ATIS-0700005

LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE (LAES) FOR 3GPP IMS-BASED VOIP AND OTHER MULTIMEDIA SERVICES

TECHNICAL REQUIREMENTS

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 23 industry committees and its Incubator Solutions Program.

< http://www.atis.org/ >

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.

ATIS-0700005, *Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services*

Is an ATIS Standard developed by the **Lawful Interception (LI)** Subcommittee under the **ATIS Wireless Technologies and Systems Committee (WTSC)**.

Technical Requirements for

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

Secretariat

Alliance for Telecommunications Industry Solutions

Approved May 2007

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.

This ATIS Standard is a 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 Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

The WTSC Committee, which was responsible for the development of this ATIS Standard, had the following members:

M. Younge, WTSC Chair
D. Zelmer, WTSC Vice-Chair
C. Underkoffler, ATIS Chief Editor

Organization Represented	Name of Representative	Organization Represented	Name of Representative
Alcatel USA Inc.	Ken Biholar Laurent Cruchant (Alt.)	Nokia Siemens Networks	Nagaraja Rao David Francisco (Alt.)
ArrayComm, Inc.	Joanne Wilson Mel Woinsky (Alt.)	Nokia Telecommunications Inc.	Ed Ehrlich Shou Gung (Alt)
AT&T	Randolph Wohlert Chuck Bailey	Nortel	Amar Deol Ronald D. Ryan (Alt)
C.S.I. Telecommunications	Michael S. Newman Thomas G. Croda (Alt.)	PSEP Canada	Sim Simanis Gary Hutchinson (Alt)
Cingular Wireless LLC	Don Zelmer Marc Grant (Alt.)	Qualcomm Incorporated	Mark Epstein Ed Tiedemann (Alt.)
Department of Defense	Chris Fitzgerald	Qwest	Michael Fargano
Embarq	Carl M. Coopage John M. Heinz (Alt)	Research In Motion	Atul Asthana Adrian Buckley
Ericsson Incorporated	Jim Ragsdale Pierre Truong (Alt)	Rogers Wireless Inc.	Edward O'Leary Tak Wing Wan
FBI ESTS	Marybeth Paglino Edward Ignacio (Alt)	SOMA Networks	Jonathan Jaeger
Hewlett-Packard	Steve Mills	SS8 Networks Inc.	Cemal Dikman Scott Coleman (Alt)
InterDigital Communications	Brian Kiernan Gil LaVean (Alt.)	Telcordia Technologies	Jim Garrahan Cliff Halevi (Alt.)
Kineto Wireless	Mike Gallagher Rajeev Gupta (Alt)	Tellabs Operations, Inc.	Kevin Mooney William A. Walker (Alt.)
Kyocera International	Dr. R. Canchi Terry Lingren (Alt)	T-Mobile USA Inc.	Gary K. Jones Mark Younge (Alt.)
LGE Mobile Research LLC	Soon Yil Kwon	TruePosition, Inc.	Gustavo Pavon
Lucent Technologies	Robert B. Beeson Jane Brownley (Alt.)	Union Telephone Company	David Cotton, Jr.
Motorola Inc.	Syed Husain	VeriSign Inc.	Anthony M. Rutkowski
National Communications System	Carol-Lyn Taylor Nicholas Andre (Alt.)	Verizon Communications	Wendy Pugh J. Martin Carroll (Alt)
National Telecom & Info Admin – NTIA	Tim Riley		
Navini Networks	David Maez Sai Subramanian (Alt)		

The WTSC Lawful Interception (LI) Subcommittee, which was responsible for the development of this ATIS Standard, had the following members:

Peter Musgrove (Cingular/AT&T), WTSC LI Chair
Nagaraja Rao (Nokia Siemens Networks), WTSC LI Vice-Chair
Nagaraja Rao (Nokia Siemens Networks), WTSC Technical Editor

Technical Contributors (alphabetical by company name)

Name	Company
Terry Jacobson	Alcatel-Lucent
Peter Musgrove	Cingular Wireless/AT&T
Pierre Truong	Ericsson
Margaret Livingston	ETSC/CIU
Selvam Rengasami	ETSC/CIU
Bob Beeson	Lucent Technologies
Brye Bonner	Motorola
Ming Shou Gung	Nokia
Nagaraja Rao	Nokia Siemens Networks
Amar Deol	Nortel Networks
Ron Ryan	Nortel Networks
Takwing Wan	Rogers Wireless
Leonti Dailis	SS8
Michael McAdoo	T-Mobile
Mark Younge	T-Mobile

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Technical Requirements for

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 Content (CC), Communication-Identifying Information (CII), or both – 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 and 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.

Push to talk over Cellular (PoC) is example of an IMS-based multimedia services. The specification of the interface between a TSP and an LEA for the reporting of LAES for 3GPP IMS-based PoC service is beyond the scope of this ATIS Standard. PoC can be viewed as an IMS-based interactive conferencing application with additional features such as buddy list updates, presence updates, and floor control management.

 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.

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 6 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 6)*, v6.1.14.0.

[229]   3GPP TS 24.229, *IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 6)*, v6.11.0.

[107]   3GPP TS 33.107, *Lawful interception architecture and functions (Release 6)*, v6.6.0.

[108]   3GPP TS 33.108, *Handover interface for Lawful Interception (Release 6)*, v6.10.0.

2.2 Alliance for Telecommunications Industry Solutions (ATIS)

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

[678]   ATIS-1000678.2006, *LAES for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2*; and ATIS-1000678.a.2007, *Supplement for LAES for Voice over Packet Technologies in Wireline Telecommunications Networks*.

[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)

[99-230]   FCC 99-230, CC Docket No. 97-213, *Third Report and Order*, Released August 31, 1999.[1]

[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).[2]

[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).[3]

2.6 103rd Congress

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

---

[1] Available at < www.fcc.gov/Bureaus/Engineering_Technology/Orders/1999/fcc99230.pdf >.

[2] Available at < http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf >.

[3] Available at < http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.doc >.

[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 which 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 which 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 network operator, access provider, service provider, and the results of interception are delivered from a network operator, access provider, 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.

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
CC DF	Communication Content Delivery 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
GMT	Greenwich Mean Time
FCC	Federal Communications Commission
HI	Handover Interface
HI2 IRI	Handover Interface 2 Intercept Related Information
HI3 CC	Handover Interface 3 Communication Content
HSS	Home Subscriber System
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
I-CSCF	Interrogating CSCF
IMS	IP Multimedia core network Subsystem

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
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
PoC	Push to talk over Cellular
PSTN	Public Switching Telephone Network
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SGSN	Serving General Packet Radio Service (GPRS) Support Node
TCP	Transaction Control Protocol
THIG	Topology Hiding Inter-network Gateway
TSP	Telecommunications Service Provider
USC	United States Code
VoIP	Voice over IP
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 1.
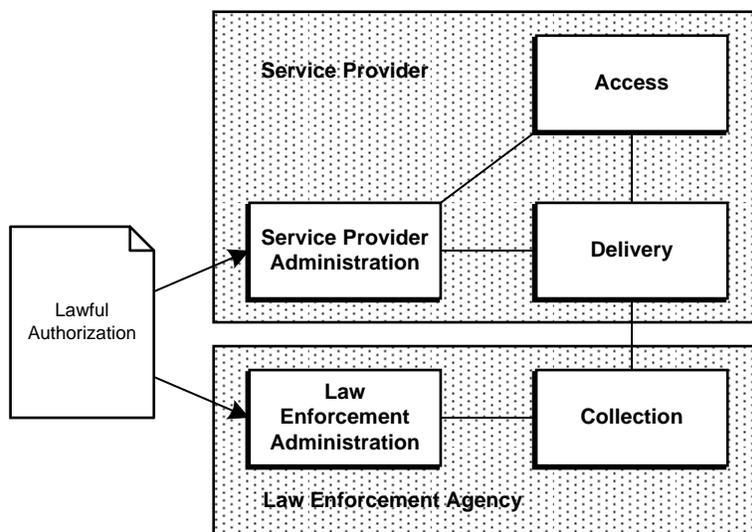
Figure 1: Electronic Surveillance Model

- 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.

When the voice, video, other IMS-based multimedia based services or any combination of these communication services are bundled as part of a single architecture (i.e., IMS), the LI capabilities shall be provided.

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").

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 is for further study.

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.

4.4.1.1 CII Mapped Event Reporting

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

♦ Answer
♦ Change
♦ Origination
♦ Redirection
♦ Release
♦ ServingSystem
♦ ConferencePartyChange
♦ TerminationAttempt
♦ Connection
♦ ConnectionBreak
♦ NetworkSignal
♦ SubjectSignal
♦ MediaAndAddressReporting
♦ DirectSignalReporting (DSR)

The DSR message may be used in conjunction with the above messages to report signaling that cannot be mapped.

See Annex A of this ATIS Standard for the LAES support for IMS-based VoIP and other multimedia services specific SIP to surveillance message mapping.

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.

4.4.1.2 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 established, the TSP shall isolate and report to the LEA the dialled or signalled digits, when reasonably available, as CII to the LEA. A TSP may report dialled or signalled digits, when reasonably available, as CII. See Annex F of [678] for additional information. The following message is used for the Dialed Digit Extraction (DDE) event reporting:

♦ DialedDigitExtraction

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

4.4.1.3 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 provides 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.

The location information in TerminationAttempt described in [678] shall not be reported.

4.4.1.4 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).

4.4.1.5 CII Event Reporting Requirements

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

4.4.2 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.

♦ A CII message shall be sent from the TSP's IAP to the LEA's CF within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the CII event time-stamped to an accuracy of at least 200 milliseconds as defined in [99-230].

♦ If the GMT offset, as defined in [X-680], of the CII IAP is available at the CII IAP or available at the MF/DF, it shall be reported as part of the timestamp information.

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

♦ When the CC is intercepted, the IAP shall expeditiously transmit the CC towards the MF/DF.

4.4.3 CC Related Events

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

♦ CCOpen
♦ CCChange
♦ CCClose
♦ CCUnavailable
♦ UUContent

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 2 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.
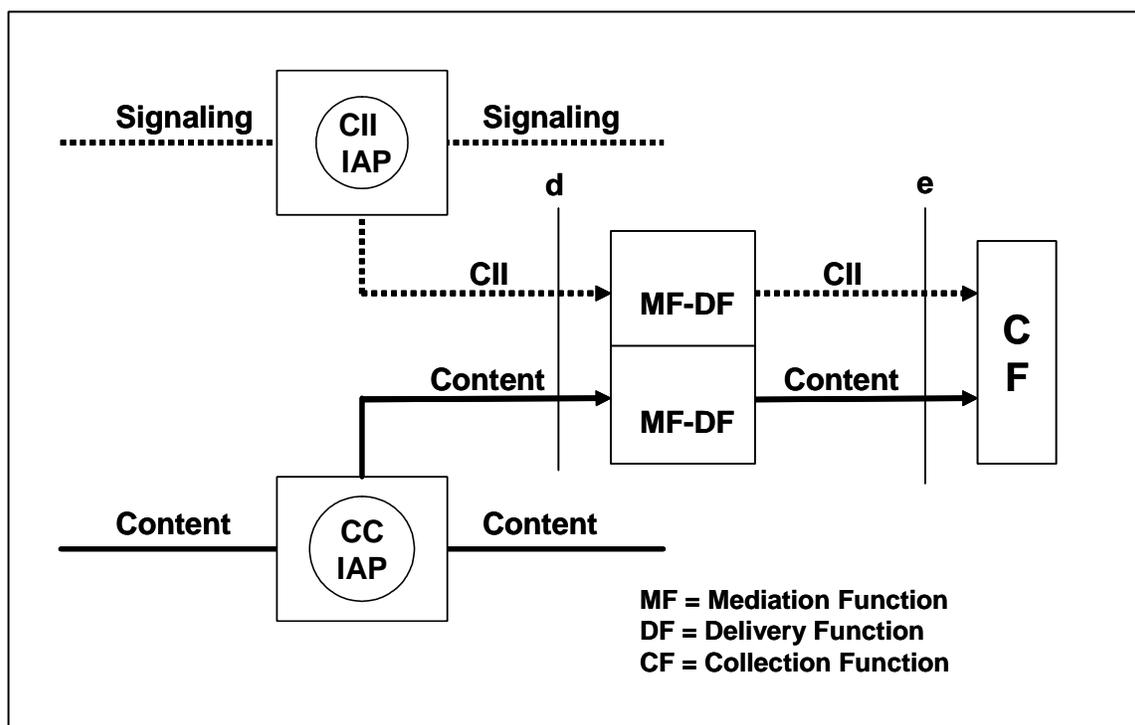
Figure 2: Functional LI Architecture

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

With respect to multimedia services, IAP(s) are located in the network where multimedia (e.g., VoIP) communications are lawfully intercepted. There are two fundamental types of IAP(s):

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

CII-IAP is associated with CII intercept functions that perform the actual interception of CII, and 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.   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.

