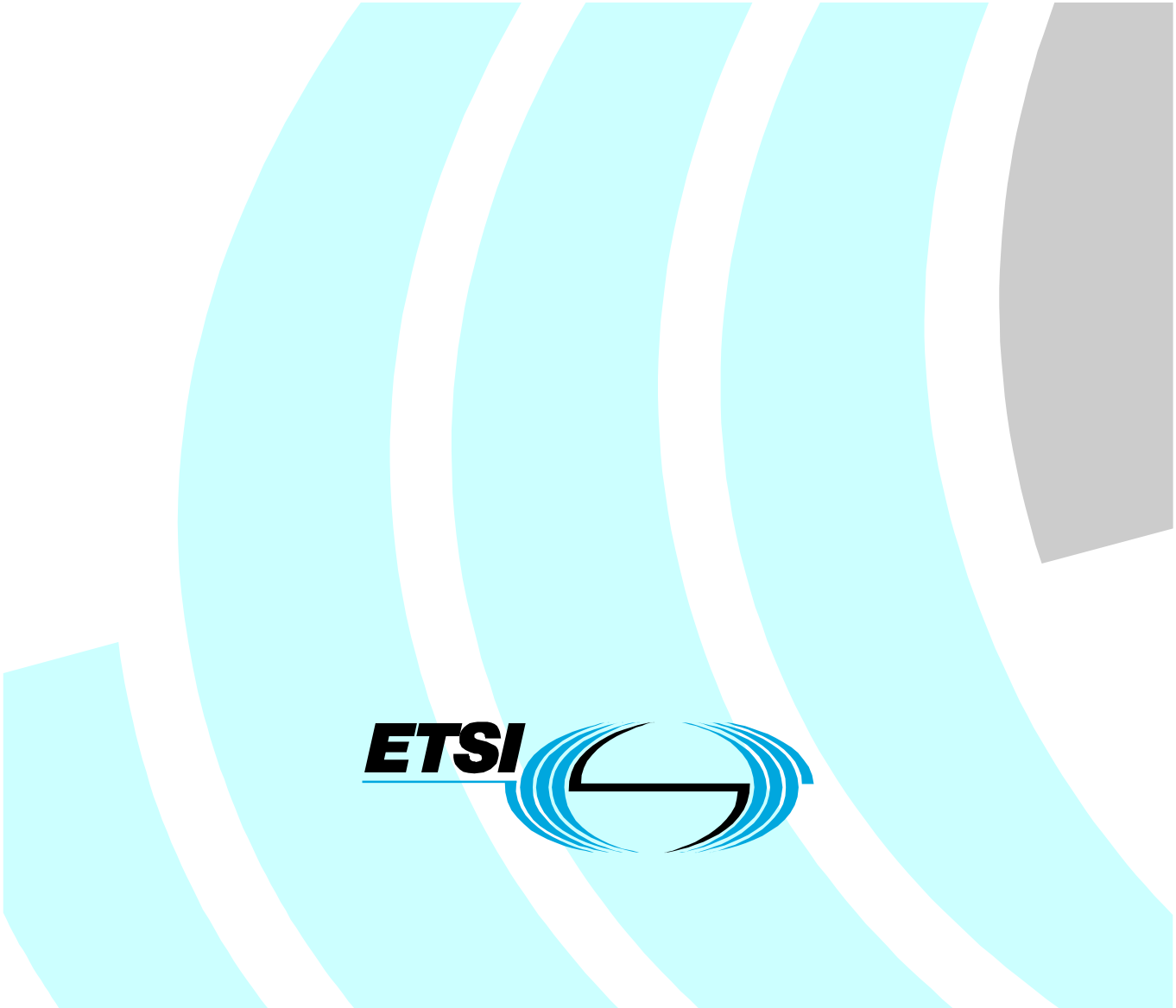
ETSI TR 102 528 V1.1.1 (2006-10)

Technical Report

Lawful Interception (LI);
Interception domain Architecture for IP networks



Reference
DTR/LI-00025

Keywords
Lawful Interception, architecture, IP, data,
security, telephony, multimedia

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Introduction

The objective of the present document is to describe a high level architecture in IP networks for use by both telecommunications service providers and network operators, including Internet Service Providers that will deliver the interception information required by Law Enforcement Authorities under various European treaties and national regulations.

