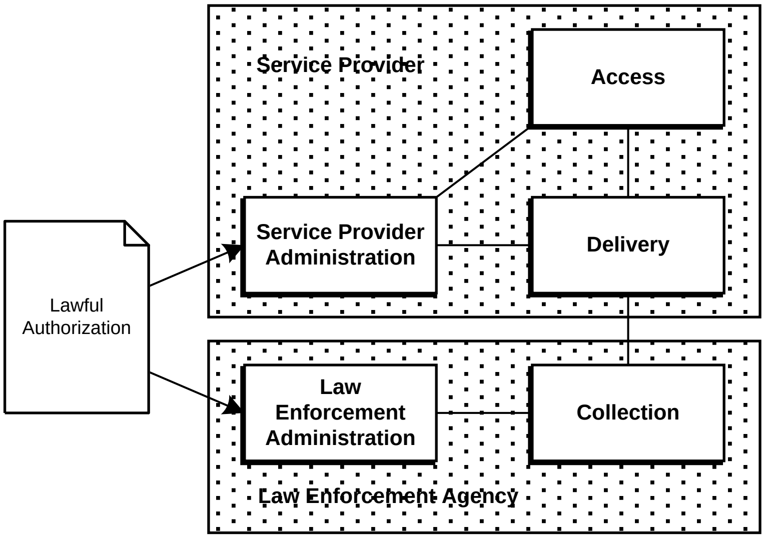


**Figure 4.1 – Electronic Surveillance Model**

- The *Access Function*, consisting of one or more IAP(s), isolates an intercept subject’s communications unobtrusively.
- The *Delivery Function*, consisting of one or more entities, is responsible for delivering intercepted communications to one or more Collection Function(s).
- The *Service Provider Administration Function* is responsible for informing the TSP Access and Delivery Functions of the intercept subject’s identity and the type of communications to be intercepted.
- The *Collection Function* is responsible for collecting and analyzing intercepted communications.  The Collection Function is the responsibility of the LEA.
- The *Law Enforcement Administration Function* is responsible for controlling and configuring the LEA CF. The Law Enforcement Administration Function is the responsibility of the LEA.

## *4.3 Requirements*

A TSP shall provide access to the VoIP CC and CII or only CII, as required by the lawful authorization, for all calls including redirected calls and, when possible, transferred calls.

It shall be possible to provide CII for all sessions regardless of media type (i.e., the media type sub-field of a media description "m=" as defined in [SDP]) such as "audio", "video", "application", "data", or "control". Note that a session description may contain a number of media descriptions. Support for CII mapped into discrete messages delivered to an LEA is based on the methodology described in [678] and expanded in this ATIS Standard.

Subject to lawful authorization, CC shall be provided for sessions with audio, video, or both media streams.

NOTE: Audio may be embedded in the video media stream.

Subject to lawful authorization, CC shall be provided for other media type values (e.g., the media type sub-field="application", "text").

In the United States, TSP(s) shall be able to perform multiple simultaneous interceptions which include:

- The ability to access and monitor all simultaneous communications originated or received by the intercept subject;
- The ability for multiple LEA(s) to simultaneously monitor the same intercept subject while maintaining transparency, including between agencies; and
- The ability of the TSP to support up to five (5) simultaneous and separate lawful interceptions on the same intercept subject.

The LAES capabilities to provide CII and CC to an LEA for Server-based Conferencing as defined in 3GPP TS 24.147 [147] shall be according to IMS Conferencing functions defined in Release 13 versions of 3GPP TS 33.107 [107] and 3GPP TS 33.108 [108]. The LAES capabilities for subject-initiated ad hoc conference calls shall be according to this Standard.

When lawfully authorized access to VoIP CC is not available for certain calls, the TSP shall provide a notification to the LEA that CC is unavailable.

## *4.4 Surveillance Events*

This section identifies communication-related events (termed surveillance events) that generate CII and CC.

### 4.4.1 CII Events

A CII event is a user action or signal that may cause a communication state change. These events are generally reflected by protocol messages that convey the state change. These events are not intended to reflect a particular technology, but to describe the event in general. The mapping is intended to report those events based upon analysis of the intercepted messages.

[678] contains the Stage 1 description for the CII events in this section.

### 4.4.2 CII Mapped Event Reporting

The following [678] mapped messages are used to report CII events:

- Answer
- Origination
- Redirection
- Release
- ServingSystem
- ConferencePartyChange
- TerminationAttempt

- Connection
- ConnectionBreak
- NetworkSignal
- SubjectSignal
- MediaAndAddressReporting
- DirectSignalReporting (DSR)

The DSR message shall only be used when a mapped message is not defined.

See Annex A of this ATIS Standard, which provides SIP to surveillance message mapping specific to this document.

For SIP message mapping of the call hold event, SubjectSignal and ConnectionBreak messages shall be sent. For SIP message mapping of the call retrieve event, SubjectSignal and Connection messages shall be sent. This applies even when a conference is placed on hold or retrieved from hold.

For SIP message mapping of the conference party add or drop event, a conference party change message shall be sent.

### 4.4.2.1 CII Dialed Digit Extraction Event Reporting

In IMS-based VoIP, when the intercept subject dials or signals digits in the VoIP content stream after the session is connected to another TSP's service for processing and routing, the TSP shall isolate and report to the LEA the dialed or signaled digits, when reasonably available, as CII to the LEA. The TSP that reports the CII dialed digit extraction information is not obligated to ensure that the connection is with another TSP's service. The TSP shall support a dialed digit extraction capability, with a toggle feature that can activate/deactivate this capability (per lawful authorization) and shall report dialed or signaled digits as CII when reasonably available and if authorized. See Annex F of [678] for additional information. The following message is used for the Dialed Digit Extraction (DDE) event reporting:

- DialedDigitExtraction

NOTE 1: The CII Dialed Digit Extraction event reporting is not required for other IMS-based multimedia services.

NOTE 2: The session that is connected to another TSP's service for processing and routing may be provided by the same TSP.

### 4.4.2.2 CII Location Reporting

When the location is available at the IAP (e.g., P-Access-Network-Info-Header in [229]) and delivery is authorized to identify the location of the intercept subject's mobile terminal, location information shall be provided for the following events:

- Answer
- Origination
- Release

Annex A illustrates the message and parameter mappings from SIP standard signaling to the surveillance messages reported to the LEA by the TSP for location information related to the intercept.

### 4.4.2.3 IMS 3GPP VoIP CII Serving System Event Reporting

The serving system identification information includes the identity of the current system assigned to provide service for the Mobile Station (MS). Information regarding the occurrence of the event (e.g., identity of the system providing the intercept access, time, date) should be included.

The IMS 3GPP VoIP ServingSystem event message shall be used to report the serving system identity currently serving the intercept subject (i.e., resulting from MS registration).

The IMS 3GPP VoIP ServingSystem event message shall also be used to report addressing and contact information registered by the intercept subject (i.e., registered via the SIP “REGISTER” method).

#### 4.4.2.4 CII Event Reporting Requirements

When an LEA is only authorized to receive CII for an intercept subject, only CII events shall be reported.

### 4.4.3 Timing Requirements

Timing information enables LEA(s) to associate CII with the content of communication. Timing information includes two elements:

1. *Event Time-stamp* – Each event report 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).
2. *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 from shall apply to the delivery of CII.

- Each CII surveillance message shall be sent toward the LEA within eight seconds of detection of a CII event to be reported at least 95% of the time.
- The CII event shall be timestamped with accuracy of at least 200 milliseconds as defined in [99-230]. The resolution of all reported timestamps shall be at least 1 ms. The timestamp 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 intercepted CC:

- Timestamps shall be provided with CC messages delivered toward the LEA with the same properties as for the CII timestamps above.
- CC shall be transmitted toward the LEA concurrently with its interception. The interval to commence transmission of CC shall be limited to the computational delay of the IAP and DF.

### 4.4.4 CC Related Events

The following [678] messages are used to report CC-related events:

- CCOpen
- CCChange
- CCClose
- CCUnavailable
- UUContent

The UUContent message shall be used to deliver the content of Short Messaging Service (SMS).

## *4.5 Performance, Reliability & Security*

The following are the performance, reliability, and security requirements:

- The service provider shall be capable of using an assured delivery mechanism (i.e., Transaction Control Protocol [TCP]) on the "e" interface.

  NOTE: The specific protocol to be used (e.g., TCP, U ser Datagram Protocol [UDP], or other protocols) is determined by negotiation between the LEA and the TSP.
- The service provider shall protect the presence of an intercept from being known to unauthorized persons and protect intercept data from being accessed by unauthorized persons. Related to this, specific requirements are:
  - Ensure that the intercept is unobtrusive and not easily detectable by the intercept subject, the associates, other parties to the communication, unauthorized employees or others acting on behalf of the carrier, and other LEAs (including other LEAs that may be receiving intercept data related to the same communication based on a different intercept order), including preventing knowledge of the fact that an intercept is being conducted, confidentially activating/deactivating the intercept or accessing captured CC CII, and preventing intercept subjects from being notified of service changes caused by an intercept;
  - Provide capabilities to protect the carrier capabilities used to facilitate intercepts and to prevent the interception of CC and CII not authorized for collection by LE; and
  - Securely deliver intercepted CC and CII from the carrier's DF to LE by implementing security measures on the delivery interface, including but not limited to authentication, confidentiality, message integrity (e.g., via hashing), and non-repudiation.

## 4.6 Decryption Requirements

The TSP shall:

1. Transmit communication content toward the LEA collection system in decrypted form, or
2. Provide the LEA collection system the information necessary to decrypt the communication content.

LEAs in general prefer option 1, especially if proprietary or specialized means of achieving this function is used.

# 5 Stage 2 Description: Network Perspective

## 5.1 Introduction

This section identifies and describes the following:

- The triggering events and usage for the IMS 3GPP VoIP CII event messages;
- The information to be reported with each IMS 3GPP VoIP CII event message; and
- The application level CC delivery format and associated delivery information.

Note that for the purpose of this ATIS Standard, the term *IMS 3GPP VoIP CII* pertains not only to the VoIP service but also to the other IMS-based multimedia services.

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

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

The information to be carried by each parameter is identified. Please note that both optional and conditional parameters at Stage 2 are considered to be OPTIONAL syntactically in Abstract Syntax Notation One (ASN.1) Stage 3 descriptions.

## *5.2 Architecture*

### 5.2.1 Functional LI Architecture

Figure 5.1 shows a general functional LI architecture where both CC and CII are intercepted and delivered to LEA(s). This functional architecture assumes that one TSP is providing both CC and packet transport.  The DF can be separated into CII delivery and CC delivery or can be combined into CII and CC delivery.  There may be one or more IAP(s) in the network for both CII and CC.

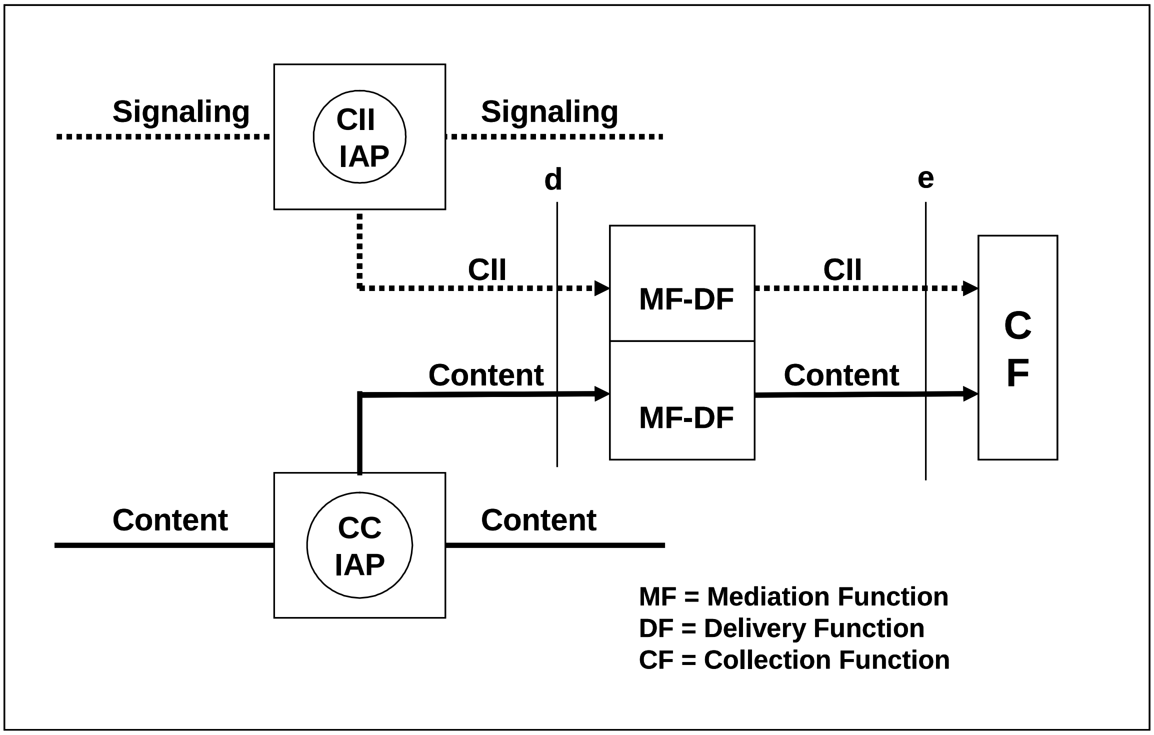


**Figure 5.1 – Functional LI Architecture**

The “e” interface is the only interface addressed in this ATIS Standard. The “d” interface is out of scope of this ATIS Standard.   It is assumed that the LEA collection equipment maintains current state information concerning the associations between communication entities [i.e., intercept subject and associate(s)]. The collection equipment assumes that the last reported association remains in effect until a subsequent message explicitly changes that association.

### 5.2.2 Intercept Access Points

There are two fundamental types of IAP(s):

- Communication-Identifying Information IAP (CII-IAP).
- Communication Content IAP (CC-IAP).

The CII-IAP is associated with CII intercept functions that perform the actual interception of CII, and the CC-IAP is associated with CC intercept functions that perform the actual interception of CC.  The CII-IAP may be distributed to enable the interception and reporting of CII from different network elements. The CC-IAP may be distributed to enable the interception and reporting of the CC from different network elements. The network element that performs the CC interception may depend on the network configuration and the call scenario. Placement of IAP(s) is network-specific and may vary between networks.  However, it is not required to report redundant CII from different network elements. For example, if a P-CSCF exists in a home network, it may not be necessary to have

CII-IAP(s) at both a P-CSCF and S-CSCF because all necessary CII may be intercepted and reported at the S-CSCF.

For VoIP and other multimedia services, the CII-IAP provides expeditious access to the reasonably available CII for communications made by an intercept subject or for communications made to an intercept subject or for communications made on behalf of the intercept subject. The CII-IAP shall access the CII for the intercept subject unobtrusively. Access to CII shall not deny the availability of any service to either the intercept subject or associates. CII intercept functions may be collocated within the same network element or may be distributed among multiple network elements. The placement of CII-IAP(s) is dependent on the TSP implementation.

For VoIP and other multimedia services, the CC-IAP(s) intercepts CC between an intercept subject and the associate(s). When legally authorized, the TSP shall access and deliver CC, if reasonably available, for the duration of communications originated by and terminated to the intercept subject's equipment, facilities, or service. CC intercept functions may be collocated within the same network element or may be distributed among multiple network elements. The placement of CC-IAP(s) is dependent on the TSP implementation.

The interception of CII and CC is required for all calls including forwarded calls and, when possible, transferred calls. This may require the TSP to support the capability to activate the CC IAP dynamically during a call.

The CC shall be correlated with the CII; this may require the TSP to support a capability for a SIP signaling element to send signaling information to a CC Intercept Triggering Function (CC ITF). The CC ITF activates the CC interception at the CC IAP. The placement of the CC ITF is dependent on the TSP implementation, the call scenario and the placement of the CC IAP. A SIP signaling node can contain the CC ITF.

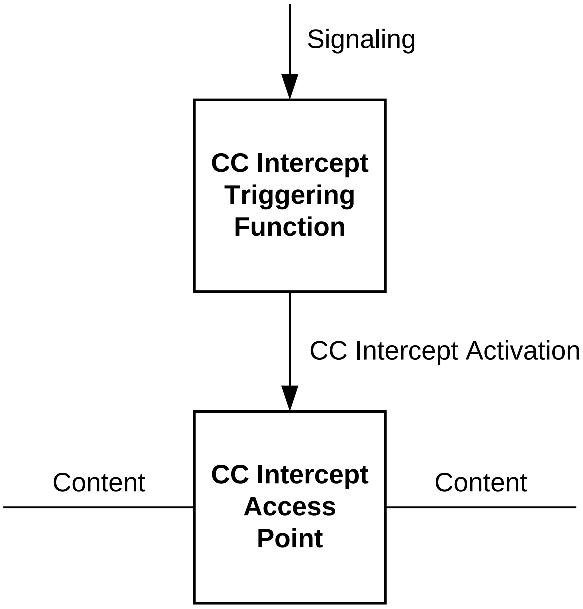


**Figure 5.2 – CC Interception Configuration for VoIP and other Multimedia Services**

The details of CC intercept activation are outside the scope of this Standard, however, the intercept activation shall include:

- Correlation Identifier
- Media Identifier

The Correlation Identifier is used to provide a correlation between the CC and the CII. The Media Identifier is used to identify the actual media that has to be intercepted.

The TSP shall have the capability to notify the LEA about the availability of CC; start of CC interception, end of CC interception, and unavailability of CC within the TSP's network.

### 5.2.3 Media Information Associated with the Intercepted CC

In an IMS-based VoIP call, the S-CSCF (P-CSCF in the visited network) provides the CII IAP functions.  The P-CSCF may optionally provide the CII IAP functions in the home network. The CC IAP functions are provided by various nodes depending on the call scenario. The media information associated with the CC is taken from the SDP offer and SDP answer present in the SIP messages, and are reported to the LEAs in the CII messages.  The LEAs may use that media information to process the received CC.

In some situations, the media information known to the CII IAP can be different from the media information associated with the CC delivered to the LEA.  For example, when transcoding is involved in the media path, the media information (e.g., codec used) can change at the time transcoding is done and the S-CSCF that normally provides the media information (in the CII) to the Mediation Function/Delivery Function may not have the knowledge of media information associated with the CC delivered to the LEA. In such situations, the CC ITF (which is aware of the media information associated with the intercepted CC) shall send the media information to the Mediation Function/Delivery Function.

When media information is received from the CC ITF, the Mediation Function/Delivery Function shall always use that information for reporting purposes over the "e" interface (e.g., in the CCOpen message).

A general concept of this is illustrated in Figure 5.3 below:

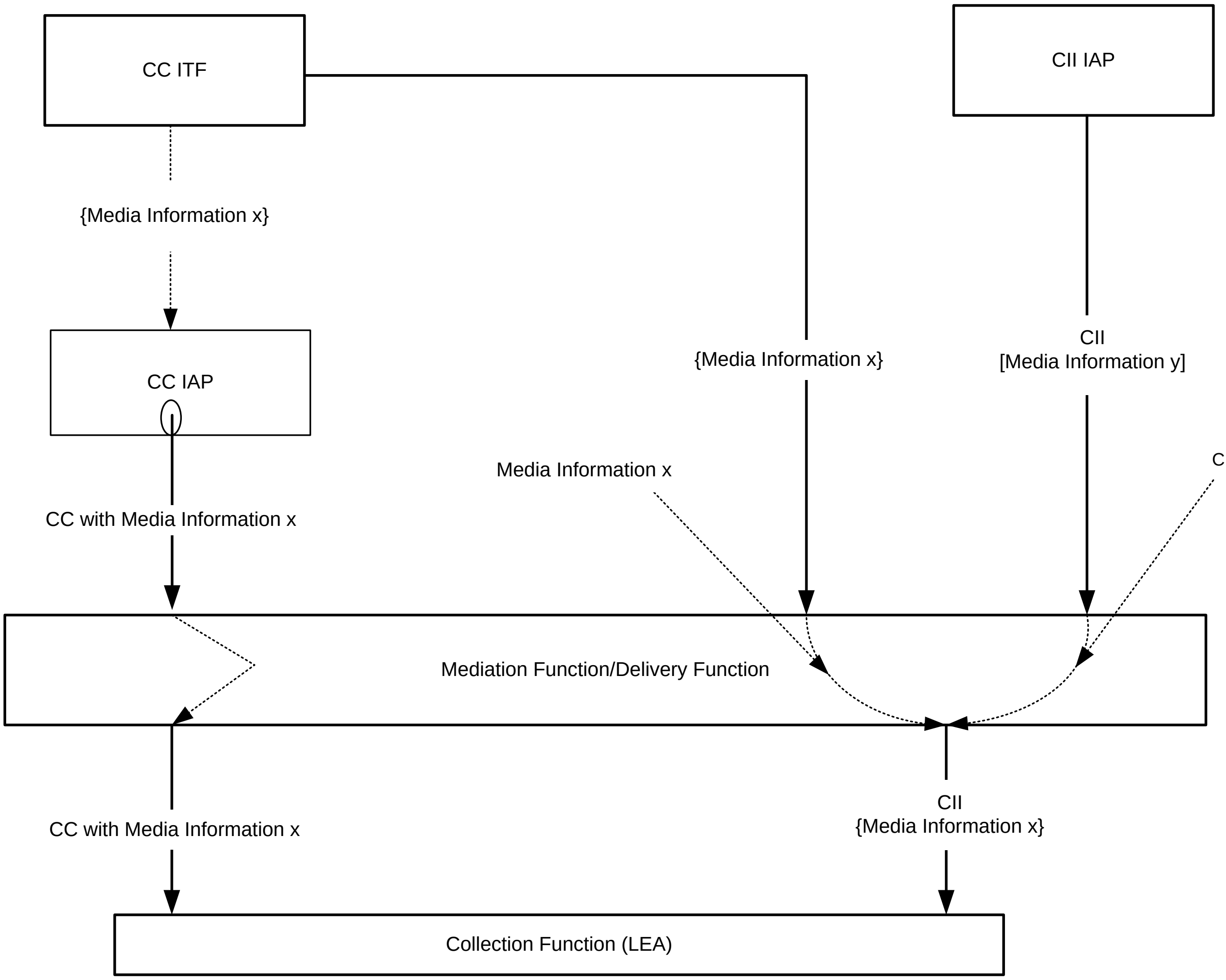


**Figure 5.3 – Media Information for an intercepted CC**

Figure 5.3 illustrates that the Media Information x is associated with the intercepted CC and the media information known to the CII-IAP is Media Information y. In this case, the CC ITF delivers the Media Information x to the Mediation Function/Delivery Function, which in turn uses that media information for reporting purposes (e.g., in the CCOpen message).

As an implementation option, CC ITF, which is aware of the details of the CC interception, can always send the media information to the Mediation Function/Delivery Function, and in that case, the Mediation Function/Delivery Function shall always use that media information for reporting purposes.

In case the media information associated with the intercepted CC is different from the media information associated with the CC delivered to the LEA over the “e” interface, the media information associated with the CC delivered to the LEA shall also be reported to the LEA.

Along with the media information, the SDP may also carry the Session Description Protocol Security Descriptions (SDES) crypto attribute (aka SDES Keys) when the SDES-based encryption is used. When received, the Mediation Function/Delivery Function shall use the SDES keys received from the CC ITF for its handling (i.e., either to perform the CC decryption or for reporting purposes over the “e” interface when the CC is delivered in an encrypted form). If the CC interception itself is done in a decrypted form, then the CC ITF shall not send the SDES Keys to the Mediation Function/Delivery Function.

### 5.2.4 CC Interception in Home Network with IMS Roaming

For roaming Intercept Subjects who are physically not in the legal jurisdiction of the home network, depending on the roaming architecture deployed, media of the Intercept Subject may not enter the home network for certain call scenarios when optimal media routing is employed. In such situations, the home network served with lawfully authorized interception request shall do the following:

- Perform the interception without the CC and report CII messages to the LEA(s).
- If the lawful authorization requires the CC interception, since the media is not available, report to the LEA (s) that CC is unavailable due to roaming situation using the CCUnavailable message.

Note that when the Intercept Subject is roaming in another network, the home network sends a ServingSystem message to the LEA (s) indicating that the Intercept Subject is currently in another network.

## *5.3 LAES CII Messages*

### 5.3.1 IMS 3GPP VoIP CII Event Reporting

The following LAES messages are utilized for IMS 3GPP VoIP CII reporting:

- Answer
- CCChange
- CCClose
- CCOpen
- CCUnavailable
- ConferencePartyChange
- Connection
- ConnectionBreak
- DialedDigitExtraction (DDE)
- DirectSignalReporting
- MediaAndAddressReporting
- NetworkSignal
- Origination
- Redirection
- Release
- ServingSystem
- SubjectSignal
- TerminationAttempt message

Of the messages listed above, the following messages are defined in this Standard:

- Answer
- Origination
- Release
- TerminationAttempt

All other messages are defined in [678]. The events that trigger those messages are also defined in [678].

When the sending of an LAES message is triggered by one or more SIP messages, the EncapsulatedSignalingMessage field contains those SIP messages with the following rules:

a. Location-information headers and message bodies recognized by the IAP (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;

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

### 5.3.2 Answer Message

The events that trigger the reporting of Answer message are defined in [678]. The following parameters shall apply to the Answer message:

**Table 5.1 – 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 IMS network. |
| AnsweringMediaInformation | C | Include when answering party's media information is known. This identifies the SDP information for the answering party. |
| EncapsulatedSignalingMessage | C | The SIP message that triggered the sending of the Answer message. |

### 5.3.3 Origination Message

The events that trigger the reporting of Origination message are defined in [678]. The following parameters shall apply to the Origination message:

**Table 5.2 – 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. |
| 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. |
| Input | M | Identifies specific user or translation input including when a call or session is attempted without input (e.g., hot line). |

| Parameter | MOC | Usage |
|---|---|---|
| One of the following:<br>UserInput<br>TranslationInput | | Included to identify the input digits, address or name signaled by the calling party to originate the call, when known. Examples include:<br>generic: “hot line,” “123”<br>specific: “sip:UserA@here.com”<br>Included to identify the input to an address translation process, when an address translation occurs. Examples include:<br>generic: “hot line,” “123”<br>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 IMS 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 triggered the sending of the Origination message. |
| ForkedCalls | O | Provide the call IDs and destinations for forked calls (e.g., forked INVITE). |

### 5.3.4 Release Message

The events that trigger the reporting of Release message are defined in [678]. The following parameters shall apply to the Release message:

**Table 5.3 – 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. The call identity is released. |
| 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 IMS network. |
| Cause | C | Included to identify the signaling type in which the release event occurred (e.g., Registration, Admission and Status [RAS] signaling) 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). |
| EncapsulatedSignalingMessage | C | The SIP message triggered the sending of the Release message. |

### 5.3.5 ServingSystem Event Reporting

#### 5.3.5.1 ServingSystem Event Reporting for SIP Registration

For SIP registration reporting, the ServingSystem message as defined in [678] is used.

#### 5.3.5.2 ServingSystem Event Reporting for Terminal Registration

As defined in this ATIS Standard, the ServingSystem Event is also used to report terminal registration. The ServingSystem message shall be triggered when the intercept subject's MS is authorized for service with another TSP or in another service area. The event may be optionally reported when the intercept subject registers in the home network.

For terminal registration, the parameters shown in Table 5.4 shall apply:

**Table 5.4 – ServingSystem Message Parameters for Terminal Registration**

| Parameter | MOC | Usage |
|---|---|---|
| CaseIdentity | M | Identifies the Intercept Subject. |
| IAPSystemIdentity | C | Include to idenity 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 | Include, when authorizing service to a TSP, to identify the TSP. |

ServingSystem message is also used when the S-CSCF receives the SIP REGISTER message. In that case, the SystemIdentity will carry the visited network identity if received in the SIP REGISTER message.

### 5.3.6 Termination Attempt

The events that trigger the reporting of TerminationAttempt message are defined in [678]. The following parameters shall apply to the TerminationAttempt message:

**Table 5.5 – 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. |

| Parameter | MOC | Usage |
|---|---|---|
| CalledPartyIdentity | C | Included when more specific than the intercept subject identity associated with the CaseIdentity to identify the called party. |
| 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 contains redirection information and is delivered in the order presented in the SIP message. |
| EncapsulatedSignalingMessage | C | The SIP message that stimulated the sending of the TerminationAttempt message. |

# 6 Stage 3 Description: Implementation Perspective

## *6.1 Abstract Syntax Notation*

The stage 3 descriptions for the mapped messages are defined in the form of Abstract Syntax Notations (ASN) in Annex B of this ATIS Standard.

## *6.2 CC Delivery*

### 6.2.1 CC Delivery Protocols

Various delivery protocols (e.g., TCP/IP, UDP/IP) can be used to support delivery of VoIP CC over the "e" interface between a TSP and an LEA.

### 6.2.2 CC Delivery Format

Delivery of CC for IMS VoIP and other multimedia services is based on the CC delivery method in [678]. See the IMS-VoIP-CC-Module in Annex B of this ATIS Standard for the content delivery format.

When CC is intercepted, a LAES CCOpen message is sent to the LEA(s) indicating CC will be delivered. As part of that CCOpen message, the format of the CC Headers encapsulating the intercepted CC is identified. See the "ContentDeliveryFormat" parameter description in [678].

### 6.2.3 CC Delivery Format Identifier

With respect to the CC delivery format, the CC module object identifier (OID) containing the definition (i.e., the defined format) for the CC Header is sent in the "ContentDeliveryFormat" parameter to the LEA(s) to identify the specific CC header format being used. The specific ASN.1 field containing the OID is the "cc-APDU" field in "ContentDeliveryFormat" (see [678]).

For IMS VoIP CC delivery, the OID for the IMS CC module (IMS-VoIP-CC-Module) is used and sent in the "cc-APDU" field of the LAES CCOpen message (see the IMS-VoIP-CII-Module ASN.1 in Annex B of this ATIS Standard).

## *6.3 CC IAP*

For IMS-based VoIP and other multimedia sessions, the network nodes that provide the CC IAP depend on the TSP network configuration and the call scenario. The CC ITF dynamically activates the CC interception at the CC IAP as described in clause 5.2.2.

When the Intercept Subject originates a call or receives a terminating call within the TSP's network, or when an Intercept Subject's incoming call is redirected within the TSP's network, the CC IAP shall be within the IP Connectivity Access Network (IP-CAN) or at another network node that has access to the CC.  For a basic VoIP call, the IAP may be at an IMS Access Gateway (IMS-AGW) (if the TSP's network includes an IMS-AGW).

When the CC is redirected away from the IP-CAN (or IMS-GW) to another network, the CC IAP shall be at the Transit Gateway (TrGW) (e.g., VoIP call redirected to another IMS network) or at the IM-MGW (i.e., call redirected to the PSTN) or at another network node that has access to the CC.

The TrGW also provides the CC IAP function when the IP-CAN (or the IMS-AGW) is in another IMS network due to IMS roaming of the intended party involved in the call.

When an Intercept Subject initiates an ad-hoc conference call, CC interception may also be provided by the Media Resource Function Processor (MRFP). To distinguish the CC intercepted at the MRFP and the CC intercepted at the other CC ITF (e.g., IP-CAN or the IMS-AGW), a separate Call Identity shall be used for the two CC. Accordingly, the CCOpen and CCClose message shall use the Call Identity value that corresponds to the associated CC.

**Annex A**

(Informative)

# A Mapping of SIP CII Messages

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

This annex provides the message and parameter mappings from SIP standard signaling to the surveillance messages reported to the LEA by the TSP for an IMS 3GPP VoIP intercept that are not defined in [678].

The tables in [678] Annex B even though informative illustrate the SIP standard signaling to surveillance messages for those [678] messages used in this document. The term "CMS" as used in [678] Annex B is replaced by the term "CSCF".

This annex provides additions or enhancements to the mapping tables illustrated in [678] Annex B to support IMS 3GPP VoIP.

The message and parameter mappings from SIP standard signaling to the surveillance messages reported to the LEA by the TSP for location information related to the intercept are provided below. Location Information related to the call may be available in one or more forms:

- SIP P-Access-Network-Info Header
- SIP Geolocation header of a SIP message*

* NOTE: Geolocation header of a SIP message is applicable in 3GPP Release 7 and beyond of [229].

Annex B of [678] can still be used to understand the mapping of SIP messages to Origination (from SIP INVITE), Answer (from SIP 200 OK) and Release (from SIP BYE) with the exception of Location parameter. For the SIP header to Location parameter mapping refer to the clauses A.1 and A.2 below.

Note that, depending on the circumstance, a Release message may be triggered for reasons other than the SIP BYE message.

## *A.1 SIP P-Access-Network-Info Header*

Table A.1 describes the Mapping of SIP P-Access Location Information to LAES Messages. When this mapping is used the LocationType sub-parameter is coded as "P-A-N-I-Header".

**Table A.1 – Mapping of SIP P-Access Location Information to LAES Messages**

| SIP<br>Message Header | LAES<br>Message Parameter | Description |
|---|---|---|
| 200-OK(INVITE)<br>P-Access-Network-Info | Answer<br>location | Provides location information when available. |
| INVITE<br>P-Access-Network-Info | Origination<br>location | Provides location information when available. |
| BYE<br>P-Access-Network-Info | Release<br>location | Provides location information when available. |

NOTE: Intercept subject's location information is mapped. In the event, the BYE is sent from the network to the intercept subject, the P-Access-Network-Info (if received) in the 200 OK (BYE) is not reported. Further, the P-Access-Network-Info that might have been received in other SIP messages is not reported.

## A.2 SIP Geolocation Header of a SIP Message

Table A.2 shows the Mapping of SIP GeoLocation Information to LAES Messages. When delivering the location information contained in a Geolocation header of a SIP message, the LocationType sub-parameter is coded as “Geoloc-Header”.

**Table A.2 – Mapping of SIP GeoLocation Information to LAES Messages**

| SIP<br>Message Header | LAES<br>Message Parameter | Description |
|---|---|---|
| 200-OK(INVITE)<br>Geolocation | Answer<br>location | Provides location information when available. |
| INVITE<br>Geolocation | Origination<br>location | Provides location information when available. |
| BYE<br>Geolocation | Release<br>location | Provides location information when available. |

## A.3 Multiple Location Information Types

If multiple location information types are available, then all are reported (e.g., P-Access-Network-Info header and SIP GeoLocation Information header).

## A.4 Mapping of P-Visited-Network to a Serving System

For IMS roaming scenarios, the visited IMS network information may be included within P-Visited-Network-Id header of the SIP REGISTER message. The following table shows how the P-Visited-Network-Id is mapped and reported to the LEA within the ServingSystem message.

**Table A.3 – Mapping of SIP REGISTER P-Visited-Network-Id**

| SIP<br>Message Header | LAES<br>Message Parameter | Description |
|---|---|---|
| REGISTER<br>P-Visited-Network-Id | ServingSystem<br>SystemIdentity | Provides visited network identity when available. |

**Annex B**

(Normative)

# B IMS-3GPP VoIP Abstract Syntax Notation

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

The following object tree and ASN.1 definitions apply to IMS-based VoIP and other multimedia services.

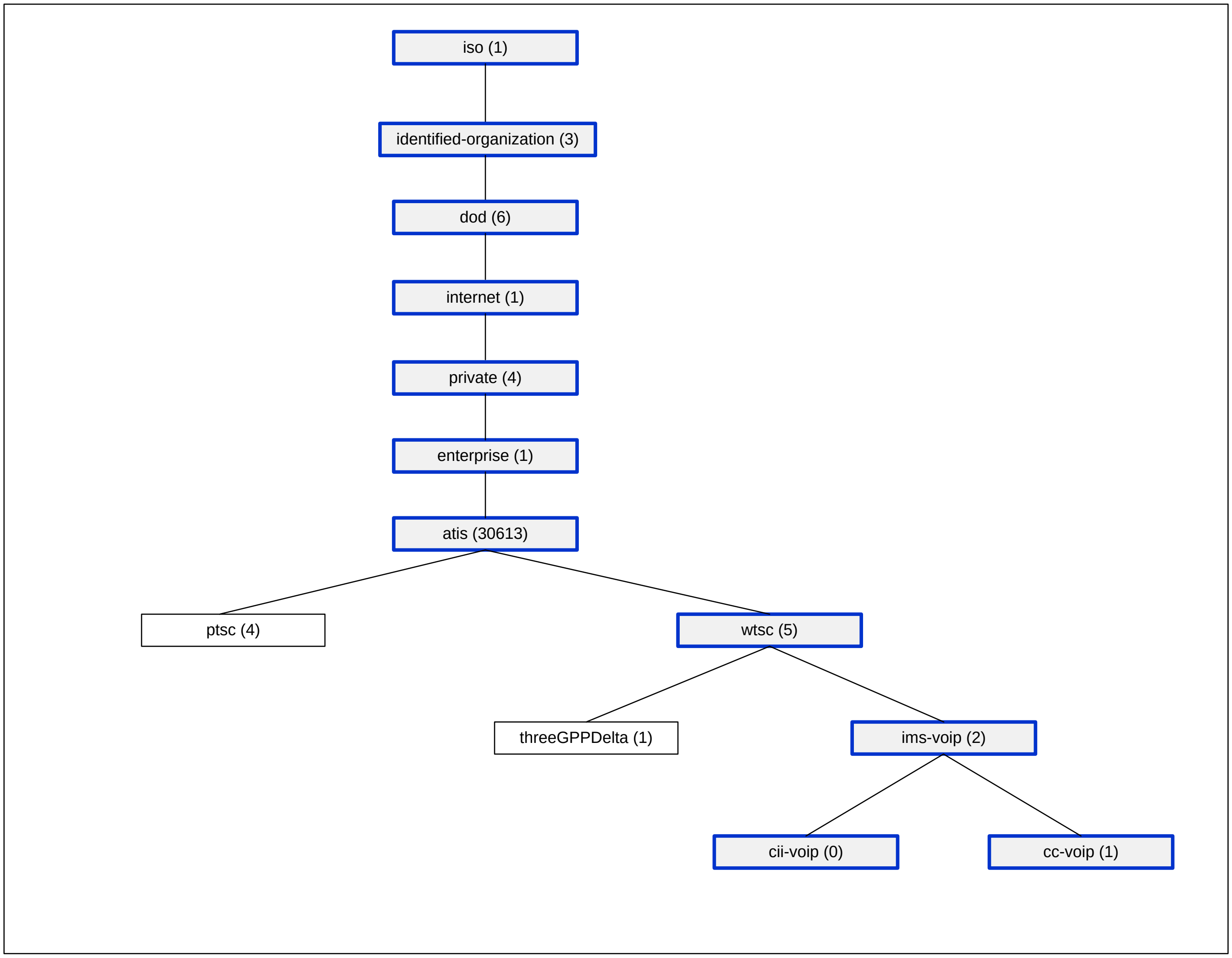


**Figure B.1 – IMS 3GPP VoIP Object Tree**

NOTE: IMS-3GPP-VoIP-CII-Module and IMS-3GPP-VoIP-CC-Module in Annex B of this ATIS Standard has also been formatted as a separate plain text file and electronically packaged with this document.

```
-- IMS 3GPP VoIP CII Delivery Module

IMS-3GPP-VoIP-CII-Module
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atis(30613)
wtsc(5) ims-voip(2) cii-voip(0) version-3(0)}
```

```
DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

-- Imports from ATIS-1000678.v3.2015 Module

CCClose,
CCOpen,

Redirection,

ConferencePartyChange,
Connection,
ConnectionBreak,
DialedDigitExtraction,
ForkedCallInformation,
NetworkSignal,
SubjectSignal,
DirectSignalReporting,
MediaAndAddressReporting,
CCChange,
CCUnavailable,
UUContent,
TransitCarrierIdentity,
CaseIdentity, Cause, CallIdentity, EncapsulatedSignalingMessage, IAPSystemIdentity, SDP,
PartyIdentity, TimeStamp

FROM ATIS-LAES-VoP-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)};



ims-3GPP-VoIP-CII-Module-OID  OBJECT IDENTIFIER ::=
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atis(30613)
wtsc(5) ims-voip(2) cii-voip(0) version-3(0)}

LAESProtocol ::= SEQUENCE {
     ims-3GPP-VoIP-CII-Module-OID [0]    OBJECT IDENTIFIER,
     laesMessage                  [1] IMS-3GPP-VoIP-CII-Message
}


IMS-3GPP-VoIP-CII-Message ::= CHOICE {
     ims-3GPP-VoIP-answer        [1] Answer,
     ims-3GPP-VoIP-ccClose       [2] CCClose,
     ims-3GPP-VoIP-ccOpen        [3] CCOpen,
     null-4                      [4] NULL,
     ims-3GPP-VoIP-origination   [5] Origination,
     null-6                      [6] NULL,
       -- [6] reserved by [025B] for Packet Envelope
     ims-3GPP-VoIP-redirection   [7] Redirection,
     ims-3GPP-VoIP-release       [8] Release,
     ims-3GPP-VoIP-servingSystem [9] ServingSystem,
     ims-3GPP-VoIP-termAttempt   [10] TerminationAttempt,
     null-11                     [11] NULL,
       -- [11] reserved by [025B] for Connection Test
     ims-3GPP-VoIP-conferencePartyChange      [12] ConferencePartyChange,
     ims-3GPP-VoIP-connection    [13] Connection,
     ims-3gpp-VoIP-connectionBreak      [14] ConnectionBreak,
     ims-3GPP-VoIP-dialedDigitExtraction      [15] DialedDigitExtraction,
     ims-3GPP-VoIP-networkSignal [16] NetworkSignal,
     ims-3GPP-VoIP-subjectSignal [17] SubjectSignal,
     ims-3GPP-VoIP-directSignalReporting      [18] DirectSignalReporting,
     ims-3GPP-VoIP-mediaAndAddressReporting   [19] MediaAndAddressReporting,
     ims-3GPP-VoIP-ccChange       [20] CCChange,
     ims-3GPP-VoIP-ccUnavailable  [21] CCUnavailable,
     null-22                      [22] NULL,
       -- [22] reserved  by [678] for Surveillance Status
     null-23                      [23] NULL,
       -- [23] reserved by [678] for Feature Management
     ims-3GPP-VOIP-uuContent      [24] UUContent

}

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
}

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
}

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,
     signalingMsg                 [7] SET OF EncapsulatedSignalingMessage        OPTIONAL
}

ServingSystem ::= SEQUENCE {
       caseId                     [0]   CaseIdentity,
       iAPSystemId                [1]   IAPSystemIdentity            OPTIONAL,
       timestamp                  [2]   TimeStamp,
       sysId                      [3]   SystemIdentity               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
}

Location ::= SET OF LocationInfo

LocationInfo ::= SEQUENCE
{
        locationType       [0] UTF8String,
        locationData       [1] UTF8String
}
RedirectedFromInformation ::= SEQUENCE OF PartyIdentity

SystemIdentity ::= CHOICE {

packetDataSystemID         [0]    PacketDataSystemID,

evolvedPacketSystemID      [1]    EvolvedPacketSystemID,

visitedNetworkId           [2]    VisitedNetworkID

}


PacketDataSystemID ::= SEQUENCE {

servingSGSN-number         [0]    OCTET STRING (SIZE (1..20)) OPTIONAL,

servingSGSN-address               [1]    OCTET STRING (SIZE (5..17)) OPTIONAL,

-- Octets are coded according to [3GPP-23.003]

servingS4-SGSN-address            [2]    OCTET STRING OPTIONAL

-- Diameter Origin-Host and Origin-Realm of the S4-SGSN based on the [3GPP-29.272].

-- Only the data fields from the Diameter AVPs are provided concatenated with a

-- semicolon to populate this field.

}


EvolvedPacketSystemID ::= SEQUENCE {

servingMMEaddress          [0]    OCTET STRING OPTIONAL,

-- Contains the data fields from the Diameter Origin-Host and Origin-Realm AVPs

-- as received in the HSS from the MME according to the [3GPP 29.272].

-- Only the data fields from the Diameter AVPs are provided concatenated

-- with a semicolon to populate this field.

visitedNetworkId                  [1]    VisitedNetworkID OPTIONAL

-- contains the visited network identifier inside the EPS Serving System

-- Update for non 3GPP access, coded according to [3GPP 29.273].

}

VisitedNetworkID ::= UTF8String

END -- of IMS-3GPP-VoIP-CII-Module
```

```
-- IMS 3GPP VoIP Communication Content Delivery Module

IMS-3GPP-VoIP-CC-Module
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atis(30613)
wtsc(5) ims-voip(2) cc-voip(1) version-3(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

-- Imports from ATIS-1000678.v3.2015 Module

CC-APDU

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


-- Notations for IMS-3GPP-VoIP-CC-Module

ims-3GPP-VoIP-CC-Module-OID   OBJECT IDENTIFIER ::=
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) atis(30613)
wtsc(5) ims-voip(2) cc-voip(1) version-3(0)}

IMS-3GPP-VoIP-CCProtocol ::= SEQUENCE {
ims-3GPP-VoIP-CC-Module-OID      [0]    OBJECT IDENTIFIER,
ims-3GPP-VoIP-CC-APDU            [1]    CC-APDU
}

END  -- of IMS-3GPP-VoIP-CC-Module
```

**Annex C**

(Informative)

# C Call Flows for Mapping from SIP to LAES Messages

See [678] for example SIP information flows with event mapping. The call flows that are only applicable to the LAES capabilities specified in this ATIS Standard are illustrated in this annex.

## *C.1 Video Session Downgraded to Audio Session*

This call flow is an example where an intercept subject (shown as A) invites a SIP user B for a video session. The User B's device does not seem to have the capabilities for the video session (or the user may not be interested in the video session). The intercept subject downgrades the session to an audio session. The session continues as an audio session.