5.3 LAES CII Messages

5.3.1 IMS 3GPP VoIP CII Event Reporting

The following LAES messages, which are defined in [678], are utilized for IMS 3GPP VoIP CII reporting:

- ♦ Answer
- ♦ CCChange
- ♦ CCClose
- ♦ CCOpen
- ♦ CCUnavailable
- ♦ Change
- ♦ ConferencePartyChange
- ♦ Connection
- ♦ ConnectionBreak
- ♦ DialedDigitExtraction (DDE)
- ♦ DirectSignalReporting
- ♦ MediaAndAddressReporting

- ♦ NetworkSignal
- ♦ Origination
- ♦ Redirection
- ♦ Release
- ♦ ServingSystem
- ♦ SubjectSignal
- ♦ TerminationAttempt message

5.3.2 ServingSystem Event Reporting

5.3.2.1 ServingSystem Event Reporting for SIP Registration

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

5.3.2.2 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, either of the following alternatives can be used:

- ♦ The ServingSystem message as described in the [J-STD-025-B] – e.g., for legacy HLR(s).
- ♦ The ServingSystem message as described in the [678] – e.g., for HSS(s).

In the latter case, only the parameters shown in Table 1 shall apply:

Table 1: 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.

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 a 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 reside within the IP connectivity access network (IP-CAN).

Subject to lawful authorization, CC redirected away from the IP-CAN to another network (e.g., PSTN), shall be provided if it is reasonably available within the TSP's network (e.g., at MGW).

Subject to lawful authorization, CC that is not available at the IP-CAN, but is reasonably available elsewhere within the TSP's network (e.g., at a MGW) shall be provided.

Annex A
(normative)

A MAPPING OF SIP CII MESSAGES

This annex is normative and is 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 provide 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 section provides additions or enhancements to the mapping tables 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].

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

Table A.1 describes the Mapping of SIP P-Access Location Information to [678] Mapped Messages. When this mapping is used the LocationType sub-parameter shall be coded as "P-A-N-I-Header".

Table A.1: Mapping of SIP P-Access Location Information to [678] Mapped Messages

SIP Message Header	ATIS-678 Mapped Message Parameter	Description
200-OK(INVITE) P-Access-Network-Info	Answer location [5] Location	Provides location information when available.
INVITE P-Access-Network-Info	Origination location [8] Location	Provides location information when available.
BYE P-Access-Network-Info	Release location [4] 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 [678] Mapped Messages. When delivering the location information contained in a Geolocation header of a SIP message, the LocationType sub-parameter shall be coded as "Geoloc-Header".

Table A.2: Mapping of SIP GeoLocation Information to [678] Mapped Messages

SIP Message Header	ATIS-678 Mapped Message Parameter	Description
200-OK(INVITE) Geolocation	Answer location [5] Location	Provides location information when available.
INVITE Geolocation	Origination location [8] Location	Provides location information when available.
BYE Geolocation	Release location [4] Location	Provides location information when available.

A.3 Multiple Location Information Types

If multiple location information types are available, then all shall be 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 Message Header	ATIS-678 Mapped Message Parameter	Description
REGISTER P-Visited-Network-Id	ServingSystem protocolSpcificParameters [14] sip [0] sipHeader [0]	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.
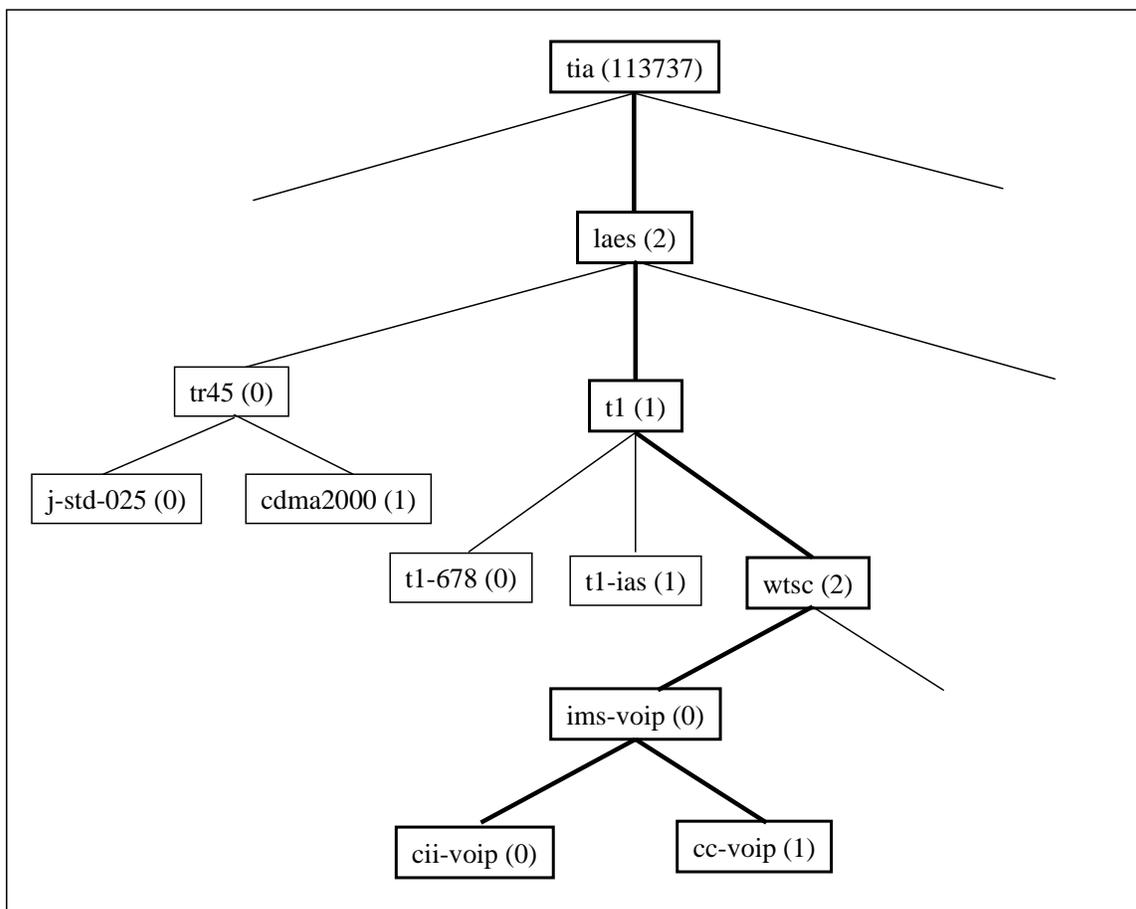
Figure B.1: IMS 3GPP VoIP Object Tree

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) member-body(2) us(840) tia(113737) laes(2) t1(1) wtsc (2)  ims-voip(0) cii-voip(0)
version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN

IMPORTS
```

-- Imports from ATIS-1000678-2006 Module

```
Answer,
CCClose,
CCOpen,
Change,
Origination,
Redirection,
Release,
ServingSystem,
TerminationAttempt,
ConferencePartyChange,
Connection,
ConnectionBreak,
DialedDigitExtraction,
NetworkSignal,
SubjectSignal,
DirectSignalReporting,
MediaAndAddressReporting,
CCChange,
CCUnavailable,
UUContent

FROM T1S1-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-
2(1)}
```

-- Imports from IMS-3GPP-VoIP-CC- Module

```
ims-3GPP-VoIP-CC-DeliveryHeaderModule-OID

FROM IMS-3GPP-VoIP-CC-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wtsc(2)  ims-voip(0) cc-voip(1)
version-1(0)};
```

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

```
cc-DeliveryHeaderModule-OID OBJECT IDENTIFIER ::=
{ims-3GPP-VoIP-CC-DeliveryHeaderModule-OID}

ims-3GPP-VoIP-CII-Module-OID  OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wtsc(2)  ims-voip(0) cii-voip(0)
version-1(0)}

protocolIdentifier  OBJECT IDENTIFIER  ::=  {ims-3GPP-VoIP-CII-Module-OID}

LAESProtocol ::= CHOICE {
     enhancedProtocol      IMS-3gpp-VoIP-CII-Protocol,
     laesMessage    IMS-3gpp-VoIP-CII-Message
}

IMS-3gpp-VoIP-CII-Protocol ::= SEQUENCE {
     protocolIdentifier                             OBJECT IDENTIFIER,
     ims-3gpp-VoIP-CII-Message          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,
     ims-3gpp-VoIP-change        [4] Change,
     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

}

Location ::= SET OF LocationInfo

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

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

-- IMS 3GPP VoIP Communication Content Delivery Module

IMS-3GPP-VoIP-CC-Module
```
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wtsc(2)  ims-voip(0) cc-voip(1)
version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS
```

-- Imports from ATIS-1000678-2006 Module

```
CC-APDU

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

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

```
ims-3GPP-VoIP-CC-DeliveryHeaderModule-OID   OBJECT IDENTIFIER  ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wtsc(2)  ims-voip(0) cc-voip(1)
version-1(0)}
```

```
IMS-3GPP-VoIP-CC-APDU  ::=  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. CSCF sends all the SIP messages to the MF/DF. 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.
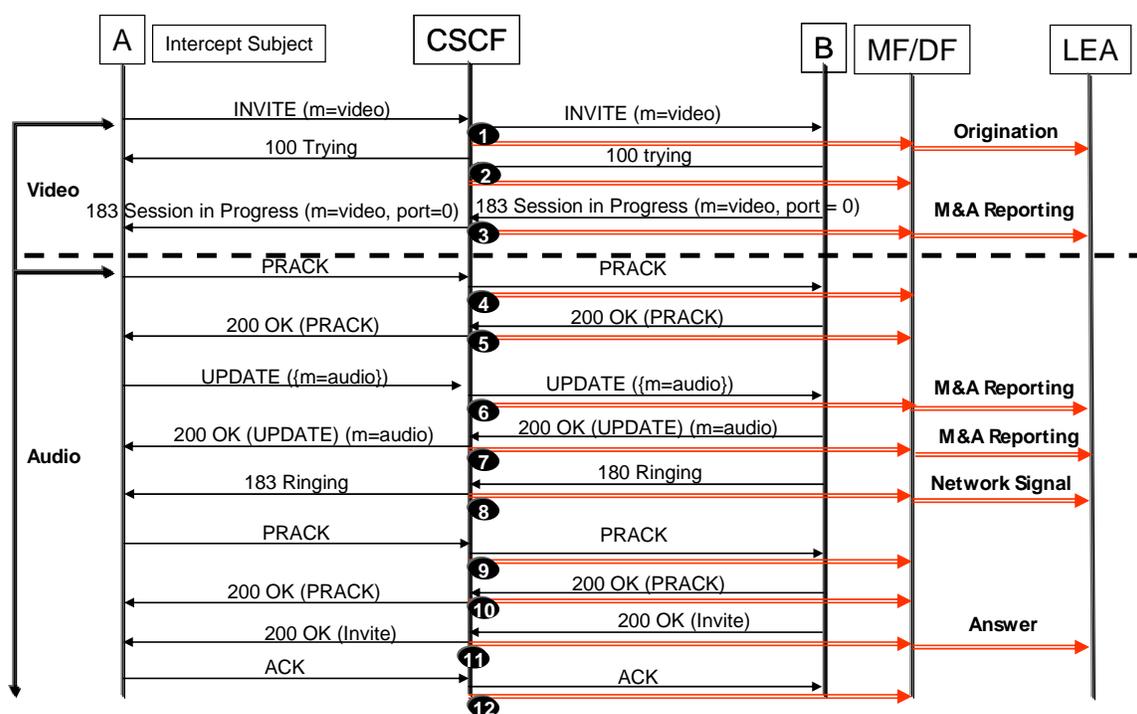

Figure C.1: Call Flow Example: Video Session downgraded mid-stream to Audio Session

C.1.1 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 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 SIGNALLING 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.

In principle, an IMS-based VoIP SIP session establishment is independent of the IP connectivity access network that provides the interception access points for the interception of CC. Within the flow diagrams, the IP connectivity access network is identified as IP-CAN and it could be GPRS, WLAN, or another network to which the requirements identified within this ATIS Standard are applicable.

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]).
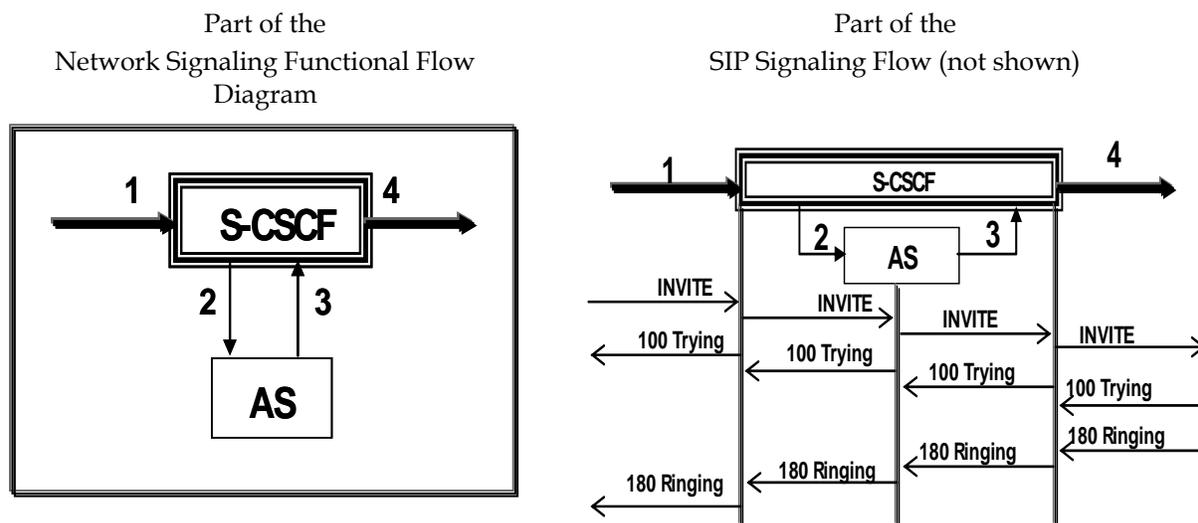

Figure D.1: Functional Flow Diagram and Sample Signaling Flow – Illustration 1

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 3-line box. The Interfaces from which that node delivers the intercepted SIP messages are shown using the thick lines.