The distributed nature of IP networks, and the increasing number of access technologies require Internal Intercept functions in a large number of devices. The present document provides a general reference architecture that has a minimum set of common Internal Network functions and Interfaces. It is intended to be general enough to be used in a variety of situations, including but not limited to lawful interception of IP Multimedia services, layer 2 data services and layer 3 data services, delivered over any access technology.

1 Scope

The present document describes a high level reference architecture for supporting lawful interception in network operator and communication service providers" domain for IP networks.

The document contains:

- A reference model in the network operator and communication service provider domain.
- A High level description of Internal Network Functions and Interfaces.
- Application of the reference model to voice and multimedia over IP services, data layer 3 and layer 2 services.

It does not intend to replace any existing document which specifies network operator and communication service provider's architecture and internal network interfaces. The present document does not override or supersede any specifications or requirements for the lawful interception within GSM/UMTS PS domain, which is defined in TS 133 106 [9] and TS 33 107 [8].

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[2] ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".

[3] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[4] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the Lawful Interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[5] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[6] ETSI TS 102 232-01: "Lawful Interception (LI); Handover specification for IP delivery".

[7] ETSI TS 102 232-03: "Lawful Interception (LI); Service-specific details for internet access services".

[8] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[9] ETSI TS 133 106: "Universal Mobile Telecommunications System (UMTS); Lawful interception requirements (3GPP TS 33.106)".

[10] ETSI TS 142 033: "Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1 (3GPP TS 42.033 version 5.0.0 Release 5)".

[11] ETSI TS 143 033: "Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 2 (3GPP TS 43.033 version 5.0.0 Release 5)".

[12] ETSI TS 102 227: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception".

[13] IETF RFC 3924: "Cisco Architecture for Lawful Intercept in IP Networks".

[14] PKT-SP-ESP1.5-I01-050128: "PacketCable™ Electronic Surveillance Specification".

[15] IETF RFC 3414: "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)".

[16] IETF RFC 3415: "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)".

[17] Warnicke, E.: "A Suggested Scheme for DNS Resolution of Networks and Gateways".

NOTE: Work in Progress.

[18] IETF RFC 3261: "SIP: Session Initiation Protocol".

[19] IETF RFC 3435: "Media Gateway Control Protocol (MGCP) Version 1.0".

[20] ITU-T Recommendation H.248.1: "Gateway Control Protocol: Version 3".

[21] ITU-T Recommendation H.323: "Packet-based Multimedia Communications Systems".

[22] ITU-T Recommendation H.245: "Control Protocol for Multimedia Communications".

[23] IETF RFC 2327: "SDP: Session Description Protocol".

[24] IETF RFC 4588: Rey, J., Leon, D., Miyazaki, A., Varsa, V., and R. Hakenber: "RTP Retransmission Payload Format".

NOTE: Work in Progress.

[25] IETF RFC 3550: "RTP: A Transport Protocol for Real Time Applications".

[26] IETF RFC 2474: "Definition of the Differentiated Services (DS Field) in the IPv4 and IPv6 Headers".

[27] IETF RFC 2475: "An Architecture for Differentiated Services".

[28] ETSI TS 102 815: "Lawful Interception (LI); Service-specific details for Layer 2 Lawful Interception".

[29] ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".

[30] PKT-SP-ES-INF-I01-060406: "PacketCable™ Electronic Surveillance Intra-Network Specification".

[31] IETF RFC 3603: "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture ".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 331 [1], ES 201 158 [2] and the following apply:

Access Provider (AP): provides a user of some network with access from the user's terminal to that network

NOTE 1: This definition applies specifically to the present document. In a particular case, the access provider and network operator may be a common commercial entity.

NOTE 2: The definitions from TS 101 331 [1] have been expanded to include reference to an access provider, where appropriate.

authorizing authority: authority, such as court of law, that is entitled to authorize Lawful Interception (LI)

call: any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.

NOTE: In this context a user may be a person or a machine

CC (CC): information exchanged between two or more users of a telecommunications service, excluding Intercept Related Information (IRI).

NOTE: This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Domain Name System (DNS): set of network elements, which function as translators between logical names and network addresses on the Internet

NOTE: This type of element is widely used for IP traffic today. It can be anticipated that similar functionality will be introduced also for telephony in the near future.