Only one CSCF is shown in the flow. The CSCF sends all the SIP messages to the MF/DF. The MF/DF maps certain SIP messages to the [678] messages and delivers the same to the LEA(s). The CC Delivery or the related messages (CCOpen) are not shown.

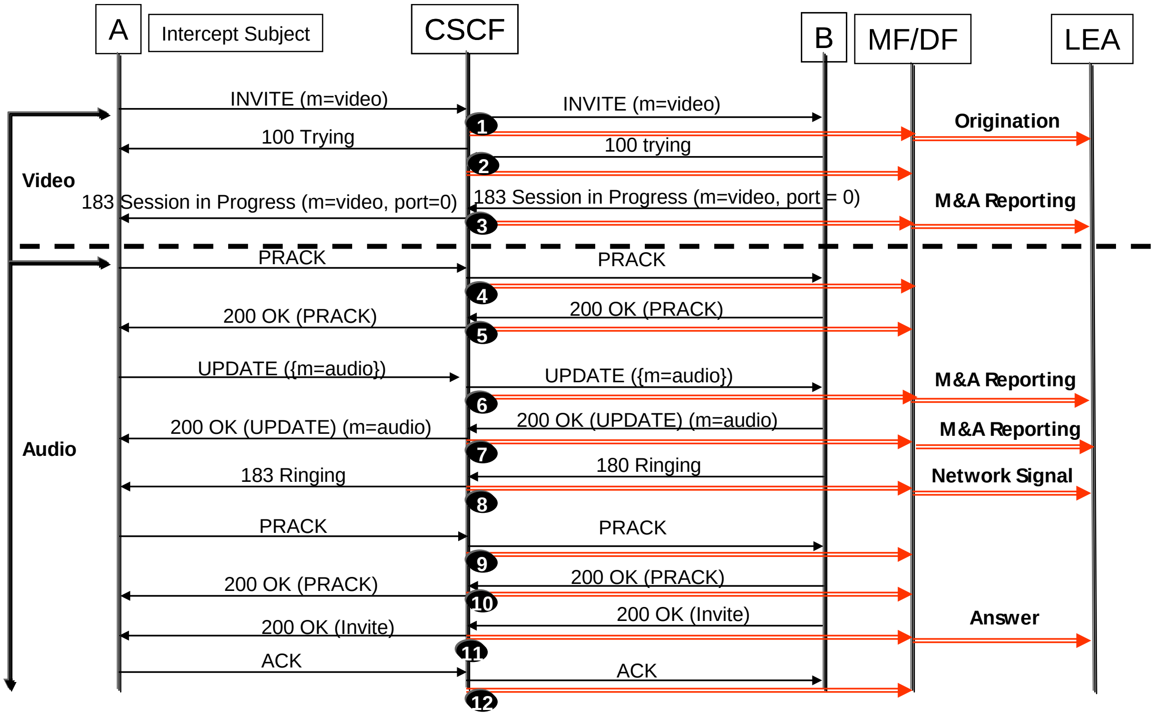


**Figure C.1 – Call Flow Example: Video Session downgraded mid-stream to Audio Session**

***CII IAP Steps***

1. INVITE (m=video) is mapped to an Origination message. The SIP message contains an SDP offer.
2. 100 Trying is not mapped.
3. 183 Session In Progress is mapped to a MediaAndAddressReporting (M&A Reporting) message. The port=0 indicates the User B is not supporting video services (or the user is not interested in the video service). The SIP message contains an SDP answer.
4. PRACK does not have the conditions for the mapping and hence is not mapped.
5. 200 OK (PRACK) is not mapped.

6. UPDATE is mapped to MediaAndAddressReporting (M&A Reporting). The session is downgraded from a video session to an audio session. The SIP message contains an SDP offer.
7. 200 OK (UPDATE) is mapped to MediaAndAddressReporting (M&A Reporting). The SIP message contains an SDP answer.
8. 180 Ringing is mapped to NetworkSignal.
9. PRACK does not have the conditions for the mapping and hence is not mapped.
10. 200 OK (PRACK) is not mapped.
11. 200 OK (INVITE) is mapped to an Answer message.
12. ACK is not mapped.

**Annex D**

(Informative)

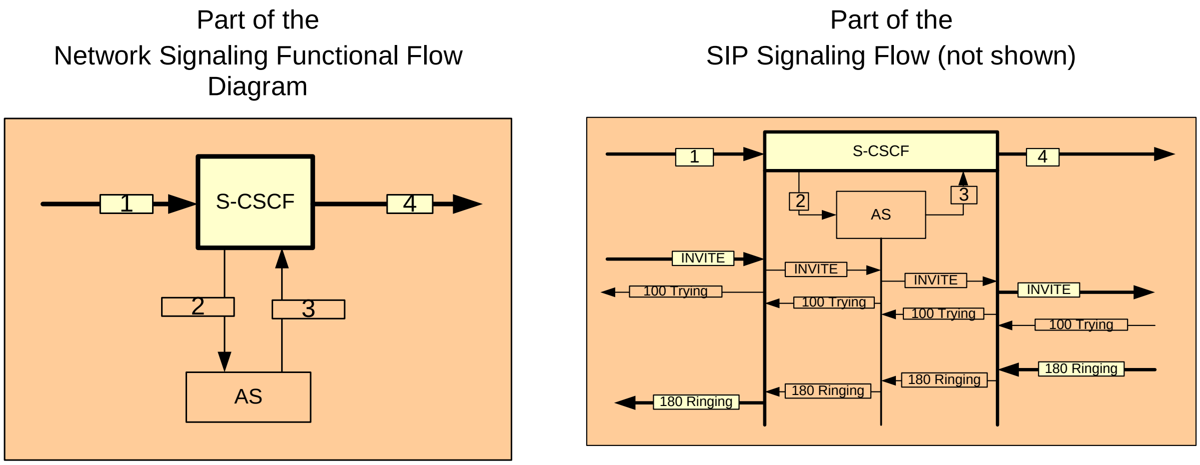
# D Network Signaling Functional Flow Diagrams

This annex contains a series of network signaling functional flow diagrams that identify the different network entities involved along the SIP signaling path for various scenarios of an IMS-based VoIP session establishments. The examples illustrated here focus on the CII message delivery.

In principle, an IMS-based VoIP SIP session establishment is independent of the IP connectivity access network. Therefore, within the flow diagrams, the method used by the MS to access the IMS network is not shown.

In all the diagrams, the interface to the LEA (shown as CF, CF-1, or CF-2) is provided by a Mediation Function/Delivery Function and shown as MF/DF and the actual interface is identified as “e” interface.

*Notes applicable to the entire Network Signaling Functional Flow Diagrams*: The diagrams are drawn to illustrate signaling path of a call flow. The arrow indicates how the call progresses along the network. The SIP messages that are exchanged between the two network elements are always bi-directional. For example, in the following figure, the arrow 1 indicates that an incoming call arrives at the S-CSCF on the Interface 1. The arrow 2 indicates that S-CSCF routes the call to the Application Server (AS) on the Interface 2. The arrow 3 indicates that the AS routes the call back to the S-CSCF on the Interface 3. The arrow 4 indicates that an outgoing call leaves the S-CSCF on the Interface 4. The SIP signaling messages that are exchanged on the Interfaces 1, 2, 3, and 4 are always bi-directional (as defined in [229]).


Part of the Network Signaling Functional Flow Diagram

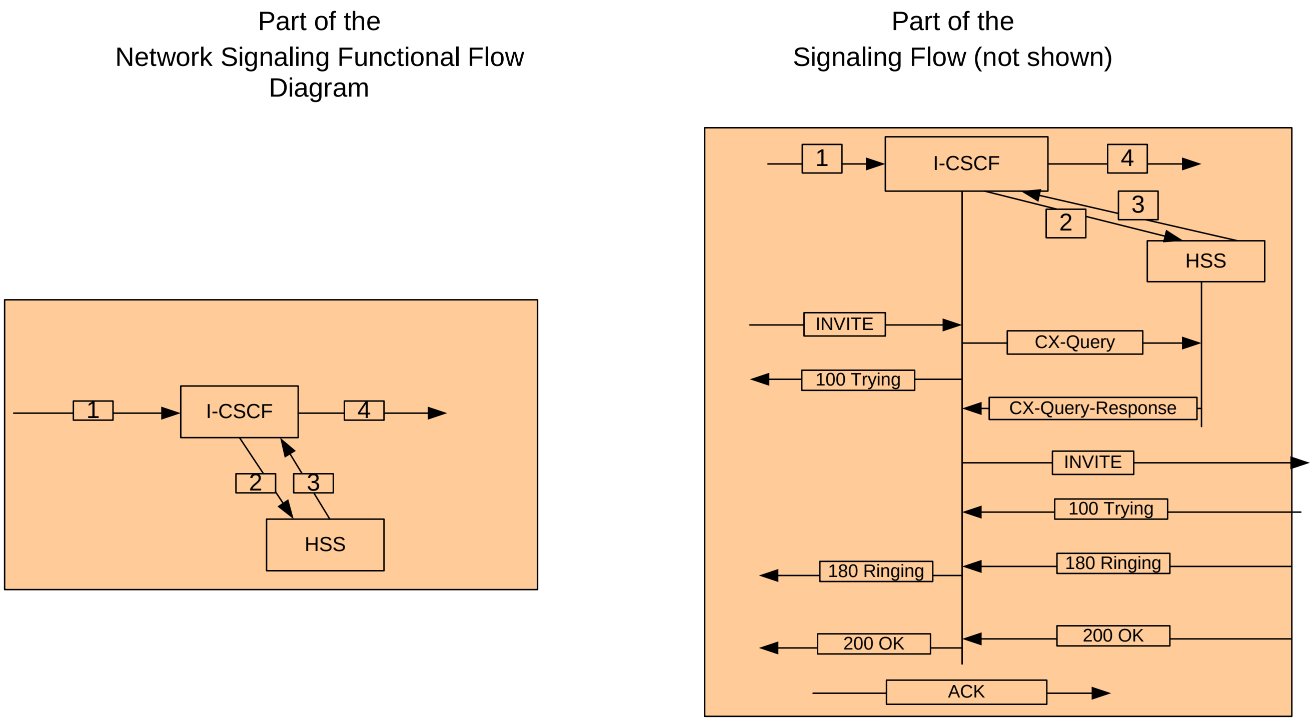
Part of the SIP Signaling Flow (not shown)

**Figure D.1 – Functional Flow Diagram and Sample Signaling Flow – Illustration 1**

The presence of an AS within the IMS domain is an option and hence, the AS may or may not be involved along the signaling path.

The network node that provides the IAP for the CII is shown with a different colored box with thicker boundary. The Interfaces from which that node delivers the intercepted SIP messages are also shown with a different colored box.

When an incoming call arrives at the I-CSCF within the Egress IMS network, the I-CSCF would query the Home Subscriber System (HSS) (using Diameter protocol) to determine the S-CSCF associated with the IMS user. The arrows shown between I-CSCF and HSS are not bi-directional. For example, in the following figure, the arrow 2 indicates that I-CSCF sends a query to the HSS on the Interface 2 and the arrow 3 indicates that the HSS sends the response on the Interface 3. The arrows 1 and 4 indicate that an incoming call arrives at I-CSCF on Interface 1 and an outgoing call leaves the I-CSCF on Interface 4.



Part of the
Network Signaling Functional Flow
Diagram

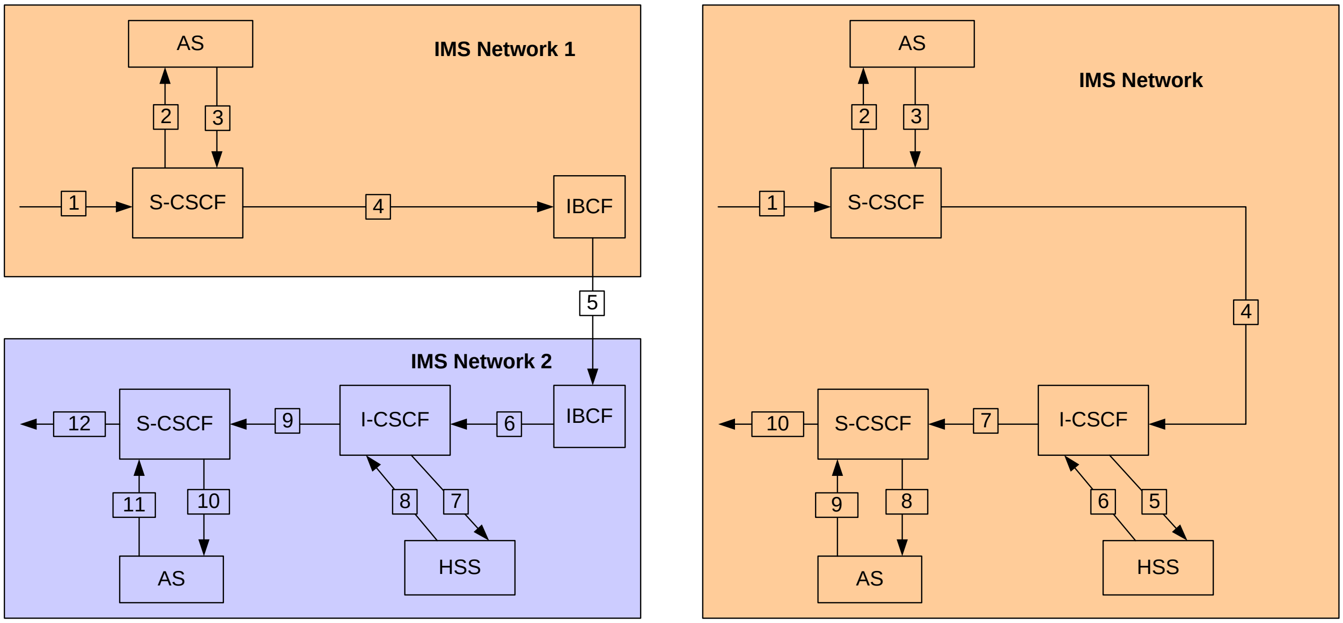
Part of the
Signaling Flow (not shown)

**Figure D.2 – Functional Flow Diagram and Sample Signaling Flow – Illustration 2**

Furthermore, I-CSCF and BGCF do not stay on the signaling path after the initial call setup dialogue is completed.

The network topology diagrams that include the illustration of CC interception are shown in a separate annex. The signaling flow diagrams illustrated here, however, do identify the network entities that send the CC intercept trigger to the CC IAP. The network entity that sends the CC intercept Trigger is referred to CC Interception Triggering Function (CC ITF), see clause 5 and Annex F for the details.

When a call is between two IMS users, the signaling flow diagrams show that the two IMS users are served by two different IMS networks. However, both users may also be served by the same IMS network. For the purpose of illustration, the difference between the two is the absence of IBCs when the call is intra-network. Figure D.3 below illustrates the differences.



Two IMS Networks – Signaling go through IBCF

One IMS Network – No IBCFs

**Figure D.3 – Intra-network VS Inter-network IMS to IMS call**

An IBCF at the entry point of a network is referred to as Ingress IBCF and an IBCF at the exit point of a network is referred to as Egress IBCF. In the same way, an MGCF at the entry point of a network is referred to as Ingress MGCF and an MGCF at the exit point of a network is referred to as Egress MGCF. An IBCF controls and manages the media at a TrGW whereas an MGCF controls and manages the media at an IM-MGW. When the signaling passes through an IBCF, there may or may not be an associated TrGW.

As explained in Annex F, when the P-CSCF is the CC ITF, either the PDN-GW/GGSN or the IMS-AGW is the CC IAP. . When an MGCF is the CC ITF, the corresponding IM-MGW is the CC IAP. An IBCF may also be a CC ITF, if there is an associated TrGW (which becomes the CC IAP) is deployed. Since the flow diagrams focus on the signaling aspects, none of the network entities (PDN-GW/GGSN, IM-MGW, TrGW) involved in the handling of media are shown within the diagrams.

> NOTE: Whenever a mention is made to indicate that an IBCF is the CC ITF, it is assumed that in that particular scenario there is an associated TrGW deployed. If there is no associated TrGW, then that IBCF will not become the CC ITF since there is no TrGW to which the CC Intercept Trigger can be sent.

## *D.1 IMS Originating Call*

This section gives the network signaling functional flow diagrams for the IMS originating calls where an originating IMS user happens to be the intercept subject. Two scenarios are presented:

1. P-CSCF belongs to the Home IMS Network.
2. P-CSCF belongs to a Visited IMS network.

### D.1.1 P-CSCF Belongs to the Originating Home IMS Network

P-CSCF is in the originating IMS user’s Home IMS network. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 2 and 5. The P-CSCF may optionally perform the same delivery of SIP messages on Interface 1 and 2.

The P-CSCF is the CC ITF when the CC interception is authorized.

### D.1.1.1 IMS to IMS Call

In the scenario, the intercept subject (an IMS user) originates a call to another IMS user (associate).

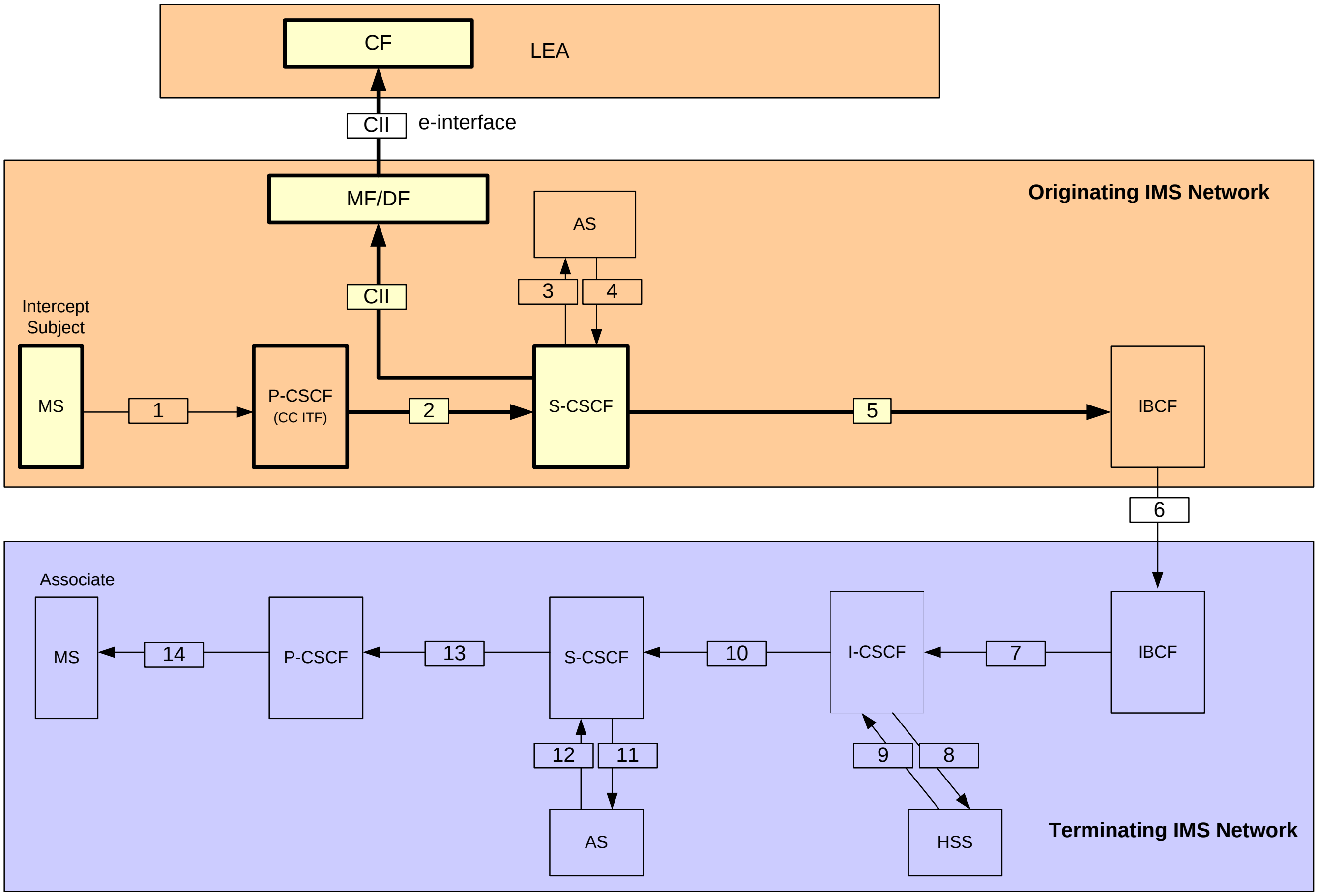


**Figure D.3 – IMS Originating Call (No Roaming) – IMS to IMS Call**

### D.1.1.2 IMS to PSTN Call

In this scenario, the intercept subject (an IMS user) originates a call to a PSTN user (associate).

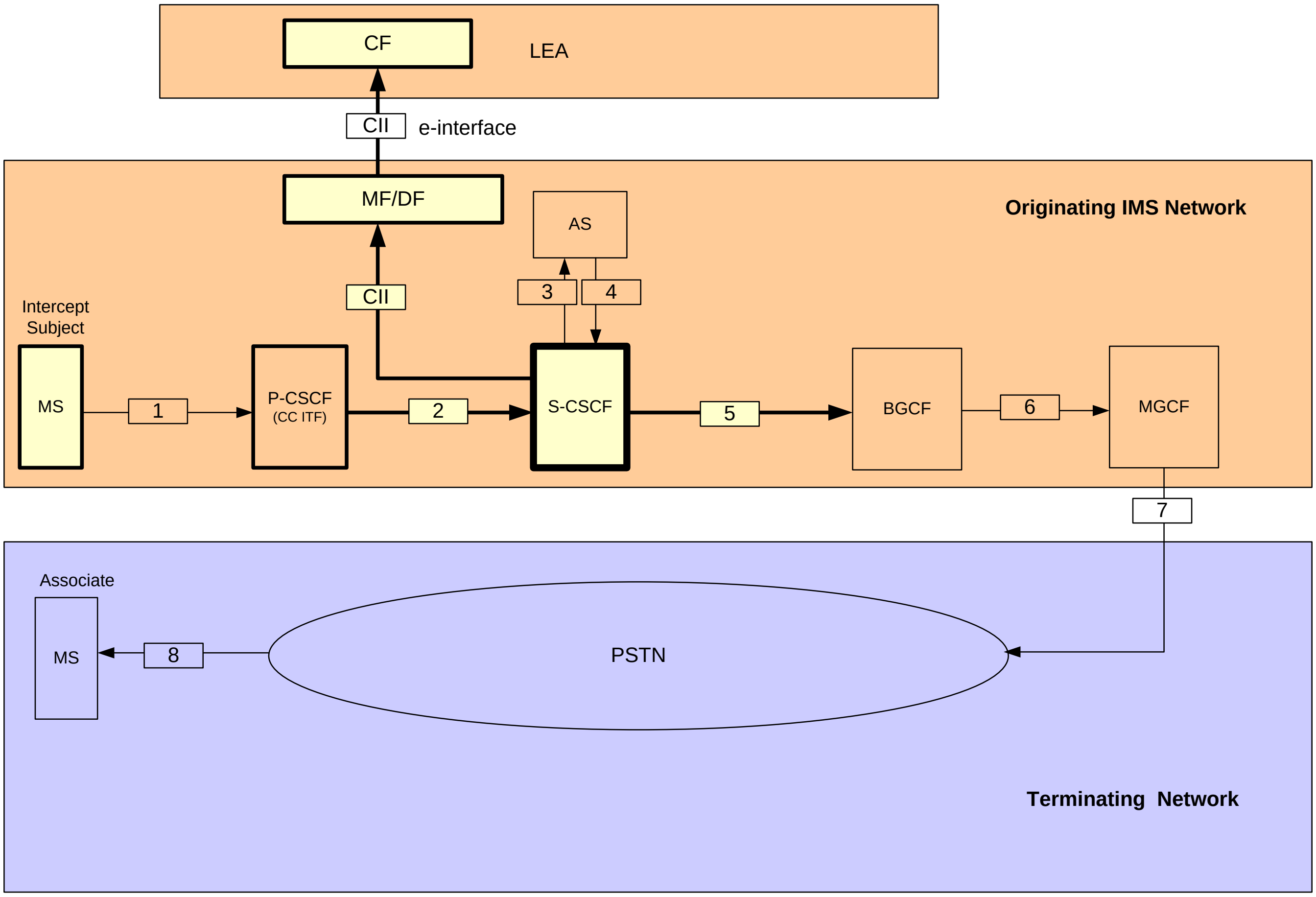


**Figure D.4 – IMS Originating Call (No Roaming) – IMS to PSTN Call**

## D.1.2 P-CSCF is in an Originating Visited IMS Network

The intercept subject (an IMS user) is in a Visited IMS network which is different from that user's Home IMS network. Two scenarios are presented here:

- Scenario 1: Both network providers are served with lawful authorization(s).
- Scenario 2: Only the Home IMS network provider is served with the lawful authorization.

Note that it is also possible to have a scenario where only the visited IMS network provider is served with the lawful authorization. In this scenario, since the lawful authorization is not applicable to the Home IMS network provider of the intercept subject, the S-CSCF of the Home IMS network will not provide any IAP for the CII.

### D.1.2.1 IMS to IMS Call

The two scenarios considered here are for the case of an IMS to IMS call (i.e., an intercept subject [IMS user] originates a call to another IMS user [associate]).

**Scenario 1**

In this scenario both the Visited IMS network provider and the Home IMS network provider are served with lawful authorization(s).

In the Originating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. The Ingress IBCF is the CC ITF when the CC interception is authorized.

In the Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 1 and 2. The P-CSCF is the CC ITF when the CC interception is authorized.

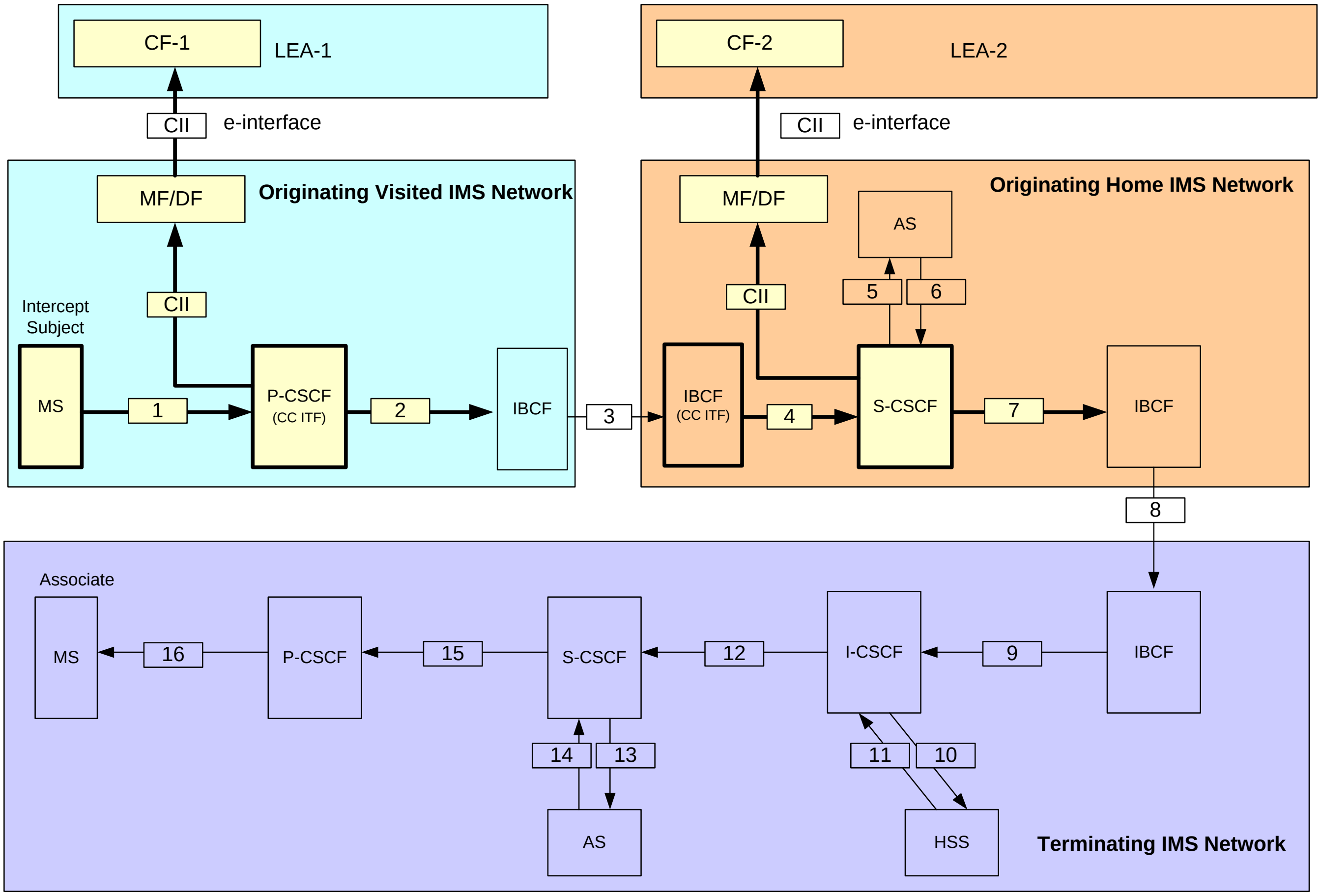


**Figure D.5 – IMS Originating Call (IMS Roaming) – IMS to IMS Call – Scenario 1**

### Scenario 2

In this scenario only the Home IMS network provider of the Intercept Subject is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. The Ingress IBCF is the CC ITF when the CC interception is authorized.

Since the lawful authorization does not apply to the visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

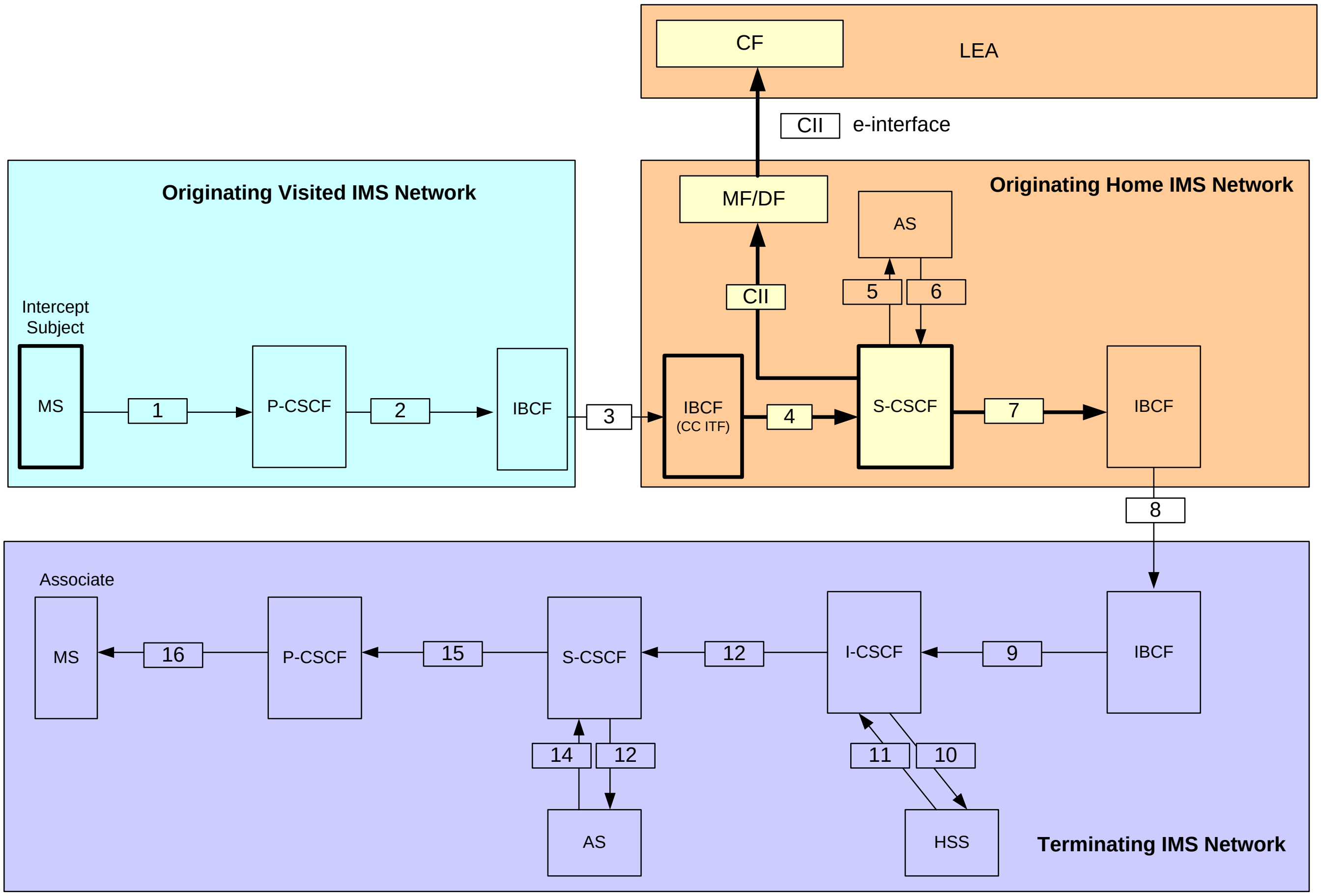


Figure D.6 – IMS Originating Call (IMS Roaming) – IMS to IMS Call – Scenario 2

### D.1.2.2 IMS to PSTN Call

The case of the IMS to PSTN call is not shown since from an inter-networking perspective (i.e., Ingress to Egress) that case is redundant to the one illustrated in D.1.1.2.

## *D.2 IMS Terminating Call*

This section gives the network signaling functional flow diagrams for the IMS terminating calls where a terminating IMS user is the intercept subject. Two scenarios are presented:

1. P-CSCF belongs to the Terminating Home IMS Network.
2. P-CSCF belongs to a Terminating Visited IMS Network.

### D.2.1 P-CSCF belongs to the Terminating Home IMS Network

P-CSCF is in the terminating IMS user's Home IMS network. The S-CSCF provides the IAP for the CII.

The P-CSCF is the CC ITF when the CC interception is authorized.

### D.2.1.1 IMS to IMS Call

In the scenario, the intercept subject (an IMS user) receives a terminating call from another IMS user (associate).

The S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13. The P-CSCF may perform the same delivery of SIP messages from the Interface 13 and 14.

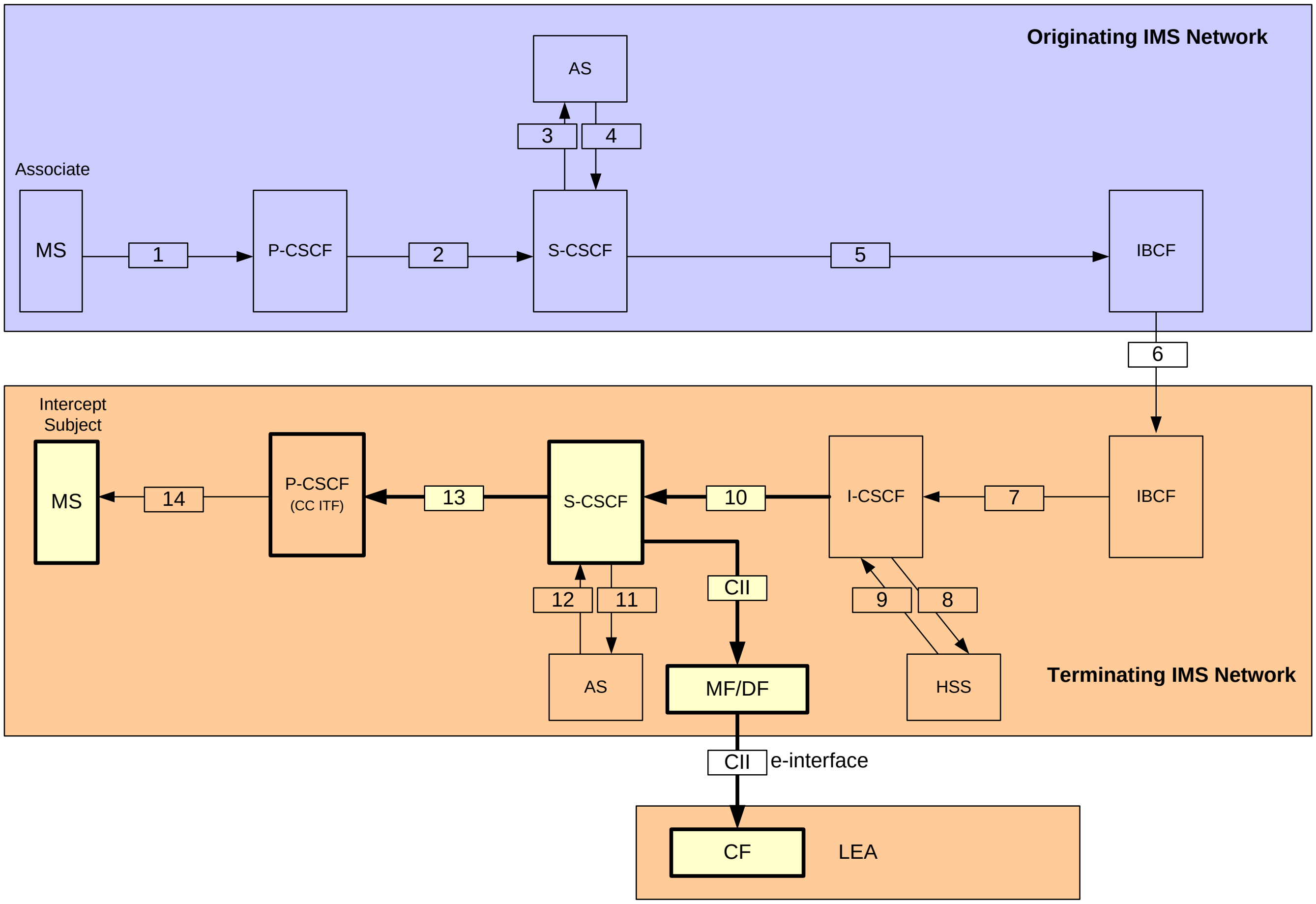


**Figure D.7 – IMS Terminating Call (No Roaming) – IMS to IMS Call**

### D.2.1.2 PSTN to IMS Call

In this scenario, the intercept subject (an IMS user) receives a terminating call from a PSTN user (associate).

The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The P-CSCF may perform the same delivery of SIP messages from the Interface 9 and 10.

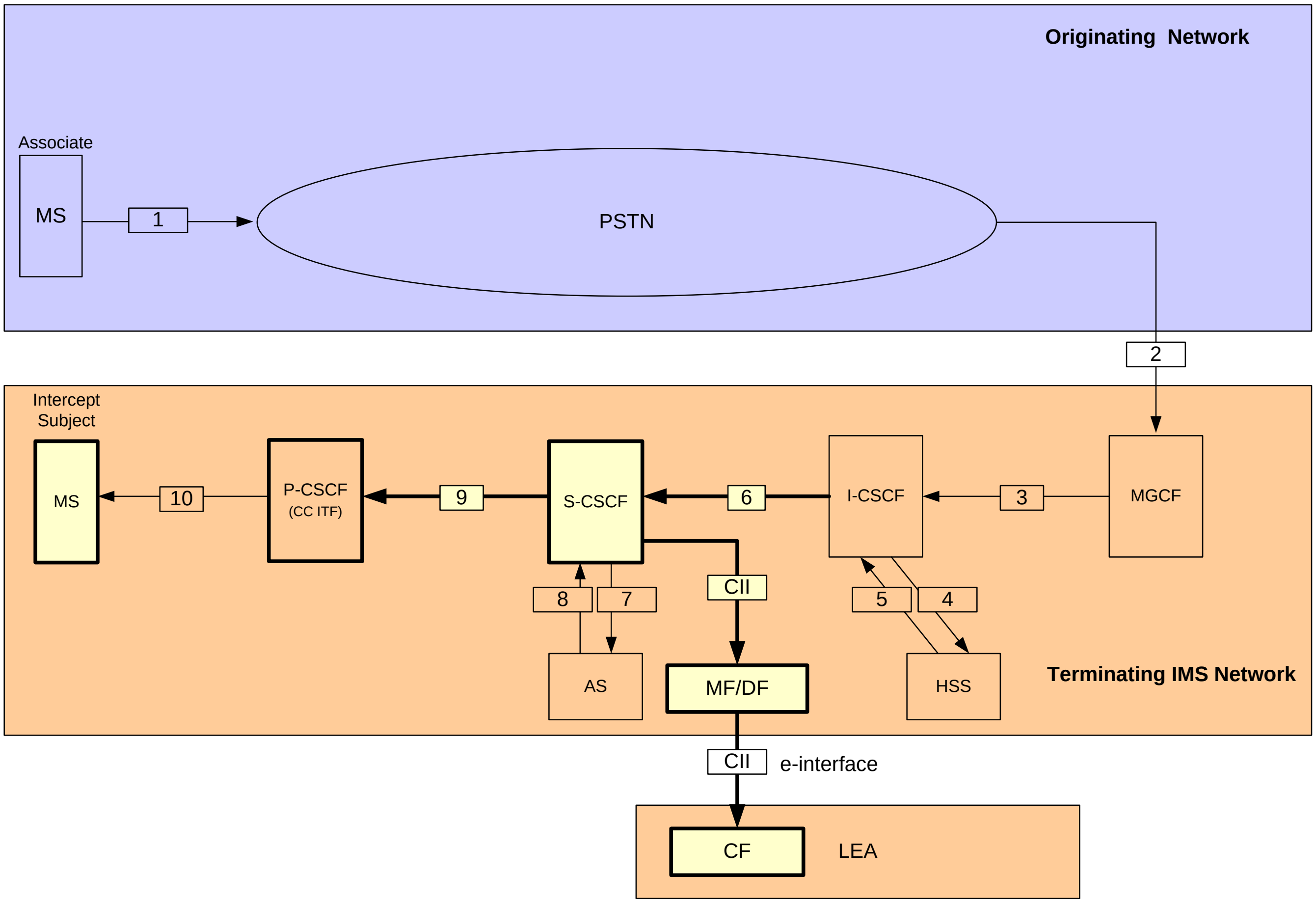


**Figure D.8 – IMS Terminating Call (No Roaming) – PSTN to IMS Call**

## D.2.2 P-CSCF is in a Terminating Visited IMS Network

The intercept subject (an IMS user) is in a Visited IMS network which is different from that user's Home IMS network. Two scenarios are presented here:

- Scenario 1: Both network providers are served with lawful authorization(s).
- Scenario 2: Only the Home IMS network provider is served with the lawful authorization.

Note that it is also possible to have a scenario where only the visited IMS network provider is served with the lawful authorization. In this scenario, since the lawful authorization is not applicable to the Home IMS network provider of the intercept subject, the S-CSCF of the Home IMS network will not provide any IAP for the CII.

### D.2.2.1 IMS to IMS Call

The two scenarios considered here are for the case of an IMS to IMS call – i.e., an intercept subject (IMS user) receives a terminating call from another IMS user (associate).

**Scenario 1**

In this scenario both the Terminating Visited IMS network provider and the Terminating Home IMS network provider are served with lawful authorization(s).

In the Terminating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13. The Egress IBCF is the CC ITF when the CC interception is authorized.

In the Terminating Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 15 and 16. P-CSCF provides the CC ITF when CC interception is authorized.

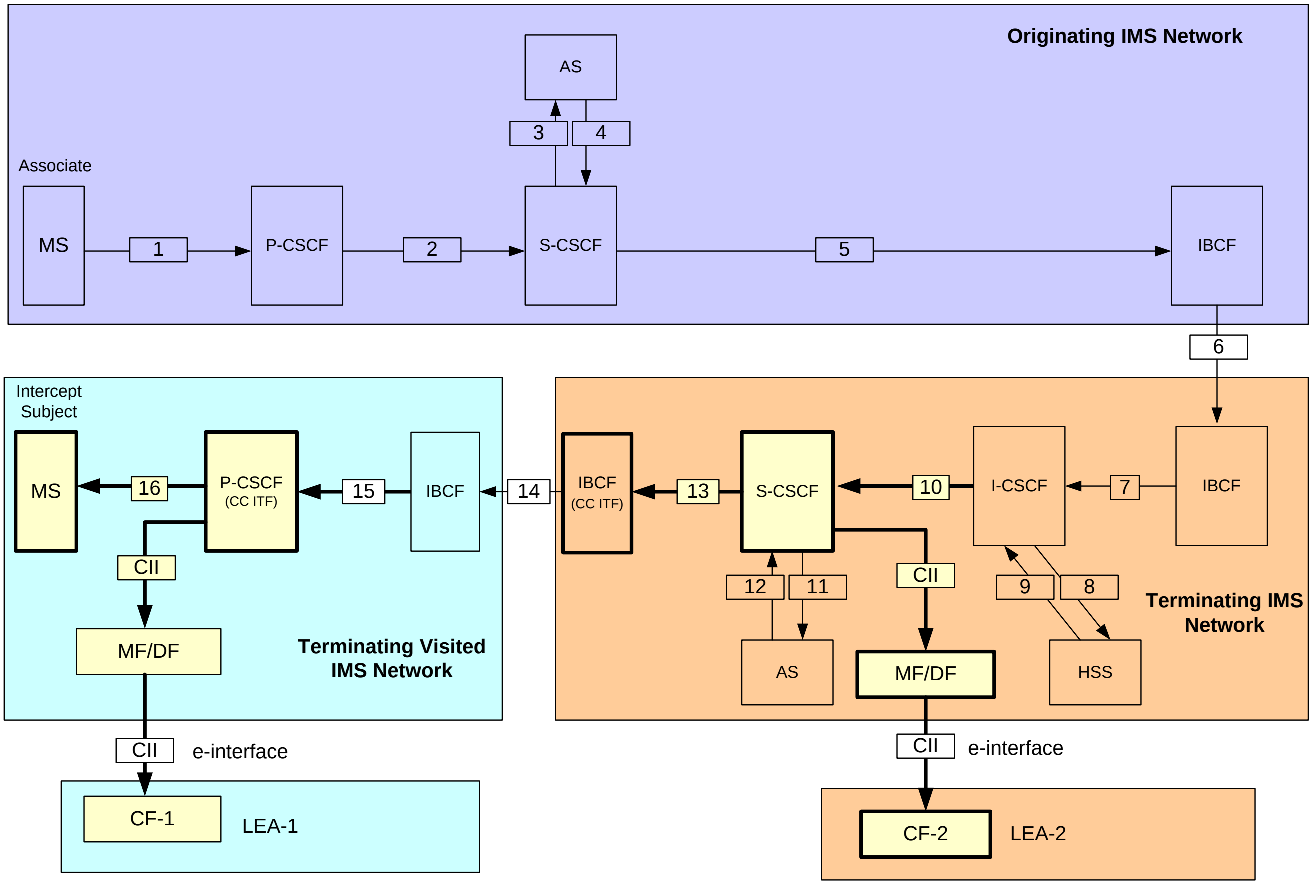


**Figure D.9 – IMS Terminating Call (IMS Roaming) – IMS to IMS Call – Scenario 1**

### Scenario 2

In this scenario only the Terminating Home IMS network provider is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13. The Egress IBCF is the CC ITF when the CC interception is authorized.