When an incoming call arrives at the I-CSCF within the Egress IMS network, the I-CSCF would query the 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.
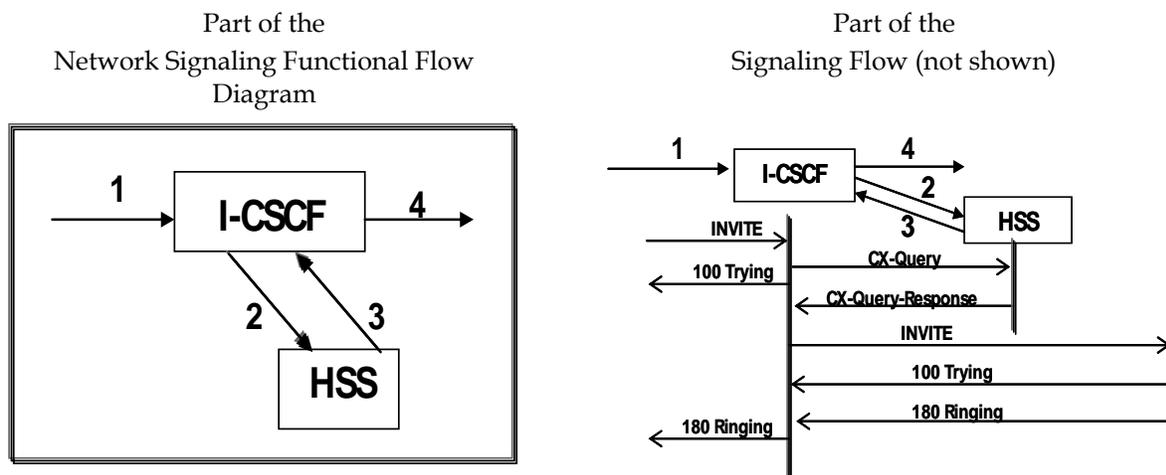

Figure D.2: Functional Flow Diagram and Sample Signaling Flow – Illustration 2

When two or more IMS networks are shown within a functional flow diagram, the implication is that those IMS networks could be owned by different service providers. In that scenario, the service provider of the Home IMS Network may deploy a Topology Hiding Inter-Network Gateway (THIG). The diagrams show the optional THIG with the dotted line.
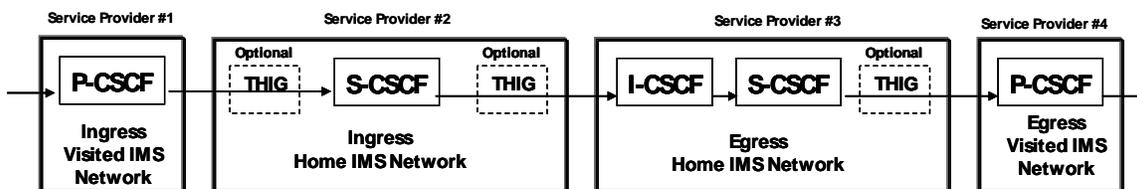

Figure D.3: Multiple IMS Networks – Illustration 3

With the exception of the optional THIG, other network elements involved along the signaling path are the same irrespective of whether those IMS networks are owned by the same service provider or not. Within the IMS-domain, the P-CSCF can either be in the user's Home IMS network or in a Visited IMS network. The latter case is referred to as IMS roaming scenario and is different from a GPRS roaming scenario.

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 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 CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.

D.1.1.1 IMS to IMS Call

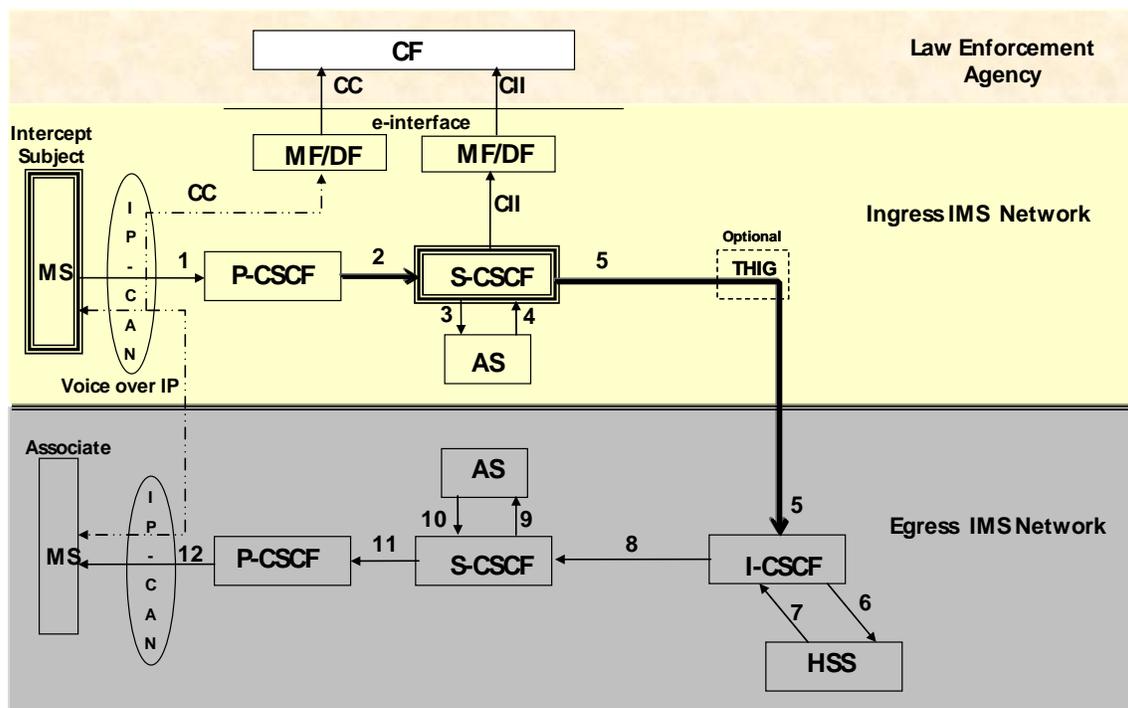In the scenario, the intercept subject (an IMS user) originates a call to another IMS user (associate).

Figure D.4: IMS Originating Call (No Roaming) - IMS to IMS Call

D.1.1.2 IMS to PSTN Call

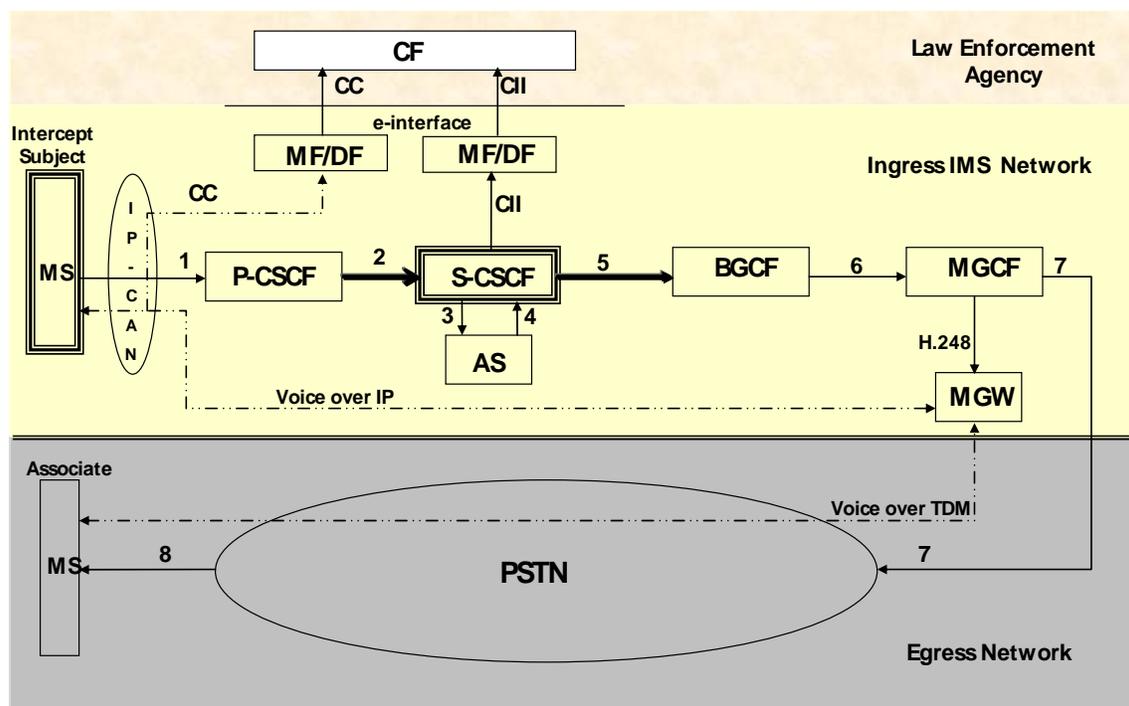In this scenario, the intercept subject (an IMS user) originates a call to a PSTN user (associate).

Figure D.5: IMS Originating Call (No Roaming) - IMS to PSTN Call

D.1.2 P-CSCF is in a 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 Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 2 and 5.

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 CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.
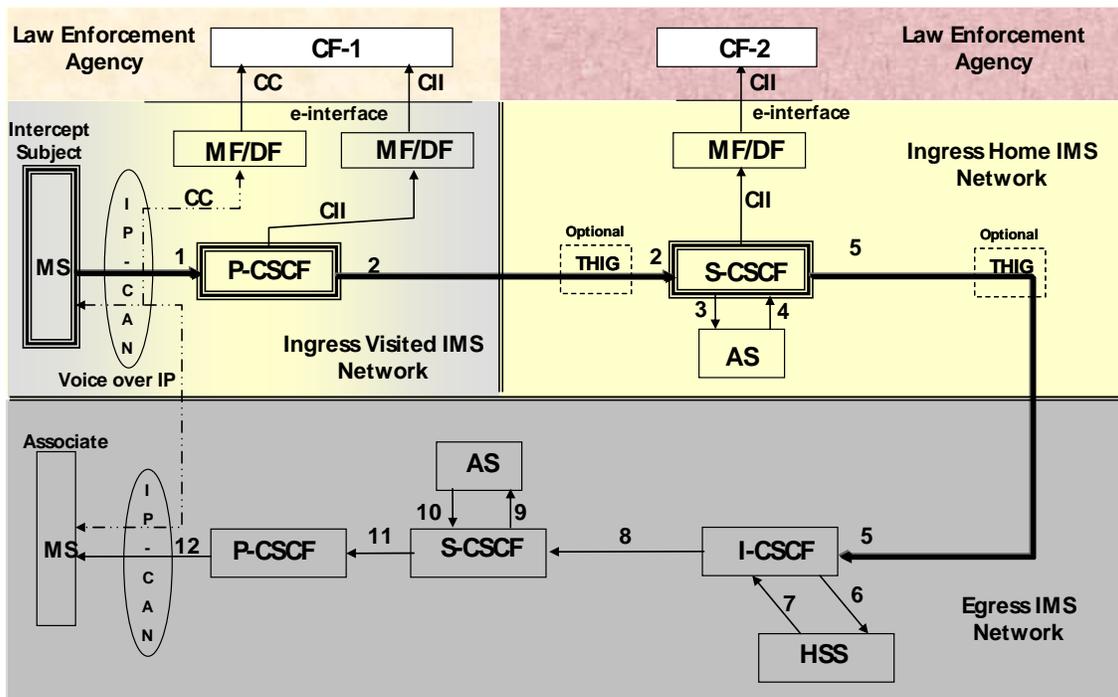
Figure D.6: IMS Originating Call (IMS Roaming) - IMS to IMS Call – Scenario 1

Scenario 2

In this scenario only the 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 2 and 5.