Handover Interface (HI): physical and logical interface across which the interception measures are requested from an AP/NWO/SvP, and the results of interception are delivered from an AP/NWO/SvP to an LEMF

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis

Intercept Related Information (IRI): collection of information or data associated with telecommunication services involving the target identity, specifically call associated information or data (e.g. unsuccessful call attempts), and service associated information or data (e.g. service profile management by subscriber) and location information

Interception (or Lawful Interception): action (based on applicable laws and regulations), performed by an AP/NWO/SvP, of making available certain information and providing that information to an LEMF

NOTE: In the present document the term *interception* is not used to describe the action of observing communications by an LEA (see below).

interception interface: physical and logical locations within the access provider's/network operator's/service provider's telecommunications facilities where access to the CC and Intercept Related Information is provided

NOTE: The interception interface is not necessarily a single, fixed point.

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

Internal Intercepting Function: point within a network or network element at which the CC is made available

Internal Network Interface: network's internal interface between the Internal Intercepting Function and a mediation function

Internet Service Provider (ISP): business entity that offers connectivity to the Internet, primarily for dial-in subscribers

NOTE: The ISP will generally also provide e-mail facilities and other higher-level Internet services.

Law Enforcement Agency (LEA): organization authorized, by a lawful authorization based on a national law, to request interception measures and to receive the results of telecommunications interceptions

Law Enforcement Monitoring Facility (LEMF): law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject

lawful authorization: permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from an AP/NWO/SvP

NOTE: Typically this refers to a warrant or order issued by a lawfully authorized body.

LEA network: network connections and special protocol functions that are required for delivery of intercept products from a mediation function or delivery function to the LEMF(s)

NOTE: This network is specified by and normally belongs to the LEA domain.

LI products: The same as **result of interception**, see below.

Location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

mail server: network element which serves as a "point of presence" (POP) for receiving and storing and forwarding e-mail on behalf of a registered mail user on that server

NOTE: A variant of the mail server is the Simple Mail Transfer Protocol (SMTP), which dispatches mail from the user to the
e-mail network. The POP usually requires login with a password on the application level, whilst the SMTP can be used after session or link validation only.

Mediation Function (MF): mechanism which passes information between an access provider or network operator or service provider and a handover interface

network element: component of the network structure, such as a local exchange, higher order switch or service control processor

network operator: operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means

Open System Interconnect (OSI) model: model with 7 layers for interconnection of network nodes

Quality of Service (QoS): quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc.

reliability: probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions

result of interception: information relating to a target service, including the CC (CC) and Intercept Related Information (IRI), which is passed by an access provider or network operator or service provider to an LEA

NOTE: Intercept related information may be provided whether or not call activity is taking place.

service information: information used by the telecommunications infrastructure in the establishment and operation of a network related service or services

NOTE: The information may be established by an access provider, network operator, a service provider or a network user.

service provider: natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network

NOTE: A service provider does not necessarily need to run his own network.

session: period of interaction with an information or communication system during which the user is authenticated and connected to a user identity with certain authorities

target identification: identity that relates to a specific lawful authorization as such

NOTE: This might be a serial number or similar. It is not related to the denoted interception subject or subjects.

target identity: identity associated with a target service used by the interception subject

target service: telecommunications service associated with an interception subject and usually specified in a lawful authorization for interception

NOTE: There may be more than one target service associated with a single interception subject.

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo-optical system

telecommunication service provider: can be a network operator, an access provider or a service provider

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 331 [1], ES 201 158 [2] and the following apply:

AF	Administration Function
AP	Access Provider
CC	CC
CCCI	CC Control Interface
CC-IIF	CC Internal Interception Function
CCTF	CC Trigger Function
CCTI	CC Trigger Interface
CLI	Command Line Interface
COPS	Common Open Policy Service
CPE	Customer Premise Equipment
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ETR	ETSI Technical Report
GSM	Global System for Mobile communications
HI	Handover Interface
HMAC	keyed-Hash Message Authentication Code
IIF	Internal Intercepting Function
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
IRI-IIF	IRI-Internal Interception Function
ISP	Internet Service Provider
L2	Layer 2
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
MAC	Media Access Control
MD5	Message Digest 5
MF	Mediation Function
MGC	Media Gateway controller
MGCP	Media Gateway Control Protocol
MGW	Media GateWay
NWO	Network Operator
NWO/AP/SvP	Telecommunication Service Provider
OSI	Open System Interconnect
P-DCS-LEAS	Private Private SIP extension for Distributed Call Signalling Lawfully-Authorized Electronics Surveillance
PES	PSTN/ISDN Emulation Service
PHB	Per Hop Behaviour
POP	Point Of Presence
PPP	Point-to-Point Protocol
PS	Packet Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transport Protocol
SBC	Session Border Controller
SDP	Session Descriptor Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SSRC	Synchronization SourRCe
STAG	Security Techniques Advisory Group
SvP	Service Provider
TDM	Time Division Multiplexing
TGCP	Trunking Gateway Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifier
USM	User-based Security Model
VACM	View-based Access Control Model
VoIP	Voice over IP

4 Reference model

The overall interception framework is extended from the model described in clause 5.2 of ES 201 158 [2] and from the architecture identified in clause 5 of TS 101 671 [4], (see figure 1).

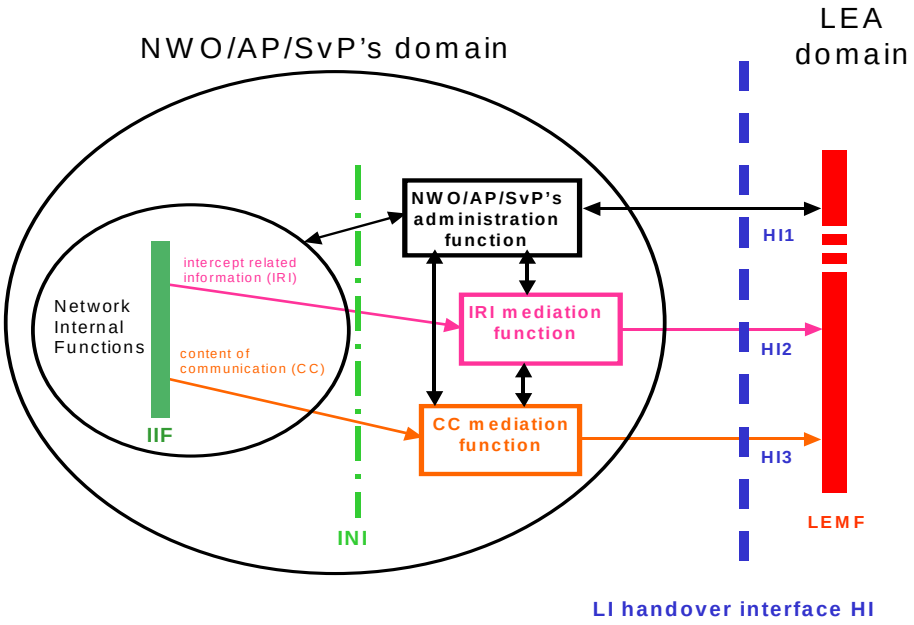


Figure 1: Functional block diagram showing Handover Interface (HI) (from TS 101 671 [4])

The scope of the present document is the NWO/AP/SvP's domain as shown in figure 1.

The present document describes a generic reference model in the interception domain, as shown in figure 2.