Since the lawful authorization does not apply to the Terminating Visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

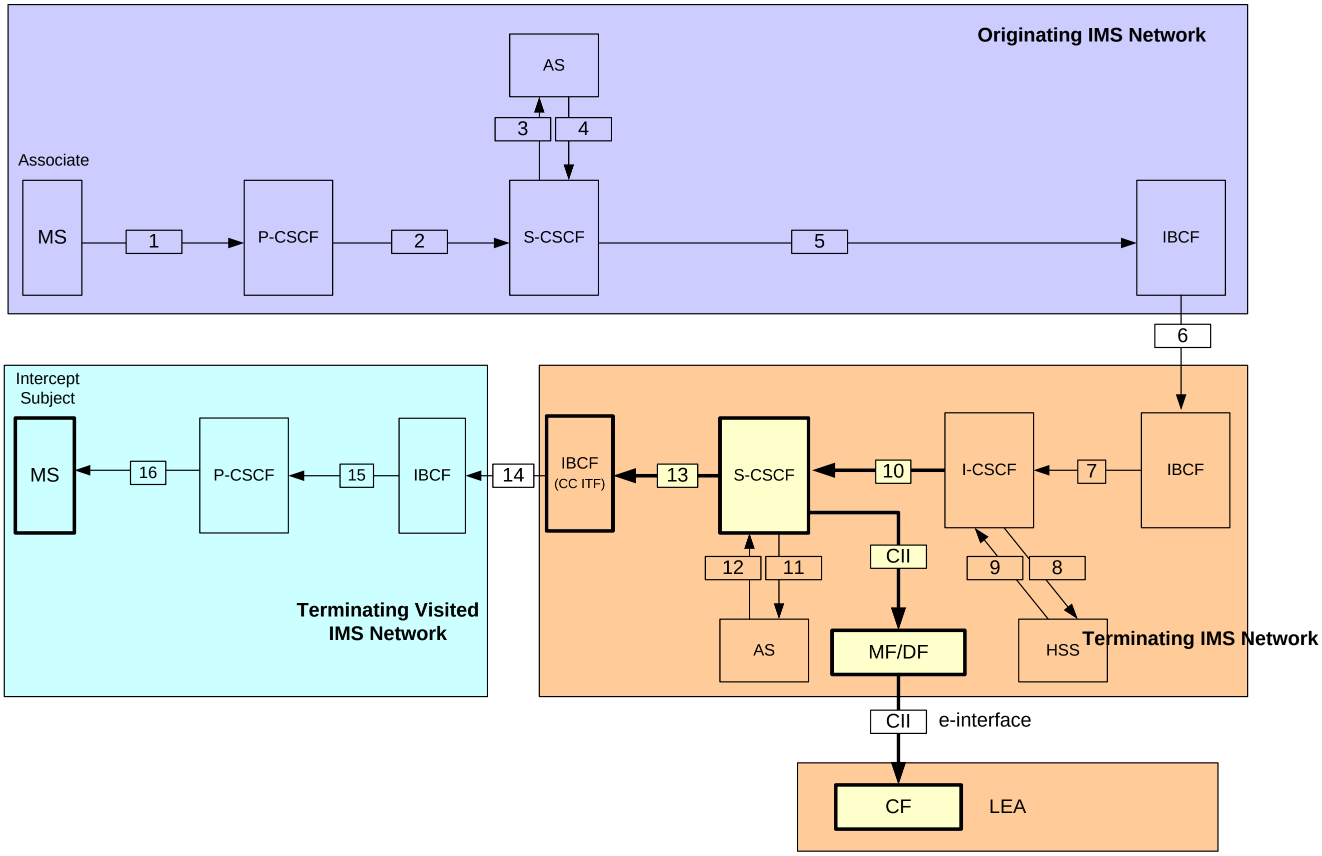


**Figure D.10 – IMS Terminating Call (IMS Roaming) – IMS to IMS Call – Scenario 2**

## D.2.2.2 PSTN to IMS Call

The two scenarios considered here are for the case of a PSTN to IMS call – i.e., an intercept subject (IMS user) receives a terminating call from a PSTN user (associate).

**Scenario 1**

In this scenario both the Terminating Visited IMS network provider and the Terminating Home IMS network provider are served with lawful authorization(s).

In the Terminating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The IBCF is the CC ITF when the CC interception is authorized.

In the Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 11 and 12. The P-CSCF provides the CC ITF when the CC interception is authorized.

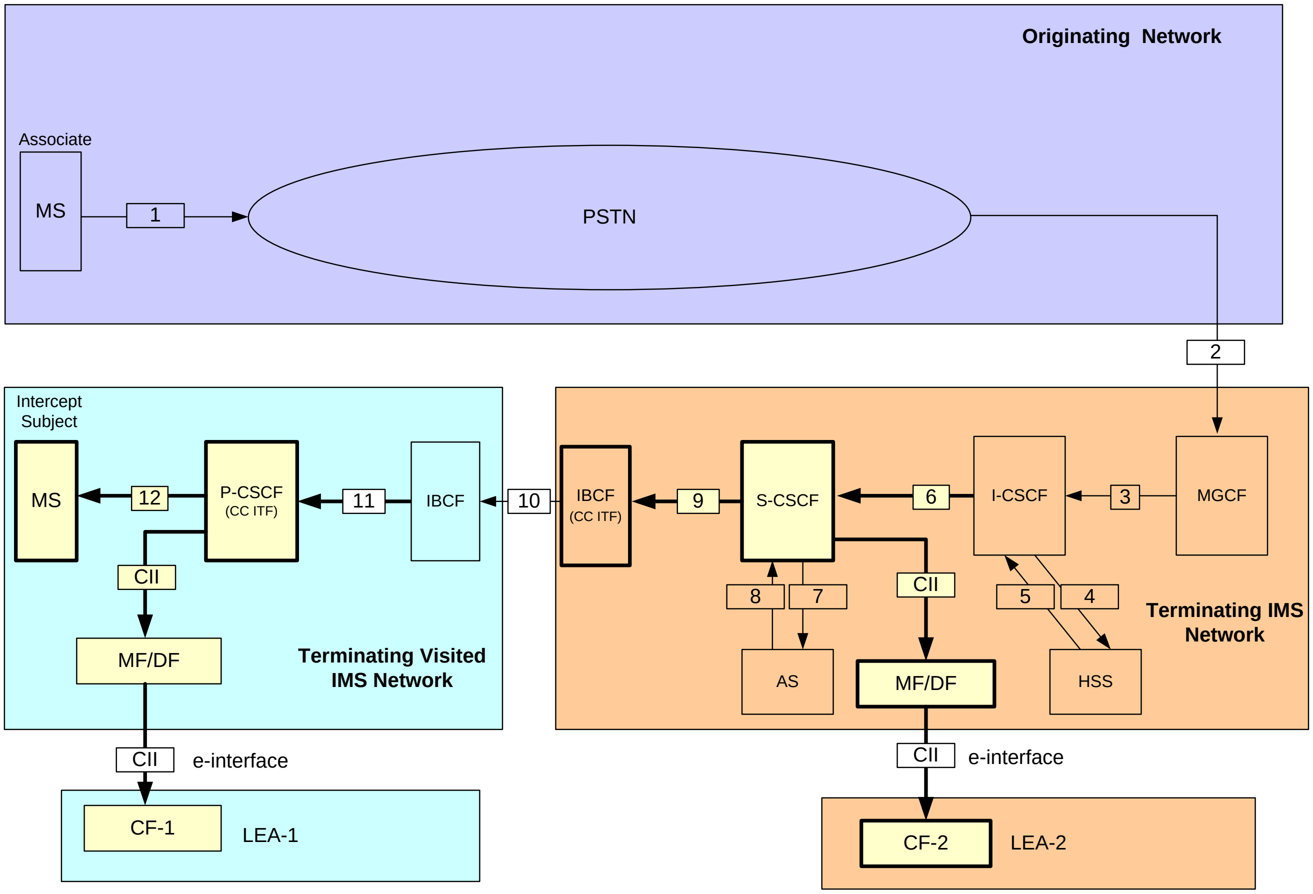


**Figure D.11 – IMS Terminating Call (IMS Roaming) – PSTN to IMS Call – Scenario 1**

### Scenario 2

In this scenario only, the Terminating Home IMS network provider is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The IBCF is the CC ITF when the CC interception is authorized.

Since the lawful authorization does not apply to the Terminating Visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

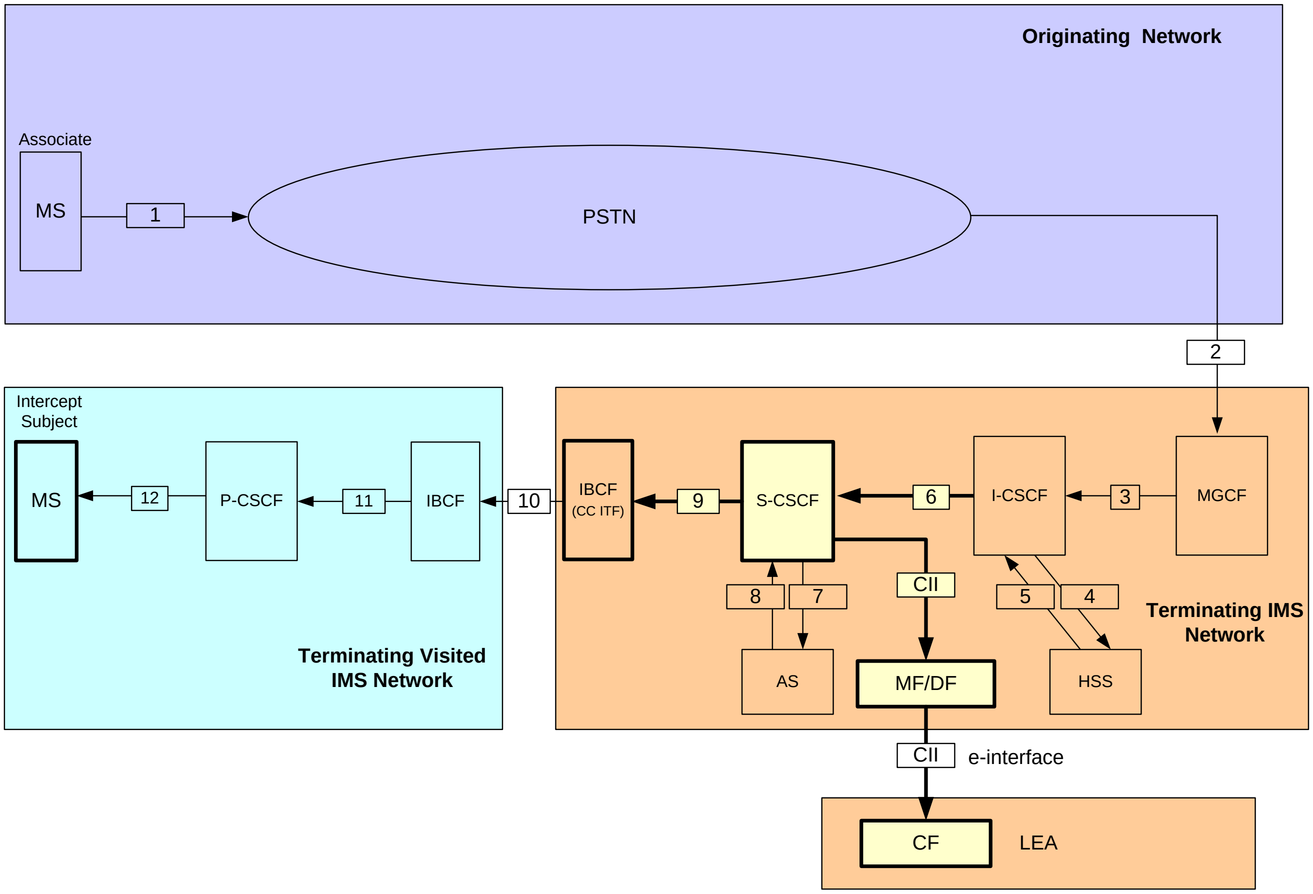


**Figure D.12 – IMS Terminating Call (IMS Roaming) – PSTN to IMS Call – Scenario 2**

## *D.3 IMS Forwarded Calls*

This section gives the network signaling functional flow diagrams for the forwarded calls where the incoming calls to an IMS user (the intercept subject) are forwarded by the network. The call forwarding is initiated by the AS or the S-CSCF present within the home IMS network of the IMS user (intercept subject).

In the scenarios presented, Originating Network is the network that handles the call control procedures from a calling user's perspective The calling user is identified within the diagrams as "Associate-1". The Forward-to Party's Terminating Network is the network that handles the call control procedures from a forward-to user's perspective. The forward-to user is identified within the diagrams as "Associate-2". The IMS user (intercept subject) who has the call forwarding active is referred to as the base IMS user. The Terminating Base IMS network is the IMS network that handles the call control procedures from the base IMS user's (intercept subject's) perspective. Since the lawful interception is on the base IMS user, the lawful interception functions are provided within the Terminating Base IMS Network.

### D.3.1 Call Forwarding Unconditional

In this scenario, all incoming calls to the intercept subject are forwarded. Since base IMS user (intercept subject who has activated the call forwarding) is not alerted, the procedures are independent of the base IMS user's IMS roaming situations.

Four cases are presented:

1. A call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

2. A call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).
3. A call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).
4. A call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

In all the scenarios, the S-CSCF of the Terminating Base IMS Network provides the IAP for the CII. The P-CSCF of the intercept subject is not involved (shown with a thin dotted boundary) in the call handling and hence, does not provide the IAP for the CII.  The MS associated with the intercept subject is also shown with a thin dotted boundary since the intercept subject is not physically involved in the call.

### D.3.1.1 IMS to IMS Call Forwarded to IMS

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13. The Egress IBCF is the CC ITF when the CC interception is authorized.

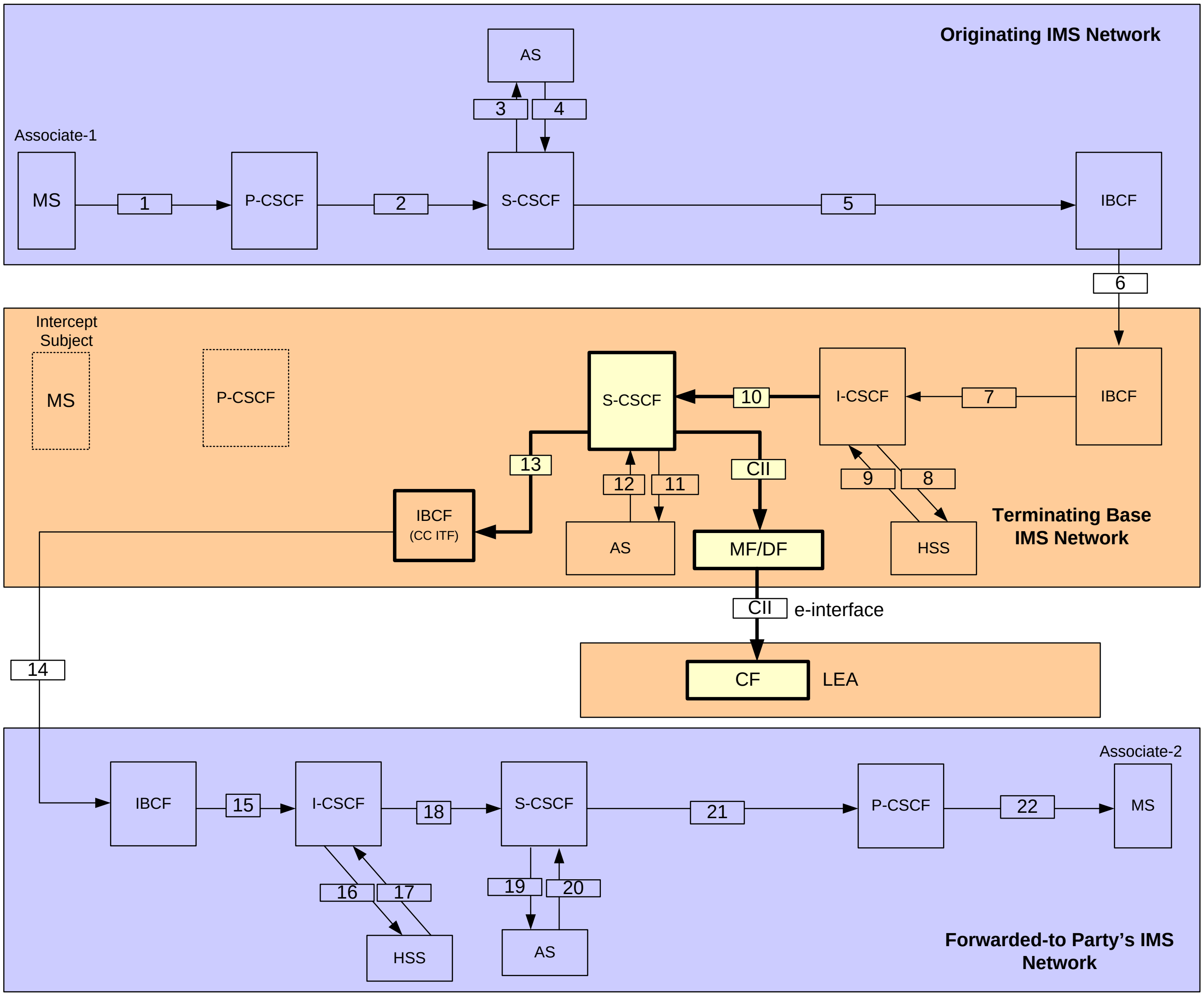


**Figure D.13 – Call Forwarding Unconditional: IMS to IMS Call forwarded to IMS**

### D.3.1.2 IMS to IMS Call Forwarded to PSTN

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13. The MGCF is the CC ITF when the CC interception is authorized. .

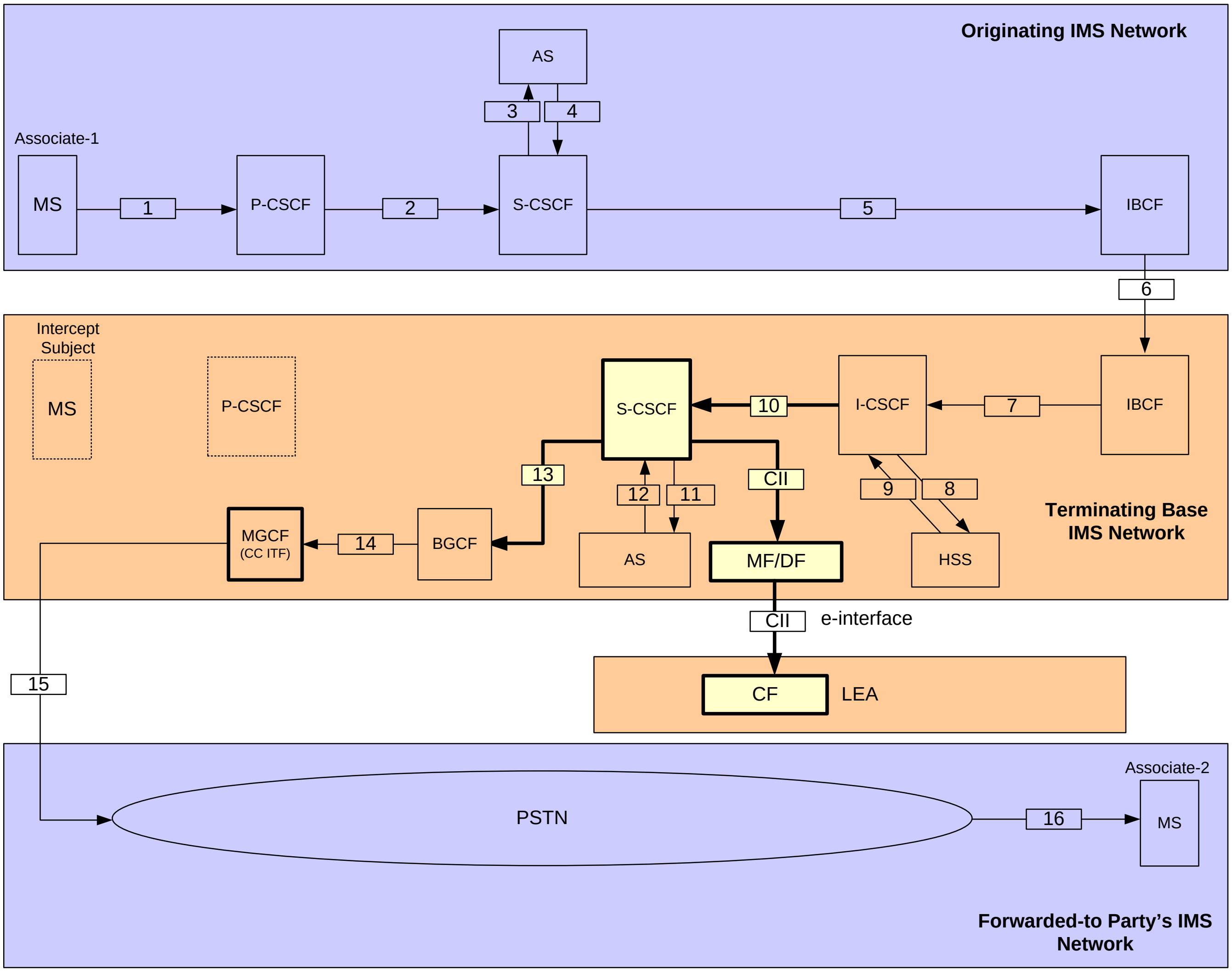


Figure D.14 – Call Forwarding Unconditional: IMS to IMS Call forwarded to PSTN

### D3.1.3 PSTN to IMS Call Forwarded to IMS

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The IBCF is the CC ITF when the CC interception is authorized.

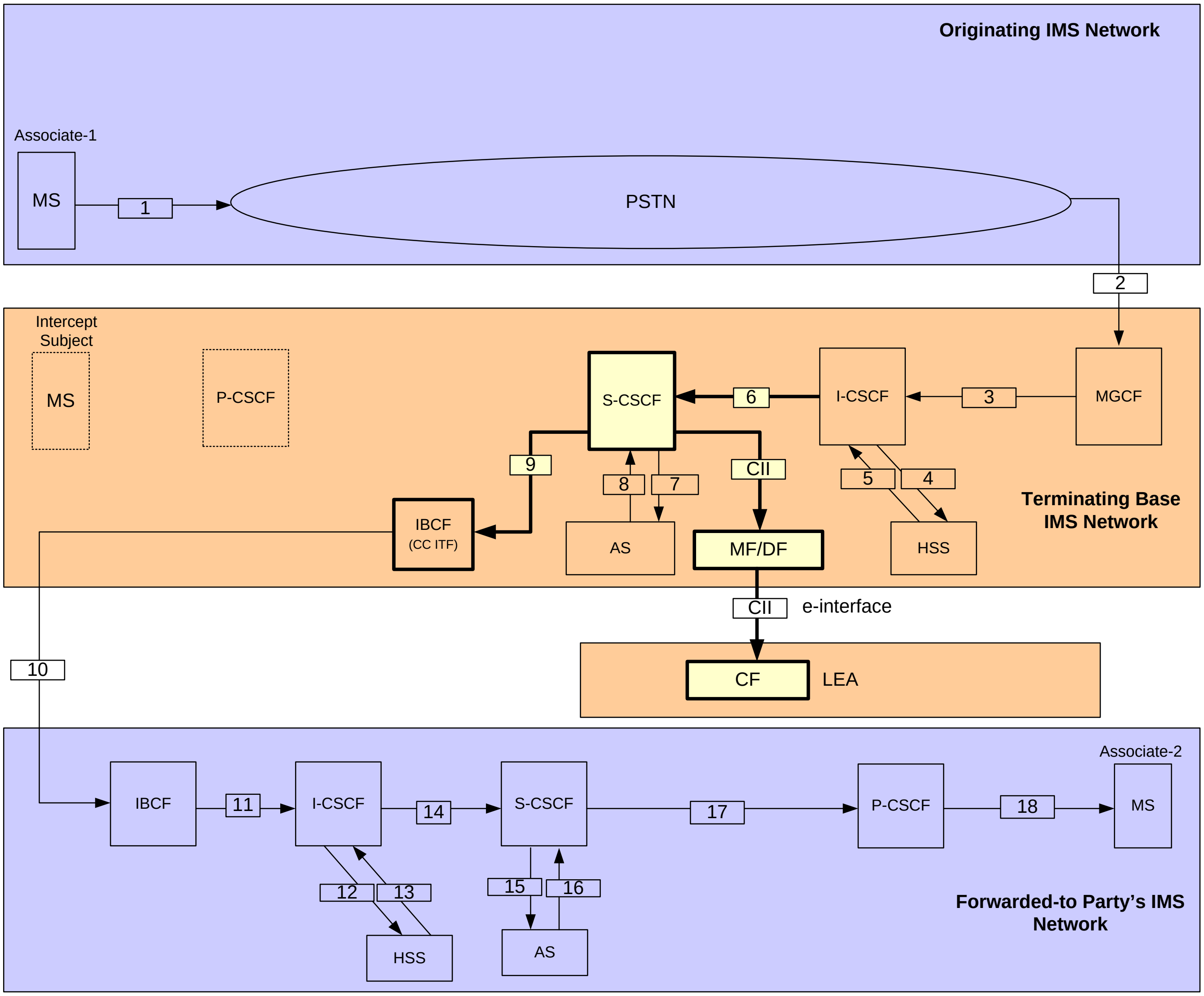


**Figure D.15 – Call Forwarding Unconditional: PSTN to IMS Call forwarded to IMS**

### D.3.1.4 PSTN to IMS Call Forwarded to PSTN

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another PSTN user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The Egress MGCF is the CC ITF when the CC interception is authorized.

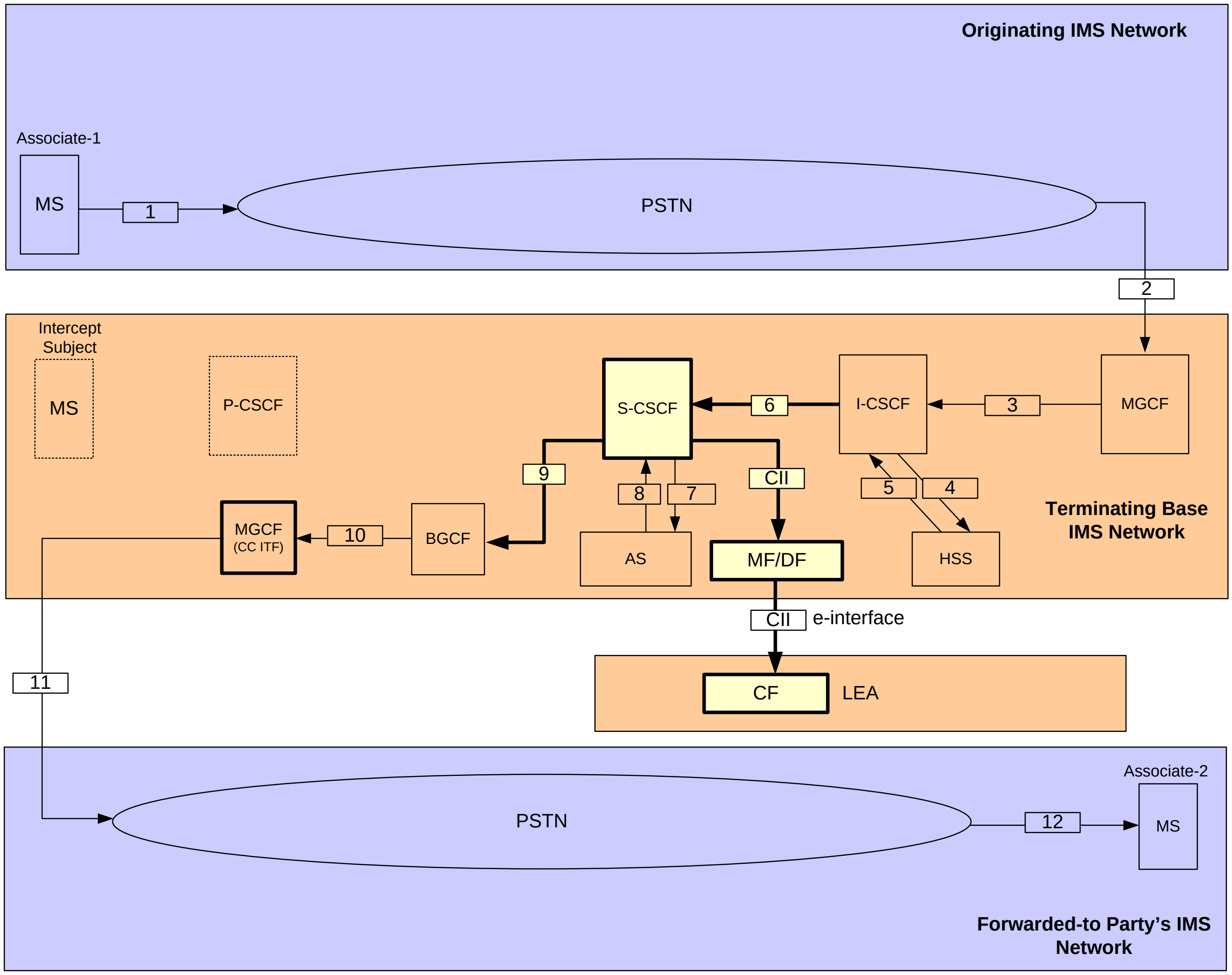


**Figure D.16 – Call Forwarding Unconditional: PSTN to IMS Call forwarded to PSTN**

## D.3.2 Call Forwarding Do Not Answer

In this scenario, the IMS user (intercept subject) is initially alerted using the normal call termination procedures (see D.2). The AS or the S-CSCF (depending on the implementation) would time the alerting and would initiate the call forwarding (once the timer is expired) in the same way as of a call forwarding unconditional case (see D.3.1). Since the call to the alerted user is abandoned before answer, the network (i.e., AS or the S-CSCF) sends a SIP CANCEL message to the base IMS user's (intercept subject's) device.

As in the case of call termination scenarios (section D.2), from a pre-alerting to the base IMS user (intercept subject) perspective, two cases are considered:

1. P-CSCF of the base IMS user belongs to the Home IMS network (shown as Terminating Base Home Network) of the base IMS user.
2. P-CSCF of the base IMS user belongs to a Visited IMS Network (shown as Terminating Base Visited IMS Network) and that Terminating Base Visited IMS Network is different from the Terminating Home IMS Network of the base IMS User.

Four cases are presented to illustrate the forwarded leg of the call (as shown in section D.3.1).

1. A call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).
2. A call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).
3. A call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).
4. A call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

In all the diagrams, the P-CSCF with a thick dotted boundary indicates that the P-CSCF is involved in the lawful interception before the call is forwarded (e.g., CC ITF). A thick dotted signaling line indicates that the SIP messages on the particular interface may be delivered to the MF/DF before the call is forwarded. The MS associated with the intercept subject is shown with a thick dotted boundary to indicate the intercept subject is physical involvement in the call only before the call is forwarded.

## D.3.2.1 P-CSCF belongs to the Terminating Base Home IMS Network

P-CSCF is in the base IMS user’s (intercept subject’s) Home IMS network. For all the scenarios, the S-CSCF provides the IAP for the CII.

### D.3.2.1.1 IMS to IMS Call Forwarded to IMS

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 16 for the forwarded leg of the call.

The P-CSCF of the intercept subject (base IMS user) may perform the same delivery of SIP messages from the Interface 13 and 14 during the alerting phase of the call. However, for the forwarded leg of the call, the P-CSCF of the intercept subject (base IMS user) is not involved in the call handling and hence, does not provide the IAP for the CII.

While the call is being alerted, the P-CSCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, Egress IBCF is the CC ITF when the CC interception is authorized.

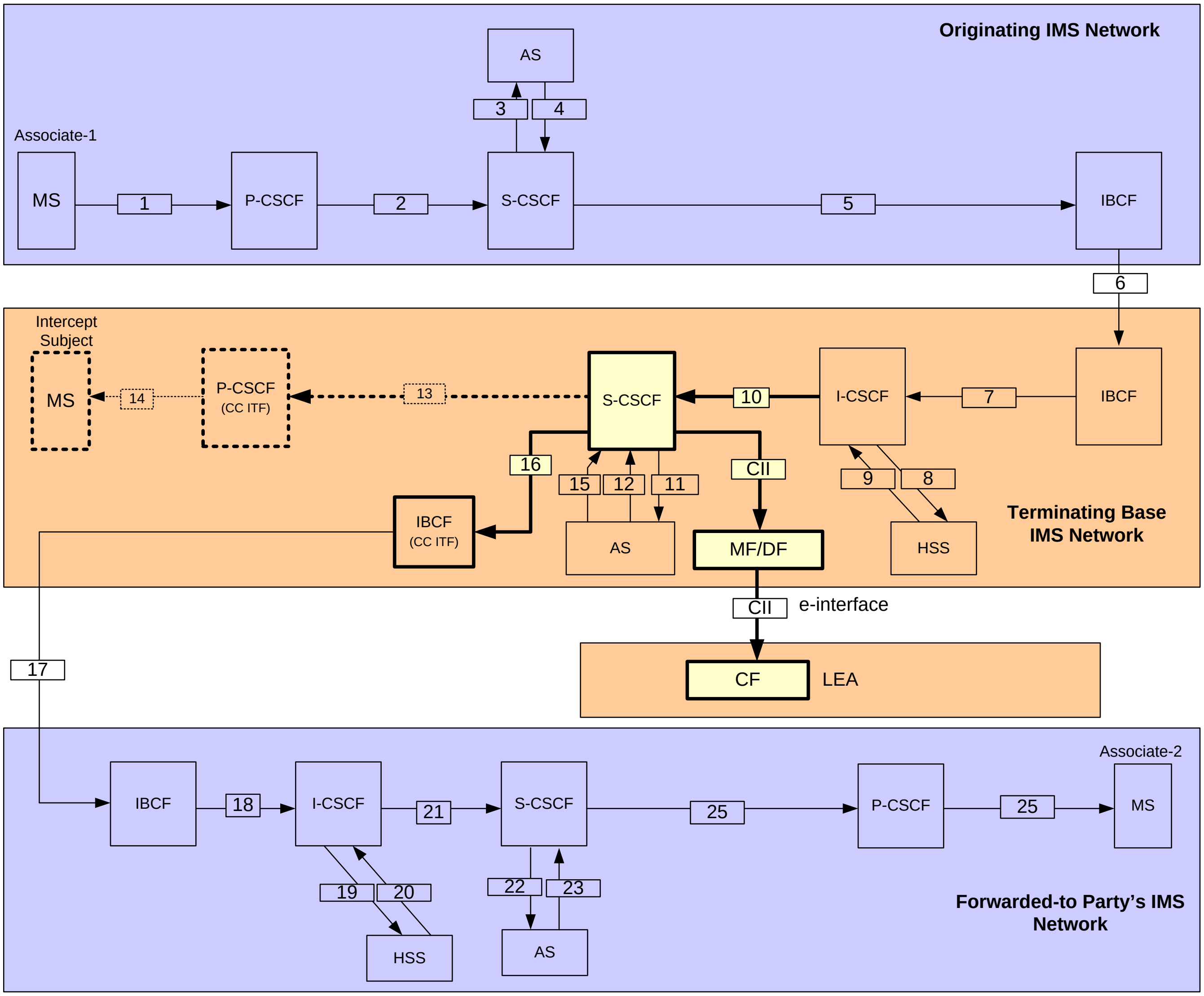


Figure D.17 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS

### D.3.2.1.2 IMS to IMS Call Forwarded to PSTN

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 16 for the forwarded leg of the call.

The P-CSCF of the intercept subject (base IMS user) may perform the same delivery of SIP messages from the Interface 13 and 14 during the alerting phase of the call. However, for the forwarded leg of the call, the P-CSCF of the intercept subject (base IMS user) is not involved in the call handling and hence, does not provide the IAP for the CII.

While the call is being alerted, the P-CSCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, MGCF is the CC ITF when the CC interception is authorized.

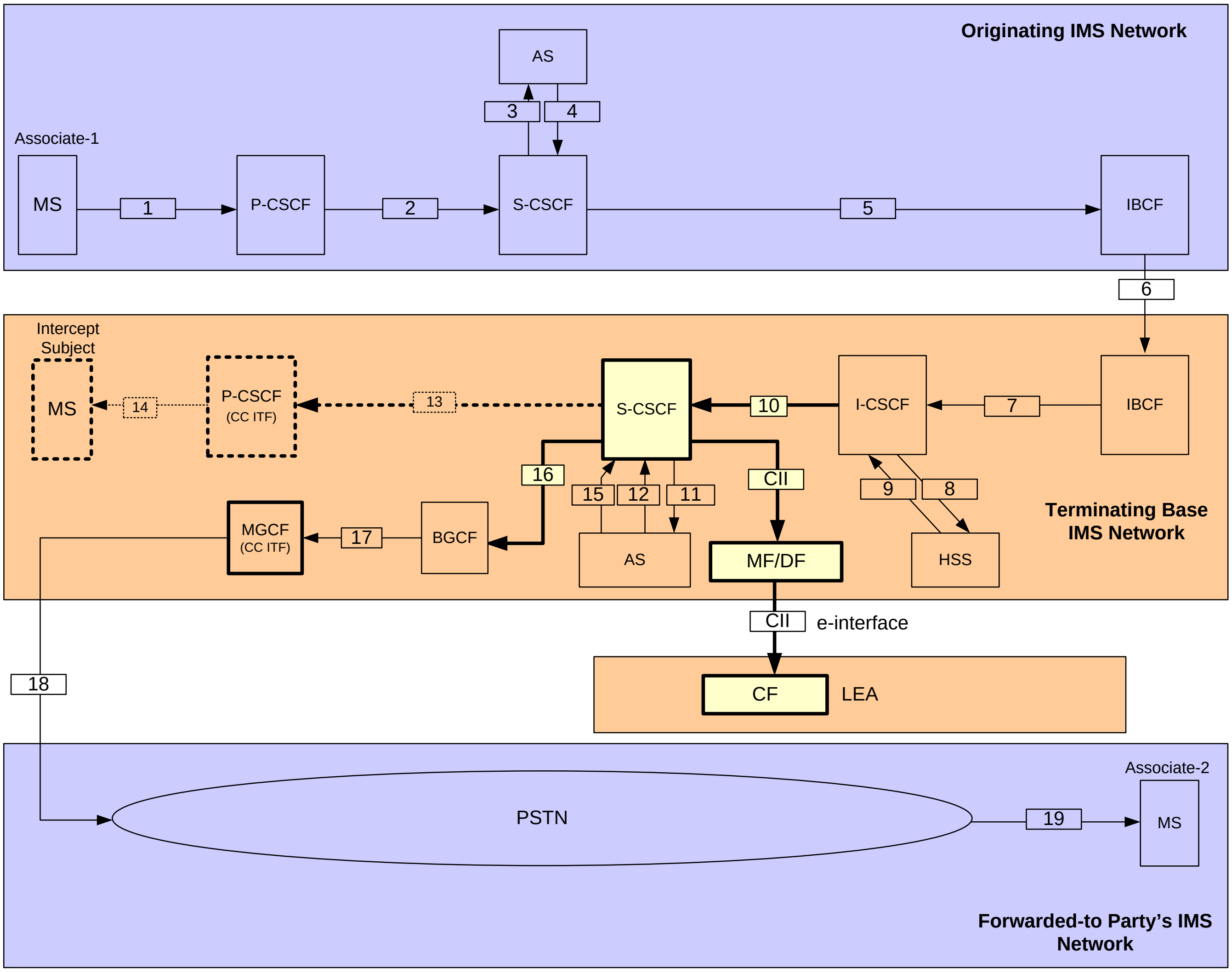


Figure D.18 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to PSTN

### D.3.2.1.3 PSTN to IMS Call Forwarded to IMS

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call.

The P-CSCF of the intercept subject may perform the same delivery of SIP messages from the Interface 9 and 10 during the alerting phase of the call. However, for the forwarded leg of the call, the P-CSCF of the intercept subject is not involved in the call handling and hence, does not provide the IAP for the CII.

While the call is being alerted, the P-CSCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, IBCF is the CC ITF when the CC interception is authorized.

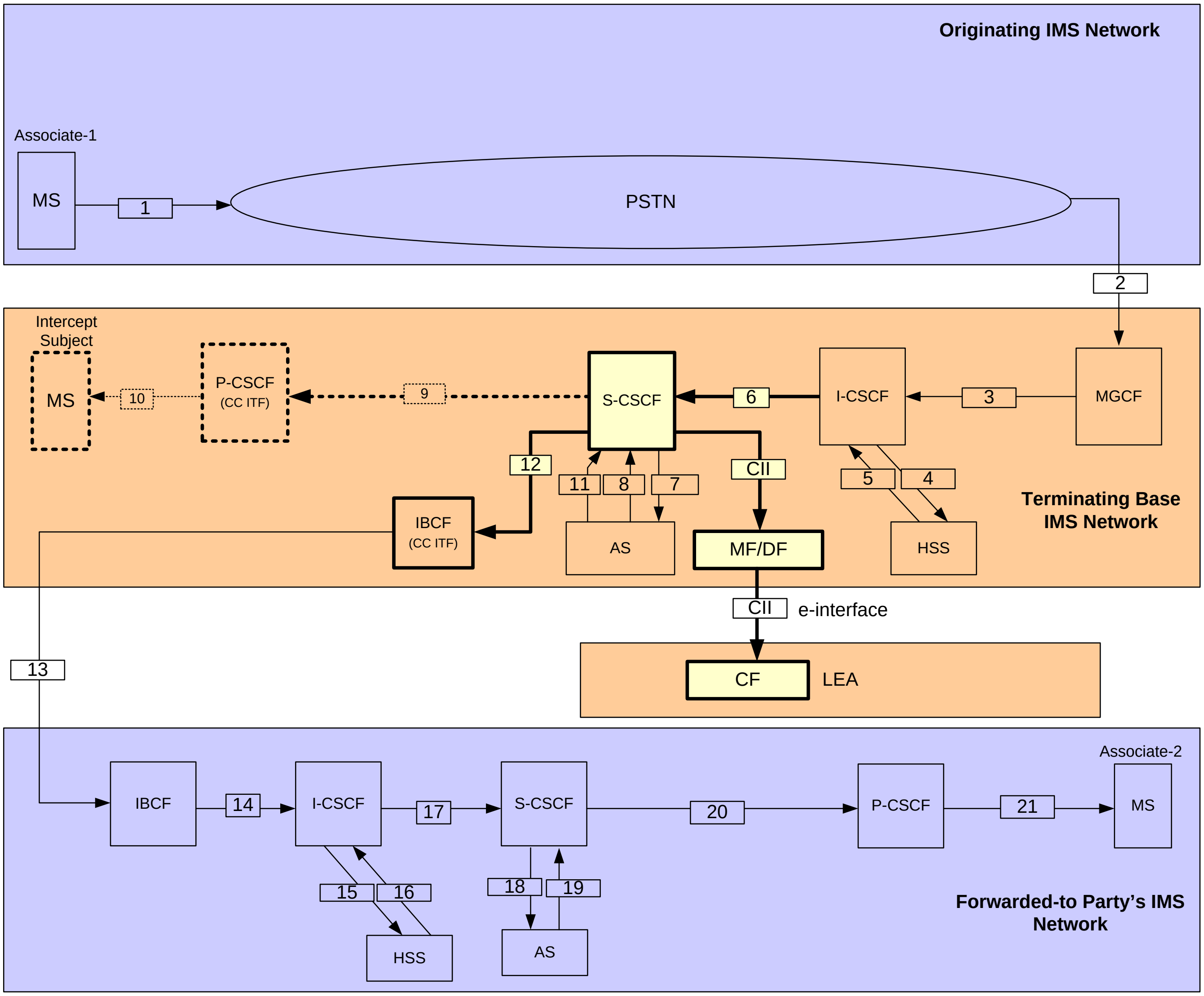


**Figure D.19 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to IMS**

### D.3.2.1.4 PSTN to IMS Call Forwarded to PSTN

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call.

The P-CSCF of the intercept subject may perform the same delivery of SIP messages from the Interface 9 and 10 during the alerting phase of the call. However, for the forwarded leg of the call, the P-CSCF of the intercept subject is not involved in the call handling and hence, does not provide the IAP for the CII.