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. For the same reason, the IP-CAN does not provide interception of CC.
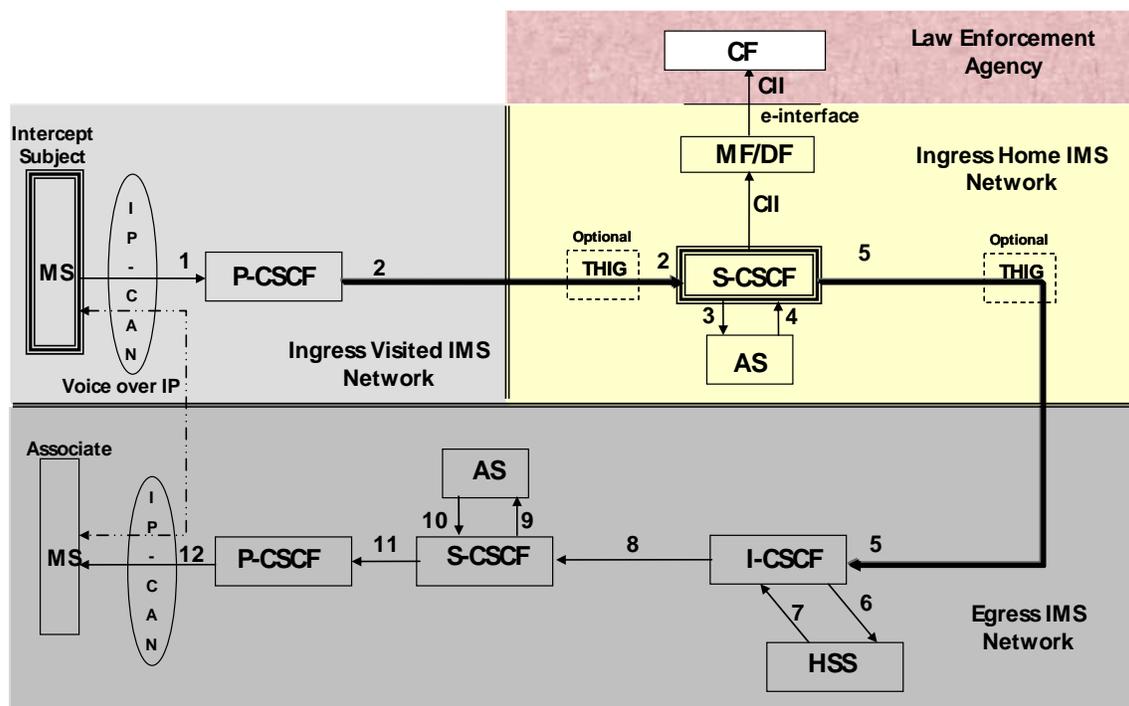
Figure D.7: IMS Originating Call (IMS Roaming) – IMS to IMS Call - Scenario 2

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

D.2.1 P-CSCF belongs to the 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 CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.

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 8 and 11. The P-CSCF may perform the same delivery of SIP messages from the Interface 11 and 12.
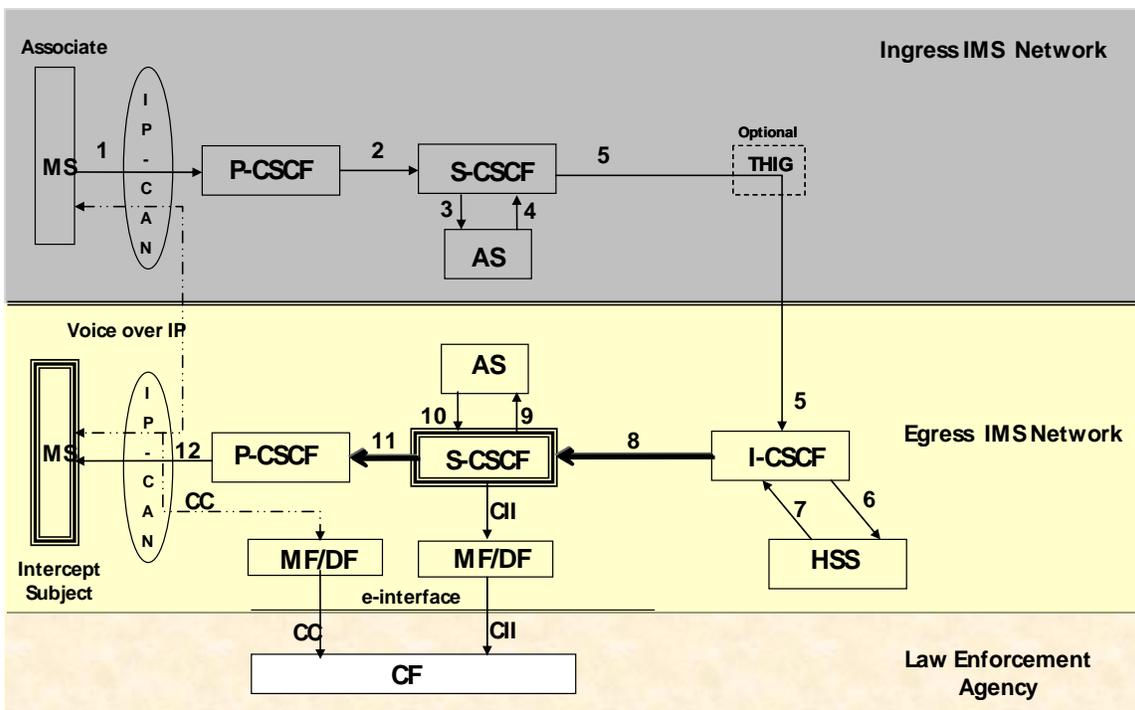
Figure D.8: IMS Terminating Call (No Roaming) - IMS to IMS Call

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.
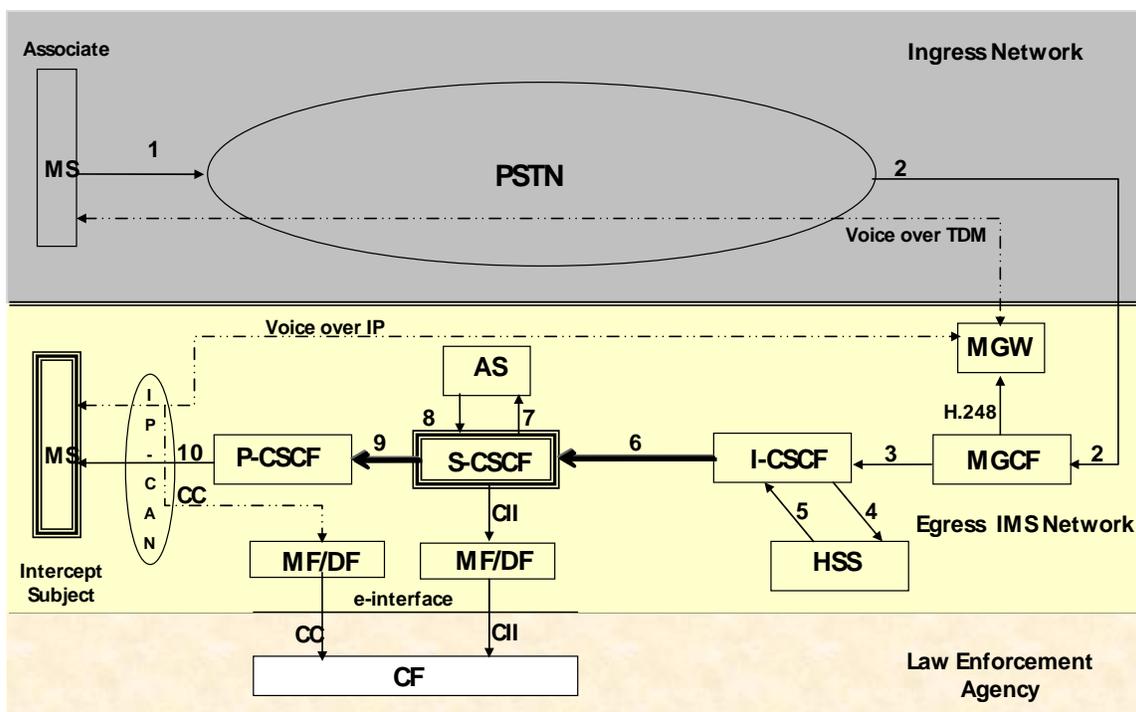
Figure D.9: IMS Terminating Call (No Roaming) – PSTN to IMS Call

D.2.2 P-CSCF is in a 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 Visited IMS network provider and the Home IMS network provider are served with lawful authorization(s).

In the Home IMS Network, S-CSCF provides the IAP for the CII. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11.

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 CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.
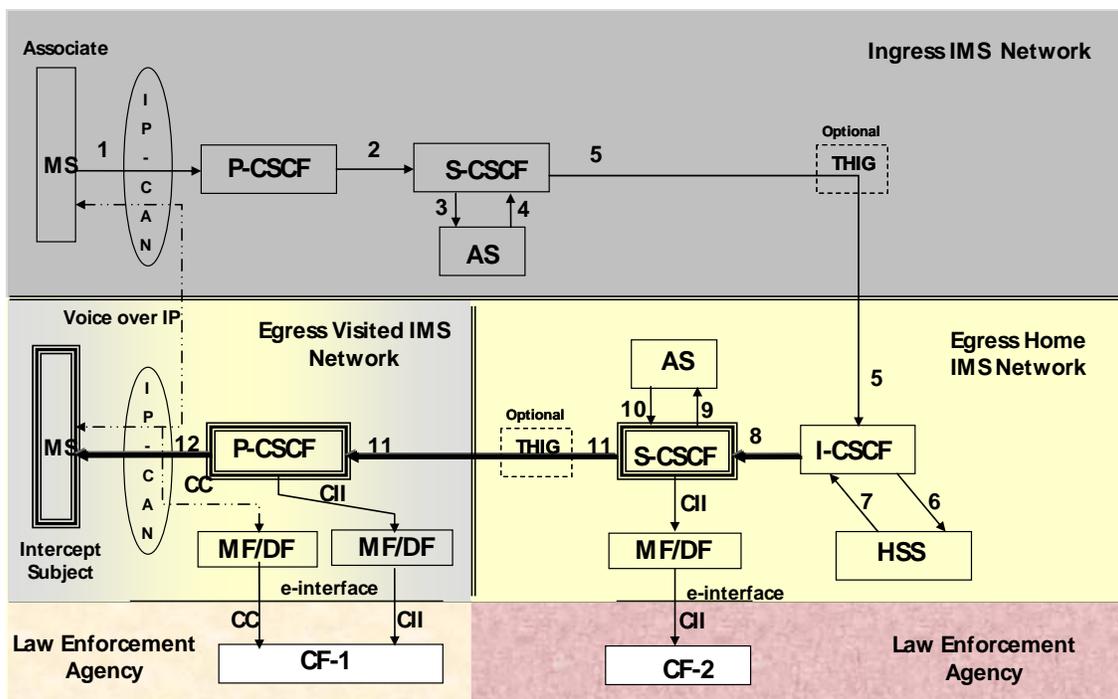

Figure D.10: IMS Terminating Call (IMS Roaming) - IMS to IMS Call – Scenario 1

Scenario 2

In this scenario only the 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 8 and 11.

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. For the same reason, the IP-CAN does not provide interception of CC.
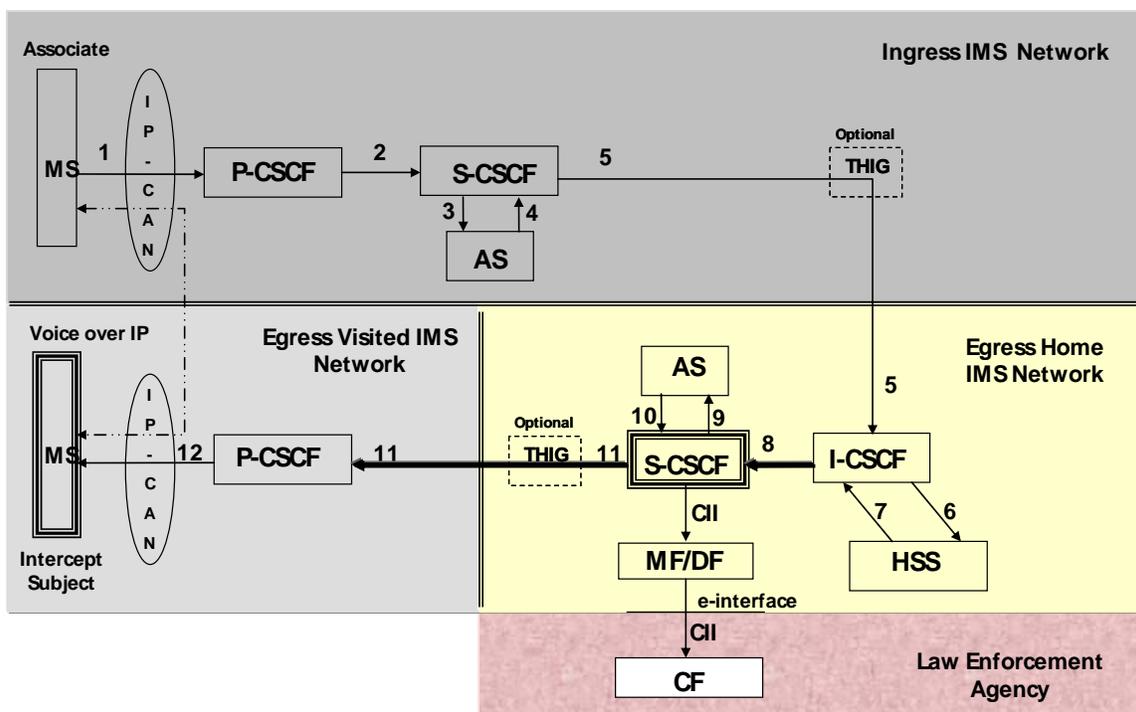
Figure D.11: IMS Terminating Call (IMS Roaming) – IMS to IMS Call - Scenario 2

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

In the 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 CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