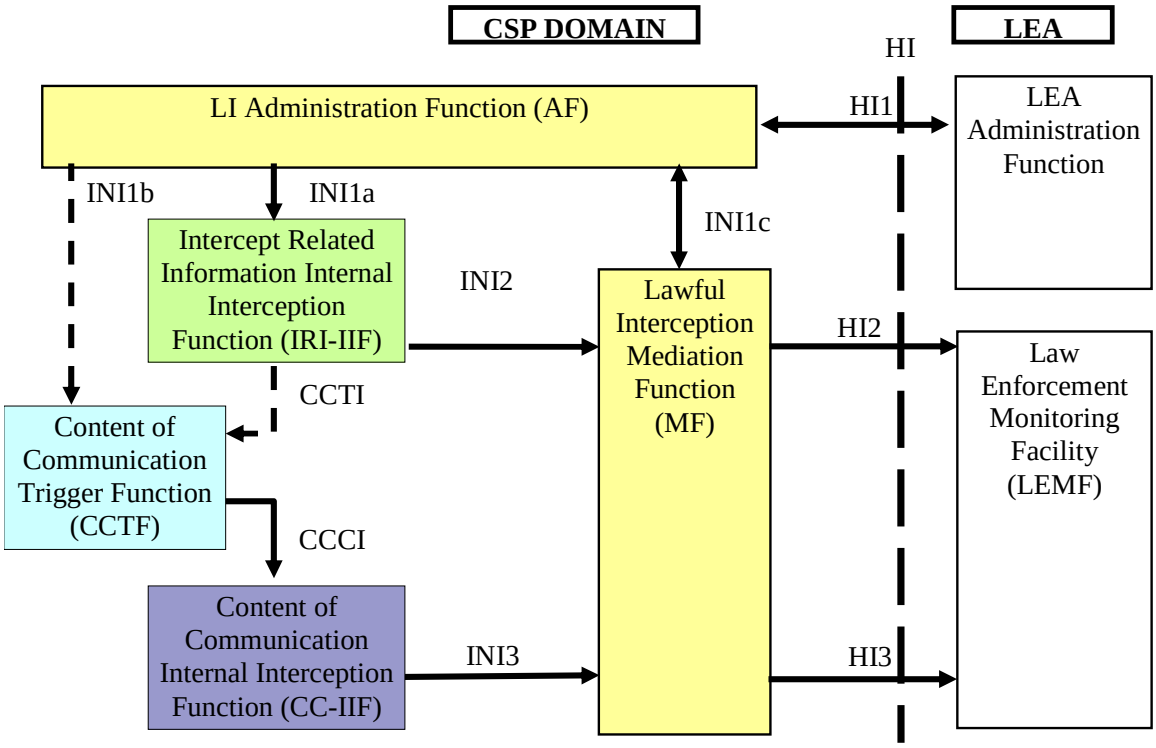


Figure 2: Reference model for Lawful Interception

- Intercept Related Information Intercept Function (IRI-IIF) generates IRI.
- CC Intercept Function (CC-IIF) generates CC.
- CC Trigger Function (CCTF) controls the CC-IIF.
- Internal interface INI1 carries provisioning information from the Lawful Interception Administration Function (AF) to the Internal Intercept Functions (IIF).
  - INI1a provisions Intercept Related Information Interception Function (IRI-IIF).
  - INI1b may (statically) provision CCs Control Function (CC-IIF).
  - INI1c provisions the Mediation Function (MF).
- Internal interface INI2 carries Intercept Related Information (IRI) from the IRI-IIF to the MF.
- Internal interface INI3 carries CC (CC) information from the CC-IIF to the MF.
- CC Trigger Interface (CCTI) carries trigger information from the IRI-IIF to the CCTF.
- CC Control Interface (CCCI) carries controls information from the CCTF to the CC-IIF.

NOTE: INI1, INI2, and INI3 are named X1, X2 and X3 in 3GPP documents.

The reference model introduces the CCTF Functional Entity to describe the different options for the provisioning of CC-IIF in an IP network. These are as follow:

- From a CCTF co-located with the LI administration Function (AF). INI1b is internal to the AF and CCTF.
- From a CCTF co-located with the IRI-IIF. CCTI is internal to the IRI-IIF and CCTF.
- From a CCTF co-located with the IRI-IIF and CC-IIF. CCTI and CCCI are internal to the IRI-IIF, CCTF and CC-IIF.
- From a CCTF co-located with the MF. CCTI is merged with INI2.
- From a stand alone CCTF. Both CCTI and CCCI are external interfaces.

4.1 Description of functional elements

4.1.1 Intercept Related Information Internal Interception Function (IRI-IIF)

The purpose of the IRI-IIF is to generate IRI information associated with sessions, calls, connections and any other information involving interception targets identified by Law Enforcement Agency (LEA) sessions.

IRI-IIF is provisioned by the AF using an identity that uniquely identifies the target. This may include login name, E.164 number, SIP URI, MAC address or any other relevant identifier of the target.

IRI-IIF notifies Target activity to the CCTF via the CCTI to optionally allow for dynamic provisioning of an intercept.

The IRI information is sent to the MF over INI2 to be delivered to the Law Enforcement Monitoring Facility (LEMF) over interface HI2.

It should be noted that while the CCTI and INI2 interfaces are functionally different, they are likely to use common information to perform their function, and in the case where the two functions are implemented in the same device there may be a common information flow used.