While the call is being alerted, the P-CSCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, Egress MGCF is the CC ITF when the CC interception is authorized.

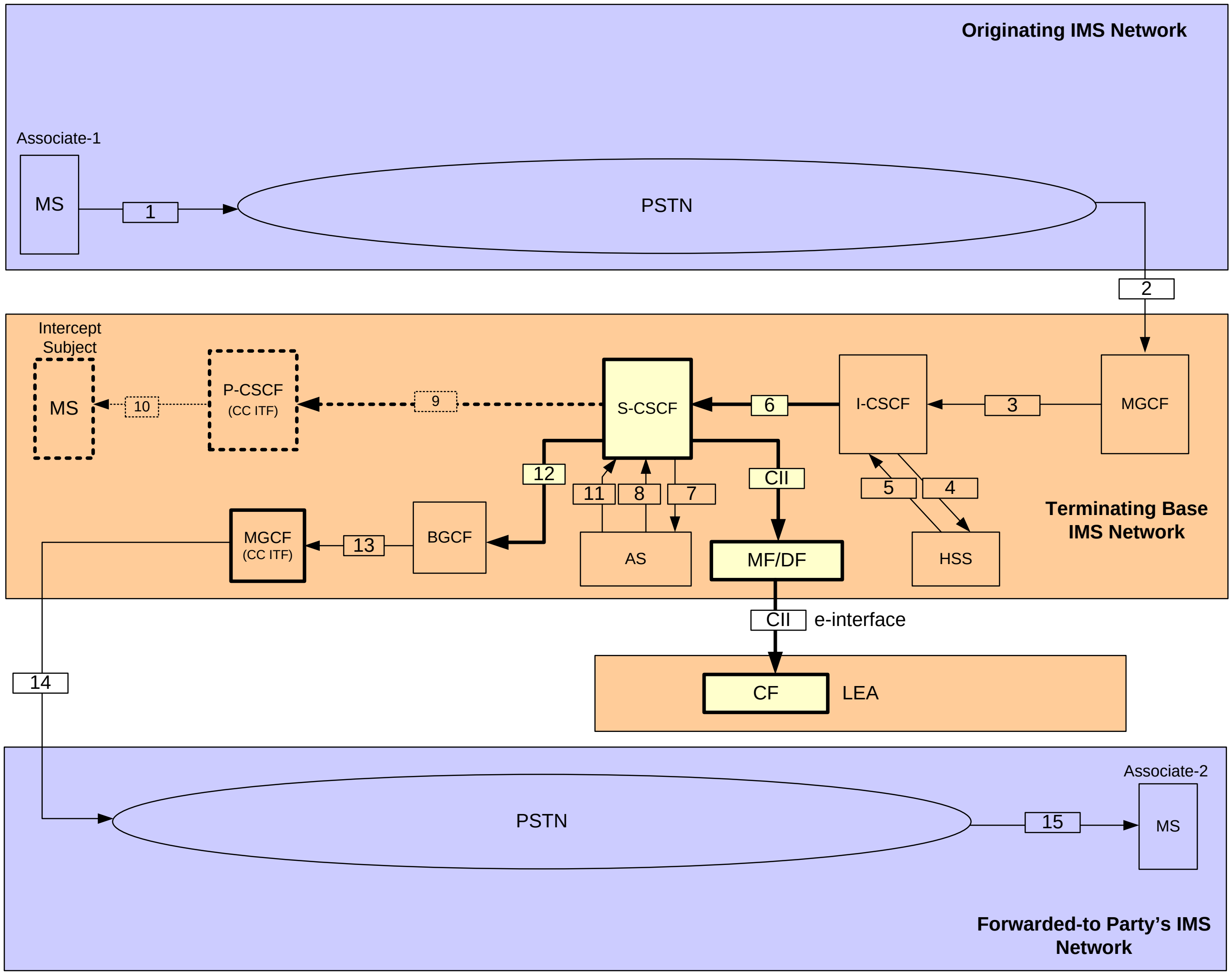


**Figure D.20 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to PSTN**

## D.3.2.2 P-CSCF is in a Terminating Base Visited IMS Network

The intercept subject (an IMS user) is in a Visited IMS network which is different from that user's Home IMS network. Two scenarios are presented:

- Scenario 1: Both network providers (Terminating Base Visited IMS Network and Terminating Base Home IMS Network) are served with the lawful authorization(s).
- Scenario 2: Only the Terminating Base Home IMS Network provider is served with the lawful authorization.

Note that it is also possible to have a scenario where only the Terminating Base Visited IMS network provider is served with the lawful authorization. In this scenario, since the lawful authorization is not applicable to the Terminating Base Home IMS network provider of the intercept subject, the S-CSCF of the Terminating Base Home IMS network will not provide any IAP for the CII.

An IBCF in the Terminating Base IMS Network is also shown with a thick dotted boundary to indicate that it is providing the CC ITF functions only before the call is forwarded.

### D.3.2.2.1 Both Network Providers are Served with Lawful Authorization(s)

In this scenario, both the Terminating Base Visited IMS network provider and the Terminating Base Home IMS network provider are served with lawful authorization(s).

In the Terminating Base Home IMS Network, S-CSCF provides the IAP for the CII.

In the Terminating Base Visited IMS network, the P-CSCF provides the IAP for the CII.

However, for the forwarded leg of the call, the P-CSCF of the intercept subject (base IMS user) is not involved in the call handling and hence, does not provide the IAP for the CII.

#### D.3.2.2.1.1 IMS to IMS Call Forwarded to IMS

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 18 for the forwarded leg of the call.

Within the Terminating Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 15 and 16 during the alerting phase of the call.

While the call is being alerted, the P-CSCF in the Terminating Base Visited Network is the CC ITF when the CC interception is authorized. The Egress IBCF (with interface 13 and 14) is the CC ITF when the CC interception is authorized.

During the call forwarding phase, Egress IBCF (with interface 18 and 19) is the CC ITF when the CC interception is authorized.

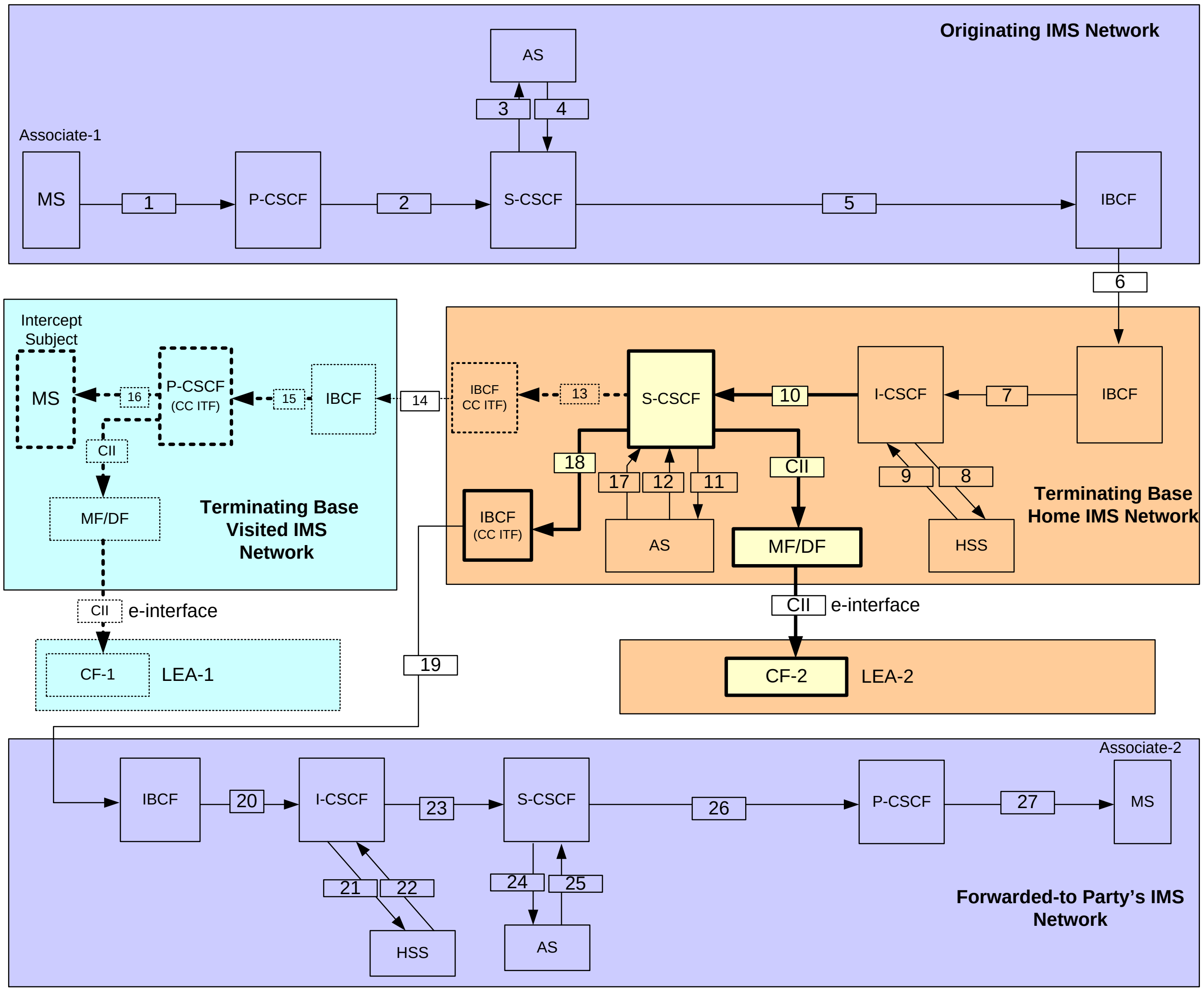


Figure D.21 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS

### D.3.2.2.1.2 IMS to IMS Call Forwarded to PSTN

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 18 for the forwarded leg of the call.

Within the Terminating Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 15 and 16 during the alerting phase of the call.

While the call is being alerted, the P-CSCF in the Terminating Base Visited Network is the CC ITF when the CC interception is authorized. The Egress IBCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, the MGCF is the CC ITF when the CC interception is authorized.

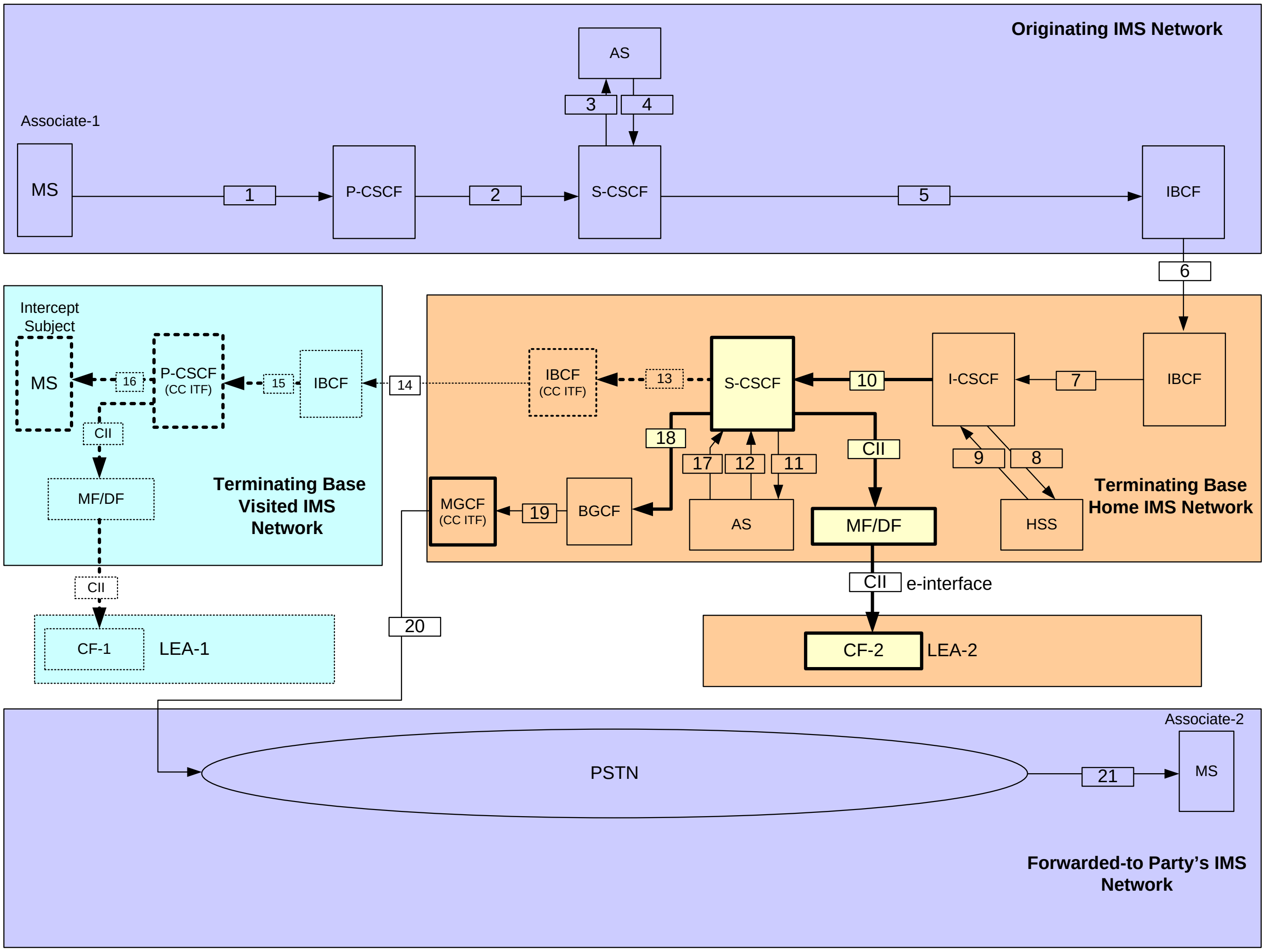


Figure D.22 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to PSTN

### D.3.2.2.1.3 PSTN to IMS Call Forwarded to IMS

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 14 for the forwarded leg of the call.

Within the Terminating Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 11 and 12 during the alerting phase of the call.

While the call is being alerted, the P-CSCF in the Terminating Base Visited Network is the CC ITF when the CC interception is authorized. The IBCF (with interfaces 9 and 10) is the CC ITF when the CC interception is authorized.

During the call forwarding phase, IBCF (with interfaces 14 and 15)  is the CC ITF when the CC interception is authorized.

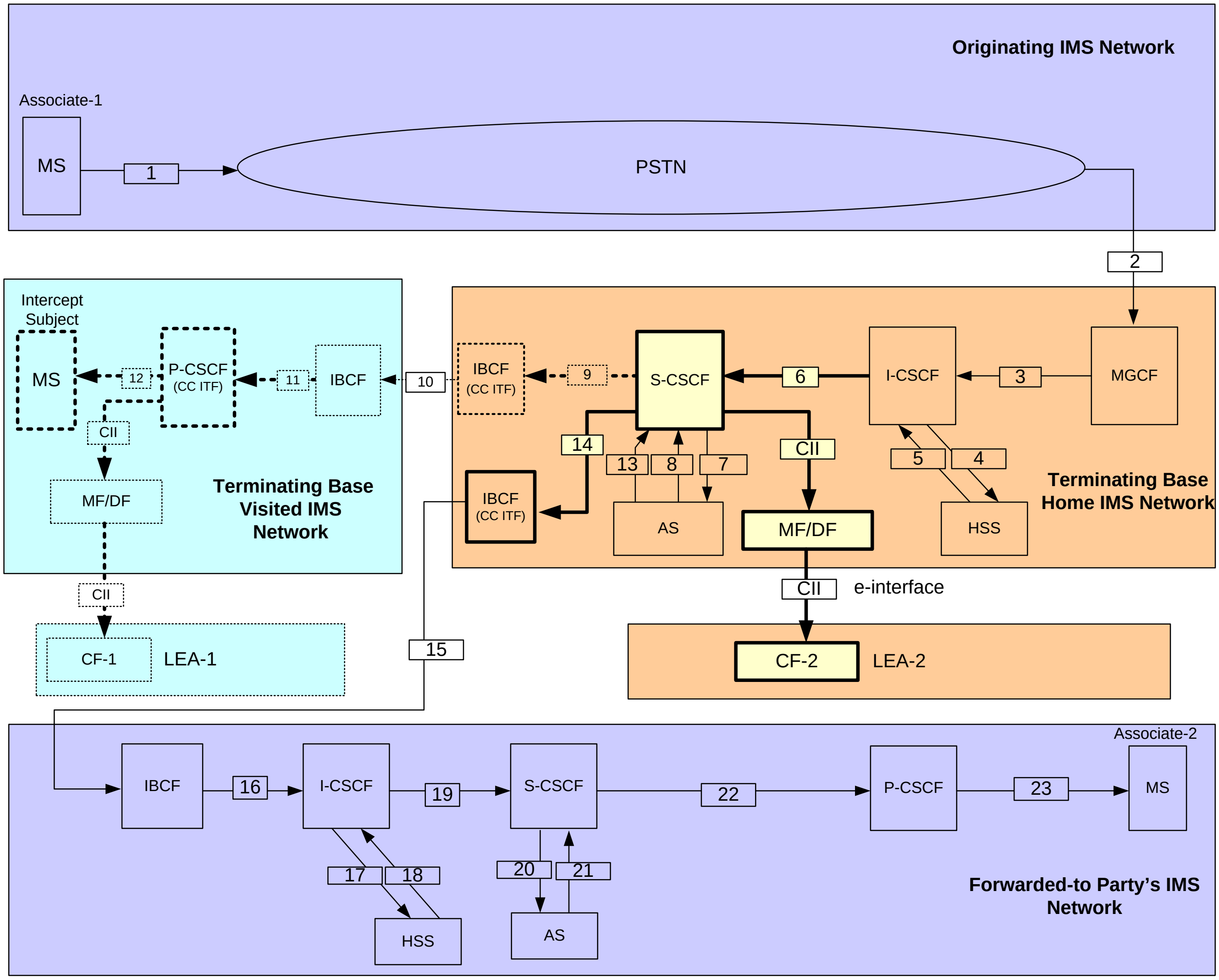


**Figure D.23 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to IMS**

### D.3.2.2.1.4 PSTN to IMS Call Forwarded to PSTN

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 14 for the forwarded leg of the call.

Within the Terminating Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 11 and 12 during the alerting phase of the call.

While the call is being alerted, the P-CSCF in the Terminating Base Visited Network is the CC ITF when the CC interception is authorized. The IBCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, the Egress MGCF is the CC ITF when the CC interception is authorized.

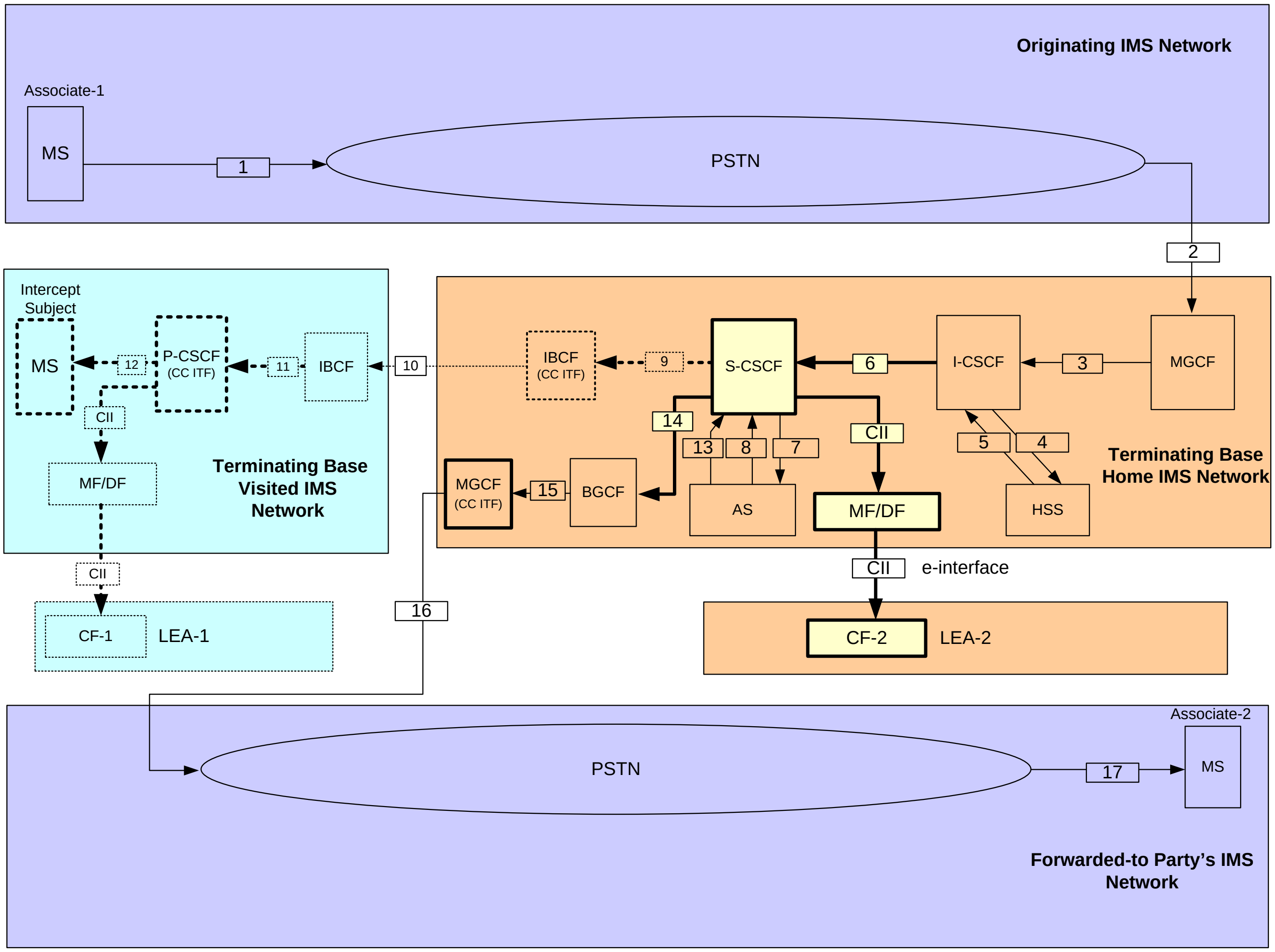


Figure D.24 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to PSTN

### D.3.2.2.2 Only Base Home IMS Network Provider is Served with Lawful Authorization

In this scenario, only the Home IMS network provider of the intercept subject (base IMS user) is served with lawful authorization.

In the Terminating Base Home IMS Network, S-CSCF provides the IAP for the CII.

Since the lawful authorization does not apply to the Terminating Base Visited IMS network provider, the P-CSCF that resides in the Terminating Base Visited IMS network does not provide any IAP for the CII even while the base IMS user (intercept subject) is being alerted.

#### D.3.2.2.2.1 IMS to IMS Call Forwarded to IMS

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 18 for the forwarded leg of the call.

While the call is being alerted, the Egress IBCF (with interfaces 13 and 14) is the CC ITF when the CC interception is authorized.

During the call forwarding phase, Egress IBCF (with interfaces 18 and 19) is the CC ITF when the CC interception is authorized.

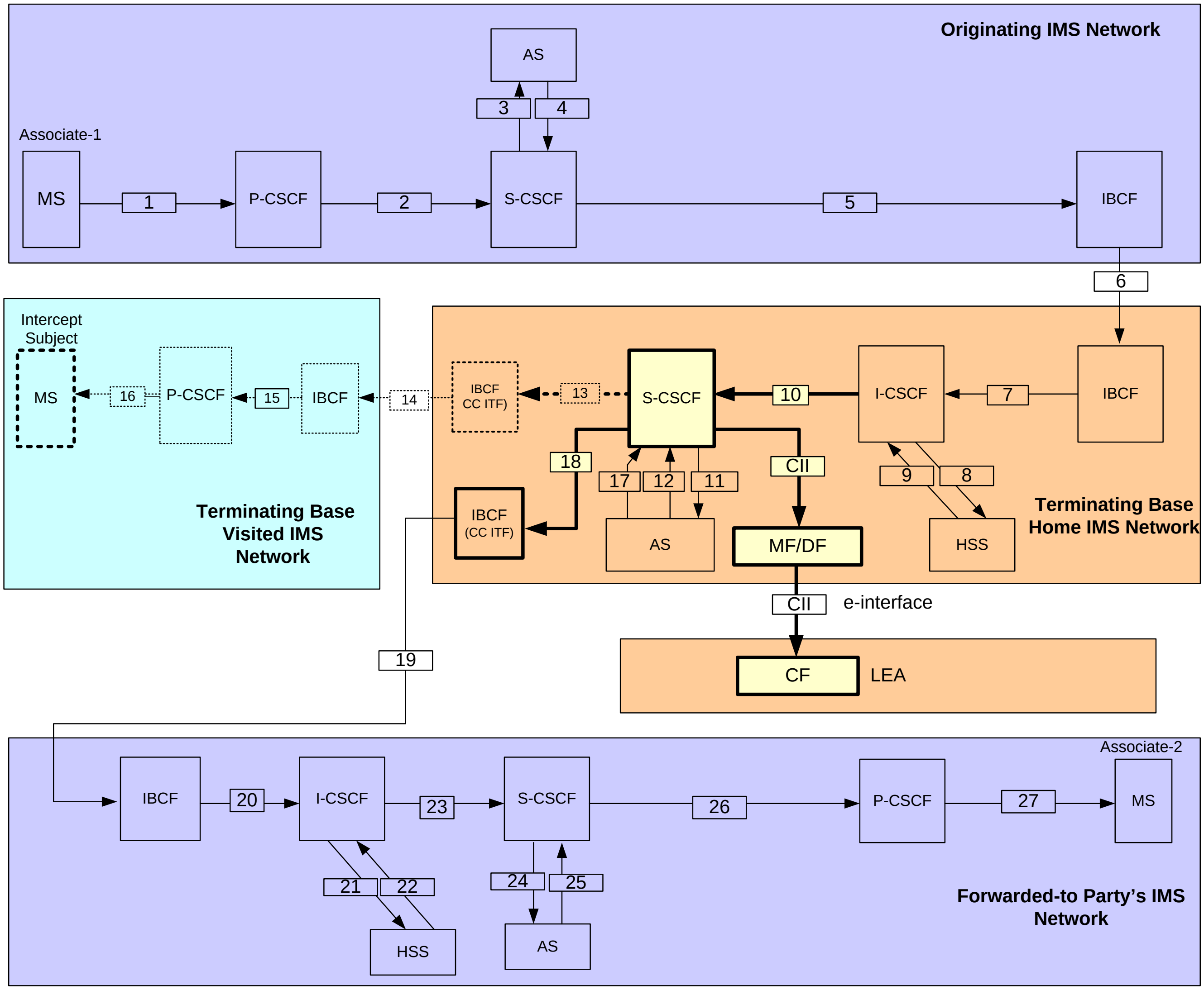


**Figure D.25 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS**

### D.3.2.2.2.2 IMS to IMS Call Forwarded to PSTN

In this scenario, an incoming call from an IMS user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on Interface 10 and 13 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 10 and 18 for the forwarded leg of the call.

While the call is being alerted, the Egress IBCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, MGCF is the CC ITF when the CC interception is authorized.

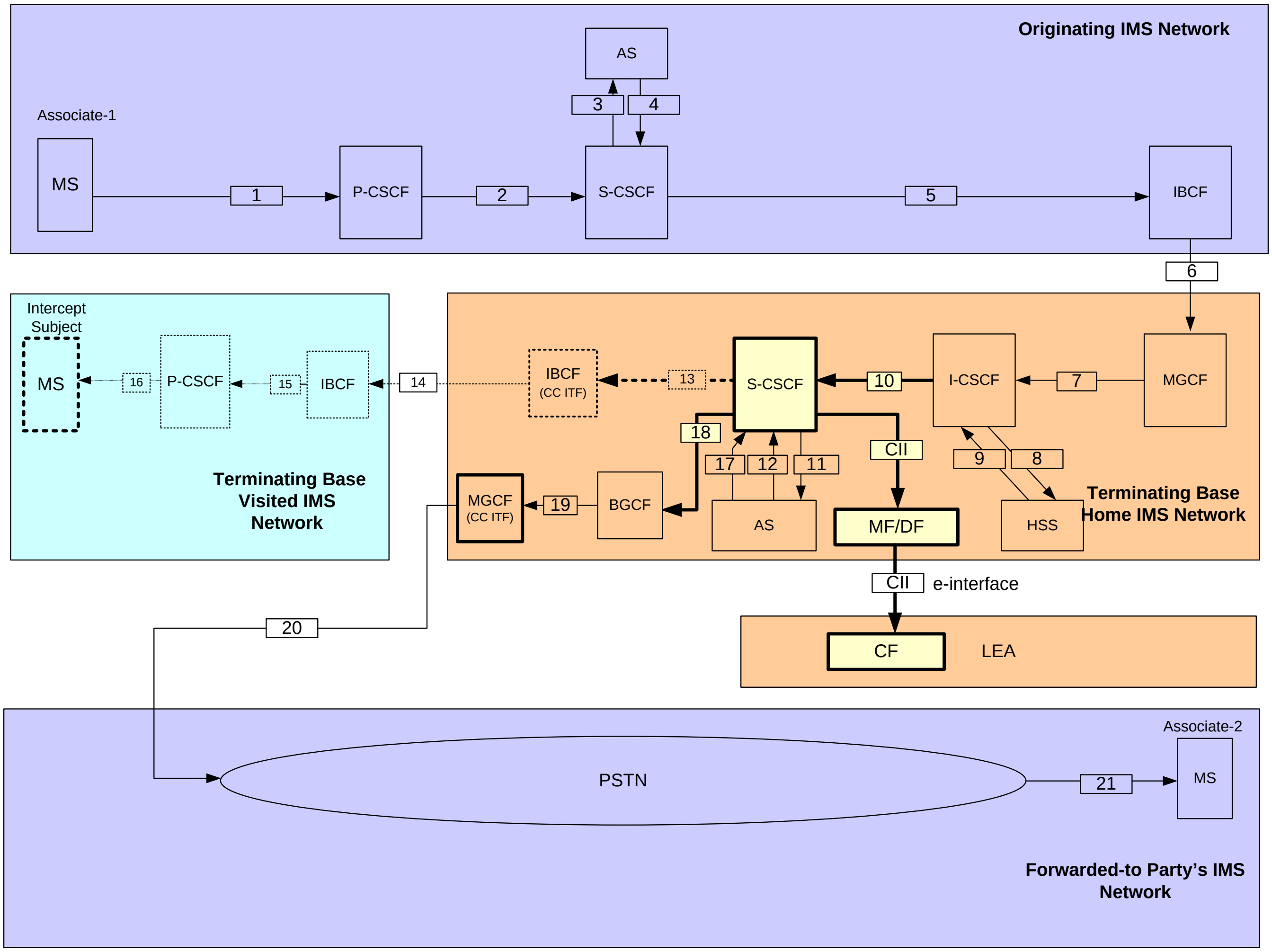


Figure D.26 – Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to PSTN

### D.3.2.2.2.3 PSTN to IMS Call Forwarded to IMS

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to another IMS user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 14 for the forwarded leg of the call.

While the call is being alerted, the IBCF (with interfaces 9 and 10) is the CC ITF when the CC interception is authorized.

During the call forwarding phase, IBCF (with interfaces 14 and 15) is the CC ITF when the CC interception is authorized.

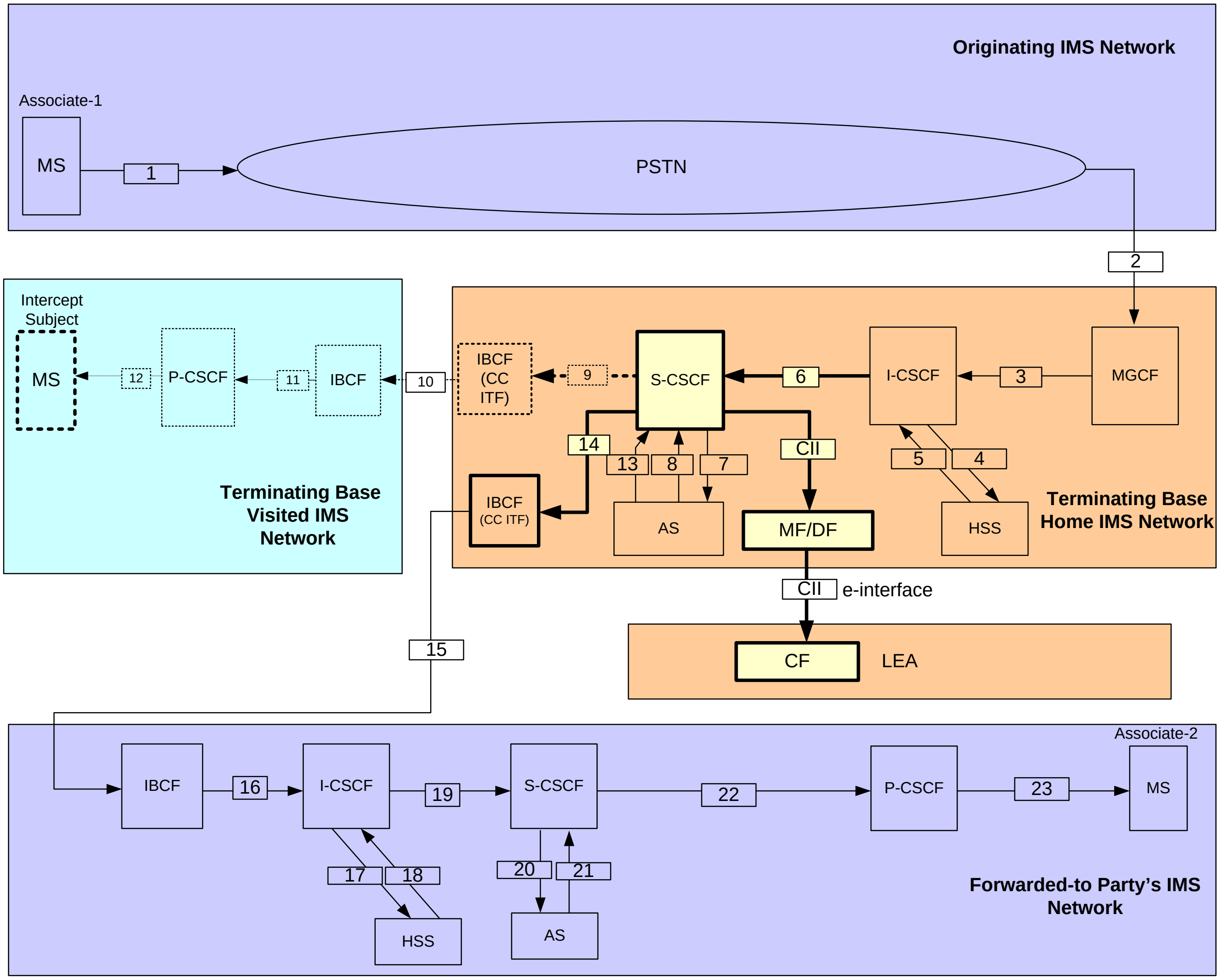


**Figure D.27 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to IMS**

### D.3.2.2.2.4 PSTN to IMS Call Forwarded to PSTN

In this scenario, an incoming call from a PSTN user (Associate-1) to the intercept subject (base IMS user) is forwarded to a PSTN user (Associate-2).

Within the Terminating Base Home IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The same S-CSCF delivers the SIP messages sent and received on the Interface 6 and 14 for the forwarded leg of the call.

While the call is being alerted, the IBCF is the CC ITF when the CC interception is authorized.

During the call forwarding phase, the Egress MGCF is the CC ITF when the CC interception is authorized.

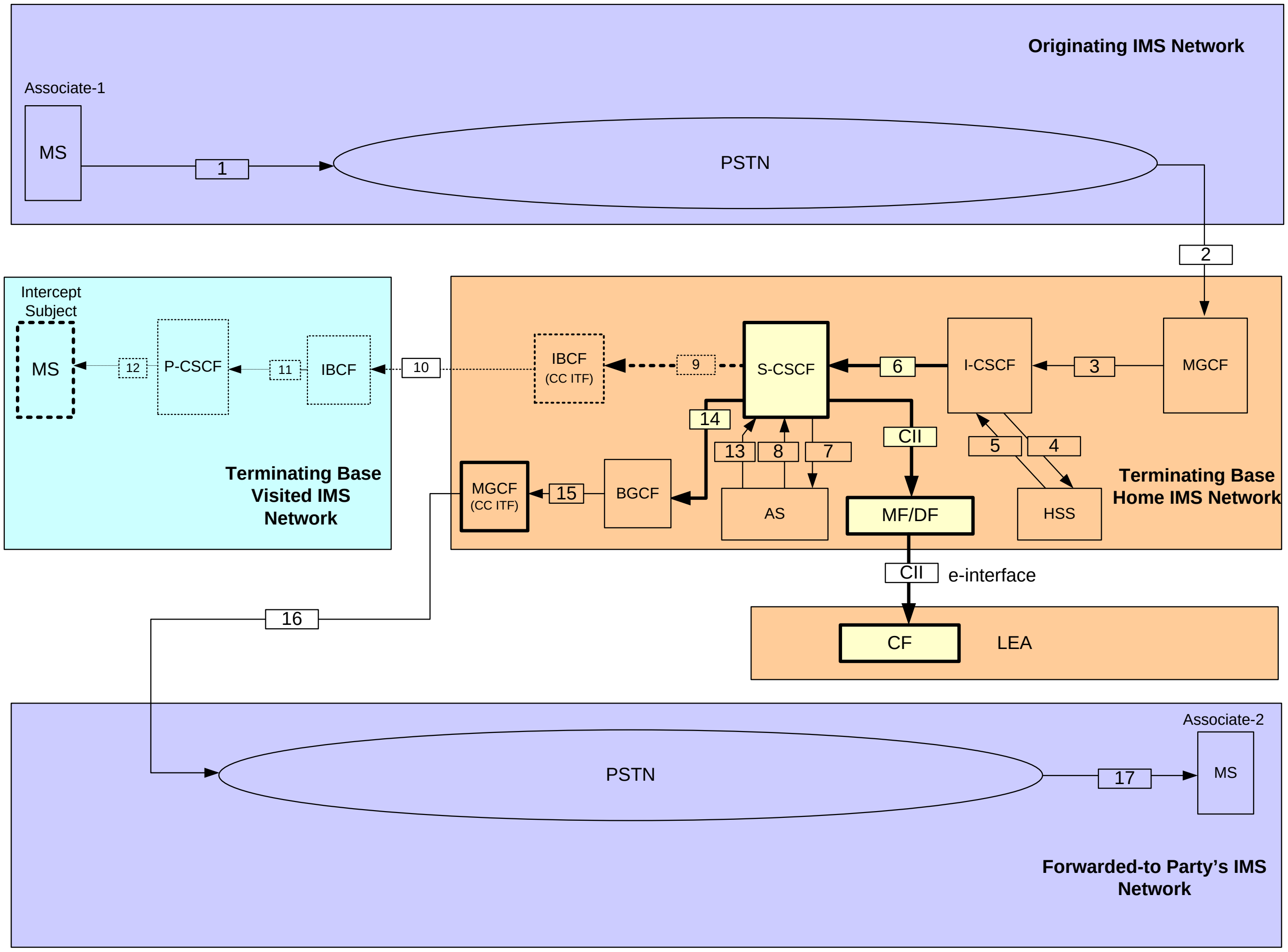


**Figure D.28 – Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to PSTN**

## D.4 Local Breakout with Loopback

An IMS subscriber is roaming while served by a Network that is different from the Home Network of that IMS subscriber. Local Breakout (LBO) is one of the roaming architectures of IMS-based VoIP calls. With LBO, the P-CSCF is in the visited network. Two routing options are available for calls originated by the roaming IMS subscriber with LBO approach.

- Home Network Routed
- Visited Network Routed

In the Home Network Routed case, Home Network routes the calls originated by the roaming IMS subscriber to the destination. The network signaling flow diagrams for these cases are same as the ones shown in clause D.1.2.

In the Visited Network Routed case, Home Network loops back the call to the Visited Network unless the called party belongs to the same Home Network and the Visited Network routes the call to the actual destination.

Three cases are presented for calls originated from roaming Intercept Subject:

- Called Party belongs to another IMS network.
- Called Party belongs to PSTN.
- Called Party belongs to in the same Visited Network where the Intercept Subject is roaming.

For each of the three cases, two scenarios are presented:

- Scenario 1: Both network providers are served with lawful authorization(s).
- Scenario 2: Only the Home IMS network provider is served with the lawful authorization.

Note that it is also possible to have a scenario where only the visited IMS network provider is served with the lawful authorization. In this scenario, since the lawful authorization is not applicable to the Home IMS network provider of the intercept subject, the S-CSCF of the Home IMS network will not provide any IAP for the CII.

## A.1.1. Called Party Belongs to Another IMS Network

The two scenarios considered here are for the case where the called party belongs to another IMS network (i.e., an intercept subject (IMS user) originates a call to another IMS user served by an IMS network that is neither the Home Network of the Intercept Subject nor the Visited Network where the Intercept Subject is roaming.

**Scenario 1**

In this scenario both the Visited IMS network provider and the Home IMS network provider are served with lawful authorization(s).

In the Originating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

In the Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 1 and 2. The P-CSCF is the CC ITF when the CC interception is authorized.

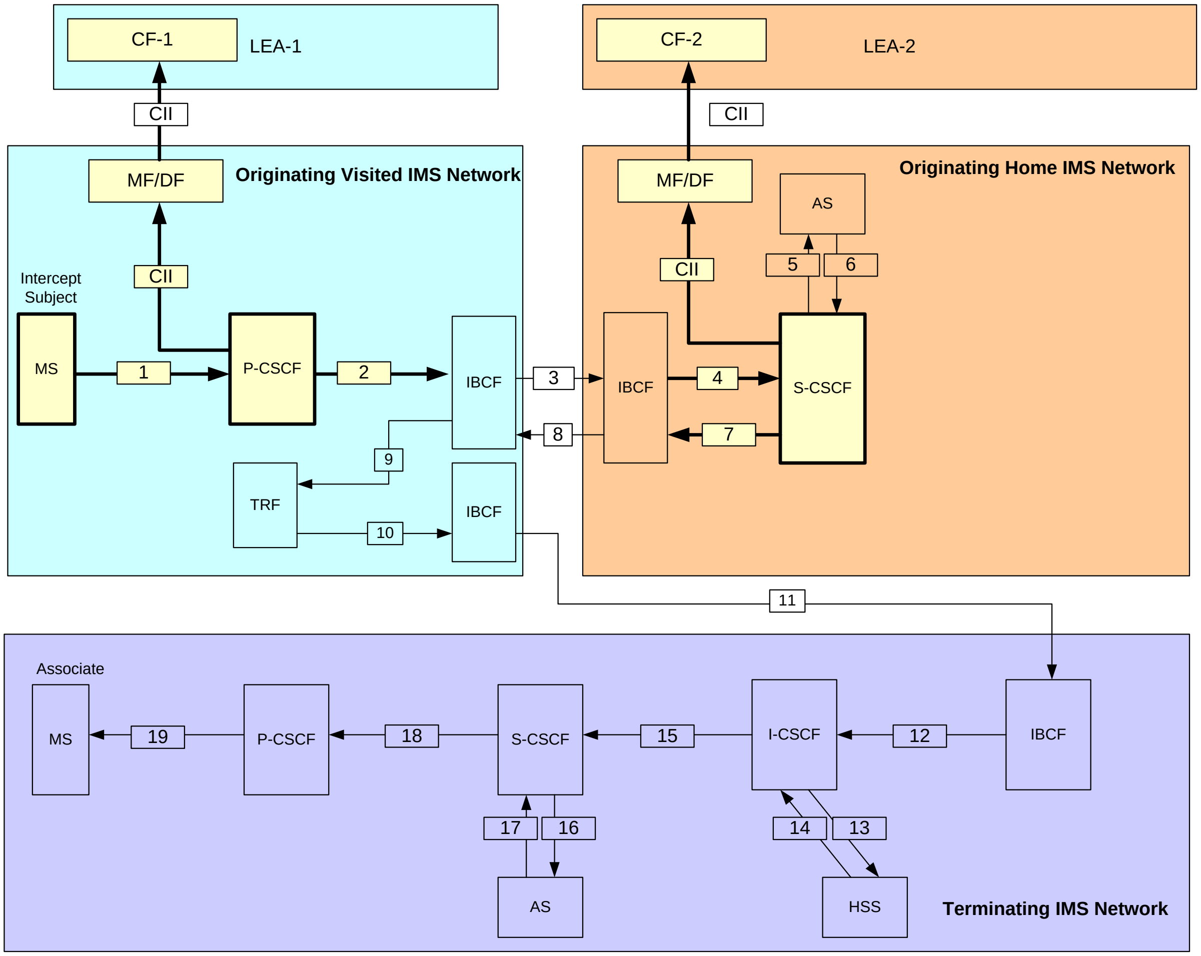


**Figure D.29 – LBO with Loopback, called party is from another IMS network – Scenario 1**

### Scenario 2

In this scenario only the Home IMS network provider of the Intercept Subject is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7.  Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

Since the lawful authorization does not apply to the visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

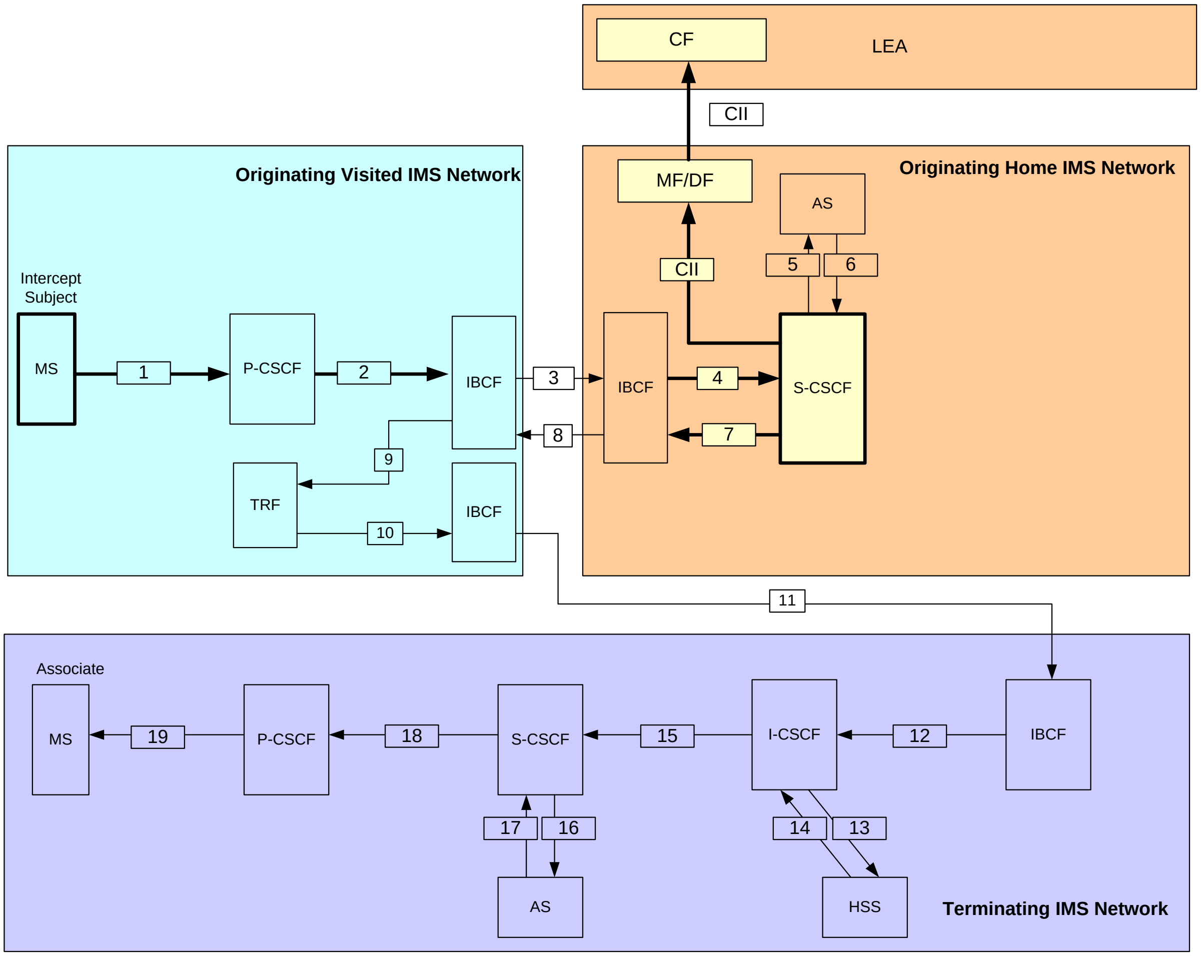


Figure D.30 – LBO with Loopback, called party is from another IMS network – Scenario 2

## D.4.2 Called Party Belongs to PSTN

The two scenarios considered here are for the case where the called party belongs to PSTN (i.e., an intercept subject [IMS user] originates a call to a user served in the PSTN).