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 9 and 10. The CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.
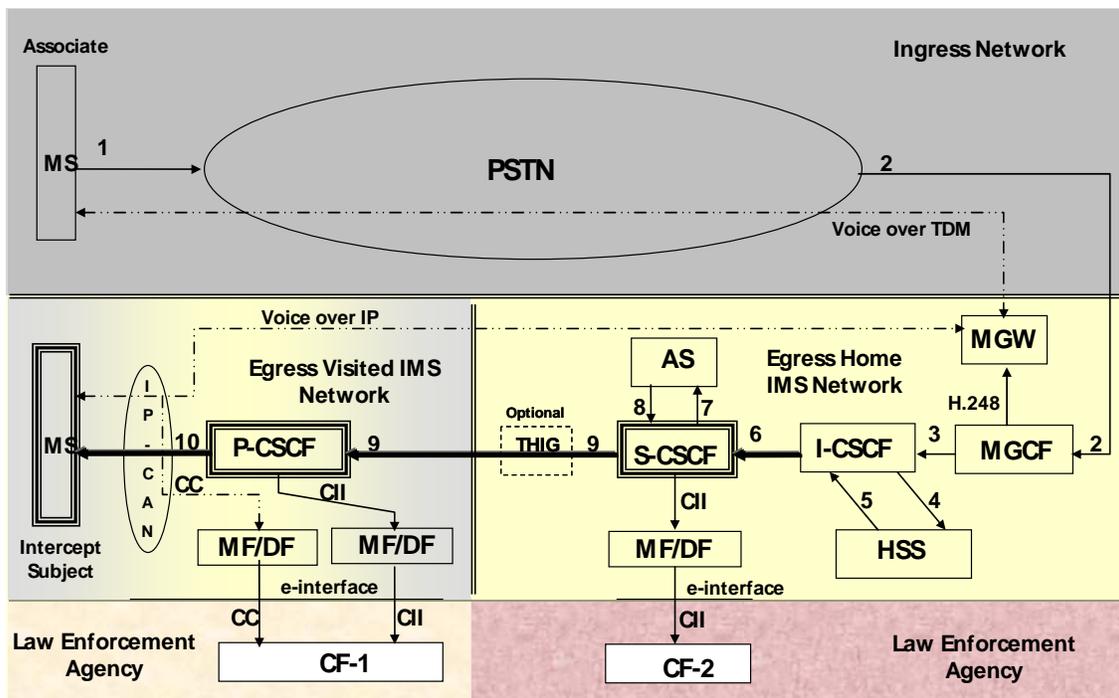
Figure D.12: IMS Terminating Call (IMS Roaming) - PSTN to IMS Call – Scenario 1

Scenario 2

In this scenario only, the 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 CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

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. For the same reason, the IP-CAN does not provide interception of CC.

Figure D.13: 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) is 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, Ingress Network is the network that handles the call control procedures from a calling user's perspective, in other words, Ingress Network is the call originating network. The calling user is identified within the diagrams as "Associate-1". The Egress Network is the network that handles the call control procedures from a forward-to user's perspective, in other words, the Egress Network is the call terminating network. 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 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 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 Base IMS Network provides the IAP for the CII. The P-CSCF of the intercept subject is not involved in the call handling and hence, does not provide the IAP for the CII. The IP-CAN associated with the intercept subject is not involved in the call and hence, does not provide the interception of CC.

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11.
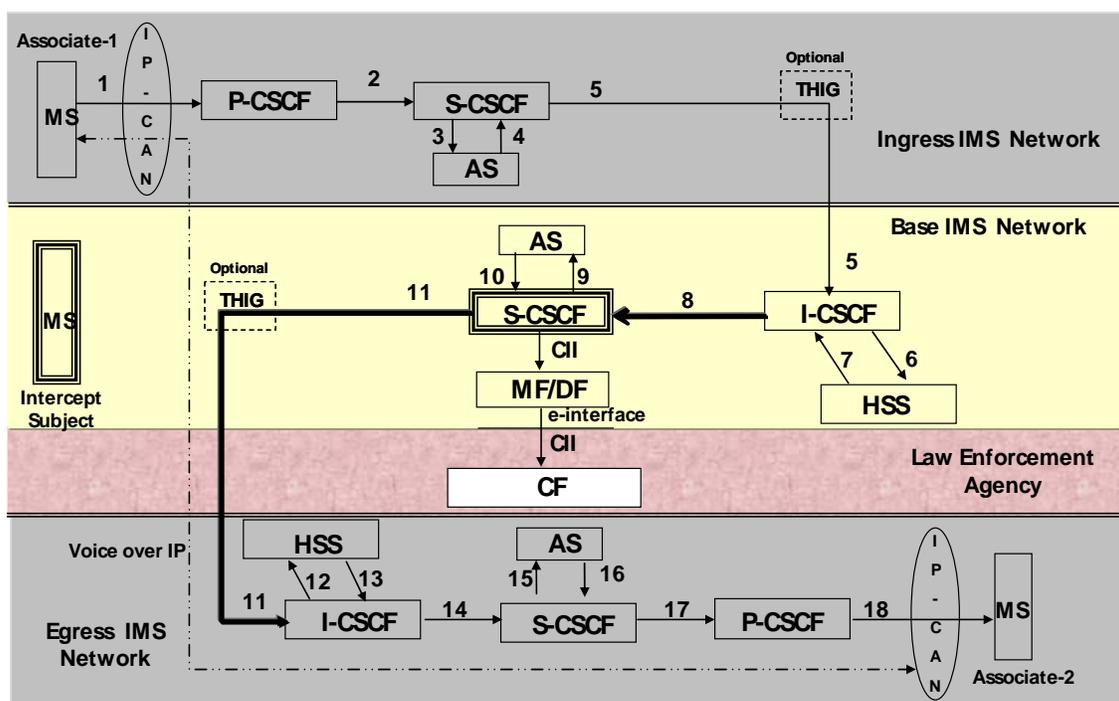
Figure D.14: Call Forwarding Unconditional: IMS to IMS Call forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11. The CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.
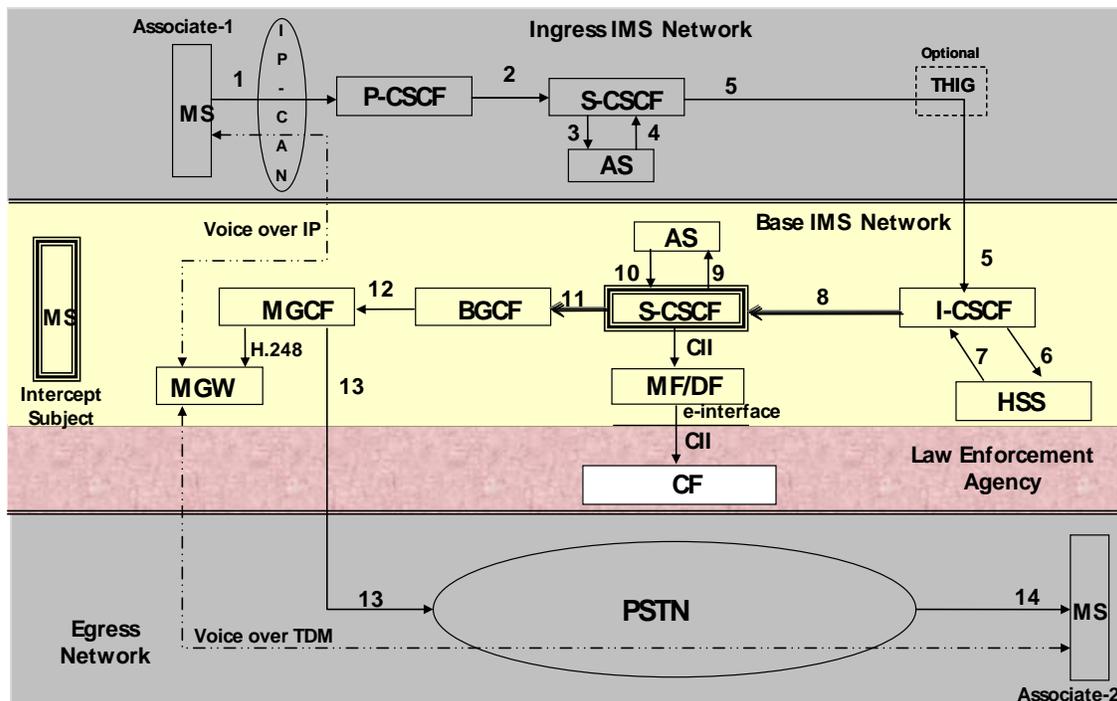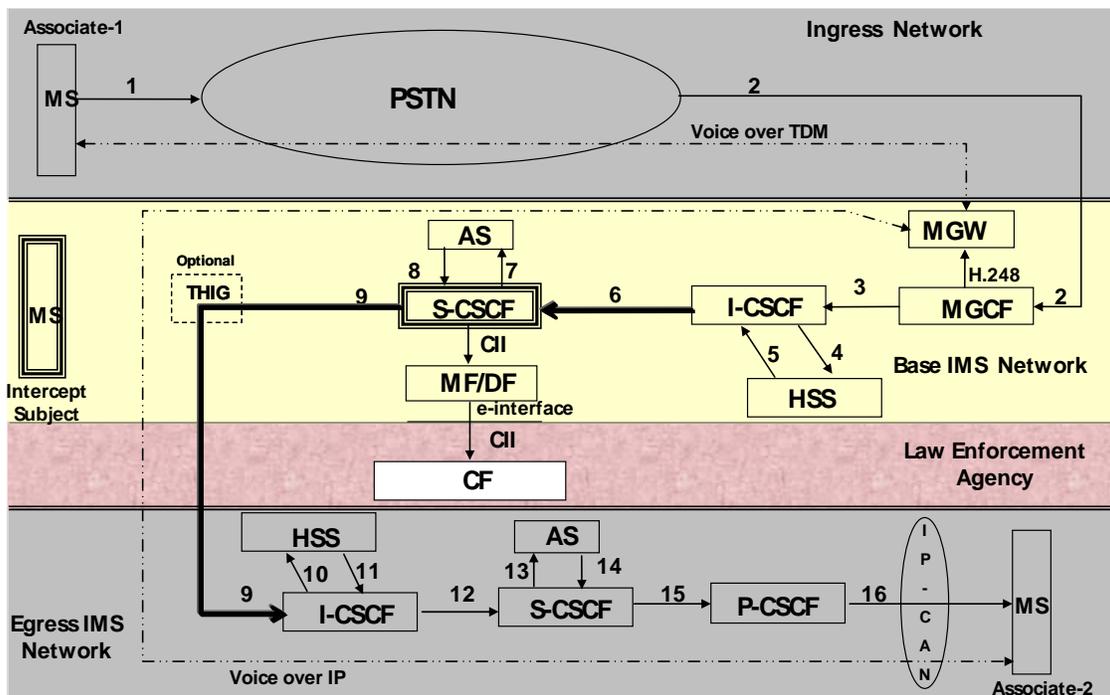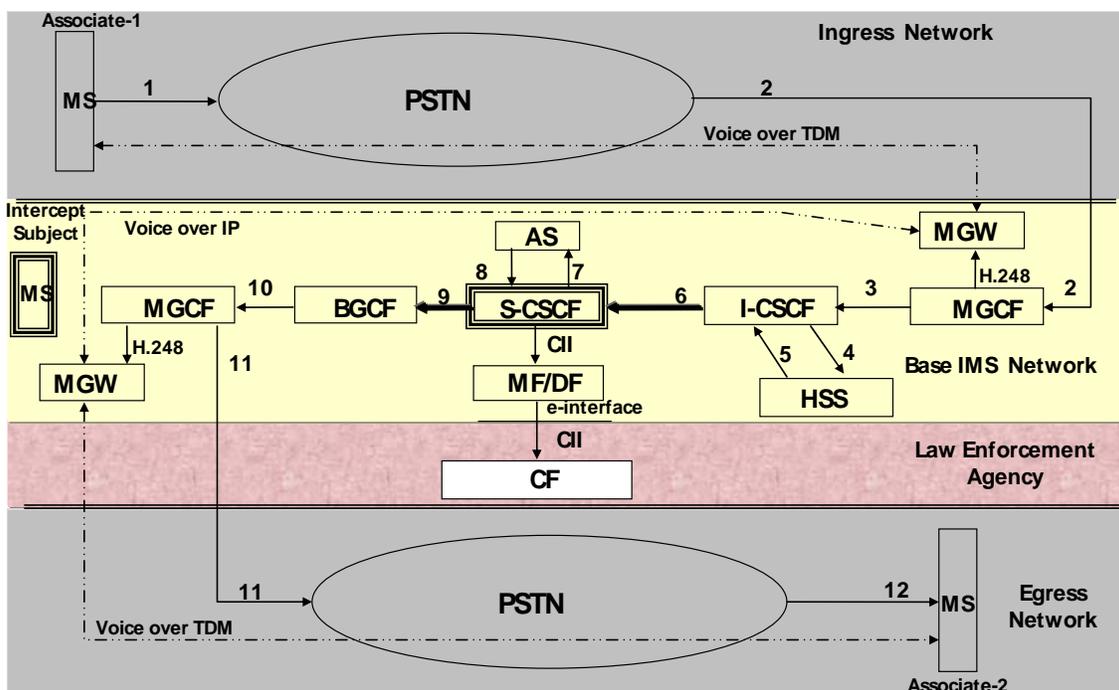

Figure D.15: Call Forwarding Unconditional: IMS to IMS Call forwarded to PSTN

D.3.1.3 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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

Figure D.16: 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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9. The CC may be intercepted at the MGW(s) and delivered to the LEA(s) via the MF/DF.