4.1.2 CC Trigger Function (CCTF)

The purpose of the CCTF is to determine the location of the CC-IIF device associated to the target CC traffic, and to control the CC-IIF via the CCCI interface.

CCTF may either be statically provisioned by the AF using INI1b interface, or dynamically controlled by IRI-IIF using CCTI.

It is possible, depending on the network scenario, to collocate the CCTF with either the MF, the IRI-IIF or with both the IRI-IIF and the CC-IIF in a single device.

4.1.3 CC Internal Interception Function (CC-IIF)

The CC-IIF shall cause the CC, specified by the CCTF, via the CCCI to be duplicated and passed to the MF. Different methods can be used to duplicate the CC provided that the sender and recipient(s) are unaware of the copying process and it is not possible to detect that an intercept is in place.

The CC-IIF is controlled from the CCTF using the CCCI interface.

The CC is sent from the CC-IIF to the MF over INI3 interface to be delivered to the LEMF over the HI3 interface.

The same network device may provide CC-IIF functions for multiple targets, and multiple services per target. For example, an aggregation router at the edge of the service provider network should be capable of providing CC for IP Multimedia services, layer 2 and layer 3 data services. A Media Gateway or Session Border Controller typically provides CC for IP Multimedia services only. It is highly desirable that the CC-IIF provides common generic functions for multiple target services. The CC-IIF function should also be able to accommodate concurrent intercepts on a single target service as well as on multiple target services.

4.1.4 Lawful Interception Mediation Function (MF)

The MF performs two main functions in the provider network, firstly it receives information related to active intercepts from the IRI-IIF(s) and CC-IIF(s) within the service provider network and secondly correlates and formats that IRI and CC information in real time for delivery to the LEMF over the HI2 and HI3 handover Interfaces. IRI-IIF and CC-IIF must provide the raw correlation information used by the MF to build the Handover Interface correlation.

The AF provisions the MF using the INI1c interface.

If there is more than one IRI-IIF within the service provider network providing IRI from IRI-IIF related to a common active target service, the MF should have the capability of combining the IRI from IRI-IIF in such a way that IRI sent to the LEMF appears as if it is from a single IRI-IIF and thus represents a consistent single instance of the active intercept.

4.1.5 Lawful Intercept Administration Function (AF)

In each service provider network there shall exist an AF to administer requests for interception. The AF ensures that an intercept request from a LEA for IRI or CC or both is provisioned for collection from the network, and subsequent delivery to the LEMF. This function is not the subject of this report and is described here only for reasons of completeness.

The information available at the AF includes:

- Identification of the interception subject.
- The agreed Lawful Interception Identifier (LIID).
- The start and end, or start and duration, of the interception.
- The kind of interception information, i.e. IRI or both IRI and CC.
- The address of the LEMF to which IRI information should be sent i.e. the HI2 destination address (if applicable).
- The address of the LEMF to which CC information should be sent i.e. the HI3 destination address (if applicable).
- Other details related to the intercept such as the value of options.
- A reference for authorization of the interception.
- Other information as required.

This information is used by the AF to provision the required intercept and is delivered via the INI1 to the relevant elements. In the reference architecture defined in the present document INI1a provisions the IRI-IIF, INI1b provisions the CCTF, and INI1c provisions the MF.

4.2 Operational considerations

In a typical operation, a lawful and authorized surveillance request for a specified intercept subject is delivered from the LEA to the AF using the handover interface, HI1. Following this request authorized personnel provisions the intercept in the AF, which may be for IRI only, or both IRI and CC. The AF provisions the intercept on the network using the internal interfaces, INI1a to the IRI-IIF, INI1b to the CCTF, and INI1c to the MF. The CCTF function can then provision the intercept via the CCCI interface to the CC-IIF either immediately for pre-provisioning or when a trigger is received from the CCTI interface.

NOTE: In practice the CCTF function is typically located either with the MF or with the IRI-IIF, thus the INI1b interface may be common with the INI1c or INI1a interfaces.