### Scenario 1

In this scenario both the Visited IMS network provider and the Home IMS network provider are served with lawful authorization(s).

In the Originating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

In the Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 1 and 2. The P-CSCF is the CC ITF when the CC interception is authorized.

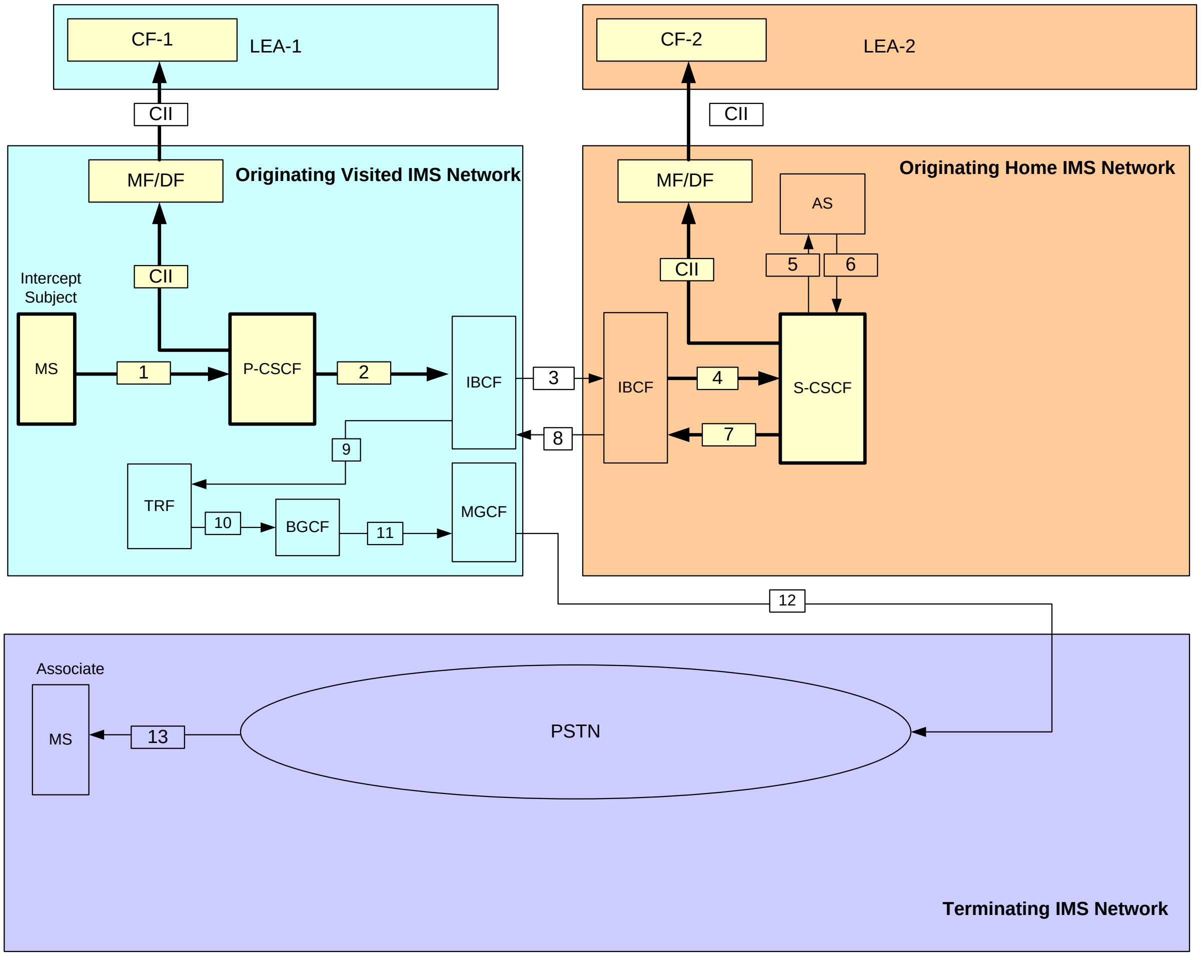


**Figure D.31 – LBO with Loopback, called party is from PSTN – Scenario 1**

### Scenario 2

In this scenario only the Home IMS network provider of the Intercept Subject is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

Since the lawful authorization does not apply to the visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

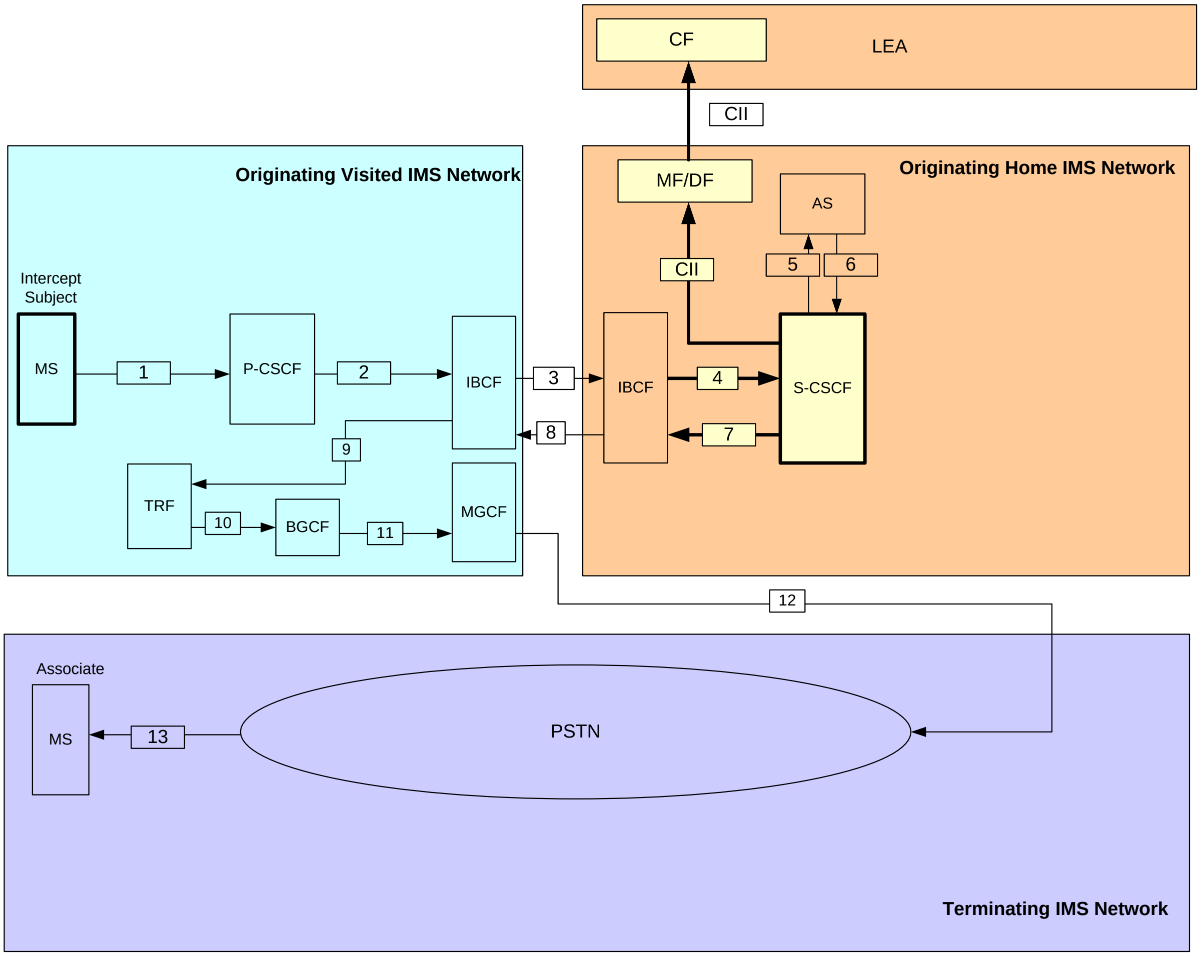


**Figure D.32 – LBO with Loopback, called party is from PSTN – Scenario 2**

## D.4.3 Called Party Belongs to Visited IMS Network

The two scenarios considered here are for the case where the called party belongs to the same Visited IMS network where the Intercept Subject is current roaming (i.e., an intercept subject [IMS user] originates a call to another IMS user served by the IMS network that is the Visited Network where the Intercept Subject is roaming).

### Scenario 1

In this scenario both the Visited IMS network provider and the Home IMS network provider are served with lawful authorization(s).

In the Originating Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7. Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

In the Visited IMS network, the P-CSCF provides the IAP for the CII. The P-CSCF delivers the SIP messages sent and received on the Interface 1 and 2. The P-CSCF is the CC ITF when the CC interception is authorized.

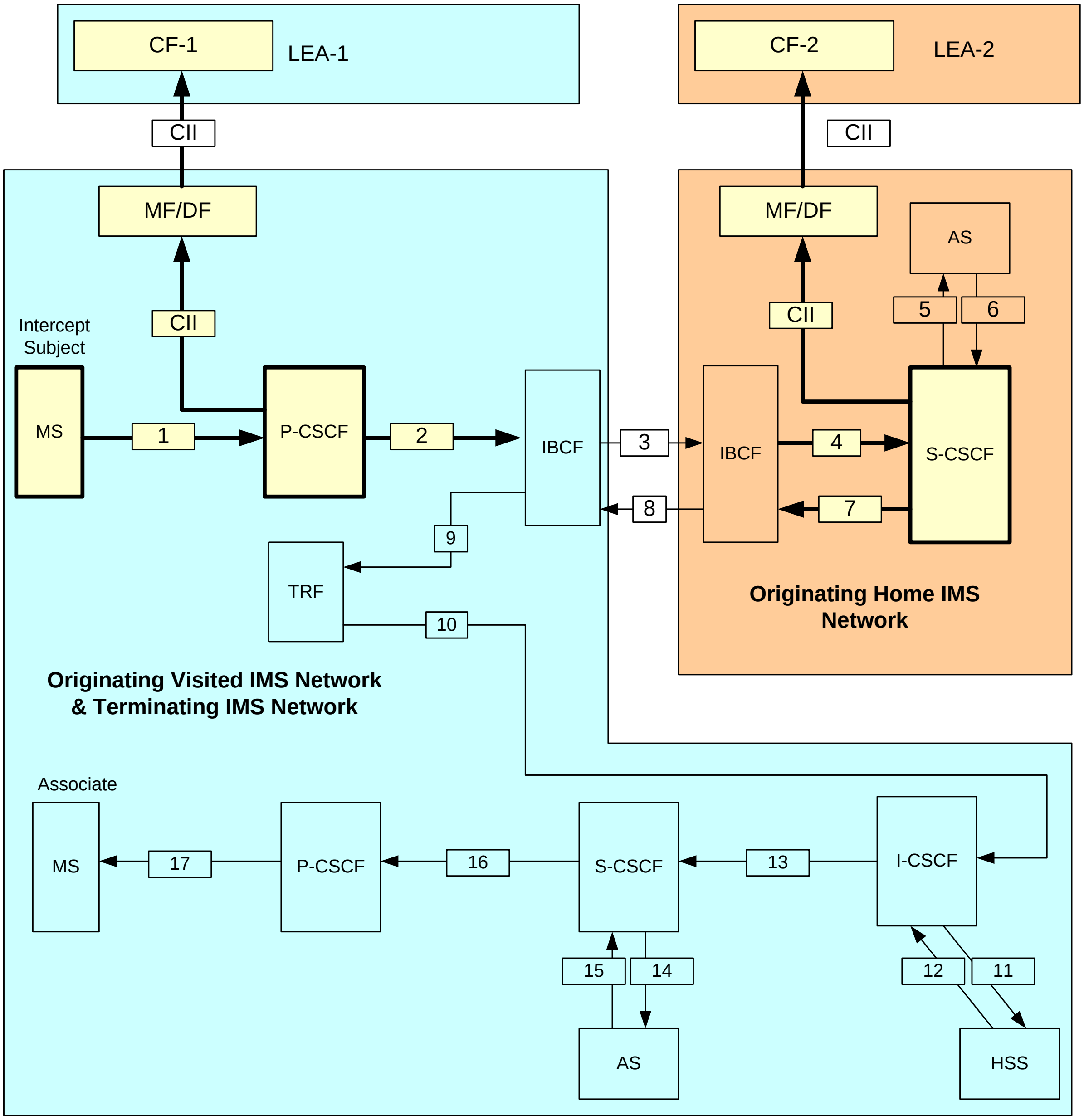


**Figure D.33 – LBO with Loopback, called party in Visited IMS network – Scenario 1**

### Scenario 2

In this scenario only the Home IMS network provider of the Intercept Subject is served with lawful authorization. The S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 4 and 7.  Since the media does not enter the Originating Home IMS Network, media interception is not possible and hence, there is no CC delivery. Originating Home IMS Network sends CC Unavailable message to the LEA-2 when the CC interception is authorized.

Since the lawful authorization does not apply to the visited IMS network provider, the P-CSCF that resides in the visited IMS network does not provide any IAP for the CII.

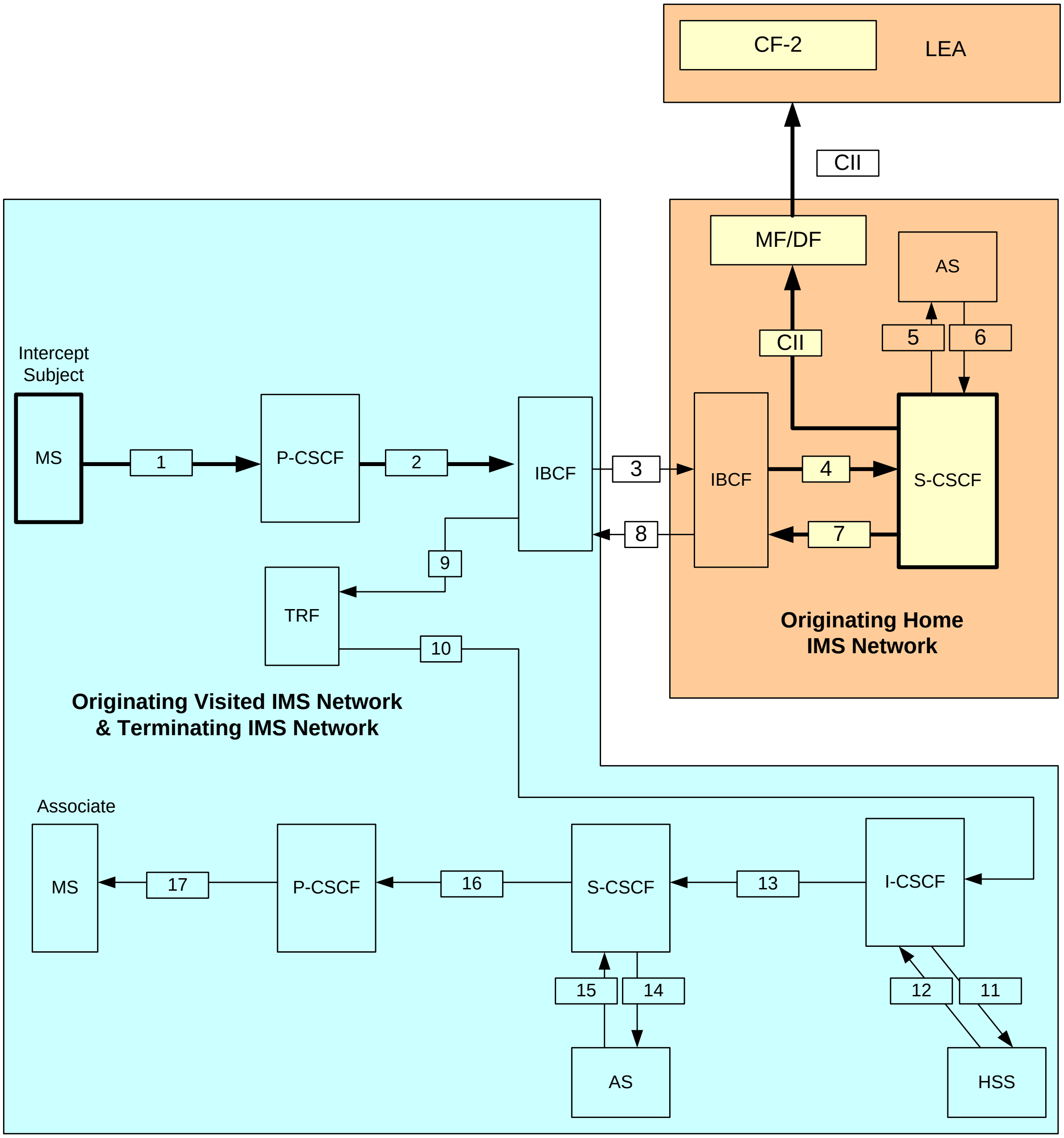


**Figure D.34 – LBO with Loopback, called party in Visited IMS network – Scenario 2**

**Annex E**

(Informative)

# E IMS 3GPP VoIP LI Implementation Options

There are various ways to implement the LAES solution defined in this ATIS Standard. The three options below are IMS 3GPP VoIP implementation options:

- Option 1: When a 3GPP DF is integrated into an IAP, then a MF/DF can be provided in addition to the existing integrated 3GPP DF to achieve an “ATIS-0700005” solution.
- Option 2: When a 3GPP DF is not integrated into the IAP, a MF/DF can be provided in addition to the existing standalone 3GPP DF to achieve an “ATIS-0700005” solution. Whether or not this MF/DF is physically separated or integrated with the existing 3GPP DF is an implementation issue.
- Option 3: It is possible to provide a MF/DF for producing “ATIS-0700005” solution without a 3GPP DF.

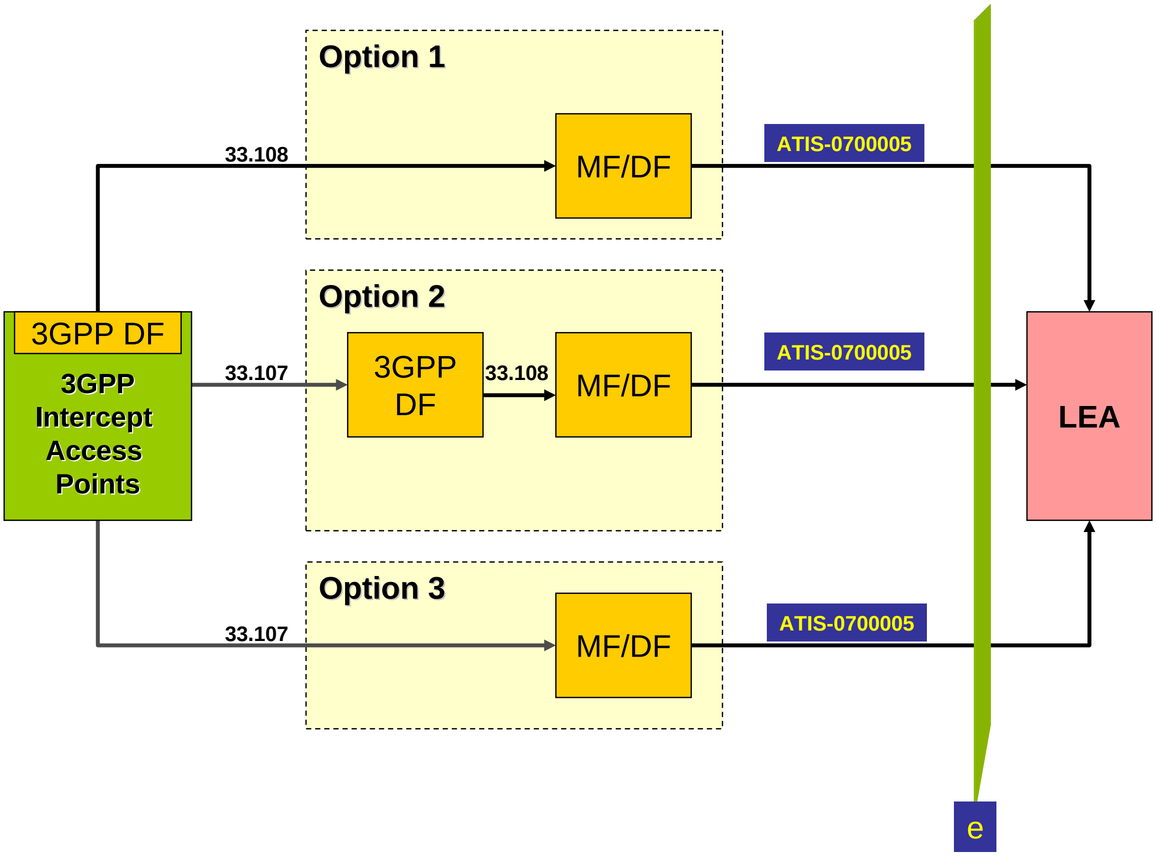


**Figure E.1 – Examples of IMS-based VoIP Implementation Options**

## *E.1 Support of 3GPP Interfaces*

This ATIS Standard supports 3GPP X2, X3, and Handover Interfaces (HI) interfaces as defined in [107] and [108]. The following are out of scope of this ATIS Standard:

- The specification of the DF2 and DF3 Delivery Functions.
- The specification of the information sent over a “d” interface.
- The specification of the X2 IRI, X3 CC and the HI2 IRI, HI3 CC.

### E.1.1 Support for X2 & X3 Interfaces

Figure E.2 shows support in a CII MF and CC MF for the mapping of the IRI and  CC delivered over the X2 and X3  ”d” interface. The resulting mapped CII and CC are delivered over an “e” interface to the LEA Collection Function (CF).  The IRI and CC delivered over this ”d” interface are based on [107] to support the mapping to the CII and the CC delivered to the LEA CF over the “e” interface.

NOTE: [107] may not specify all the necessary information for mapping of the CII and CC for delivery to the LEA CF.

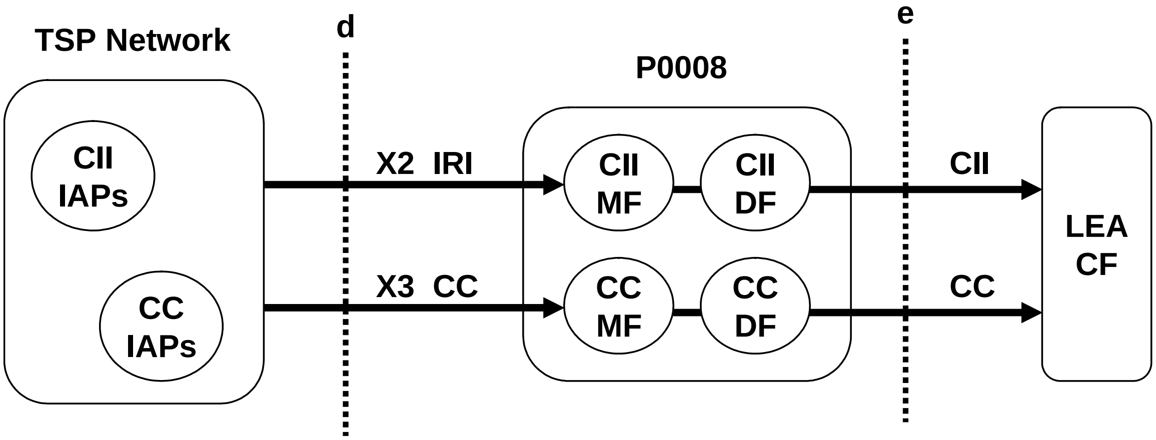


Figure E.2 – Support for X2 and X3 Interfaces

### E.1.2 Support for Handover Interfaces (HI)

Figure E.3 shows support in a CII MF and CC MF for the mapping of the HI2 IRI and HI3 CC, delivered over a “d” interface. The resulting mapped CII and CC are delivered over an “e” interface to the LEA CF.  The IRI and CC delivered over this “d” interface is based on [108] to support the mapping of the CII MF and CC MF. The DF2 and DF3 may be incorporated within the TSP network elements.

NOTE: [108] may not specify all the necessary information for mapping of the CII and CC for delivery to the LEA CF.

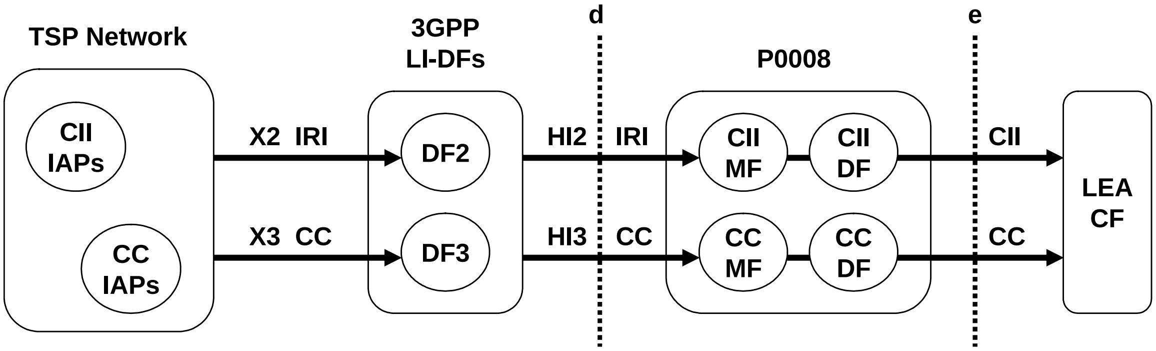


Figure E.3 – Support for Handover Interfaces (HI)

**Annex F**

(Informative)

# F CC IAPs and VoIP Call Scenarios

This informative annex provides a list of potential CC IAPs for various call scenarios of VoIP.

Table F.1 provides a list for when the originating party is the Intercept Subject and Table F.2 provides a list for when the terminating party is the Intercept Subject.

The following notations used in presenting the list within the tables:

O: Originating

T: Terminating

F: Forwarding

Home: The IMS subscriber is in the home network (non IMS roaming).

Visited: The IMS subscriber is in the visited network (IMS roaming).

IMS Domain: The IMS subscriber is in another TSP's network.

CS Domain: The CS subscriber is in another TSP's network.

For example:

Home (O): The call is originated from an IMS subscriber in the home network.

Home (T): The call is terminated to an IMS subscriber in the home network.

Home (F): The call is forwarded to an IMS subscriber in the home network.

Visited (O): The call is originated from an IMS subscriber in a visited network.

Visited (T): The call is terminated to an IMS subscriber in a visited network.

Visited (F): The call is forwarded to an IMS subscriber in a visited network.

IMS Domain (O): The call is originated from an IMS subscriber in another TSP's network.

IMS Domain (T): The call is terminated to an IMS subscriber in another TSP's network.

Visited (T), Home (F): The call is terminated to an IMS subscriber who is in the visited network, but the call is forwarded to another IMS subscriber in the home network.

Visited (T), Visited (F): The call is terminated to an IMS subscriber who is in the visited network, and the call is forwarded to another IMS subscriber who is also in a visited network.

Visited (T), IMS Domain (F): The call is terminated to an IMS subscriber who is in the visited network, but the call is forwarded to another IMS subscriber in another TSP's home network.

Visited (T), CS Domain (F): The call is terminated to an IMS subscriber who is in the visited network, but the call is forwarded to CS subscriber in another TSP's home network.

The columns of the table represent various cases of call origination points and the rows of the table represent various cases of call termination points. The entry within the table identifies the network node that performs the actual CC interception for the call scenario. The entries of the table should be read as explained below:

IP-CAN/IMS-AGW: Either a network node in IP-CAN (PDN-GW or GGSN) or IMS-AGW performs the CC interception. The CC intercept trigger is sent by the P-CSCF. For IP-CAN (PDN-GW or GGSN), the CC intercept trigger is sent by the P-CSCF via the PCRF.

TrGW: TrGW performs the CC interception. The CC intercept trigger is sent by IBCF.

IM-MGW: IM-MGW performs the CC interception and the CC intercept trigger is sent by the MGCF.

## *F1. Originating Party is the Intercept Subject*

Table F.1 gives a potential list of IAPs when an Intercept Subject originates the call.

**Table F.1 – Originating Party is the Intercept Subject**

| **Term ↓; Orig →** | Home (O) | Visited (O) | IMS Domain (O) | CS Domain (O) |
|---|---|---|---|---|
| Home (T) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| Visited (T) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| IMS Domain (T) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| CS Domain (T) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| Home (F) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| Visited (F) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| IMS Domain (F) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| CS Domain (F) | IP-CAN/IMS-AGW | TrGW (Note 1) | Originating TSP | Originating TSP |
| Visited (T), Home (F) | IP-CAN/IMS-AGW | TrGW (Note 1 | Originating TSP | Originating TSP |
| Visited (T), Visited (F) | IP-CAN/IMS-AGW | TrGW (Note 1 | Originating TSP | Originating TSP |
| Visited (T), IMS Domain (F) | IP-CAN/IMS-AGW | TrGW (Note 1 | Originating TSP | Originating TSP |
| Visited (T), CS Domain (F) | IP-CAN/IMS-AGW | TrGW (Note 1 | Originating TSP | Originating TSP |

NOTE: If the Visited TSP has an intercept order, then IP-CAN/IMS-AGW within the Visited TSP provides the CC interception for calls that originated from the Intercept Subject. P-CSCF within the Visited TSP provides the CII interception for calls originated from the Intercept Subject.

## *F.2 Terminating Party is the Intercept Subject*

Table F.2 gives a potential list of IAPs when an Intercept Subject receives a call.

**Table F.2 – Terminating Party is the Intercept Subject**

| **Term ↓; Orig →** | Home (O) | Visited (O) | IMS Domain (O) | CS Domain (O) |
|---|---|---|---|---|
| Home (T) | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW |
| Visited (T) | TrGW (Note 2) | TrGW (Note 2) | TrGW (Note 2) | TrGW (Note 2) |
| IMS Domain (T) | Terminating TSP | Terminating TSP | Terminating TSP | Terminating TSP |
| CS Domain (T) | Terminating TSP | Terminating TSP | Terminating TSP | Terminating TSP |
| Home (F) | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW |

| | | | | |
|---|---|---|---|---|
| Visited (F) | TrGW | TrGW | TrGW | TrGW |
| IMS Domain (F) | TrGW | TrGW | TrGW | TrGW |
| CS Domain (F) | IM-MGW | IM-MGW | IM-MGW | IM-MGW |
| Visited (T), Home (F) | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW | IP-CAN/IMS-AGW |
| Visited (T), Visited (F) | TrGW | TrGW | TrGW | TrGW |
| Visited (T), IMS Domain (F) | TrGW | TrGW | TrGW | TrGW |
| Visited (T), CS Domain (F) | IM-MGW | IM-MGW | IM-MGW | IM-MGW |

NOTE: If the Visited TSP has an intercept order, then IP-CAN/IMS-AGW within the Visited TSP provides the CC interception for calls that terminated to the Intercept Subject. P-CSCF within the Visited TSP provides the CII interception for calls terminated to the Intercept Subject.

**Annex G**

(Informative)

# G Stage 2 Call Flows

## G.1 Introduction

All the call flows assume that the interception is Title III (i.e., CII + CC) and illustrate that the CC delivery begins once the SDP offer and answer is completed (i.e., when the media bearer is setup). In all the call flows, the first reliable response is SIP 200 OK.

In all the call flows unless specifically illustrated differently, the originating end of the call sends the SDP offer and terminating end gives the SDP answer. Since the first reliable response is SIP 200 OK, the SDP answer is always given in the SIP 200 OK message.

The call flows do not show the method used for correlating the CII with CII and CII with CC. It is presumed that those are stage 3 details and these are stage 2 call flows.

All the call flows assume the presence of a Voice Application Server (shown as AS) that provides the voice services like digit translation, invoking the call forwarding, etc,

CII in the visited TSP is intercepted by the P-CSCF and CII in the home TSP is intercepted by the S-CSCF.

The call flows show that CC interception is done at the IP-CAN (and it should be interpreted to mean that the interception is done in the PDN-GW or GGSN depending on the packet core network), or at the TrGW or at the IM-MGW. The other possible CC interception options (e.g., IMS-AGW) are not shown, but follow a similar approach as in the case of IP-CAN scenarios. In the call flows that illustrate the conference steps, interception of CC of a conference call is done at the MRFP. Also, in the call flows that illustrate the conference steps, the AS/MRFC provide the CII that indicate when a party is joined to a conference or dropped from a conference.

Not all the functional elements are shown in the call flows. For example, the call flows do not show I-CSCF, HSS, PCRF.

All the call flows show a summary of SIP messages that are delivered to the LEA (not all SIP messages are shown).

## G.2 Call Originations from Subject in Home TSP

There are two call flows shown here. In the first flow, the Subject dials Party_B and in the second flow, the Subject dials a Special Number (e.g., speed call number or an 800-number) which is translated to Party_B’s number.

## G.2.1 Call Originations from Subject with Destination Number

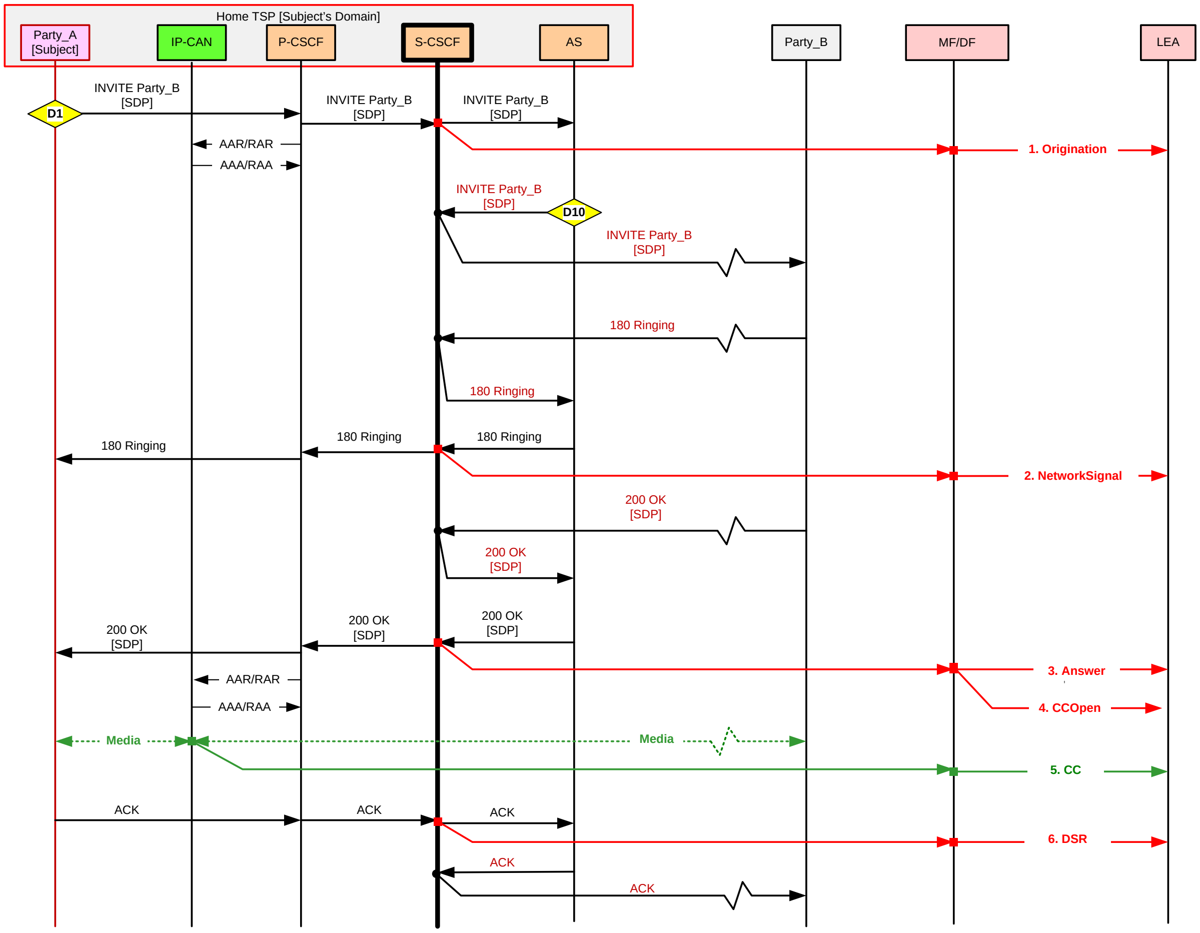


**Figure G.1 – Call Origination from Subject with Destination Number**

Description of LAES Events

1. The SIP INVITE received from the Subject's device is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field.
2. The SIP 180 Ringing sent to the Subject's device is mapped to a LAES NetworkSignal message with an indication that network has initiated the originating Subject's device to apply AudibleSignal (ringback tone).
3. The SIP 200 OK (to SIP INVITE) sent to the Subject's device is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study.
4. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the far end subscriber), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
5. At this time, the P-CSCF would have sent a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) and the PDN-GW/GGSN would start intercepting the media and send the same to the LEA via MF/DF as CC.
6. The ACK message received from the Subject's device is reported within the DSR message to the LEA.

## G.2.2 Call Originations from Subject with Special Number

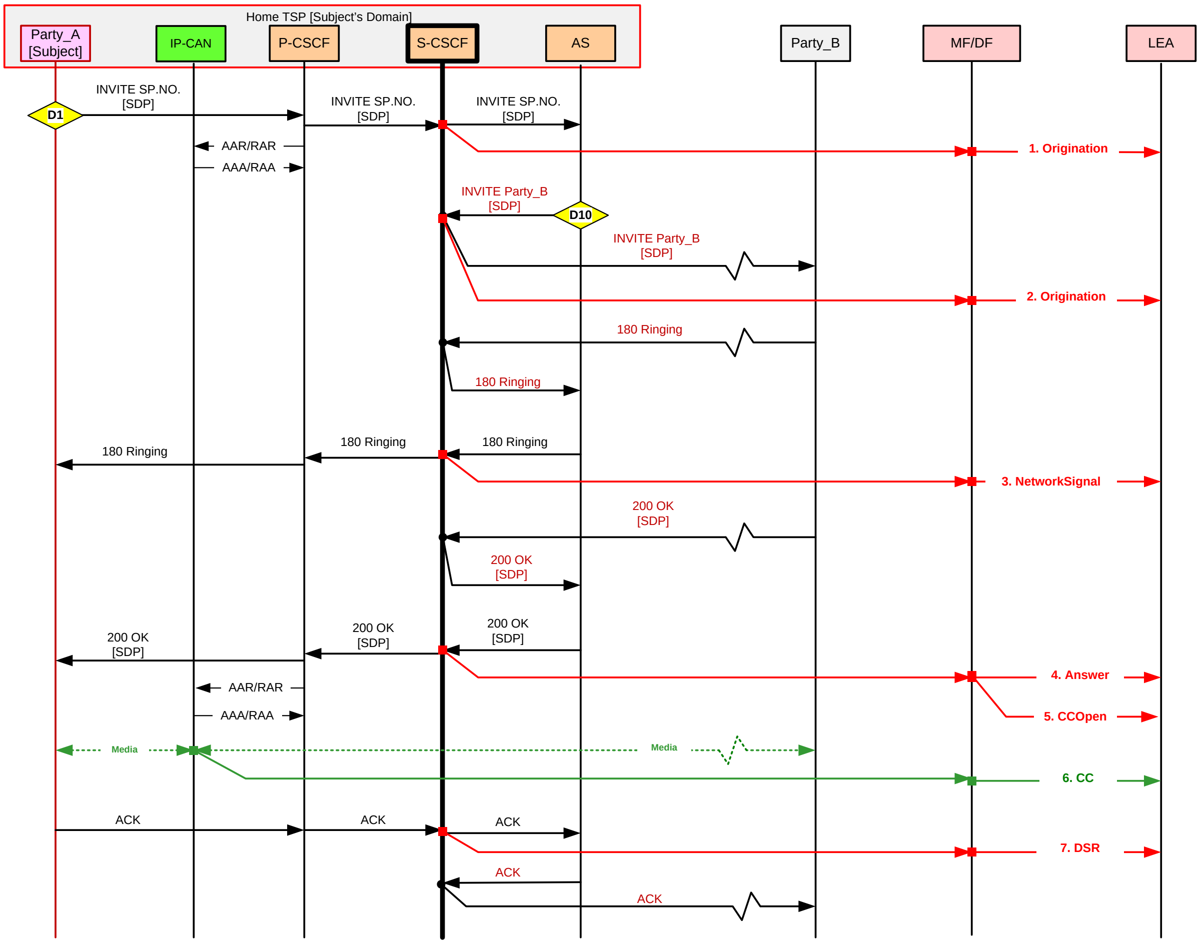


**Figure G.2 – Call Origination from Subject with Special Number**

Description of LAES Events

1. The SIP INVITE received from the Subject's device is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field.
2. The SIP INVITE sent to the destination is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field. Note that called party identity sent in this Origination message is different from the called party identity sent in the Origination message of step 1.
3. The SIP 180 Ringing sent to the Subject's device is mapped to a LAES NetworkSignal message with an indication that network has initiated the originating Subject's device to apply AudibleSignal (ringback tone).
4. The SIP 200 OK (to SIP INVITE) sent to the Subject's device is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study.
5. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the far end subscriber), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
6. At this time, the P-CSCF would have sent a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) and the PDN-GW/GGSN starts intercepting the media and send the same to the LEA via MF/DF as CC.
7. The ACK message received from the Subject's device is reported within the DSR message to the LEA.

## *G.3 Call Terminations to Subject – Home TSP*

There is one call flow shown here. The Subject receives an incoming call (also referred to as terminating call) from Party_A.