Figure D.17: 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 of the base IMS user.
2. P-CSCF of the base IMS user belongs to a Visited IMS Network (shown as Base Visited IMS Network) and that Base Visited IMS Network is different from the 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).

D.3.2.1 P-CSCF belongs to the 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.

While the base IMS user is being alerted, the CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF. The IP-CAN associated with the intercept subject (base IMS user) is not involved in the forwarded leg of the call and hence, does not provide the interception of CC for the forwarded leg.

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 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 11 and 12 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.
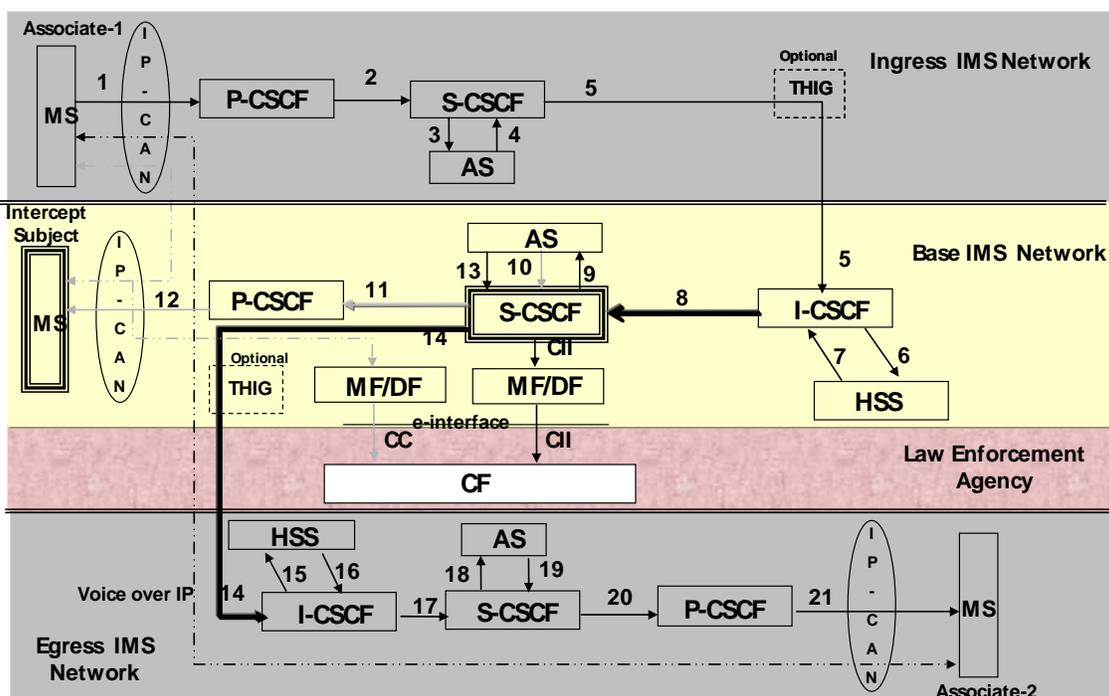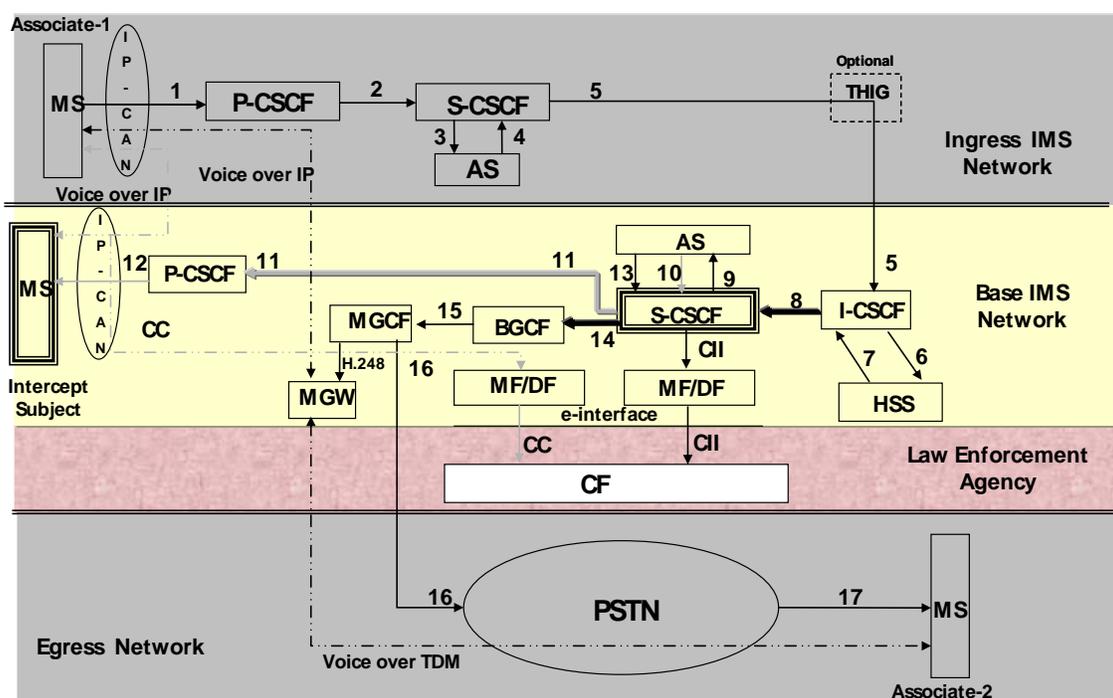

Figure D.18: Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 for the forwarded leg of the call. When the call is forwarded, the CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

The P-CSCF of the intercept subject (base IMS user) may perform the same delivery of SIP messages from the Interface 11 and 12 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.

Figure D.19: 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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

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.
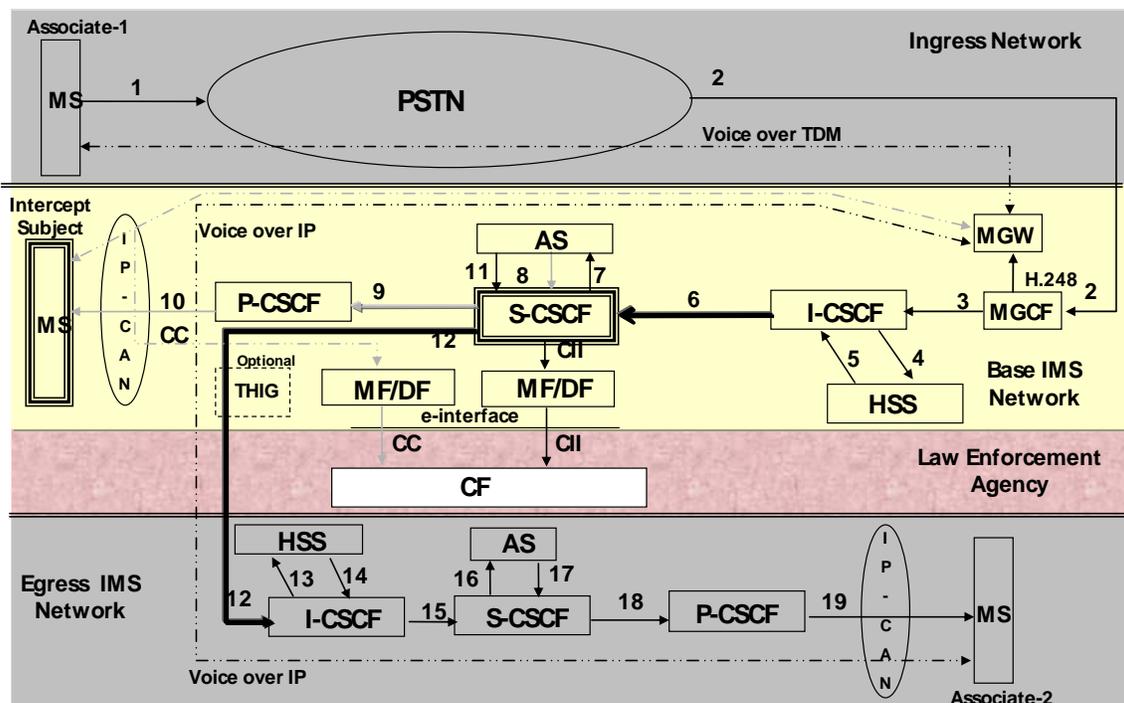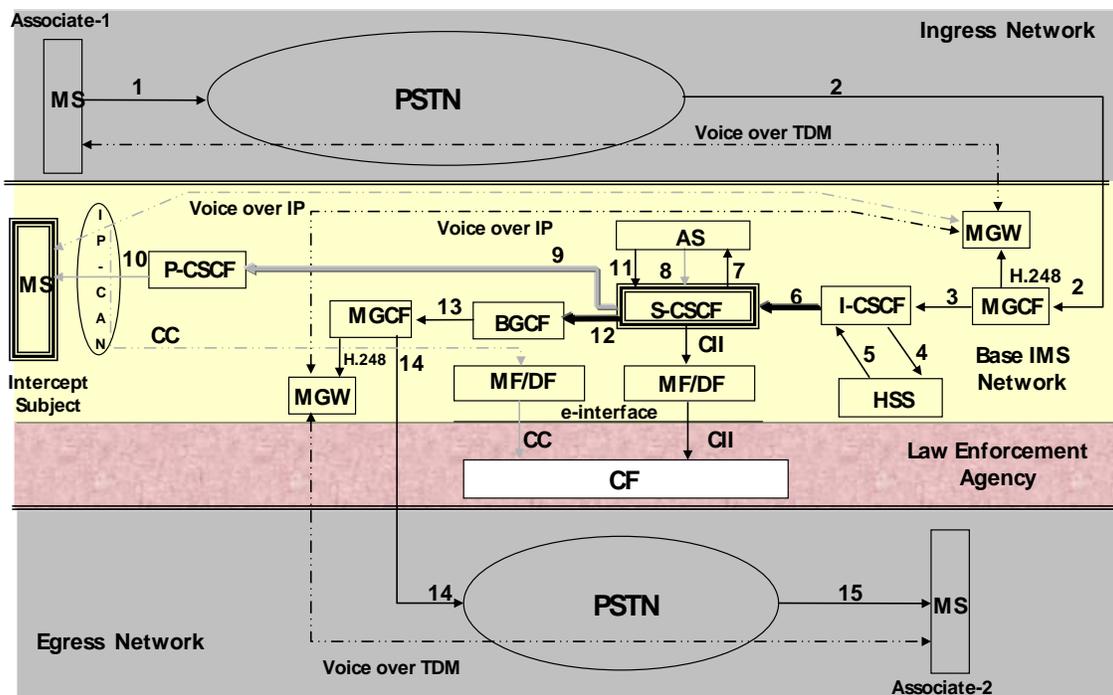
41

Figure D.20: 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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW(s) and delivered to the LEA(s) via the MF/DF.

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.

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

D.3.2.2 P-CSCF is in a 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 (Base Visited IMS Network and Base Home IMS Network) are served with the lawful authorization(s).

- ♦ *Scenario 2*: Only the Base Home IMS Network provider is served with the lawful authorization.

Note that it is also possible to have a scenario where only the Base Visited IMS network provider is served with the lawful authorization. In this scenario, since the lawful authorization is not applicable to the Base 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.3.2.2.1 Both Network Providers are served with Lawful Authorization(s)

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

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

In the Base Visited IMS network, the P-CSCF provides the IAP for the CII. The CC is intercepted within the IP-CAN network nodes and delivered to the LEA(s) via the MF/DF.

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. Likewise, the IP-CAN associated with the intercept subject (base IMS user(is not involved in the forwarded leg of the call and hence, does not provide the interception of CC for the forwarded leg.

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 for the forwarded leg of the call.