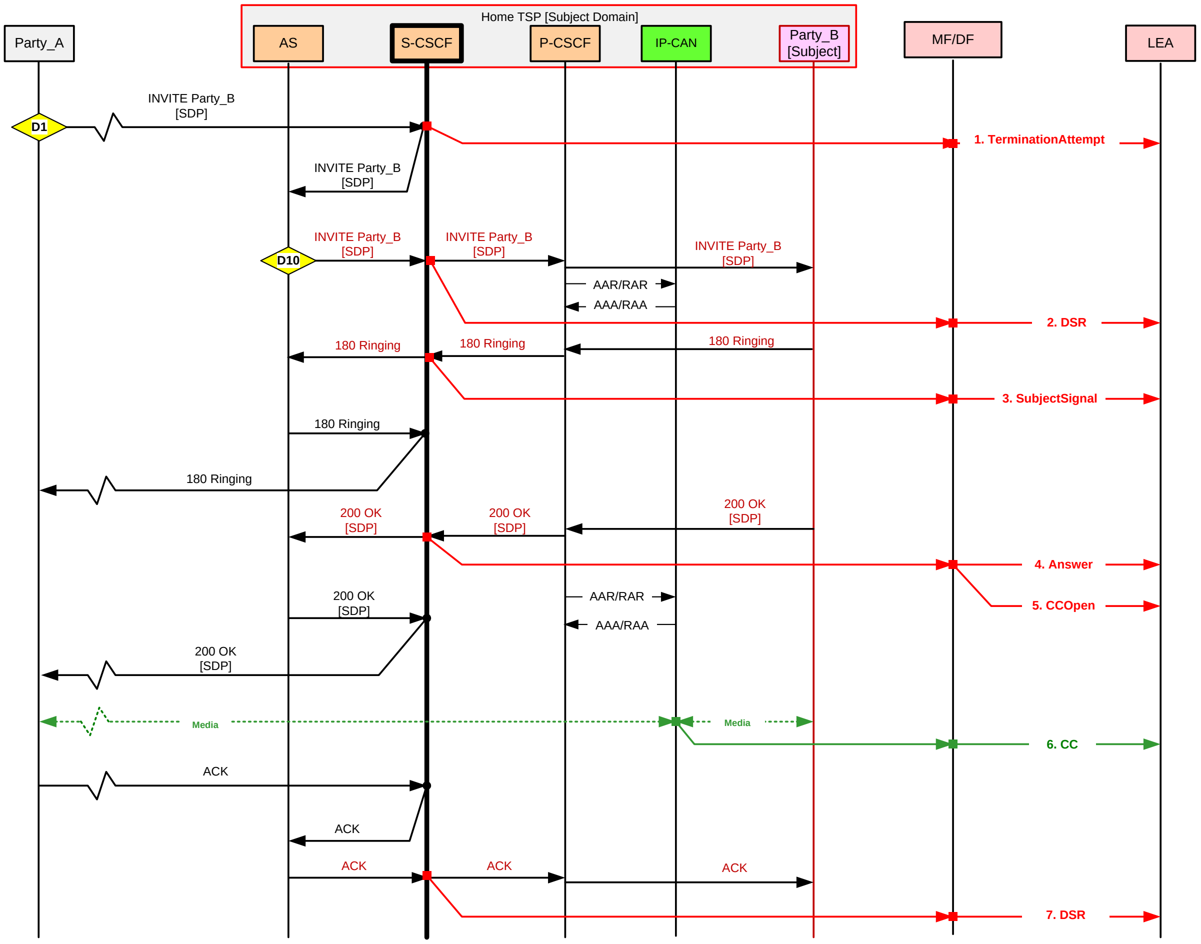


**Figure G.3 – Call Termination to Subject -- Home TSP**

<u>Description of LAES Events</u>

1. The SIP INVITE received at the S-CSCF from the far end (originating side) is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. This is an optional step. 3GPP TS 33.107 does not show the sending of this message to the LEA. If implemented, in this step, the SIP INVITE sent to Subject's device is encapsulated in a DSR message and sent to the LEA.  Since a TerminationAttempt was already sent to the LEA (in step 1), this SIP INVITE is sent to the LEA as a DSR message.
3. The SIP 180 Ringing received from the subject's device is mapped to a LAES SubjectSignal message with an indication that the network has received a "180 Ringing" from the Subject's device.
4. The SIP 200 OK (to SIP INVITE) received from the Subject's device is mapped to a LAES Answer message.  There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity, which is an optional field in the LAES Answer message, is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the Subject's device as answering party identity.

5. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of Subject's device), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
6. At this time, the P-CSCF would have sent a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) and the PDN-GW/GGSN starts intercepting the media and sends the same to the LEA via MF/DF as CC.
7. The ACK message sent to the Subject's device is reported within the DSR message to the LEA.

## *G.4 Call Forwarding – No Roaming*

There are three call flows shown here. In the first flow, an incoming call to the Subject (Party_B) is forwarded to Party_C within the TSP's network. In the second flow, an incoming call to the Subject alerts the Subject's device and then is forwarded to Party_C within the TSP's network (this case is also known as Call Forwarding No Answer). In the third flow, an incoming call to the Subject (Party_B) is forwarded to Party_C in another TSP's network. The other TSP's network could be another IMS network or a CS network.

### G.4.1 Intra-TSP Call Forwarding – Unconditional

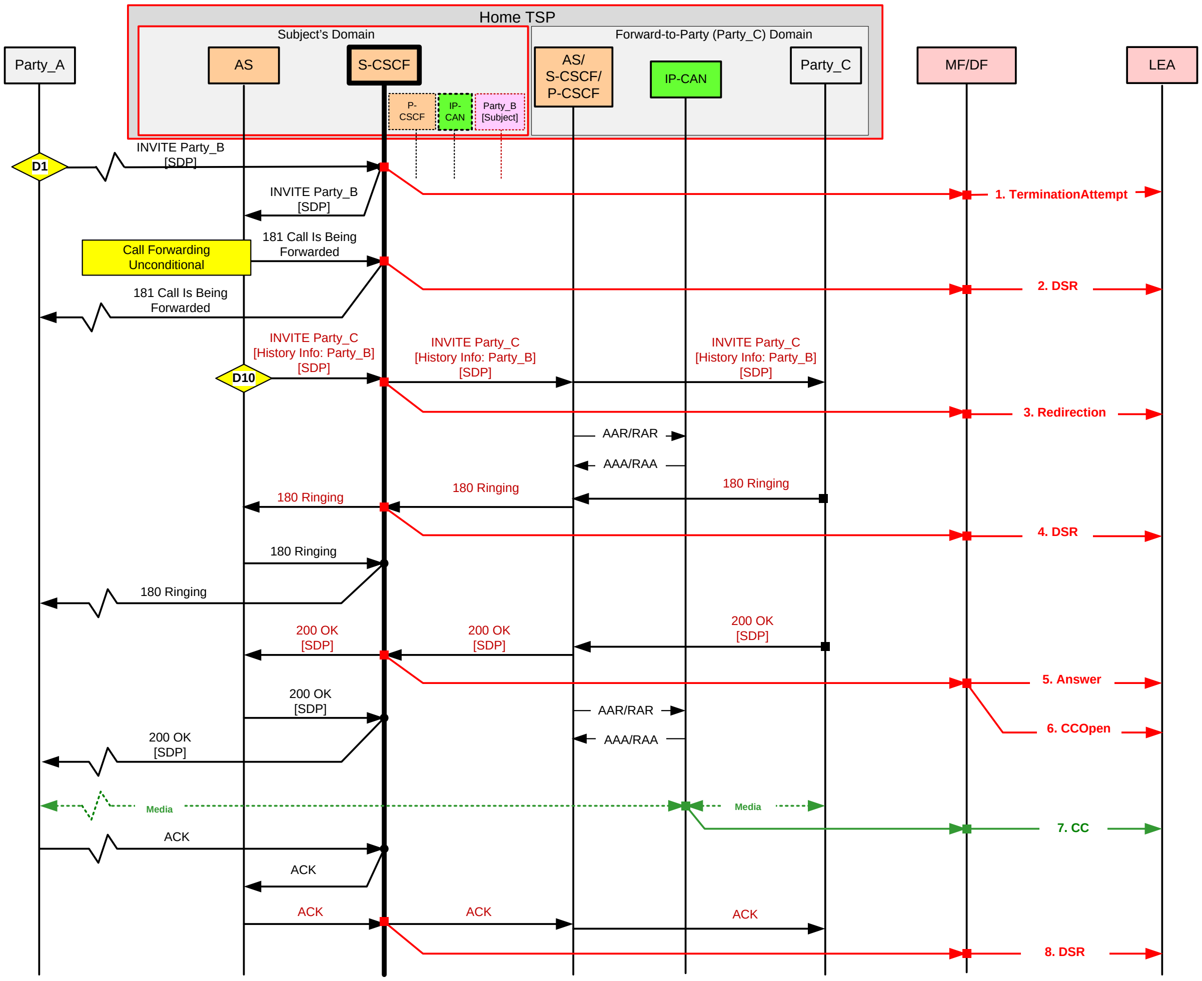


**Figure G.4 – Intra-TSP Call Forwarding Unconditional**

Description of LAES Events

1. The SIP INVITE received at the S-CSCF from the far end (originating side) is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. The call is forwarded and the SIP 181 Call Is Being Forwarded (carries no contents, this is similar to SIP 100 Trying) sent toward the originating side (to Party_A) is encapsulated in a DSR message and sent to the LEA.
3. The SIP INVITE sent to the forward-to-party (Party_C) is mapped to a LAES Redirection message. The History-Info from the SIP INVITE is mapped to the redirected from party identity and Request from SIP INVITE is mapped to the redirected-to-party identity.
4. The SIP 180 Ringing received from the forward-to-party (Party_C) is encapsulated in a DSR message and sent to the LEA.
5. The SIP 200 OK (to SIP INVITE) received from the forward-to-party (Party_C) is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the forward-to-party (Party_C) as answering party identity.
6. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of forward-to-party), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
7. At this time, the P-CSCF (serving the forward-to-party) would have sent a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) serving the forward-to-party, and the PDN-GW/GGSN serving the forward-to-party starts intercepting the media and sends the same to the LEA via MF/DF as CC.
8. The ACK message sent to the forward-to-party (Party_C) is reported within the DSR message to the LEA.

## G.4.2 Intra-TSP Call Forwarding No Answer (CFNR)

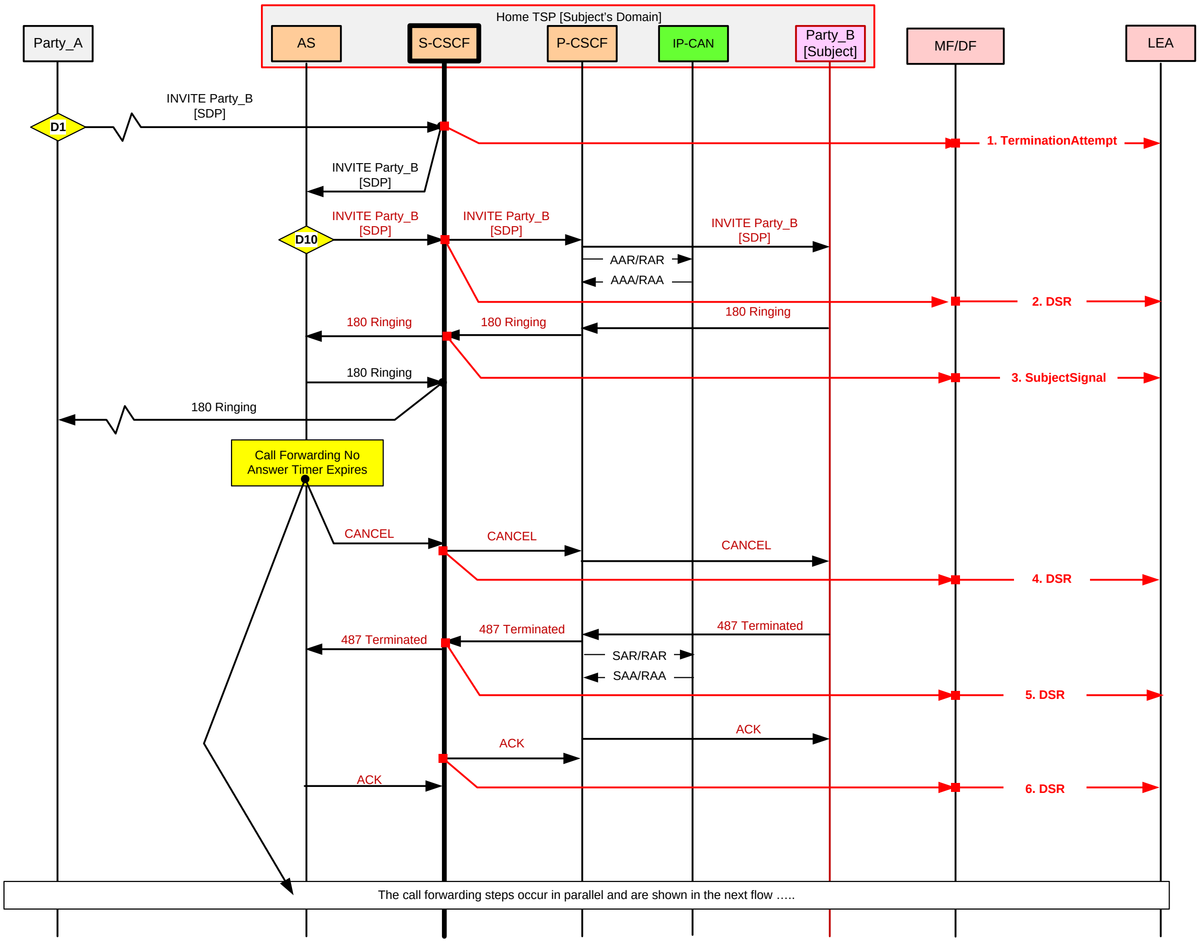


**Figure G.5 – Intra-TSP Call Forwarding No Answer (flow 1 of 2)**

Description of LAES Events

1. The SIP INVITE received at the S-CSCF from the far end (originating side) is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. This is an optional step. 3GPP TS 33.107 does not show the sending of this message to the LEA. If implemented, in this step, the SIP INVITE sent to the Subject's device is encapsulated in a DSR message and sent to the LEA. Since a TerminationAttempt was already sent to the LEA (in step 1), this SIP INVITE is sent to the LEA as a DSR message.
3. The SIP 180 Ringing received from the subject's device is mapped to a LAES SubjectSignal message with an indication that the network has received a "180 Ringing" from the Subject's device.

   When the Call Forwarding No Answer Timer (CFNR) expires, the network sends a SIP CANCEL to the Subject's device to stop the alerting signal, sends 181 Call Is Being Forwarded to the originating end (Party_A), and then sends SIP INVITE to the forward-to-party (Party_C).
4. The SIP CANCEL message sent to the Subject's device to stop the alerting signal is encapsulated in a DSR message and sent to the LEA.
5. The SIP 487 Terminated message received from the Subject's device is encapsulated in a DSR message and sent to the LEA.
6. The SIP ACK message sent to the Subject's device to send the transaction is encapsulated in a DSR message and sent to the LEA.

The flow continues in Figure G.6.

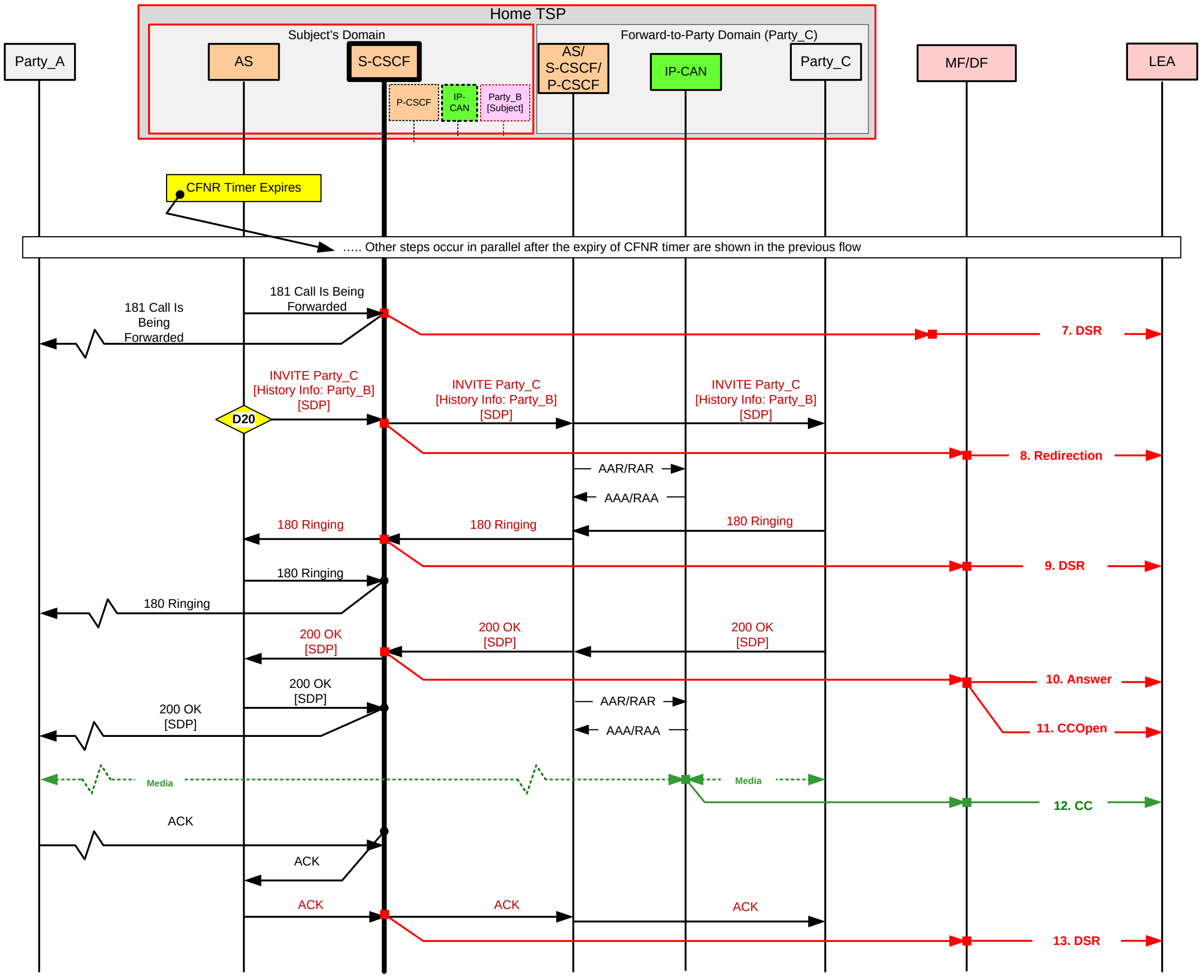


**Figure G.6 – Intra-TSP Call Forwarding No Answer (flow 2 of 2)**

Description of the LAES events:

7. When the CFNR timer expires, the AS initiates the steps to forward the call to the forward-to-party (Party_C). A SIP 181 Call Is Being Forwarded sent toward the originating side (to Party_A) is encapsulated in a DSR message and sent to the LEA.
8. The SIP INVITE sent to the forward-to-party (Party_C) is mapped to a LAES Redirection message. The History-Info from the SIP INVITE is mapped to the redirected from party identity and Request from SIP INVITE is mapped to the redirected-to-party identity.
9. The SIP 180 Ringing received from the forward-to-party (Party_C) is encapsulated in a DSR message and sent to the LEA.
10. The SIP 200 OK (to SIP INVITE) received from the forward-to-party (Party_C) is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the forward-to-party (Party_C) as answering party identity.

11. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of forward-to-party), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
12. At this time, the P-CSCF (serving the forward-to-party) would have sent a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) serving the forward-to-party and the PDN-GW/GGSN serving the forward-to-party starts intercepting the media and sends the same to the LEA via MF/DF as CC.
13. The ACK message sent to the forward-to-party (Party_C) is reported within the DSR message to the LEA.

## G.4.3 Inter-TSP Call Forwarding – Unconditional

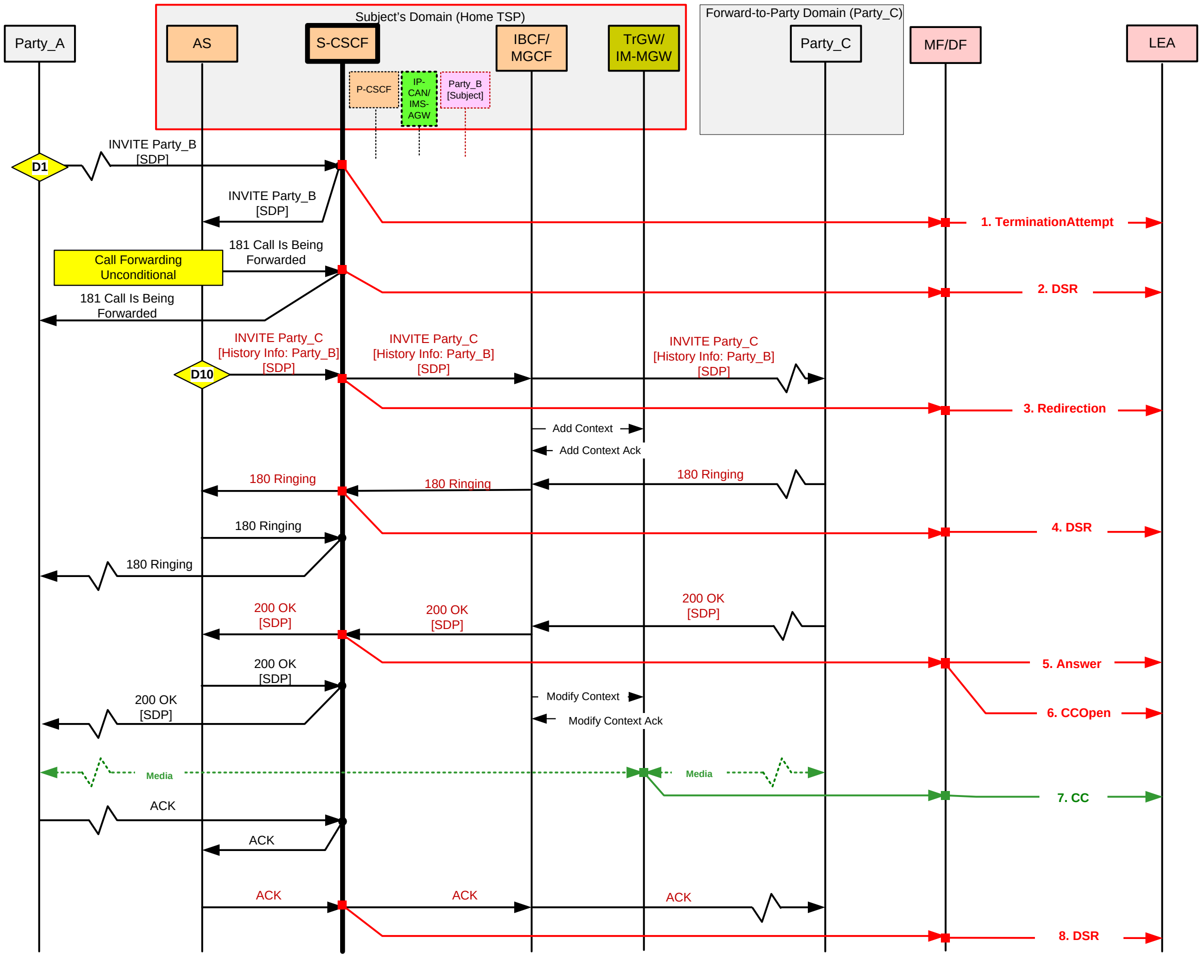


Figure G.7 – Inter-TSP Call Forwarding – Unconditional

<u>Description of LAES Events</u>

1. SIP INVITE received at the S-CSCF from the far end (originating side) is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. The call is forwarded and the SIP 181 Call Is Being Forwarded (carries no contents, this is similar to SIP 100 Trying) sent toward the originating side (to Party_A) is encapsulated in a DSR message and sent to the LEA.
3. The SIP INVITE sent in the direction of the forward-to-party (Party_C) in another TSP is mapped to a LAES Redirection message. The SIP INVITE is sent to MGCF (forward-to-party is in CS domain) or to an IBCF (forward-to-party is in another TSP's IMS network).

4. The History-Info from the SIP INVITE is mapped to the redirected from party identity and Request from SIP INVITE is mapped to the redirected-to-party identity.
5. The SIP 180 Ringing received from the direction of the forward-to-party (Party_C) is encapsulated in a DSR message and sent to the LEA.
6. The SIP 200 OK (to SIP INVITE) received from the direction of the forward-to-party (Party_C) is mapped to a LAES Answer message.   There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the forward-to-party (Party_C) as answering party identity.
7. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of forward-to-party), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
8. At this time, the MGCF (or IBCF) would have sent a CC intercept trigger to the IM-MGW (or TrGW) and the IM-MGW (or TrGW) starts intercepting the media and sends the same to the LEA via MF/DF as CC.
9. The ACK message sent in the direction of the forward-to-party (Party_C) is reported within the DSR message to the LEA.

## *G.5 IMS Roaming*

There are two call flows shown here. In the first call flow, the Subject who is roaming in another TSP's network (who has a local break-out) originates a call. In the second call flow, the Subject who is roaming in another TSP's network (who has local break-out) receives a terminating call.

## G.5.1 Call Originations from IMS Roaming Subject

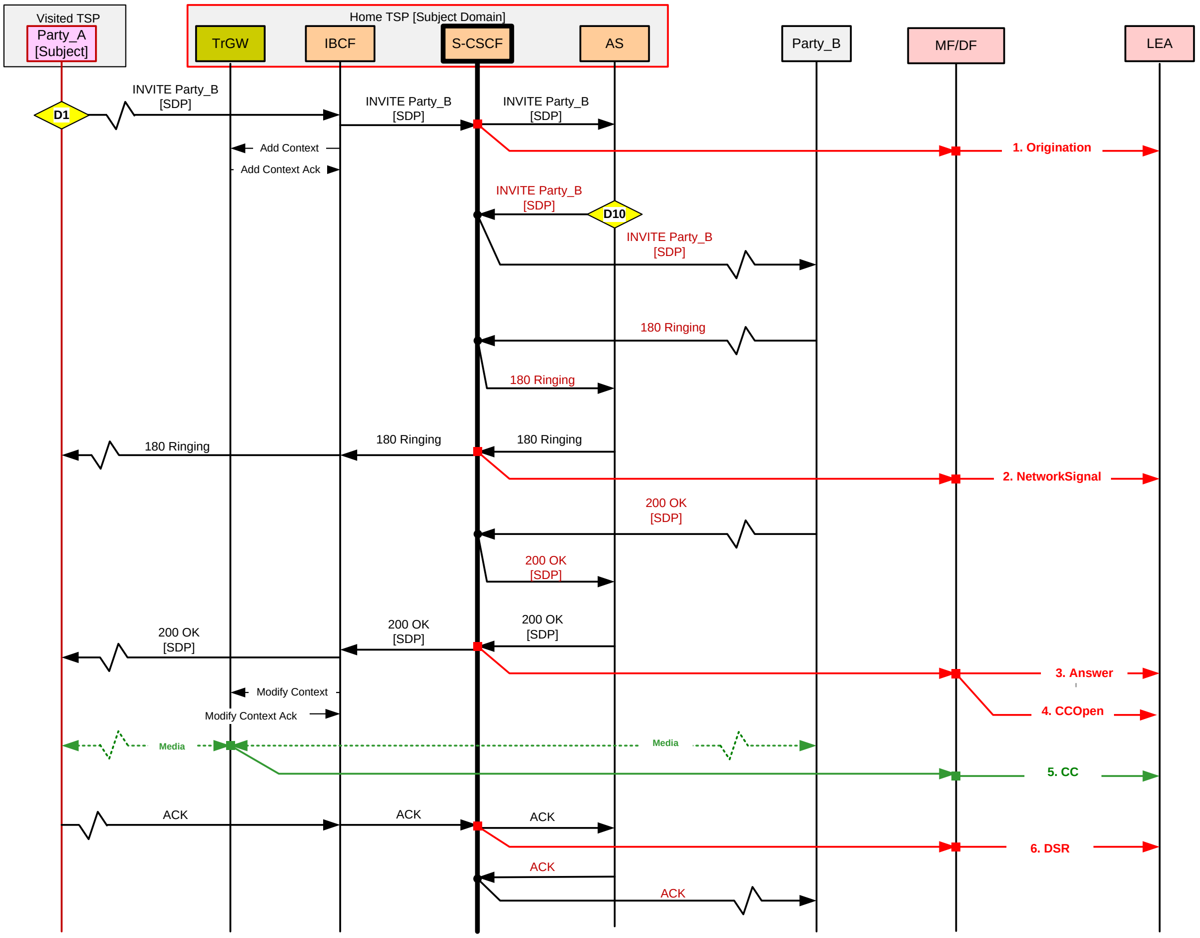


**Figure G.8 – Call Origination from an IMS Roaming Subject**

Description of LAES Events

1. The SIP INVITE received at the S-CSCF in the Home TSP's network from the Subject's device (roaming in the Visited TSP's network) is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field.
2. The SIP 180 Ringing sent in the direction of the Subject's device (roaming in the Visited TSP's network) is mapped to a LAES NetworkSignal message with an indication that the network has initiated the originating Subject's device to apply AudibleSignal (ringback tone).
3. The SIP 200 OK (to SIP INVITE) sent in the direction of the Subject's device (roaming in the Visited TSP's network) is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study.
4. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the far end subscriber [Party_B]), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
5. At this time, the IBCF would have sent a CC intercept trigger to the TrGW and the TrGW starts intercepting the media and sends the same to the LEA via MF/DF as CC.
6. The ACK message received from the direction of the Subject's device (roaming in the Visited TSP's network) is reported within the DSR message to the LEA.

NOTE: The above call flow is the case where optimal media routing is not employed. In the case where the optimal media routing is employed, the CC does not come to the TrGW.

## G.5.2 Call Terminations to IMS Roaming Subject

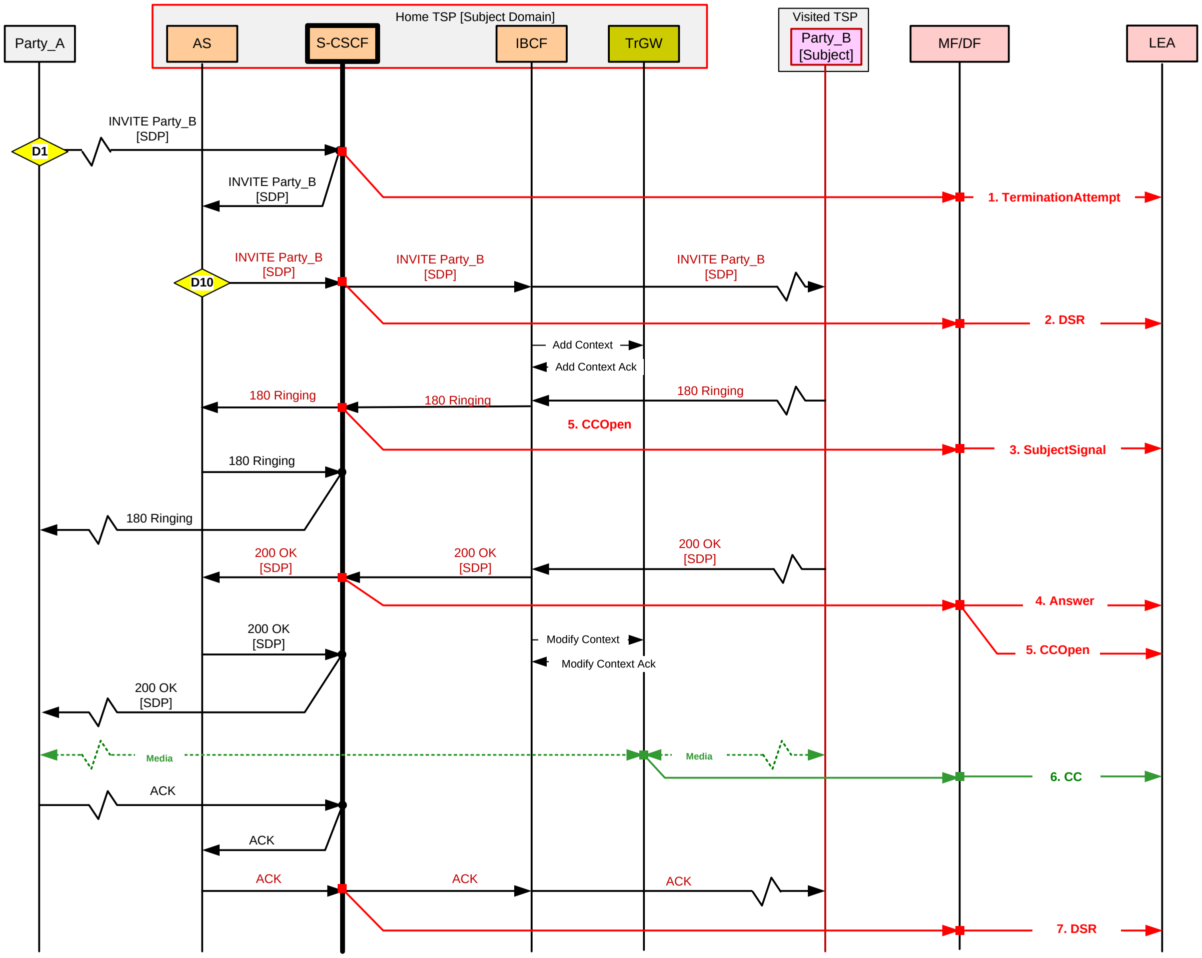


**Figure G.9 – Call Terminating to an IMS Roaming Subject**

Description of LAES Events

1. The SIP INVITE received at the S-CSCF from the far end (originating side) is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. This is an optional step. 3GPP TS 33.107 does not show the sending of this message to the LEA. If implemented, in this step, the SIP INVITE sent in the direction of the Subject's device (roaming in a Visited TSP's network) is encapsulated in a DSR message and sent to the LEA. Since a TerminationAttempt was already sent to the LEA (in step 1), this SIP INVITE is sent to the LEA as a DSR message.
3. The SIP 180 Ringing received from the direction subject's device (roaming in Visited TSP's network) is mapped to a LAES SubjectSignal message with an indication that the network has received a "180 Ringing" from the Subject's device.
4. The SIP 200 OK (to SIP INVITE) received from the direction of the Subject's device (roaming in Visited TSP's network) is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES

Answer message is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the Subject's device as answering party identity.

5. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the Subject's device), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
6. At this time, the IBCF would have sent a CC intercept trigger to the TrGW and the TrGW starts intercepting the media and sends the same to the LEA via MF/DF as CC.
7. The ACK message sent in the direction of the Subject's device (roaming in Visited TSP's network) is reported within the DSR message to the LEA.

### G.5.3 Call Originations from IMS Roaming Subject with Optimal Media Routing

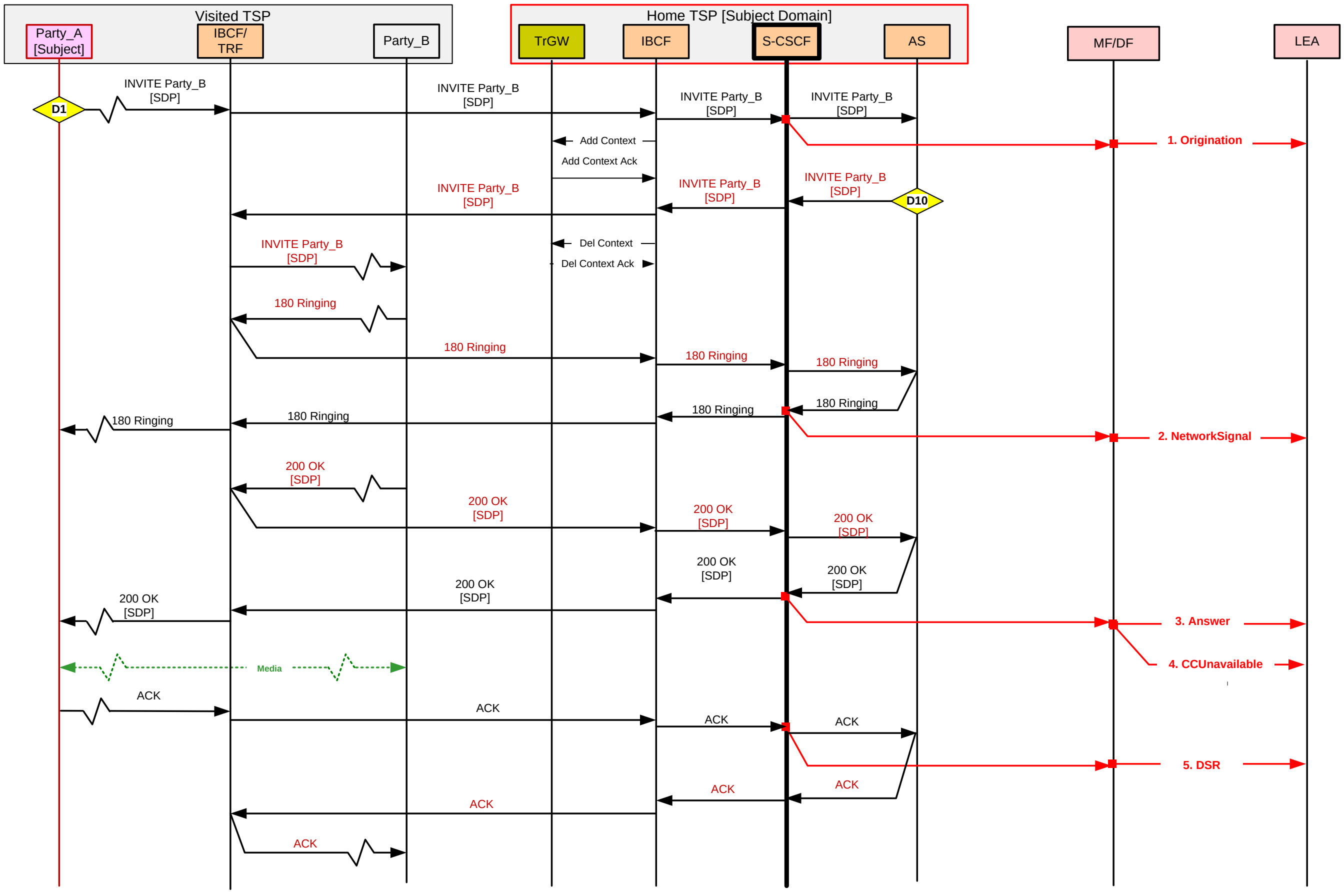


**Figure G.10 – Call Origination from an IMS Roaming Subject with optimal media routing**

Description of LAES Events

Many different call scenarios exist that employ optimal media routing. In this particular example, the called party (Party_B) happens to be served by the same Visited TSP where the Intercept Subject is currently roaming.

Note that the call flow does not show all the network nodes involved in the signaling and media paths.

1. The SIP INVITE received at the S-CSCF in the Home TSP's network from the Subject's device (roaming in the Visited TSP's network) is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field.
2. The SIP 180 Ringing sent in the direction of the Subject's device (roaming in the Visited TSP's network) is mapped to a LAES NetworkSignal message with an indication that the network has initiated the originating Subject's device to apply AudibleSignal (ringback tone).

3. The SIP 200 OK (to SIP INVITE) sent in the direction of Subject's device (roaming in the Visited TSP's network) is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study.
4. In this particular example, optimal media routing is employed and hence, the media does not come to the TrGW. The home TSP's network sends a LAES CCUnavailable message indicating that the CC is not available to the LEA.
5. The ACK message received from the direction of Subject's device (roaming in the Visited TSP's network) is reported within the DSR message to the LEA.

## *G.6 Interceptions in the Visited TSP's Network*

All these flows are applicable to a Visited TSP served with a warrant. The Home TSP may or may not have a warrant. The CII interceptions happen at the P-CSCF. There are three flows shown here. In the first flow, the Subject in the Visited TSP's network originates a call. In the second flow, the Subject in the Visited TSP's network receives an incoming call. In the third flow, the Subject in the Visited network receives an incoming call, but the Subject's feature in the Home TSP's network forwards the call due to CFNR.

### G.6.1 Call Originations from Subject

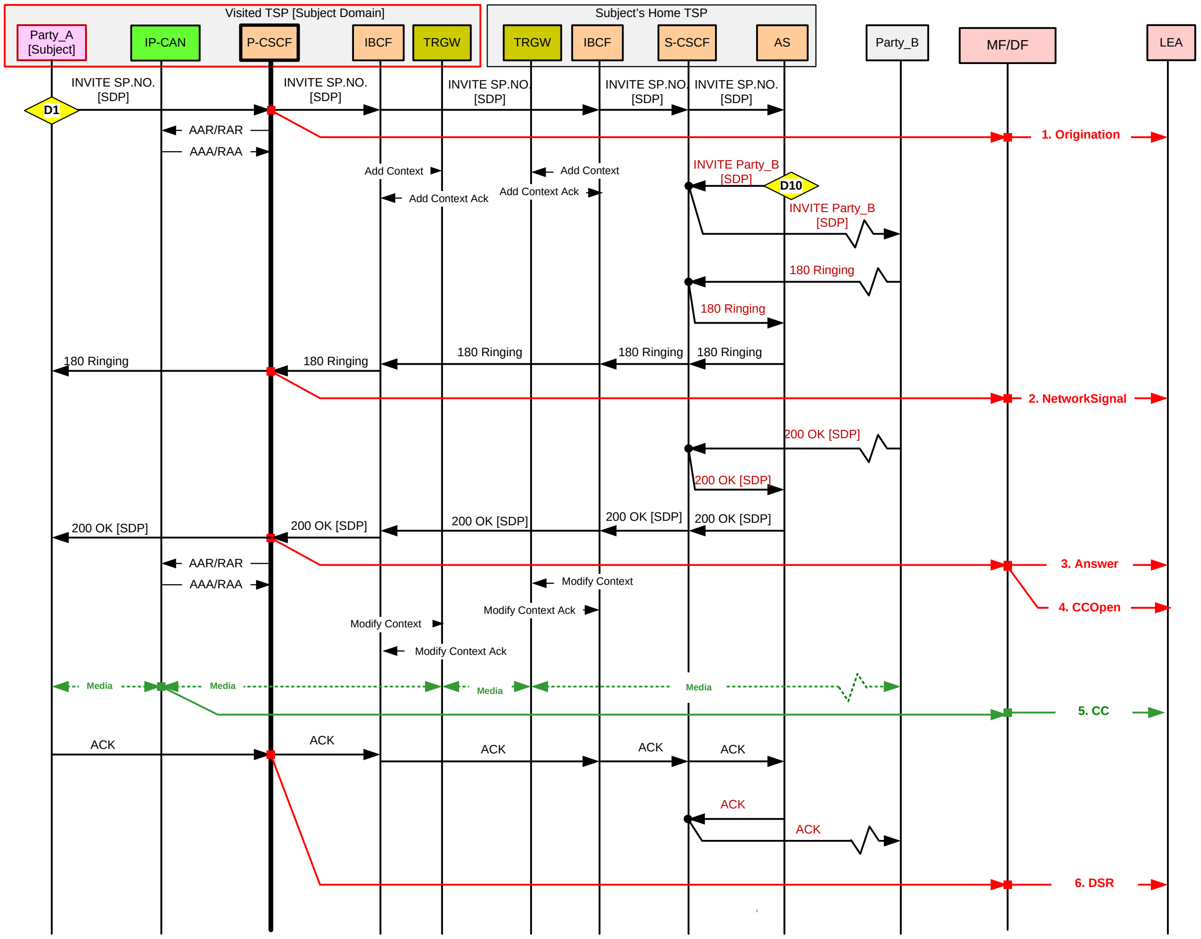


**Figure G.11 – Interception in the Visited TSP – Call Origination from Subject**

Description of LAES Events

1. The SIP INVITE received from the Subject's device is mapped to a LAES Origination message. The Request URI is mapped to the called party identity field.
2. The SIP 180 Ringing sent to the Subject's device is mapped to a LAES NetworkSignal message with an indication that the network has initiated the originating Subject's device to apply AudibleSignal (ringback tone).
3. The SIP 200 OK (to SIP INVITE) sent to the Subject's device is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study.
4. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the far end subscriber), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
5. At this time, the P-CSCF also sends a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) and the PDN-GW/GGSN starts intercepting the media and sends the same to the LEA via MF/DF as CC.
6. The ACK message received from the Subject's device is reported within the DSR message to the LEA.

## G.6.2 Call Terminations to Subject

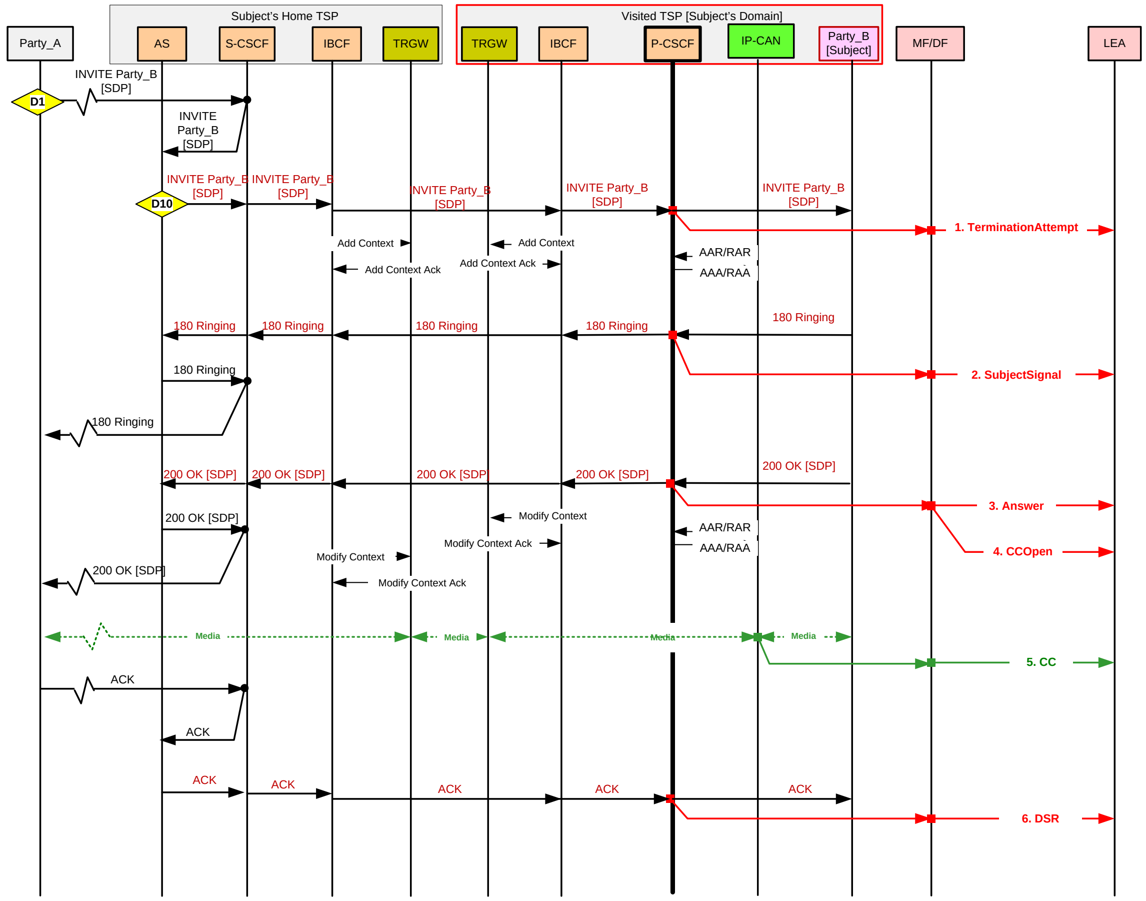


Figure G.12 – Interception in the Visited TSP - Call Termination to Subject

1. The SIP INVITE received at the P-CSCF in the Visited TSP's network from the Home TSP's network is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. The SIP 180 Ringing received from the subject's device is mapped to a LAES SubjectSignal message with an indication that the network has received a "180 Ringing" from the Subject's device.

3. The SIP 200 OK (to SIP INVITE) received from the Subject's device is mapped to a LAES Answer message. There is no indication of answering party in the SIP 200 OK and therefore, inclusion of answering party identity which is an optional field in the LAES Answer message is for further study. As an implementation option, the S-CSCF could include the Request URI present in the SIP INVITE sent to the Subject's device as answering party identity.
4. Since the SIP 200 OK carries the SDP answer (i.e., SDP information of Subject's device), a LAES CCOpen message indicating the start of CC delivery is sent to the LEA.
5. At this time, the P-CSCF also sends a CC intercept trigger to the PDN-GW/GGSP (shown as IP-CAN) and the PDN-GW/GGSN starts intercepting the media and sends the same to the LEA via MF/DF as CC.
6. The ACK message sent to the Subject's device is reported within the DSR message to the LEA.

### G.6.3 Call Termination to Subject & Call Forwarding Do No Answer (CFNR)

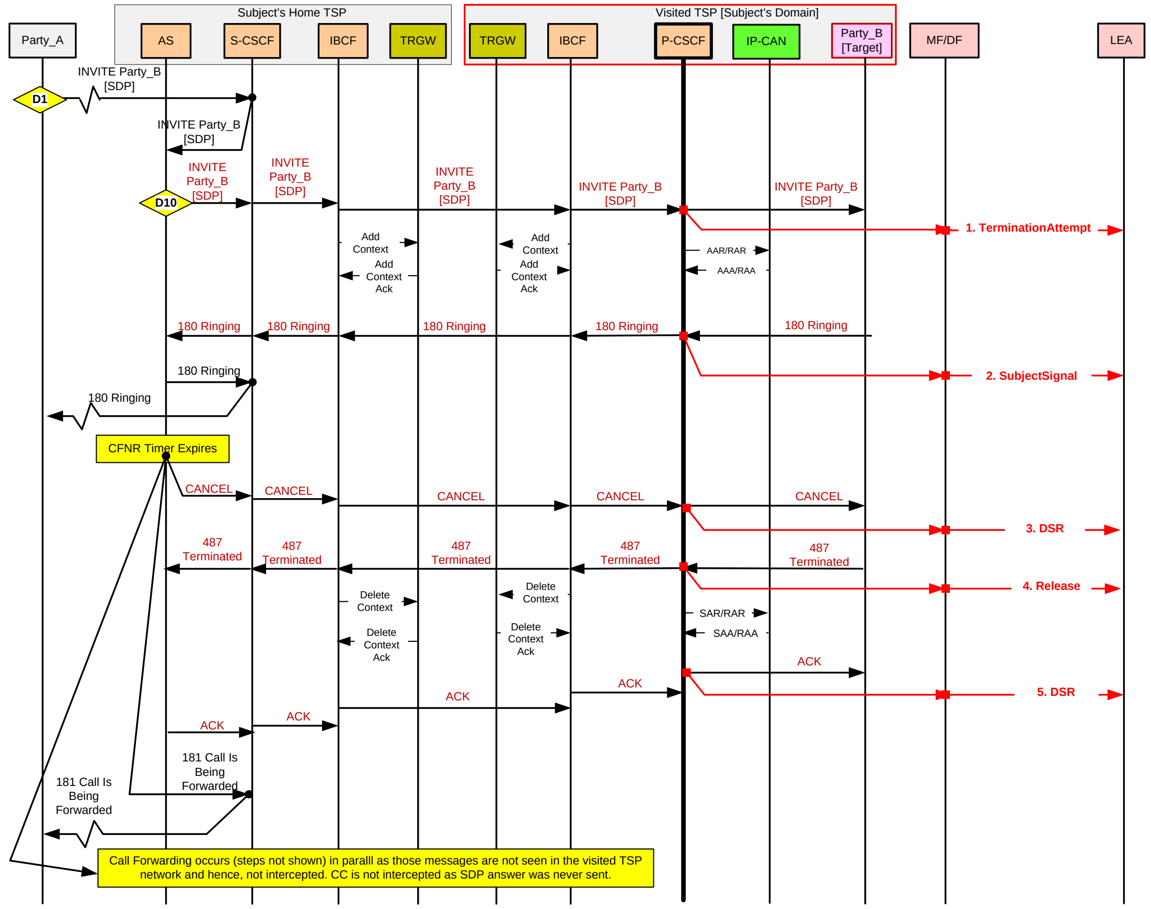


**Figure G.13 – Interception in the Visited TSP – Call Termination to Subject and CFNR**

Description of LAES Events

1. The SIP INVITE received at the P-CSCF in the Visited TSP's network from the Home TSP's network is mapped to a LAES TerminationAttempt message. The P-Asserted-Identity from the SIP INVITE is mapped to the calling party identity field. The Request URI from SIP INVITE is mapped to the called party identity field.
2. The SIP 180 Ringing received from the subject's device is mapped to a LAES SubjectSignal message with an indication that the network has received a "180 Ringing" from the Subject's device.

   When the Call Forwarding No Answer Timer (CFNR) expires, the AS residing in the Home TSP's network sends a SIP CANCEL to the Subject's device (roaming in the Visited TSP's network) to stop the alerting signal, sends 181 Call Is Being Forwarded to the originating end (Party_A) and then sends SIP INVITE to the forward-to-party (Party_C).

3. The SIP CANCEL message sent to the Subject's device (received from the Home TSP's network) to stop the alerting signal is encapsulated in a DSR message and sent to the LEA.
4. The SIP 487 Terminated message received from the Subject's device and sent to the Home TSP's network is mapped to a LAES Release message and sent to the LEA.
5. The SIP ACK message sent to the Subject's device to end the transaction is encapsulated in a DSR message and sent to the LEA.

## *G.7 Subject-initiated Ad-hoc Conference Call*

This clause gives nine call flows that illustrate the steps related to ad-hoc conference calling established by the Intercept Subject. The flows assume that the Party_A (Subject) has already made two calls, one to Party_B and one to Party_C, and placed both calls on hold so as to merge the two calls into a conference.

Figure G.14 illustrates the case where the Party_A (Subject) creates the conference.

Figure G.15 and Figure G.16 illustrate the case where the Party_A (Subject) brings the Party_C into the conference.

Figure G.17 and G.18 illustrate the case where the Party_A (Subject) brings the Party_B into the conference.

Figure G.19 illustrates the case where Party_C drops out of the conference call.

Figure G.20 illustrates the case where the call between two parties (Party_A [Subject] and Party_B) is converted back to a normal 2-party call.

Figure G.21 illustrates the case where Party_A (Subject) places the conference on hold.

Figure G.22 illustrates the case where Party_A (Subject) retrieves the held conference from hold.

Some of the steps may be executed by the Intercept Subject's UE automatically (i.e., no manual action is required). For example, when the Intercept Subject tries to merge the call, the Intercept Subject's UE may execute the steps shown in Figure G.14, Figure G.15, Figure G.16, Figure G.17, and Figure G.18 automatically in a serial fashion. The same way, the steps shown in Figure G.20 may be executed automatically after the steps shown in Figure G.19 when one of the conferees drop out of the conference.

Figure G.21 and Figure G.22 are not really part of the conferencing steps, however, they are included here to show how the content of a held conference call is delivered to the LEAs.

## G.7.1 Party_A (Subject) Creates the Conference

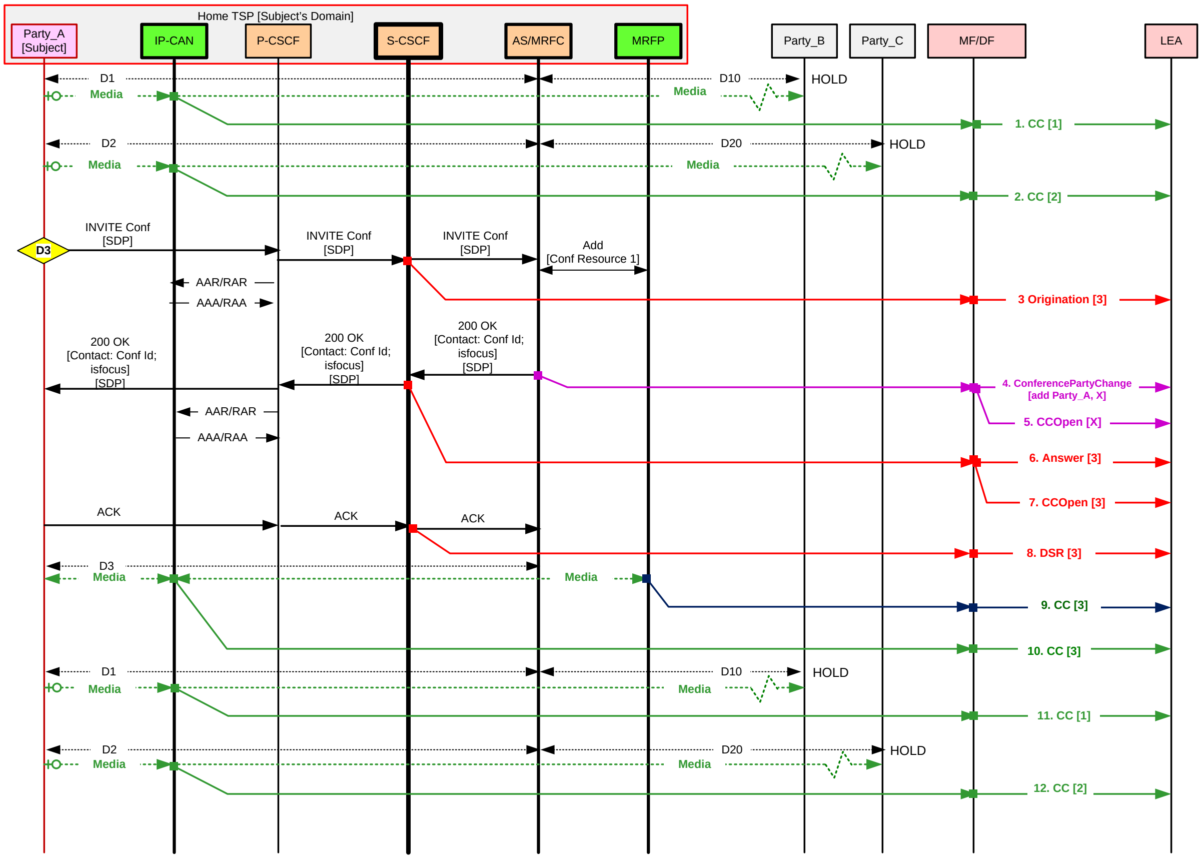


**Figure G.14 – Party_A (Subject) creates the conference**

D1 and D10 represent the dialogue of the original call between the Party_A (Subject) and the Party_B. D2 and D20 represent the dialogue of the original call between Party_A (Subject) and the Party_C. D3 represents the new dialogue of the call between Party_A (Subject) and the conference.

The CII/CC delivered for D1 and D10 use the Correlation Number 1. The CII/CC delivered for D2 and D20 use the Correlation Number 2. The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF.

<u>Description of LAES Events</u>

1. Initial condition 1: CC [1] shows the delivery of CC of a call (Party_B) on hold.
2. Initial condition 2: CC [2] shows the delivery of CC of a call (Party_C) on hold.
3. S-CSCF-based CII interception: The SIP INVITE received from the Subject's device is mapped to a LAES Origination [3] message.
4. AS/MRFC-based CII interception: The SIP 200 OK message sent toward the Subject's device is mapped to ConferencePartyChange [X] message with an indication that Party_A (Subject) has joined the conference.
5. AS/MRFC-based CII interception: Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the conference resources), a LAES CCOpen [X] message indicating the start of CC delivery is sent to the LEA.

6. S-CSCF-based CII interception: The SIP 200 OK (to SIP INVITE) sent to the Subject's device is mapped to a LAES Answer message.
7. S-CSCF-based CII interception: Since the SIP 200 OK carries the SDP answer (i.e., SDP information of the far end subscriber), a LAES CCOpen [3] message indicating the start of CC delivery is sent to the LEA.
8. S-CSCF-based interception: The SIP ACK message received from the Subject's device at the S-CSCF is delivered as a DSR [3] message to the LEA.
9. MRFP-based C interception: The MRFP starts intercepting the media. The CC [X] is delivered to the LEA.
10. IP-CAN-based CC interception: The PDN-GW/GGSP (shown as IP-CAN) starts intercepting the media. The CC [3] is delivered to the LEA.
11. CC [1] of held call to Party_B continues to be delivered.
12. CC [2] of held call to Party-C continues to be delivered.

## G.7.2 Party_C Joins the Conference

This flow is illustrated in two figures: Figure G.15 and Figure G.16.

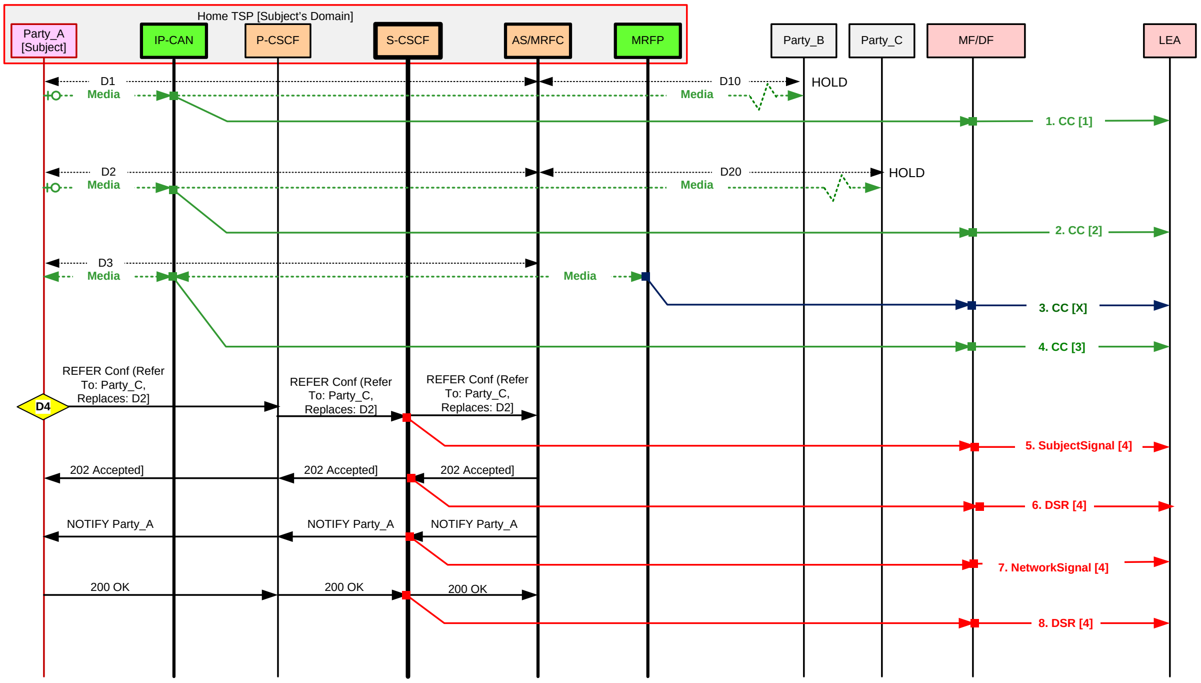


**Figure G.15 – Party_C joins the conference (flow 1 of 2)**

D1 and D10 represent the dialogue of the original call between the Party_A (Subject) and the Party_B. D2 and D20 represent the dialogue of the original call between Party_A (Subject) and Party_C. D3 represents the dialogue of the call between Party_A and the conference. D4 represents the dialogue that the Party_A (Subject) uses to refer Party_C to the conference.

> NOTE: Here, REFER is sent by Party_A outside of any existing dialogues. Sending of REFER inside a dialogue is also possible.

The CII/CC delivered for D1 and D10 use the Correlation Number 1. The CII/CC delivered for D2 and D20 use the Correlation Number 2. The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the

Correlation Number included in the CII messages initiated by the S-CSCF. The IRI for D4 uses the Correlation Number 4.

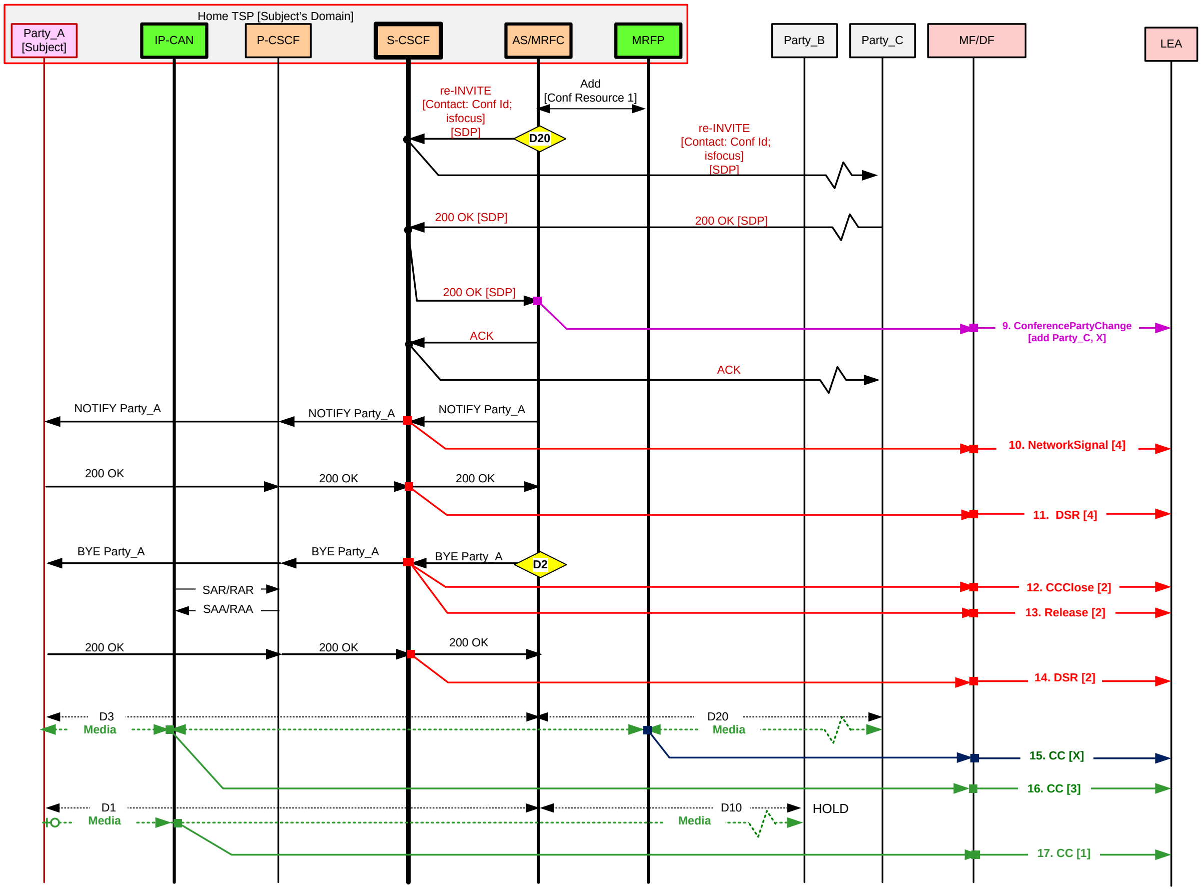


**Figure G.16 – Party_C joins the conference (flow 2 of 2)**

At the end of this flow, the Party_A (Subject) and Party_C are connected via the conference. Party_B is still on hold. Part of the original call between Party_A (Subject) and Party_C (D2) is released with D20 now representing the call between the Party_C and the conference.

## Description of LAES Events

1. Initial condition 1: CC [1] shows the delivery of CC of a call (Party_B) on hold.
2. Initial condition 2: CC [2] shows the delivery of CC of a call (Party_C) on hold.
3. Initial Condition 3: CC[X] shows the delivery of CC intercepted at MRFP of the conference.
4. Initial Condition 4: CC [3] shows the delivery of CC intercepted at IP-CAN of the conference.
5. S-CSCF-based CII interception: The SIP REFER received from the Subject's device is mapped to a LAES SubjectSignal [4] message. Conference URI present in the Request URI is mapped to the Signaled Party ID. The value of "refer" is reported in the OtherSignalingInformation of the Signal field of the LAES message.
6. S-CSCF-based CII interception: The SIP 202 Accepted sent to the Subject's device is mapped to a DSR [4] message.
7. S-CSCF-based CII interception: The SIP Notify sent to the Subject's device is mapped to a NetworkSignal [4] message.  The value of "notify" is reported as other in the signal field of the LAES message.
8. S-CSCF-based CII interception: The SIP 200 OK (for Notify) received from the Subject's device is mapped to a DSR [4] message.

9. AS/MRFC-based CII interception: The SIP 200 OK message received from the party joining the conference (Party_C) is mapped to ConferencePartyChange [X] message with an indication that Party_C has joined the conference.
10. S-CSCF-based CII interception: The SIP Notify sent to the Subject's device is mapped to a NetworkSignal [4] message. The value of "notify" is reported as other in the signal field of the LAES message.
11. S-CSCF-based CII interception: The SIP 200 OK (for Notify) received from the Subject's device is mapped to a DSR [4] message.
12. S-CSCF-based CII interception: Since the Party_C is joined to the conference, the CC [2] delivery stops. A CCClose [2] message is delivered to the LEA.
13. S-CSCF-based CII interception: Since the Party_C is joined to the conference, the original call leg between Party_A (Subject) and Party_C is released. The BYE message sent to the Party_A (Subject) is mapped to a Release [2] message.
14. S-CSCF-based CII interception: The SIP 200 OK (BYE) message received from the Subject's device is reported as a DSR [3] message to the LEA.
15. MRFP-based C interception: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
16. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].
17. CC [1] of held call to Party_B continues to be delivered.

## G.7.3 Party_B Joins the Conference

This flow is illustrated in two figures: Figure G.17 and Figure G.18.

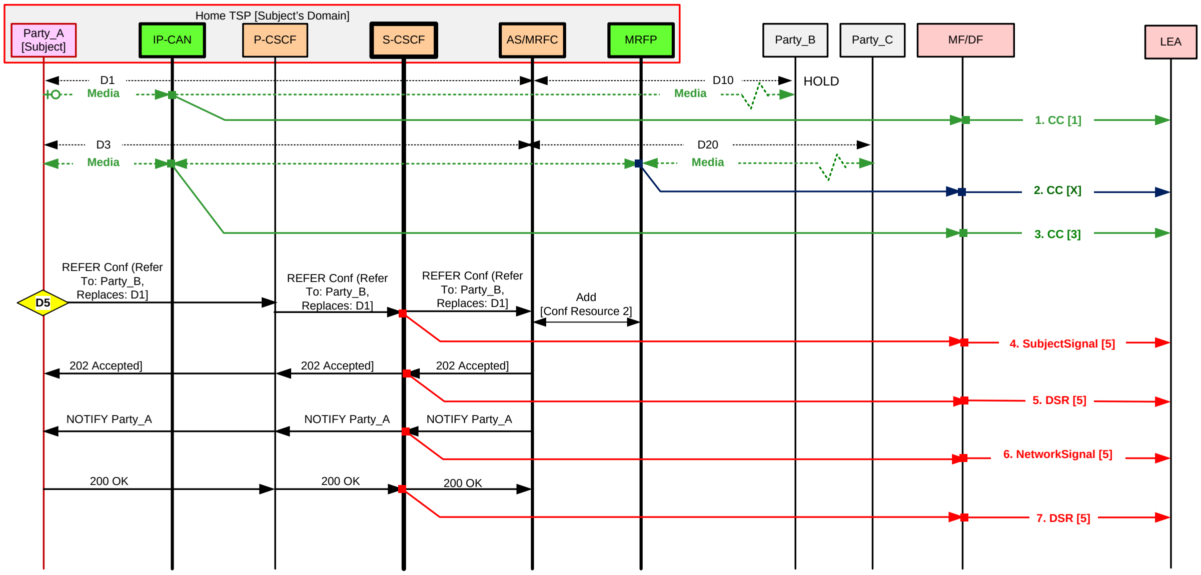


**Figure G.17 – Party_B joins the conference (flow 1 of 2)**

D3 represents the dialogue of the call between the Party_A (Subject) and the conference. D20 represents the dialogue between the Party_C and the conference. D1 and D10 represent the original dialogue of the original call between Party_A (Subject) and the Party_B. D5 represents the dialogue that the Party_A (Subject) uses to refer Party_B to the conference.

> NOTE: Here, REFER is sent by Party_A outside of any existing dialogues. Sending of REFER inside a dialogue is also possible.

The CII/CC delivered for D1 and D10 uses the Correlation Number 1. The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for

AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF. The IRI for D5 uses the Correlation Number 5.

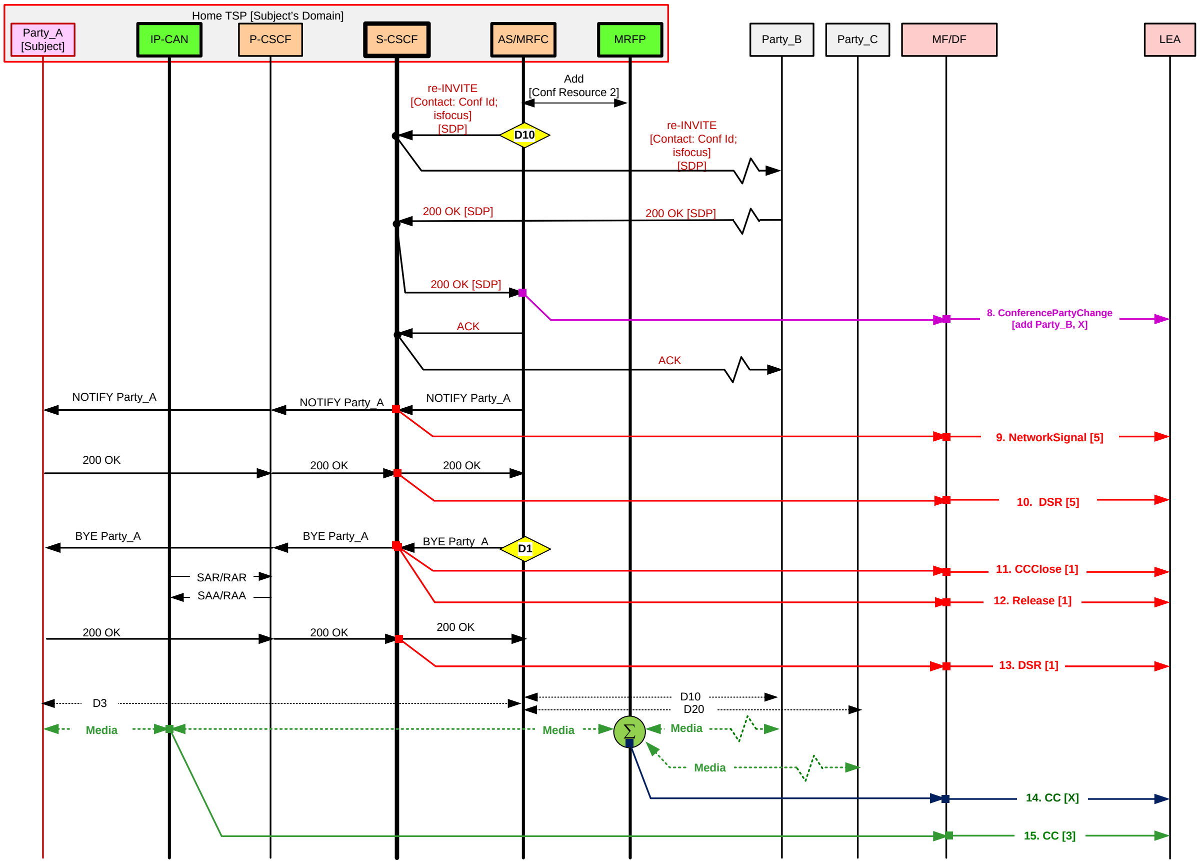


**Figure G.18 – Party_B joins the conference (flow 2 of 2)**

At the end of this flow, the Party_A (Subject), Party_B, and Party_C are connected via the conference. Part of the original call between Party_A (Subject) and Party_B (D1) is released with D10 now representing the call between the Party_B and the conference.

Description of LAES Events

1. Initial condition 1: CC [1] shows the delivery of CC of a call (Party_B) on hold.
2. Initial Condition 2: CC[X] shows the delivery of CC intercepted at the MRFP of the conference.
3. Initial Condition 3: CC [3] shows the delivery of CC intercepted at IP-CAN of the conference.
4. S-CSCF-based CII interception: The SIP REFER received from the Subject's device is mapped to a LAES SubjectSignal [5] message. Conference URI present in the Request URI is mapped to the Signaled Party ID. The value of "refer" is reported in the OtherSignalingInformation of the Signal field of the LAES message.
5. S-CSCF-based CII interception: The SIP 202 Accepted sent to the Subject's device is mapped to a DSR [5] message.
6. S-CSCF-based CII interception: The SIP Notify sent to the Subject's device is mapped to a NetworkSignal [5] message. The value of "notify" is reported as other in the signal field of the LAES message.
7. S-CSCF-based CII interception: The SIP 200 OK (for Notify) received from the Subject's device is mapped to a DSR [5] message.

8. AS/MRFC-based CII interception: The SIP 200 OK message received from the party joining the conference (Party_B) is mapped to ConferencePartyChange [X] message with an indication that Party_B has joined the conference.
9. S-CSCF-based CII interception: The SIP Notify sent to the Subject's device is mapped to a NetworkSignal [5] message. The value of "notify" is reported as other in the signal field of the LAES message.
10. S-CSCF-based CII interception: The SIP 200 OK (for Notify) received from the Subject's device is mapped to a DSR [5] message.
11. S-CSCF-based CII interception: Since the Party_B is joined to the conference, the CC [1] delivery stops. A CCClose [1] message is delivered to the LEA.
12. S-CSCF-based CII interception: Since the Party_B is joined to the conference, the original call leg between Party_A (Subject) and Party_B is released. BYE message sent to the Party_A (Subject) is mapped to a Release [1] message.
13. S-CSCF-based CII interception: The SIP 200 OK (BYE) message received from the Subject's device is reported as a DSR [1] message to the LEA.
14. MRFP-based C interception: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
15. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].

## G.7.4 Party_C Drops Out of the Conference

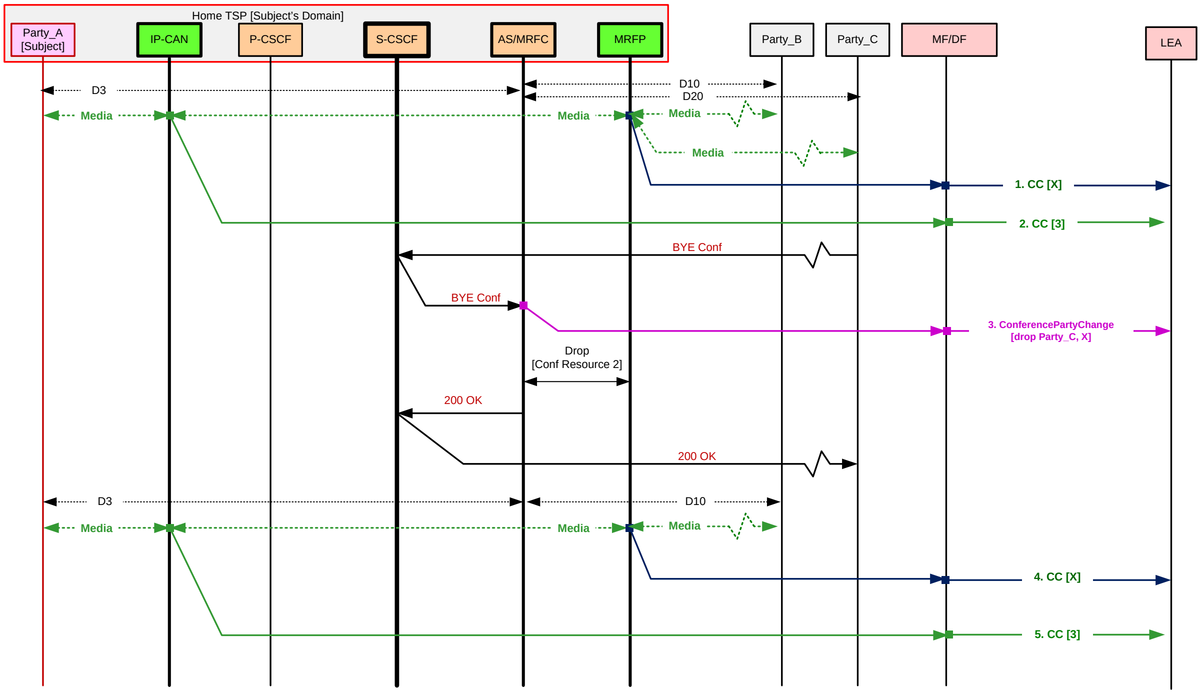


**Figure G.19 – Party_C drops out of the conference**

D3 represents the dialogue of the call between the Party_A (Subject) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF.

At the end of this flow, Party_A (Subject) and Party_B are connected through the conference.

Description of LAES Events

1. Initial condition 1: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
2. Initial condition 2: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].
3. AS/MRFC-based CII interception: The SIP BYE message received from the Party_C is mapped to ConferencePartyChange [X] message with an indication that Party_C has been dropped from the conference.
4. MRFP-based CC interception: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
5. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].

## G.7.5 Reconfiguration from Conference to Two-party Call

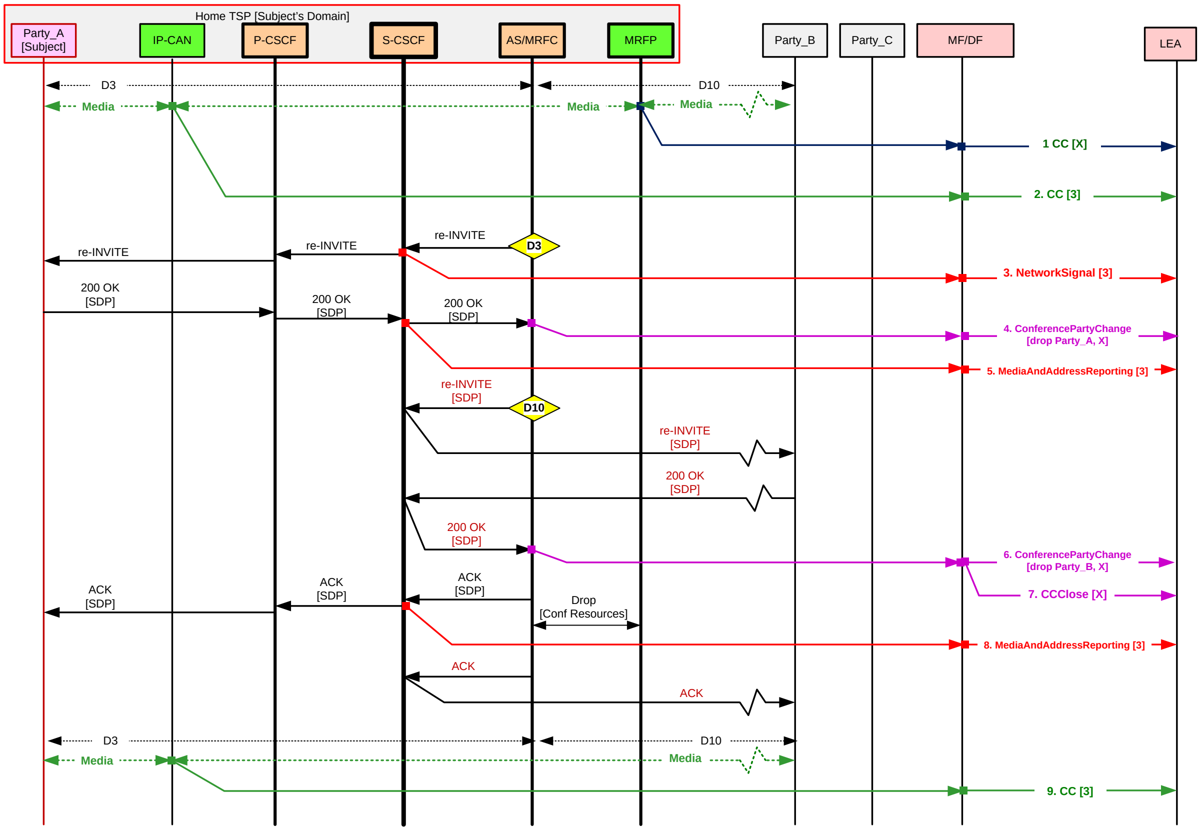


**Figure G.20 – Conference is reconfigured to a two-party call**

D3 represents the dialogue of the call between the Party_A (Subject) and the conference. D10 represents the dialogue between the Party_B and the conference.

The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF.

At the end of this flow, Party_A (Subject) and Party_B are connected directly (without the conference). The CII/CC delivered for this call between Party_A (Subject) and Party_B (D3 and D10) uses the Correlation Number 3.

NOTE: Reconfiguration may done using other ways (e.g., AS/MRFC sending a REFER to Party_A (Subject) to invite Party_B). The sequence of steps and the Correlation Number used can be different with such a flow.

Description of LAES Events

1. Initial condition 1: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
2. Initial condition 2: Media intercepted at the PDN-GW/GGSP (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].
3. S-CSCF-based interception: The SIP re-INVITE sent to the Party_A (Subject) is mapped to a NetworkSignal [3] message when the re-INVITE does not have any SDP information (as in this flow). The value of “invite” is included as other in the Signal field of the LAES message.
4. AS/MRFC-based CII interception: The SIP 200 OK (INVITE) message received from the Party_A (Subject) is mapped to ConferencePartyChange [X] message with an indication that Party_A has been dropped from the conference.
5. S-CSCF-based interception: The SIP 200 OK (INVITE) received from the Party_A (Subject) contains the SDP information and hence, is mapped to a MediaAndAddressReporting [3] message.
6. AS/MRFC-based CII interception: The SIP 200 OK (INVITE) message received from the Party_B is mapped to ConferencePartyChange [X] message with an indication that Party_B has been dropped from the conference.
7. AS/MRFC-based CII interception: When both parties (Party_A and Party_B) are dropped from the conference, the interception of CC at MRFP is no longer required. Hence, a CCClose [X] is delivered to the LEA to indicate that CC associated with Correlation Number X has been stopped.
8. S-CSCF-based interception: The SIP ACK sent to the Party_A (Subject) contains the SDP information and hence, is mapped to a MediaAndAddressReporting [3] message.
9. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].

## G.7.6 Party_A (Subject) Places Conference on Hold

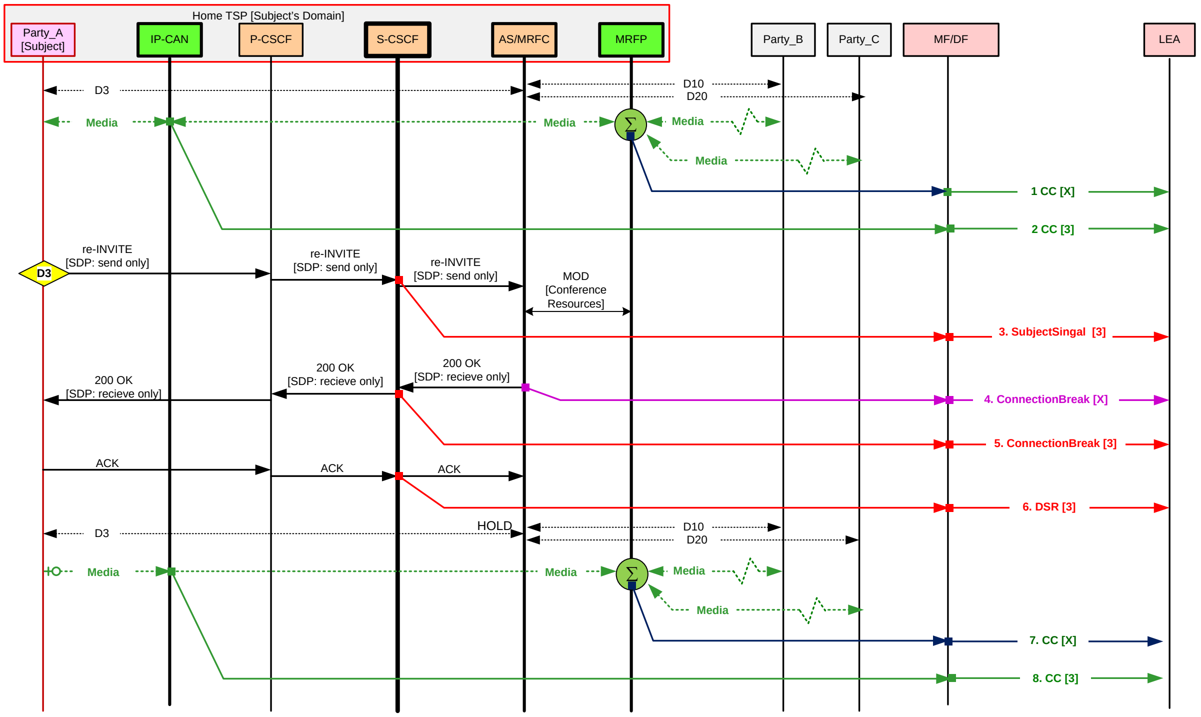


**Figure G.21 – Party_A (Subject) places a conference on hold**

D3 represents the dialogue of the call between the Party_A (Subject) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF.

At the end of this flow, Party_B and Party_C can still communicate via the conference, but without the Party_A. The CC delivered from the MRFP contains the communication content of that conversation.

NOTE: Similar steps as shown here are used when Party_A (Subject) places a two-party on call hold.

Description of LAES Events

1. Initial condition 1: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
2. Initial condition 2: Media intercepted at the PDN-GW/GGSN (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].
3. S-CSCF-based CII interception: The SIP re-INVITE received from the Party_A (Subject) is mapped to a SubjectSignal [3] message. Conference URI present in the Request URI is mapped to the Signaled Party ID. The value of “hold” is reported in the OtherSignalingInformation of the Signal field of the LAES message.
4. AS/MRFC-based CII interception: The SIP 200 OK message sent to the Party_A (Subject) is mapped to ConnectionBreak [X] message with an indication that Party_A (Subject) is temporarily out of the conference.
5. S-CSCF-based CII interception: The SIP 200 OK sent to the Party_A (Subject) is mapped to a ConnectionBreak [3] message with an indication that Party_A (Subject) is out of the call temporarily.
6. S-CSCF-based CII interception: The SIP ACK message received from the Party_A (Subject) is mapped to a DSR [3] message.
7. MRFP-based C interception: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
8. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSP (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].

## G.7.7 Party_A (Subject) Retrieves Conference from Hold

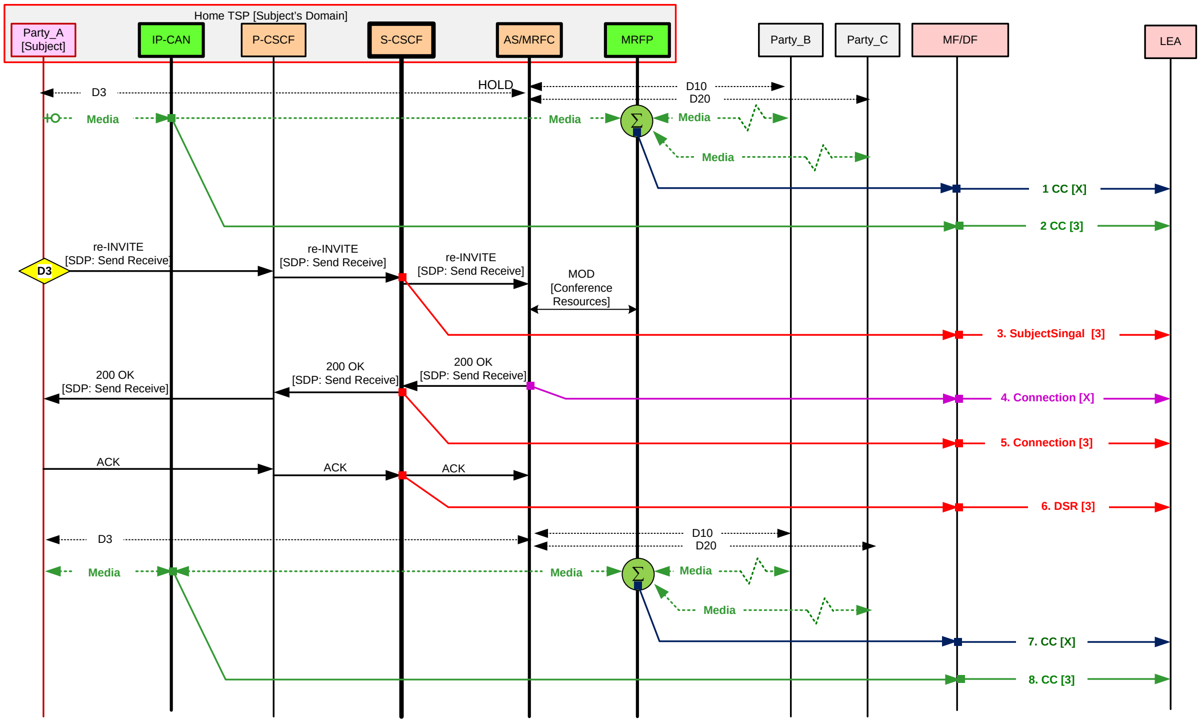


**Figure G.22 – Party_A (Subject) retrieves conference from hold**

D3 represents the dialogue of the call between the Party_A (Subject) and the conference. D20 represents the dialogue between the Party_C and the conference. D10 represents the dialogue between the Party_B and the conference.