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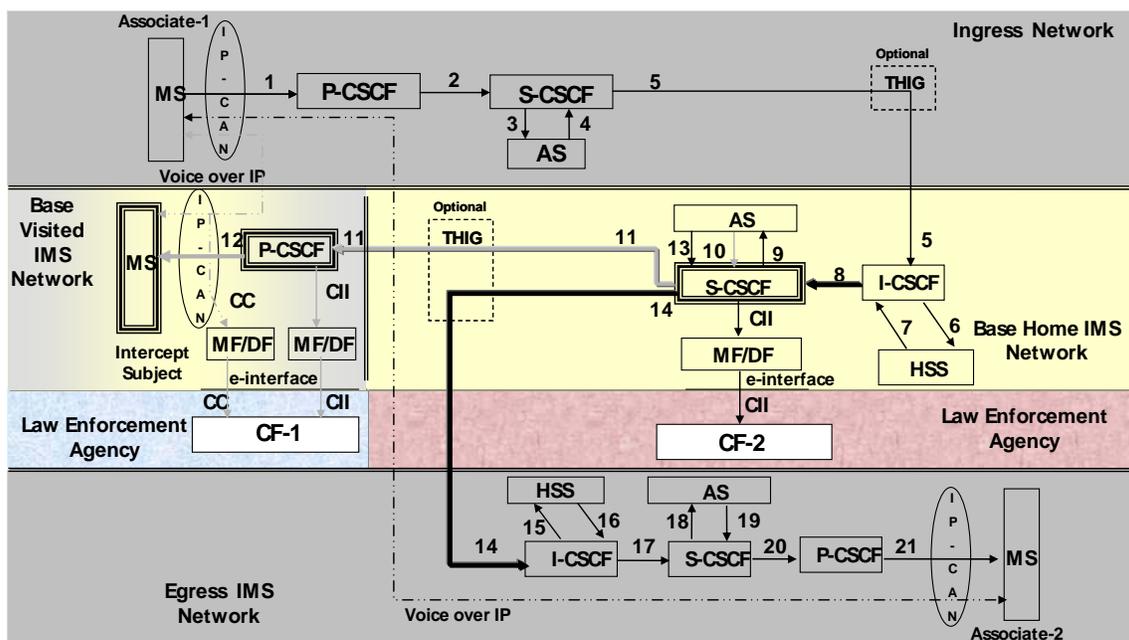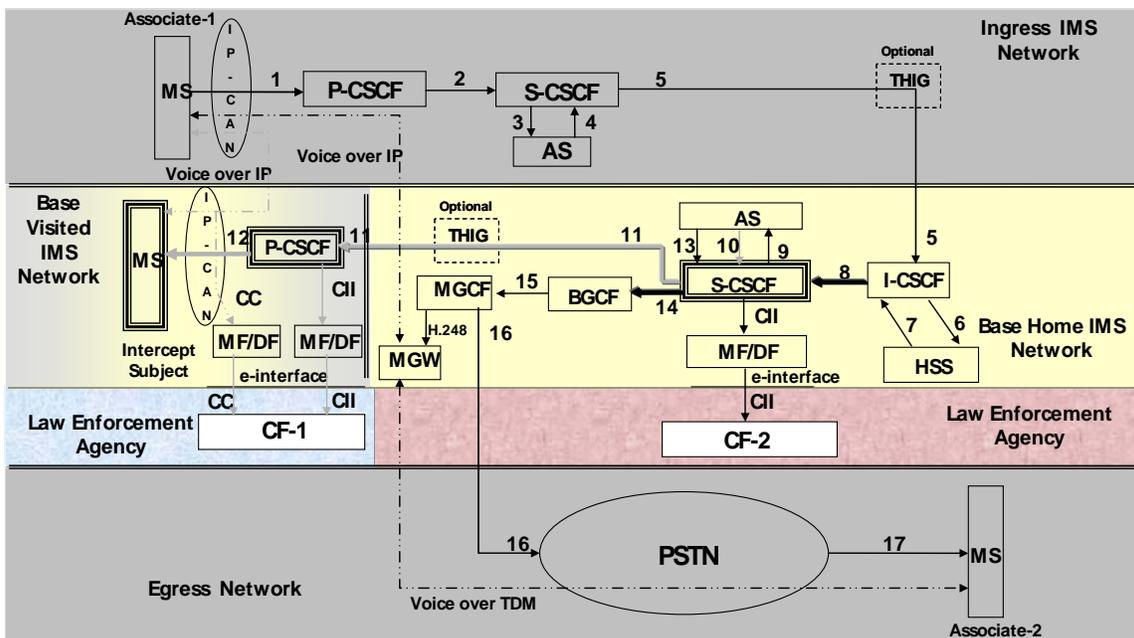

Figure D.22: Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 for the forwarded leg of the call. When the call is forwarded, the CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

Within the Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 11 and 12 during the alerting phase of the call.
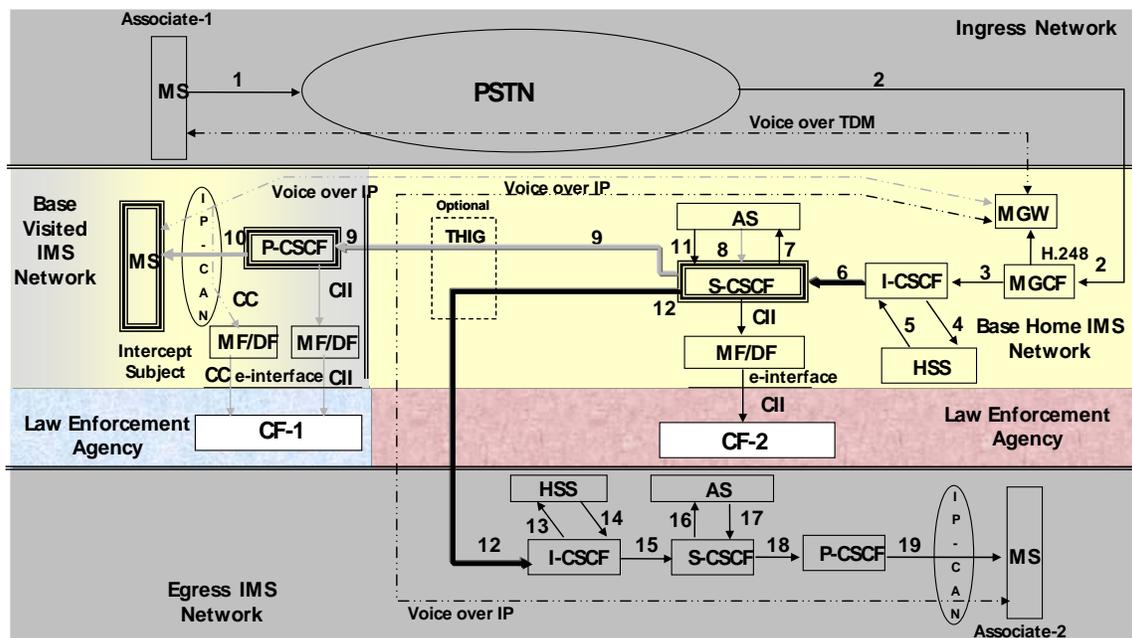
Figure D.23: Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to PSTN

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.

Within the Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 9 and 10 during the alerting phase of the call.
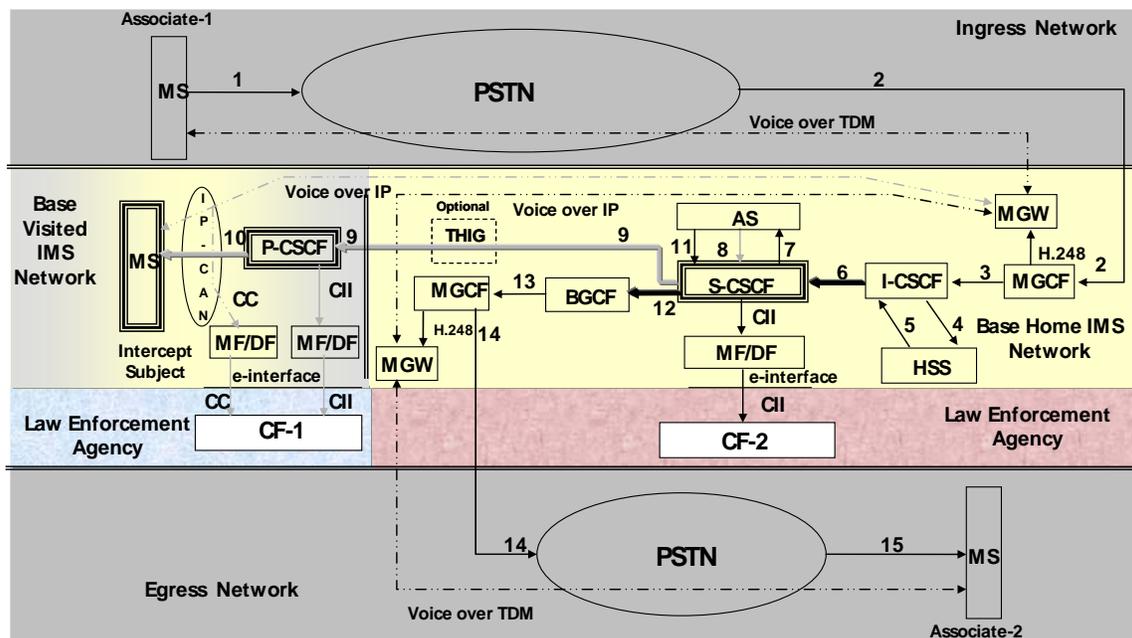
Figure D.24: Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW(s) and delivered to the LEA(s) via the MF/DF.

Within the Base Visited Network, the P-CSCF delivers the SIP messages from the Interface 9 and 10 during the alerting phase of the call.

Figure D.25: 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 Base Home IMS Network, S-CSCF provides the IAP for the CII.

Since the lawful authorization does not apply to the Base Visited IMS network provider, the P-CSCF that resides in the Base Visited IMS network does not provide any IAP for the CII even while the base IMS user (intercept subject) is being alerted. For the same reason, the IP-CAN does not provide interception of CC 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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 for the forwarded leg of the call.
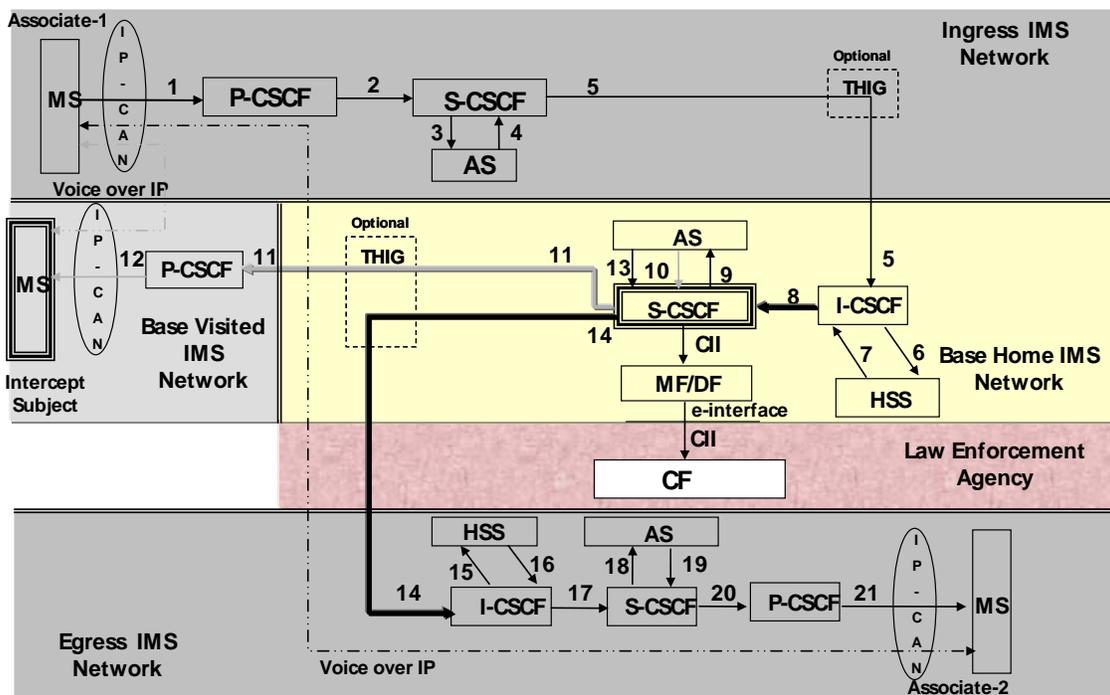
Figure D.26: Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 8 and 11 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 8 and 14 for the forwarded leg of the call. When the call is forwarded, the CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.
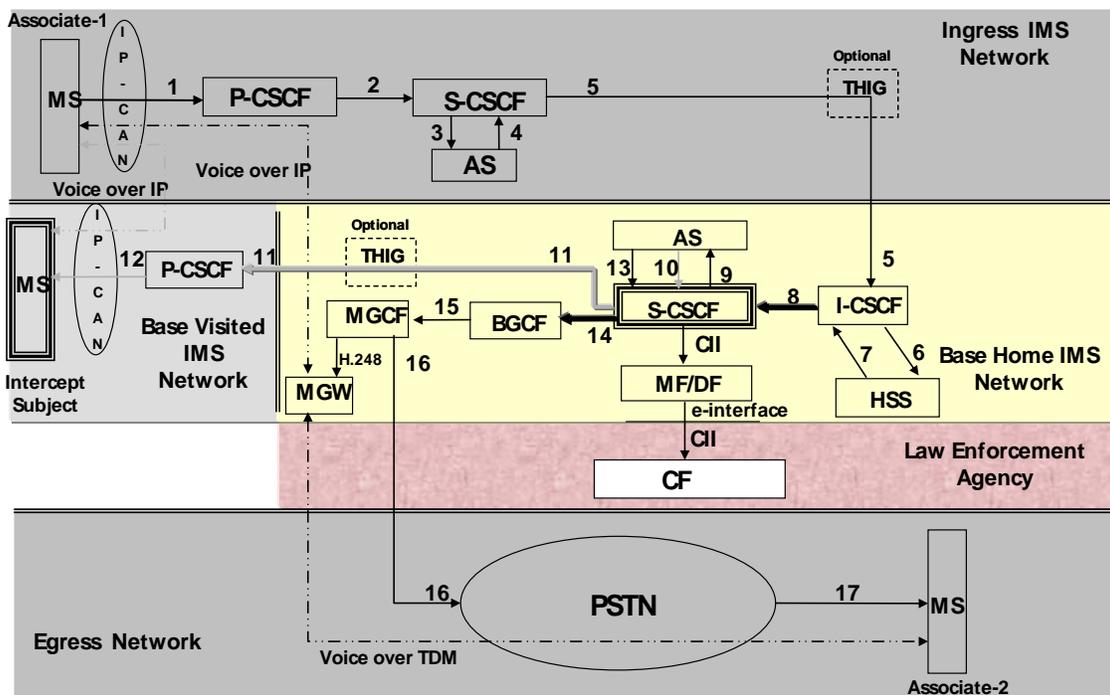
Figure D.27: Call Forwarding Do Not Answer – IMS to IMS Call Forwarded to PSTN

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW and delivered to the LEA(s) via the MF/DF.
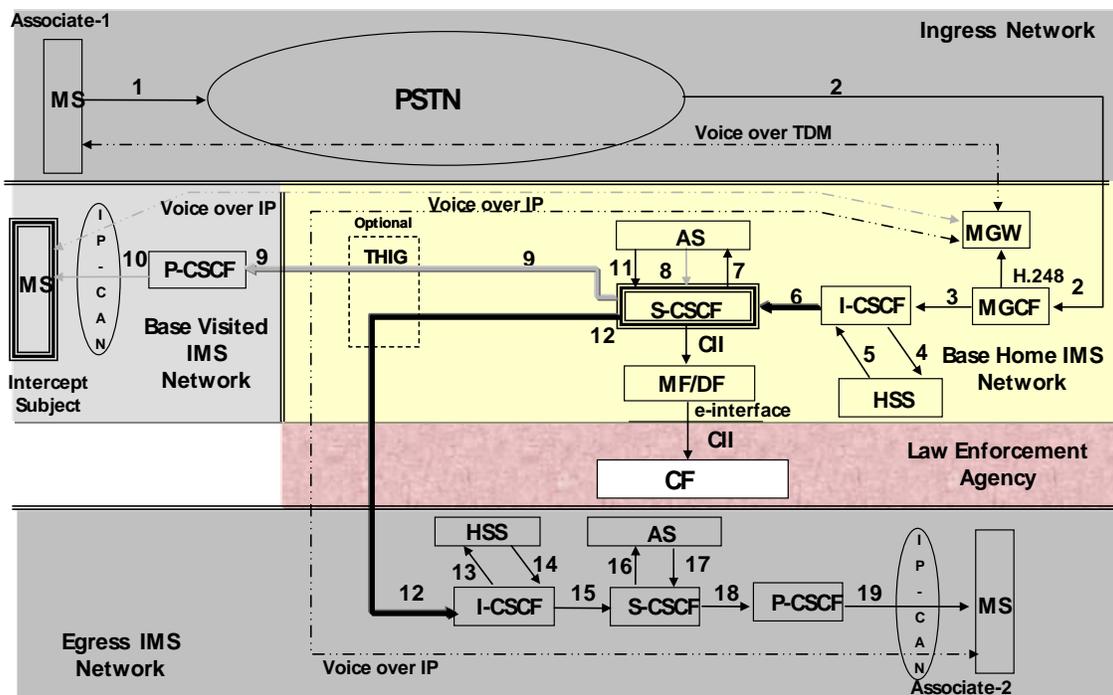
Figure D.28: Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to IMS

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 Base IMS Network, the S-CSCF delivers the SIP messages sent and received on the Interface 6 and 9 during the alerting phase. The S-CSCF delivers the SIP messages sent and received on the Interface 6 and 12 for the forwarded leg of the call. The CC may be intercepted at the MGW(s) and delivered to the LEA(s) via the MF/DF.
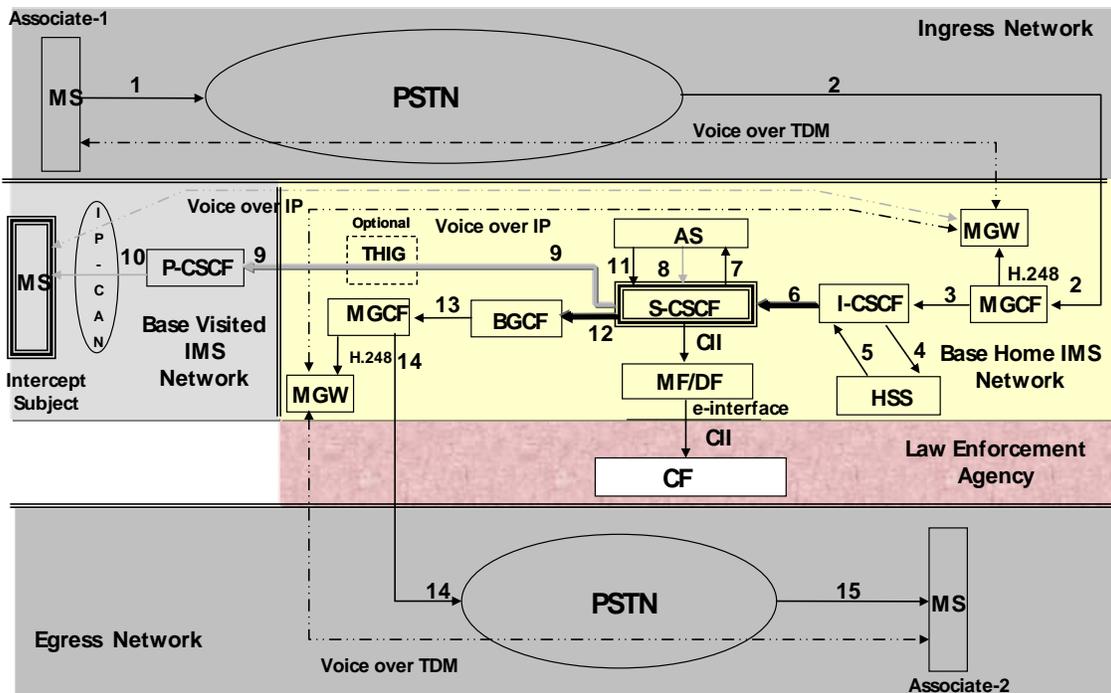
Figure D.29: Call Forwarding Do Not Answer – PSTN to IMS Call Forwarded to PSTN

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 function is integrated into an IAP, then a MF/DF function can be provided in addition to the existing integrated 3GPP DF to achieve an "ATIS-0700005" solution.

♦ *Option 2*: When a 3GPP DF function is not integrated into the IAP, a MF/DF function can be provided in addition to the existing standalone 3GPP DF to achieve an "ATIS-0700005" solution. Whether or not this MF/DF function is physically separated or integrated with the existing 3GPP DF is an implementation issue.

♦ *Option 3*: It is possible to provide a MF/DF function for producing "ATIS-0700005" solution without a 3GPP DF.
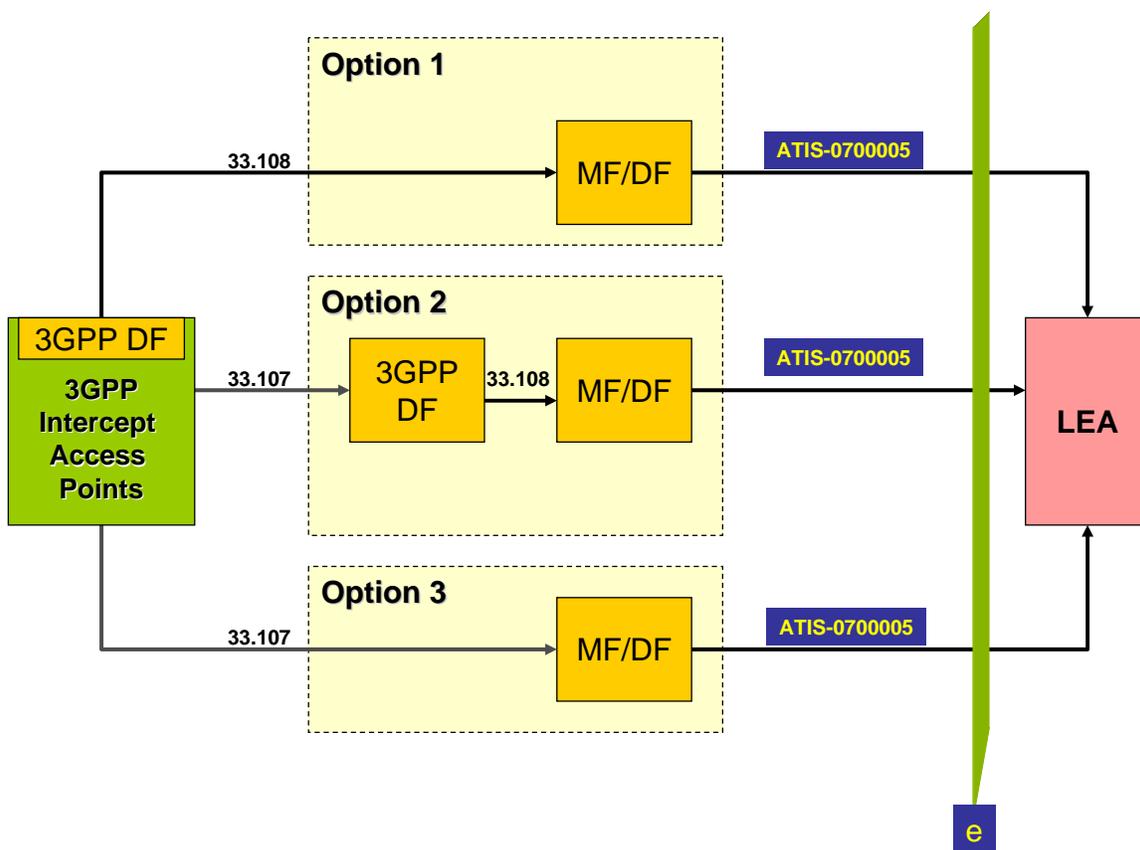

Figure E.1: Examples of IMS-based VoIP Implementation Options

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 and 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 a "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.
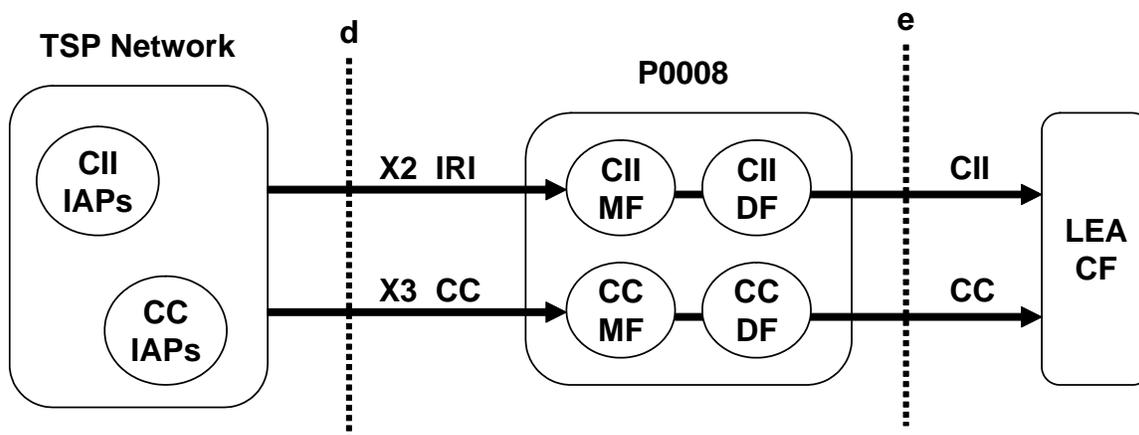

Figure E.2: Support for X2 and X3 Interfaces

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.

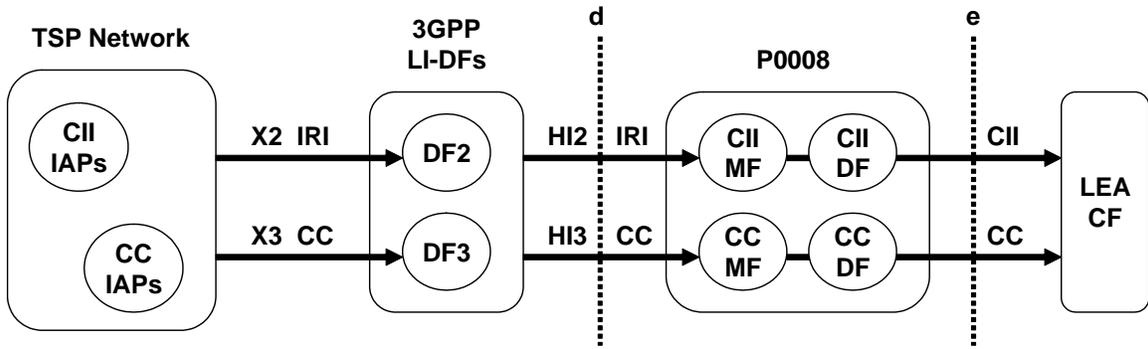NOTE - [108] may not specify all the necessary information for mapping of the CII and CC for delivery to the LEA CF.

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