The CII/CC delivered for the conferencing (i.e., D3) uses the Correlation Number 3 (for S-CSCF/IP-CAN-based CII/CC) and Correlation Number X (for AS/MRFC/MRFP-based CII and CC). The Correlation Number value of X is shown to indicate that this Correlation Number may be different from the Correlation Number included in the CII messages initiated by the S-CSCF.

At the end of this flow, Party_A (Subject), Party_B, and Party_C are communicating via the conference.

NOTE: Similar steps as shown here are used when Party_A (Subject) retrieves a two-party call from hold.

Description of LAES Events

1. Initial condition 1: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
2. Initial condition 2: Media intercepted at the PDN-GW/GGSP (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].
3. S-CSCF-based CII interception: The SIP re-INVITE received from the Party_A (Subject) is mapped to a SubjectSignal [3] message. Conference URI present in the Request URI is mapped to the Signaled Party ID. The value of “retrieve” is reported in the OtherSignalingInformation of the Signal field of the LAES message.
4. AS/MRFC-based CII interception: The SIP 200 OK message sent to the Party_A (Subject) is mapped to Connection [X] message with an indication that Party_A (Subject) is back in the conference.
5. S-CSCF-based CII interception: The SIP 200 OK sent to the Party_A (Subject) is mapped to a Connection [3] message with an indication that Party_A (Subject) is back in the call.
6. S-CSCF-based CII interception: The SIP ACK message received from the Party_A (Subject) is mapped to a DSR [3] message.

7. MRFP-based CC interception: Media intercepted at the conference is delivered to the LEA via MF/DF as CC [X].
8. IP-CAN-based CC interception: Media intercepted at the PDN-GW/GGSP (shown as IP-CAN) is delivered to the LEA via MF/DF as CC [3].

**Annex H**

(Informative)

# H Topologies of Call Content Interception

## H.1 Basic Calls

This clause includes two topology diagrams that illustrate the CC interception for basic calls.

- Call originated by an Intercept Subject.
- Call terminated to an Intercept Subject.

The diagrams show a cloud labelled “voice services” basically to indicate that the interception performed is independent from how the call is routed to, or routed from, the far end of the call.

The illustrations assume that the interception of CII and CC are required.

### H.1.1 Call Origination

The Figure H.1 illustrates a case where an Intercept Subject (Party-A) originates the call. The called party is Party-B.

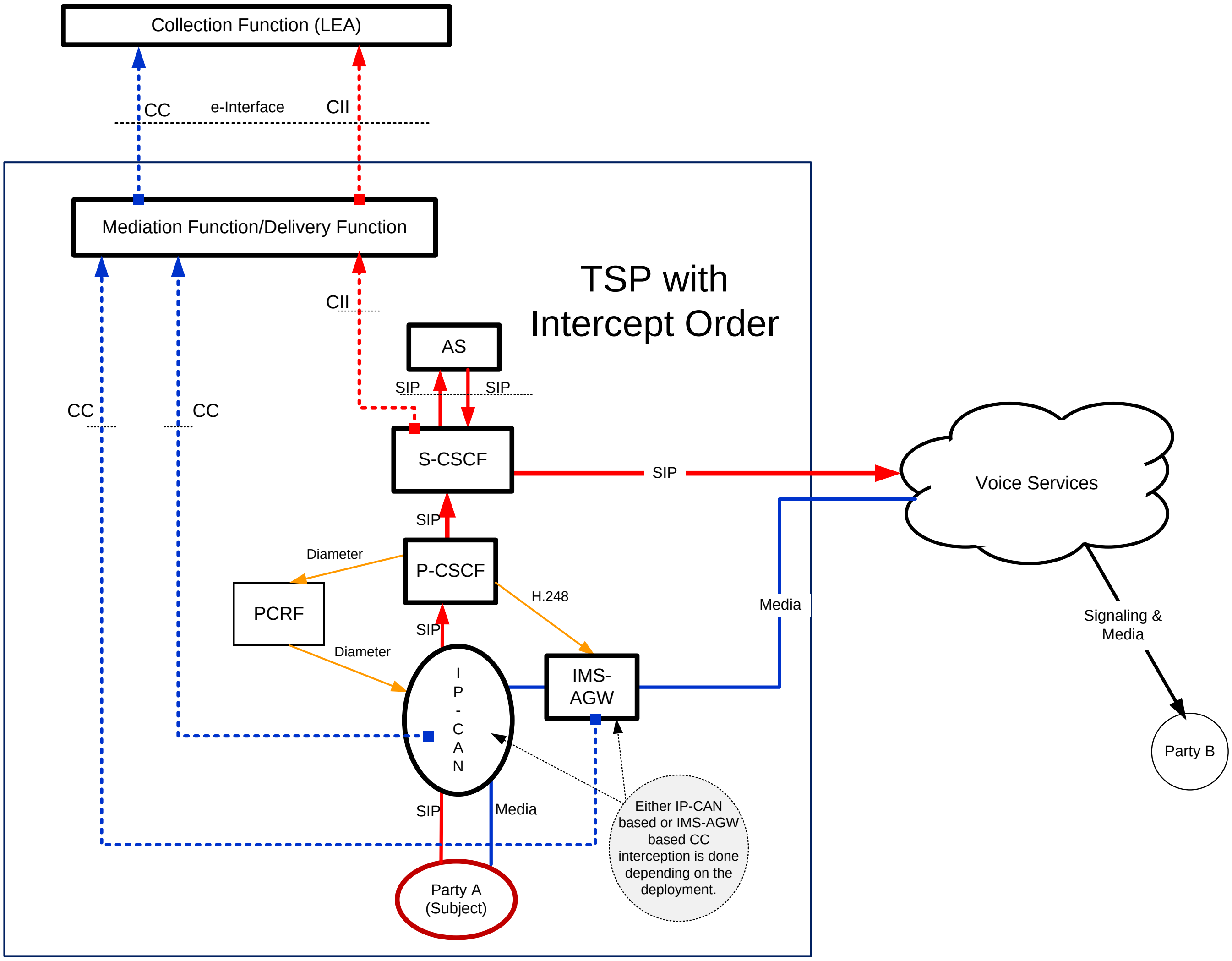


**Figure H.1 – Call Origination – CC Interception at IP-CAN or IMS-AGW**

The CII interception is done at the S-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Intercept Subject, depending on the deployment option. For example, if a network has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If a network has an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the Intercept Subject dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the intercept subject.

## H.1.2 Call Termination

The Figure H.2 illustrates a case where an Intercept Subject (Party-B) receives a call. The calling party is Party-A.

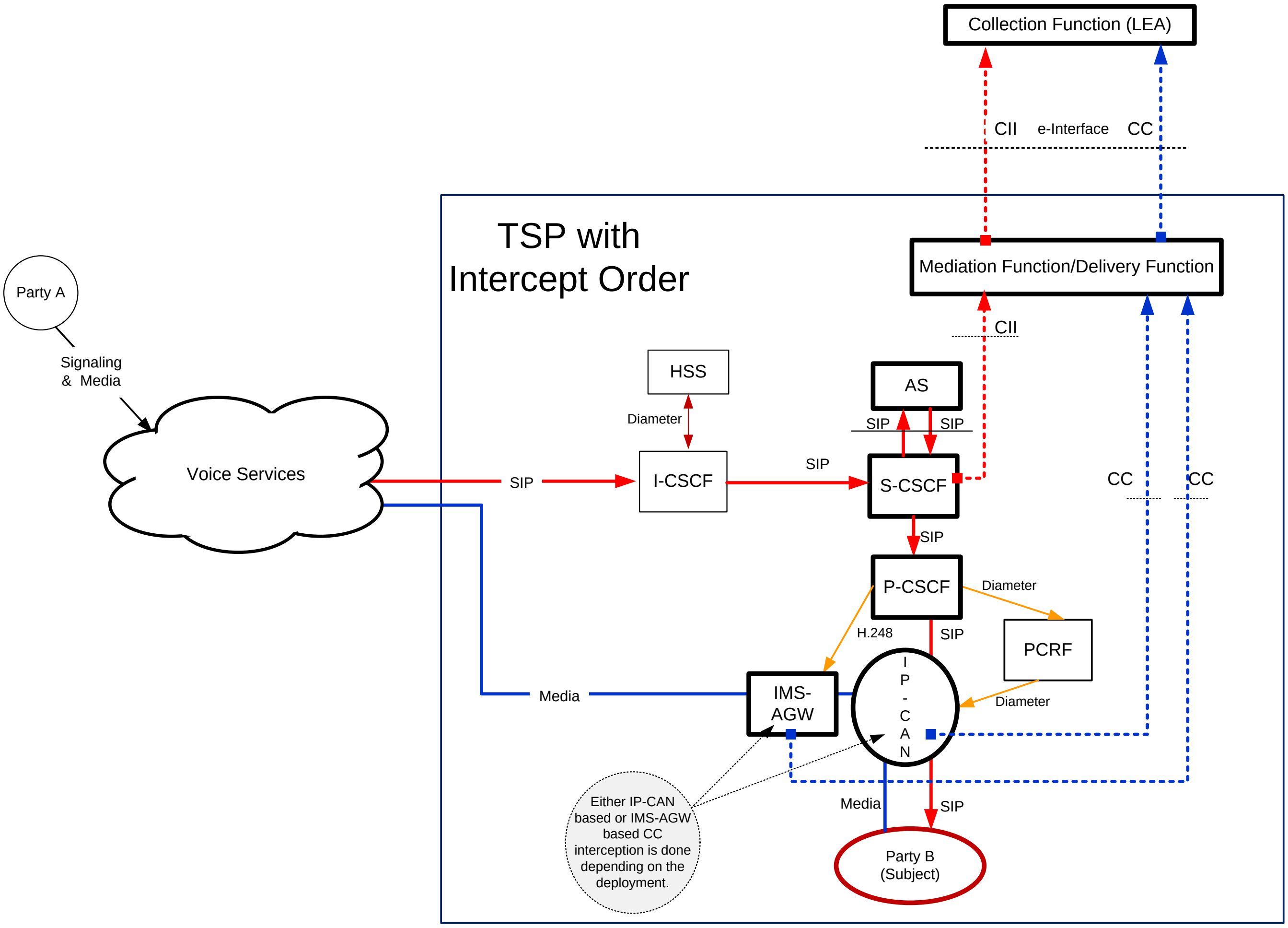


**Figure H.2 – Call Termination – CC Interception at IP-CAN or IMS-AGW**

The CII interception is done at the S-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Intercept Subject, depending on the deployment option. For example, if a network has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If a network has an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the intercept subject dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the Intercept Subject.

## *H.2 Call Forwarding*

This clause includes three topology diagrams that illustrate the CC interception for forwarded calls.

- Intra-network call forwarding.
- Inter-network call forwarding to the PSTN.
- Inter-network call forwarding to IMS.

The diagrams show a cloud labelled “voice services” basically to indicate that the interception performed is independent from how the call is routed to, or routed from, the far end of the call.

The illustrations assume that the interception of CII and CC are required.

## H.2.1 Intra-Network Call Forwarding

The Figure H.3 illustrates a case where an incoming call to the Intercept Subject (Party-B) is forwarded (unconditionally) within the same IMS network. Party-C is the forwarded-to-party. Party-A is the calling party.

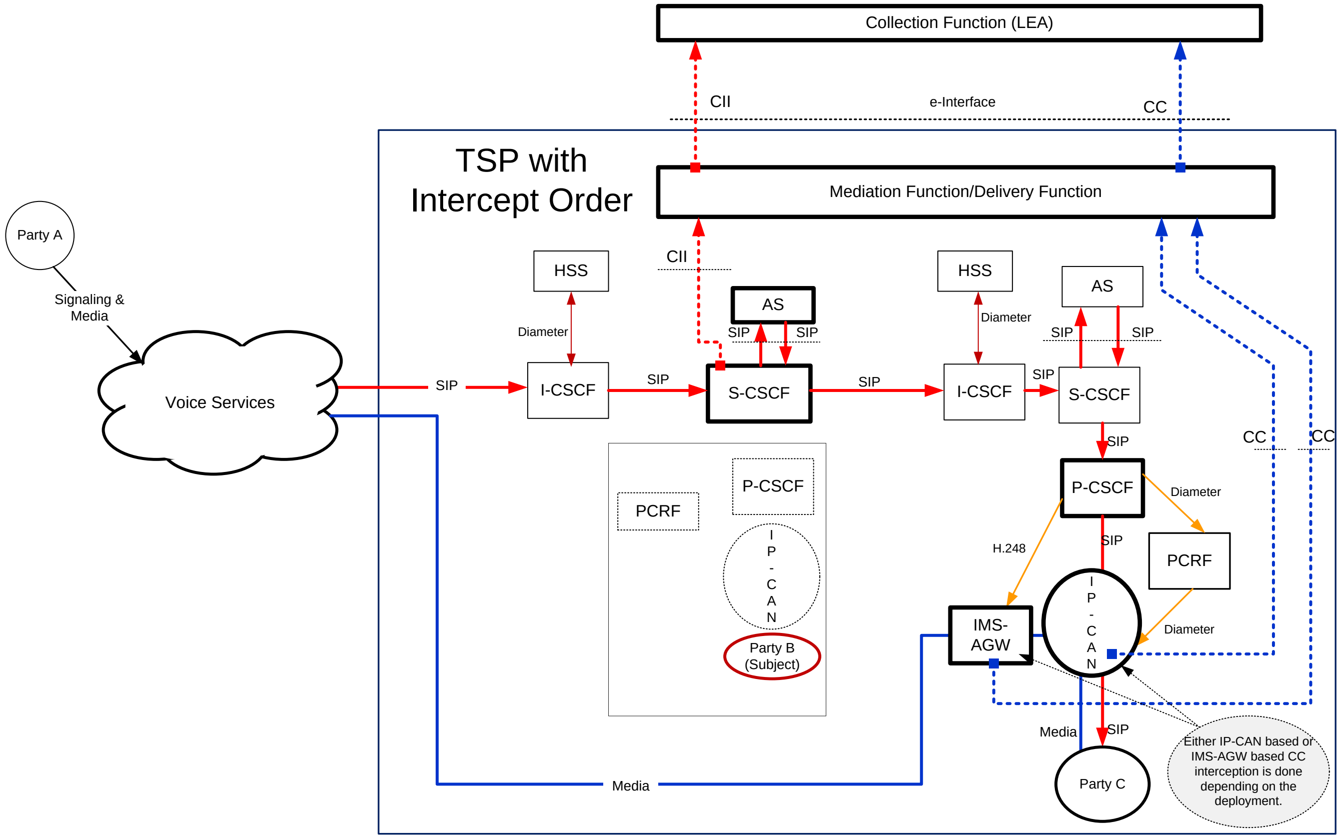


**Figure H.3 – Intra-network Call Forwarding – CC Interception at the IP-CAN or IMS-AGW**

The CII interception is done at the S-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Forwarded-to-Party (Party-C), depending on the deployment option. For example, if a network has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If a network has an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the Forwarded-to-Party dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the Forwarded-to-Party. The P-CSCF uses the History-Info or Diversion header to determine that CC interception will have to be performed. Those headers are pointing to the Intercept Subject (Party-B).

## H.2.2 Inter-network Call Forwarding – Forwarded-to-Party in PSTN

The Figure H.4 illustrates a case where an incoming call to the Intercept Subject (Party-B) is forwarded (unconditionally) to PSTN. Party-A is the calling party. Party-C is the forwarded-to-party in the PSTN.

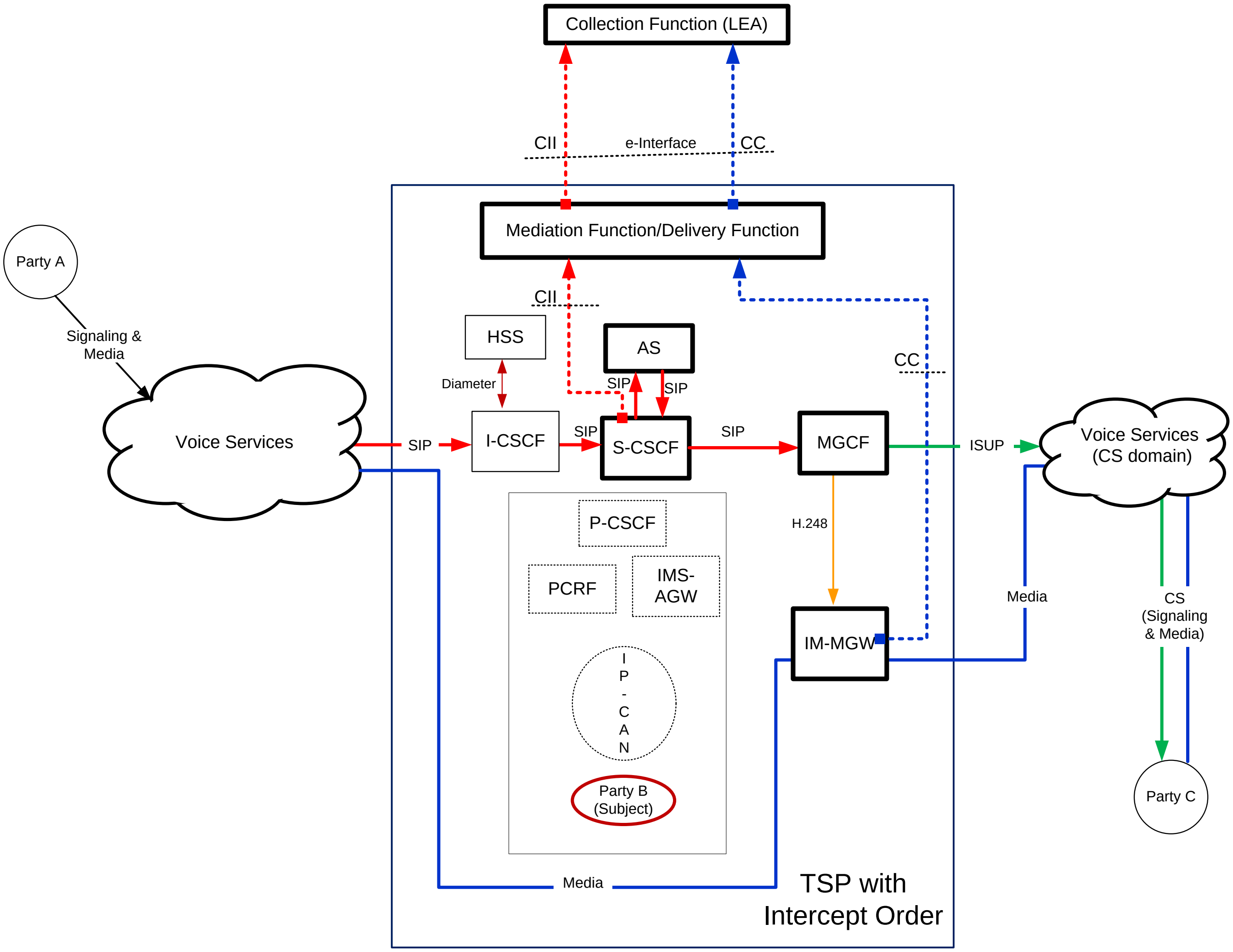


**Figure H.4 – Inter-Network Call Forwarding (to PSTN) – CC Interception at IM-MGW**

The CII interception is done at the S-CSCF that serves the Intercept Subject.  The CC interception is done at the egress IM-MGW as the call leaves the IMS network serving the Intercept Subject to the PSTN.

The egress MGCF dynamically triggers the CC interception at the egress IMS-MGW. The egress MGCF uses the History-Info or Diversion header to determine that CC interception will have to be performed. Those headers are pointing to the Intercept Subject (Party-B).

### H.2.3 Inter-network Call Forwarding – Forwarded-to-Party in IMS

The Figure H.5 illustrates a case where an incoming call to the Intercept Subject (Party-B) is forwarded (unconditionally) to a user in another IMS network.  Party-A is the calling party. Party-C is the forwarded-to-party in another IMS network.

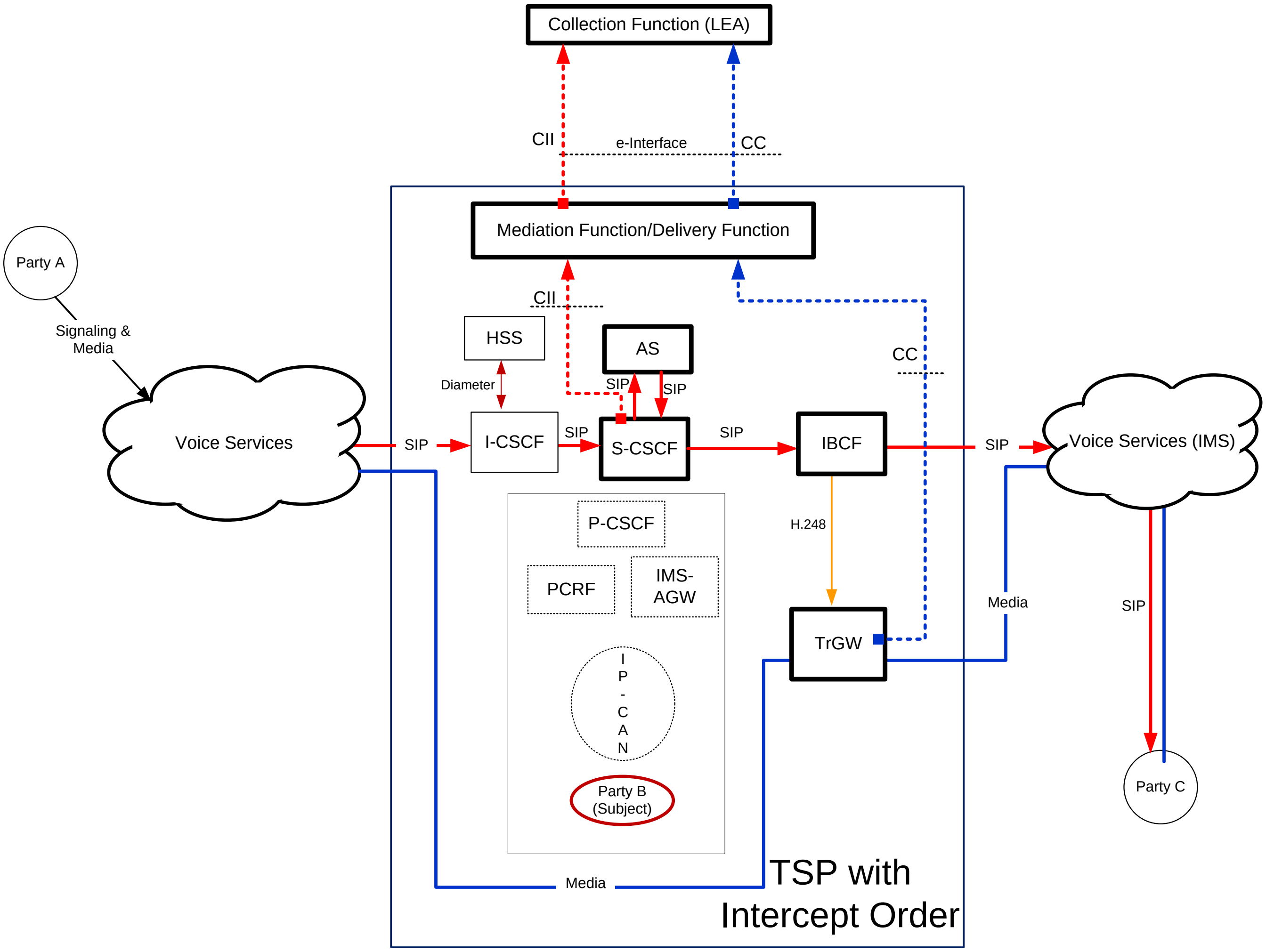


**Figure H.5 – Inter-Network Call Forwarding (to IMS) – CC Interception at TrGW**

The CII interception is done at the S-CSCF that serves the Intercept Subject. The CC interception is done at the egress TrGW as the call leaves the IMS network serving the Intercept Subject to another IMS network.

The egress IBCF dynamically triggers the CC interception at the egress TrGW. The egress IBCF uses the History-Info or Diversion header to determine that CC interception will have to be performed. Those headers are pointing to the Intercept Subject (Party-B).

## *H.3 Roaming*

This clause includes four topology diagrams that illustrate the CC interception for roaming cases.

- Call origination from a roaming Intercept Subject.
- Call termination to a roaming Intercept Subject.
- Intra-network call forwarding to a roaming Forwarded-to-party.
- Call origination from a roaming Intercept Subject when optimal media routing is employed with Local Breakout (LBO).

The diagrams show a cloud labelled “voice services” basically to indicate that the interception performed is independent from how the call is routed to, or routed from, the far end of the call.

When the Intercept Subject is roaming, the illustrations assume that both HPLMN and VPLMN have independent lawful authorization to perform the interception on the Intercept Subject. LEA-1 is monitoring in the VPLMN and LEA-2 is monitoring in HPLMN.

The illustrations assume that the interception CII and CC are required for in both HPLMN and VPLMN.

## H.3.1 Call Origination from Roaming Intercept Subject

The Figure H.6 illustrates a case where an Intercept Subject (Party-A) is roaming and originates the call. The called party is Party-B.

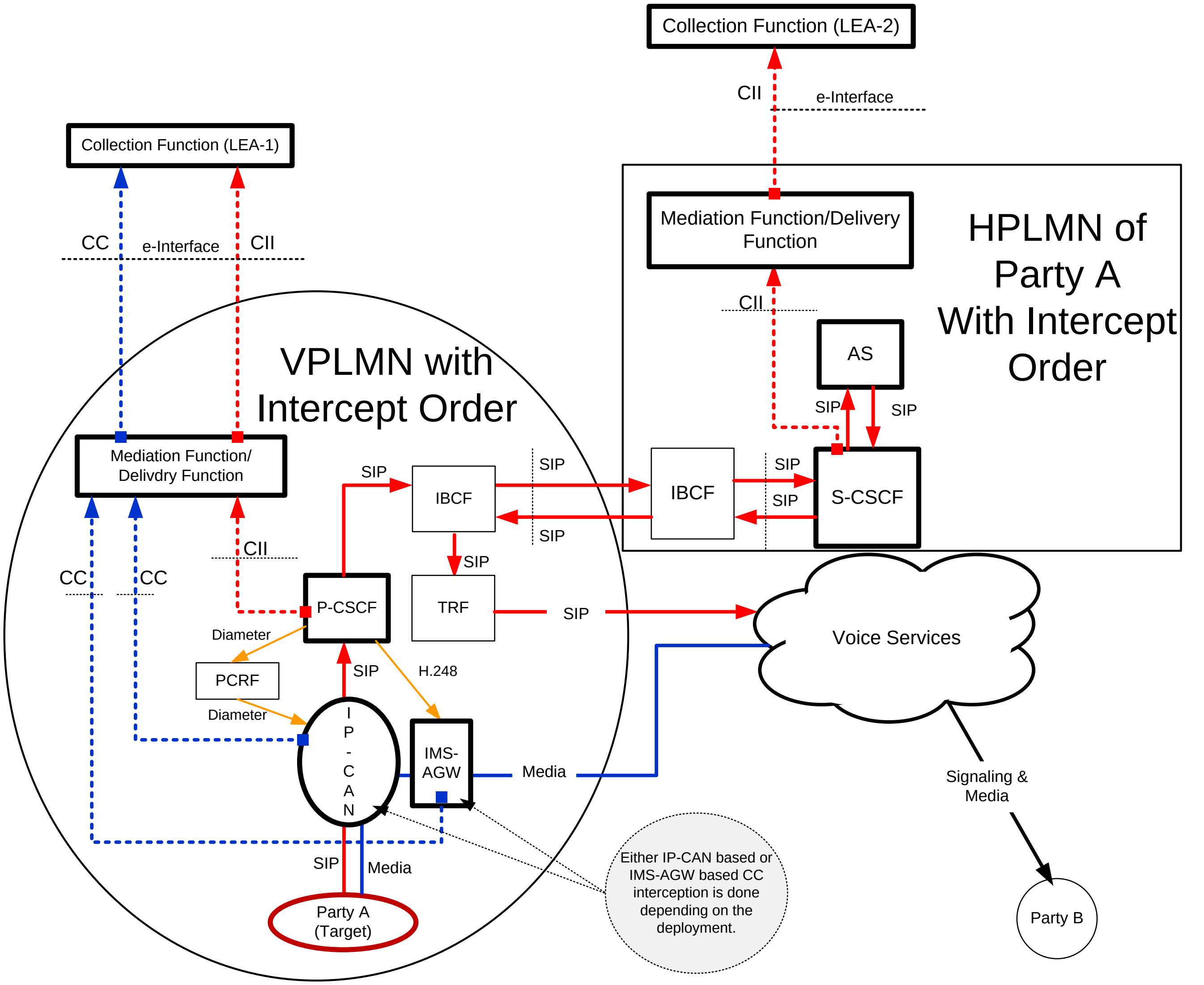

Collection Function (LEA-2)
CII
e-Interface
Collection Function (LEA-1)
CC
e-Interface
CII
Mediation Function/Delivery Function
HPLMN of Party A With Intercept Order
CII
AS
SIP
SIP
VPLMN with Intercept Order
Mediation Function/ Delivdry Function
SIP
IBCF
SIP
IBCF
SIP
S-CSCF
SIP
SIP
SIP
CII
CC
CC
P-CSCF
TRF
SIP
Voice Services
Diameter
PCRF
SIP
H.248
Diameter
I P - C A N
IMS-AGW
Media
Signaling & Media
SIP
Media
Party A (Target)
Either IP-CAN based or IMS-AGW based CC interception is done depending on the deployment.
Party B

**Figure H.6 – Call Origination with roaming – CC Interception at IP-CAN or IMS-AGW and TrGW**

### H.3.1.1 VPLMN Interception

This refers to Figure H.6.

The CII interception is done at the P-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Intercept Subject, depending on the deployment option. For example, if the VPLMN has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If the VPLMN has deployed an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the Intercept Subject dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the intercept subject.

### H.3.1.2 HPLMN Interception

This refers to Figure H.6.

The CII interception is done at the S-CSCF that serves the Intercept Subject. The CC interception is done at the ingress TrGW (within the HPLMN) through which the media enters the HPLMN.

The ingress IBCF, through which the call enters the HPLMN, dynamically triggers the CC interception at the TrGW.

## H.3.2 Call Termination to Roaming Intercept Subject

The Figure H.7 illustrates a case where an Intercept Subject (Party-B) is roaming and receives an incoming call. The calling party is Party-A.

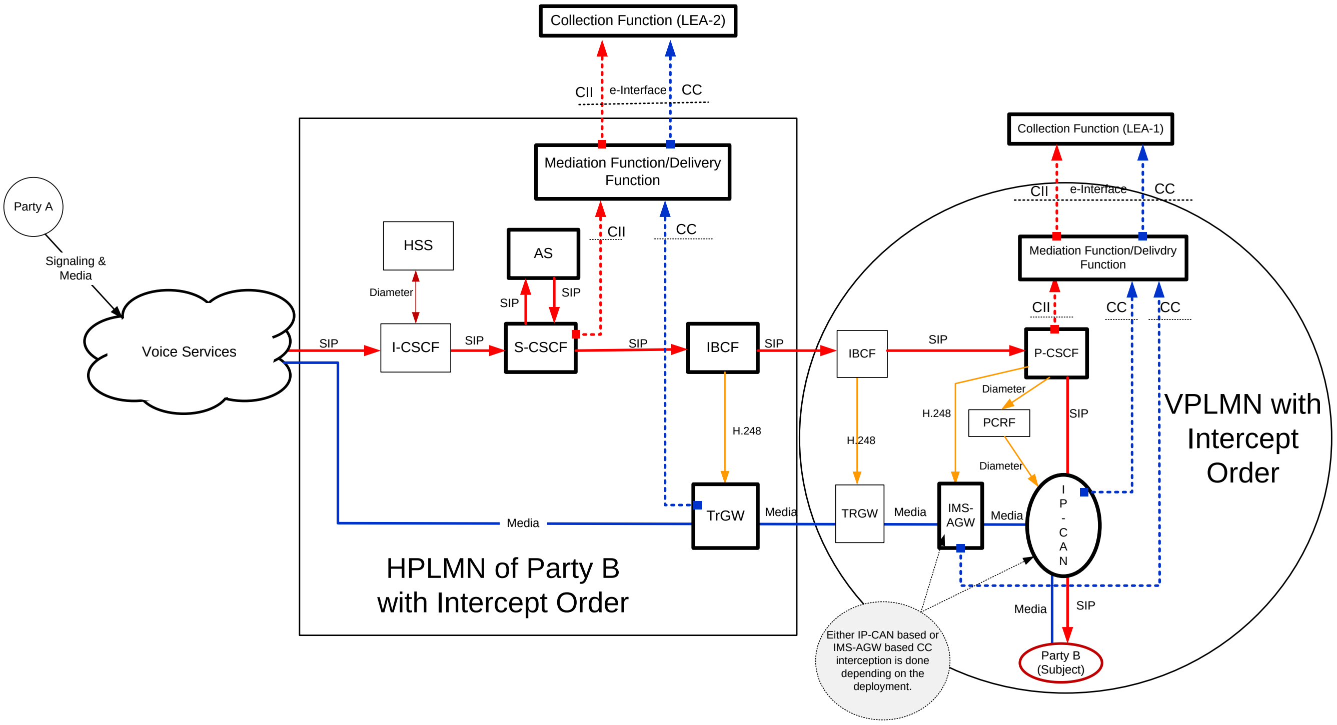

Collection Function (LEA-2)
CII
e-Interface
CC
Mediation Function/Delivery Function
CII
CC
Party A
Signaling & Media
Voice Services
HSS
Diameter
AS
SIP
SIP
SIP
I-CSCF
SIP
S-CSCF
SIP
IBCF
SIP
H.248
TrGW
Media
Media
HPLMN of Party B with Intercept Order
Collection Function (LEA-1)
CII
e-Interface
CC
Mediation Function/Delivdry Function
CII
CC
CC
IBCF
SIP
P-CSCF
Diameter
H.248
PCRF
SIP
H.248
Diameter
VPLMN with Intercept Order
TRGW
Media
IMS-AGW
Media
I P - C A N
Media
SIP
Party B (Subject)
Either IP-CAN based or IMS-AGW based CC interception is done depending on the deployment.

**Figure H.7 – Call Termination with roaming – CC Interception at TrGW and IP-CAN or IMS-AGW and TrGW**

### H.3.2.1 VPLMN Interception

This refers to Figure H.7.

The CII interception is done at the P-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Intercept Subject, depending on the deployment option. For example, if the VPLMN has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If the VPLMN has deployed an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the Intercept Subject dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the intercept subject.

### H.3.2.2 HPLMN Interception

This refers to Figure H.7.

The CII interception is done at the S-CSCF that serves the Intercept Subject.  The CC interception is done at the egress TrGW (within the HPLMN) through which the media leaves the HPLMN.

The egress IBCF, through which the call leaves the HPLMN, dynamically triggers the CC interception at the TrGW.

## H.3.3 Roaming Forwarded-to-Party

The Figure H.8 illustrates a case where an incoming call to an Intercept Subject (Party-B) who is not roaming is forwarded within the same IMS network, but the forwarded-to-party is roaming. The Party-C is the roaming Forwarded-to-Party.  The calling party is Party-A.

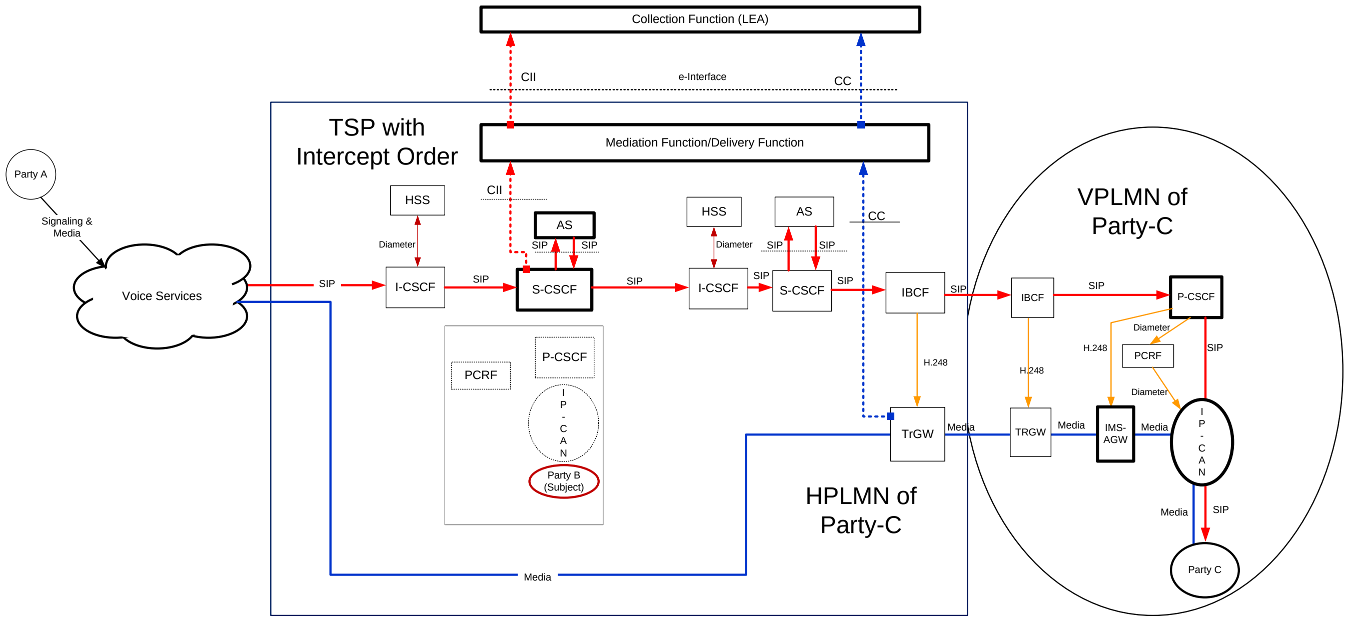


**Figure H.8 – Forwarded-to-Party Roaming – CC Interception at TrGW and IP-CAN or IMS-AGW**

### H.3.3.1 VPLMN Interception

This refers to Figure H.8.

Since the Intercept Subject is not roaming, no interception of CII or CC is done in the VPLMN even when the VPLMN provider is served with a lawfully authorized intercept order.

### H.3.3.2 HPLMN Interception

This refers to Figure H.8.

The CII interception is done at the S-CSCF that serves the Intercept Subject.  The CC interception is done at the egress TrGW (within the HPLMN) through which the media leaves the HPLMN.

The egress IBCF, through which the call leaves the HPLMN, dynamically triggers the CC interception at the TrGW. The egress IBCF uses the History-Info or Diversion header to determine that CC interception will have to be performed. Those headers are pointing to the Intercept Subject (Party-B).

## H.3.4 Roaming with Local Breakout (Origination)

The Figure H.9 illustrates a case where an Intercept Subject (Party-A) is roaming and originates the call. The called party is Party-B. In this illustration, the HPLMN loops back the call to the VPLMN. This is also known as Local Breakout with optimal media routing.

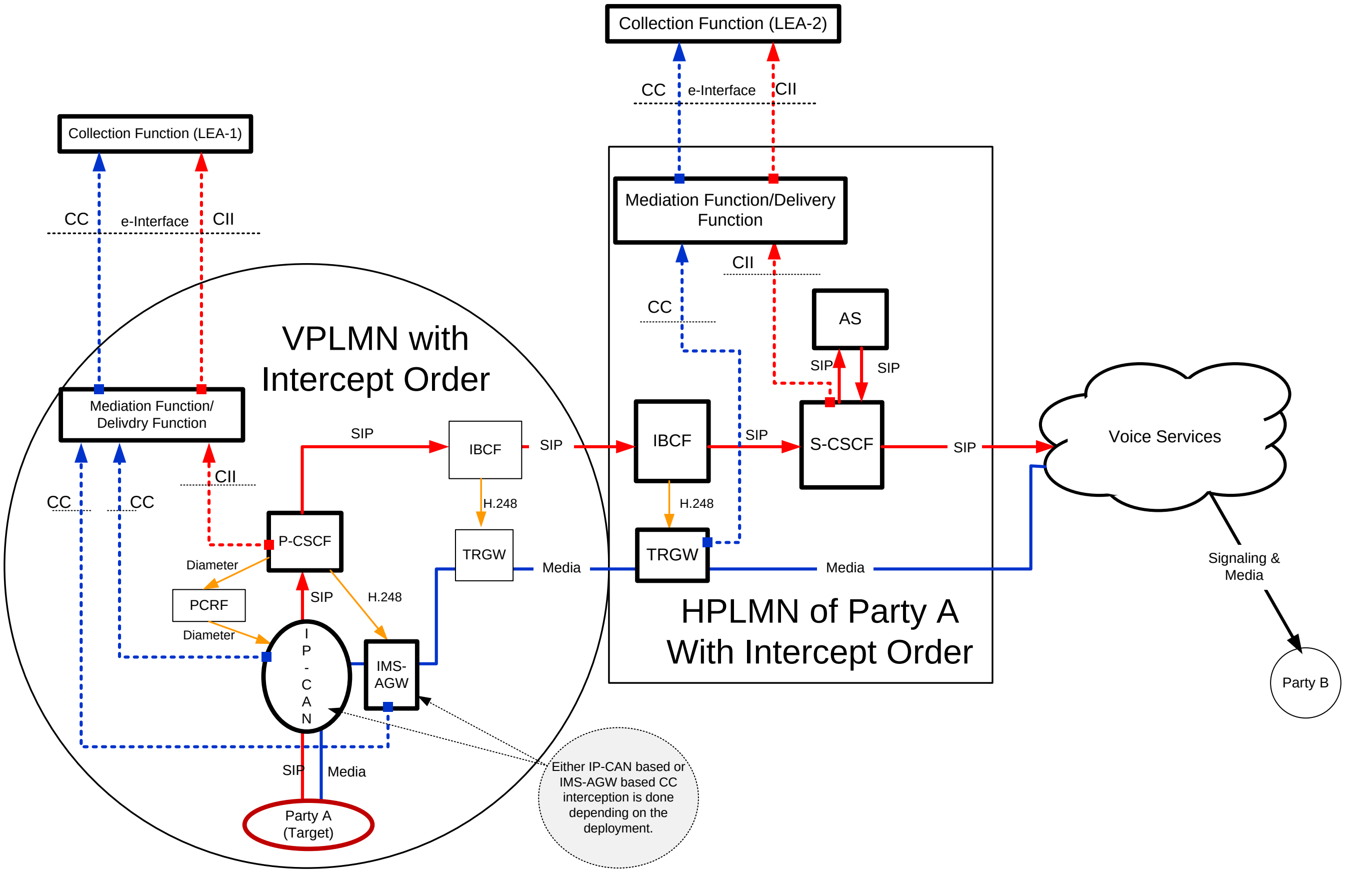

Collection Function (LEA-2)
CC
e-Interface
CII
Collection Function (LEA-1)
CC
e-Interface
CII
Mediation Function/Delivery Function
CII
CC
AS
SIP
SIP
VPLMN with Intercept Order
Mediation Function/ Delivdry Function
SIP
IBCF
SIP
IBCF
SIP
S-CSCF
SIP
Voice Services
CII
CC
CC
H.248
H.248
P-CSCF
TRGW
Media
TRGW
Media
Diameter
SIP
H.248
Signaling & Media
PCRF
HPLMN of Party A With Intercept Order
Diameter
I P - C A N
IMS-AGW
Party B
SIP
Media
Party A (Target)
Either IP-CAN based or IMS-AGW based CC interception is done depending on the deployment.

Figure H.9 – Call Origination Roaming (Local Breakout) – CC Interception at IP-CAN or IMS-AGW

### H.3.4.1 VPLMN Interception

This refers to Figure H.9.

The CII interception is done at the P-CSCF that serves the Intercept Subject. The CC interception is done at the IP-CAN (P-GW or GGSN) or IMS-AGW associated with the Intercept Subject, depending on the deployment option. For example, if the VPLMN has not deployed an IMS-AGW, then the CC interception is done at the IP-CAN. If the VPLMN has deployed an IMS-AGW deployed, then the CC interception can be done at the IMS-AGW.

The P-CSCF that serves the Intercept Subject dynamically triggers the CC interception at the IP-CAN or IMS-AGW associated with the intercept subject.

### H.3.4.2 HPLMN Interception

This refers to Figure H.9.

The CII interception is done at the S-CSCF that serves the Intercept Subject.  Since the media does not enter the HPLMN, no CC interception is performed for this call in the HPLMN. The HPLMN sends a CCUnvailable LAES message to the LEAs to indicate that the CC interception is not done due to Intercept Subject’s roaming situation.