Once an intercept becomes active the IRI-IIF delivers the IRI to the MF using the INI2 internal interface, and the CC-IIF delivers the CC to the MF using the INI3 internal interface. The MF then correlates the IRI and CC information, if not already assigned by the IIFs, it adds the LIID for identification by the LEMF and maps this into the format defined for delivery to the LEMF over the Handover interfaces HI2 and HI3. Some operational issues that need to be considered:

- **Determination of the Location of the CC-IIF:** In cases where the location and/or addressing information for the CC-IIF is not known until the subject registers (or makes a call in the case of voice), the IRI typically provides the necessary information for the provisioning of the CC-IIF (e.g., the IP address and port for the content streams).

- **Content Encryption:** If the service provider provides an encrypted service, national legislation may oblige the service provider to remove the encryption before handover to the LEMF, or alternatively provide the LEA with the encryption keys and the encryption algorithms or software. It is, however, possible for end-users to exchange keys by some other means without any knowledge of the service provider, in which case the service provider will not be able to decrypt the communications or to provide the keys. In the latter situation content transformations or mapping to a particular format could make decryption at the LEA impossible, it is therefore important that the original packets can be provided on HI3 for direct processing at the LEMF.

- **Capacity:** Active intercepts consume resources on network equipment. Therefore, support for lawful intercept requires capacity planning and network engineering to ensure that revenue-producing services are not adversely affected.

5 Internal Network Interfaces (I N I)

5.1 INI1

This clause describes some of the requirements for the INI1 interface. INI1 is split into three interfaces:

1) INI1a is used by the AF to provision the IRI-IIF. The IRI-IIF is associated with a target service, and the access method used by the network operator. The detailed parameters of INI1a may be specific to each target service.

2) INI1b is used by the AF to provision the CCTF.

3) INI1c is used by the AF to provision the MF. It is not in the scope of the present document.

For the purpose of simplification, the IRI-IIF and CC-IIF are both called Internal Interception Function (IIF) in this clause.

In order to provide a generic interface to provision the IIF, the information passed from the AF to the IIF for the purpose of activation of LI shall include at least:

- Lawful Interception Identifier (LIID) - if the implementation does not support this identifier then an alternative mechanism for correlating IRI to CC for Handover to the LEA must be implemented.

- Identity to intercept.

  - For INI1a, the target identity uniquely identifies the target inside the IRI-IIF: this may include login name, E.164 number, SIP URI, MAC address or other identifiers that are uniquely related to the target.

  - For the INI1b , the CC identity uniquely identifies the target CC filters inside the CC-IIF: this may be the IP address, and the port number associated to a session to be intercepted or other identifiers that are uniquely related to the target. This information may not be known before the subject registers or set up a multimedia call.

- Destination addresses of the MFs, for the delivery of the IRI and CC information from the IRI-IIF and CC-IIF.

- Encapsulation and Transport parameters, for example transport parameters could include quality of service mappings that can be used by the underlying network for assured delivery.

- Credentials to fulfil the security service requirements for the delivery to the MF.

5.2 INI2

INI2 carries the following information from IRI-IIF to MF:

- The IRI data records required by the MF to generate HI2.
- Lawful Interception Identifier (LIID) or a correlator to correlate IRI and CC for Handover.

For the content of the IRI data records, two options have to be considered:

- Selection of the parameters which are requested by LEMF. Those parameters are independent of the session, call, and connection or authentication protocol. The IRI parameters are independent of the protocol used by the target to set up the session or connection. This option minimizes the impact in the LEMF or in the MF to understand the different session, call, connection, or authentication protocols.
- Transmission of the full session, call, connection or authentication messages. It is the responsibility of the LEA to discriminate between relevant and irrelevant information. This option minimizes the impact on IRI-IIF and MF when the session, call, connection or authentication protocol evolves with new IRI information.

NOTE: In the case the INI2 interface carries the full session, call, connection or authentication messages, there is still the option for the MF to map the information on the selection of the parameters which are requested by LEMF.

The structure of INI2 information must enable the MF to generate HI2 structure of information related to the, session, call, or connection using Begin, Continue, End or Report messages.

The transport layer must enable secure and reliable transport of IRI.

PKT-SP-ESP1.5-I01-050128 [14] describes a Radius protocol for INI2 transport. The IRI parameters which are requested by the LEMF, are mapped into Electronic Surveillance Indication attributes.

PKT-SP-INF-I01-060406 PacketCable 2.0 [30] describes a Diameter protocol for INI2 transport. The SIP signalling messages are encapsulated into Diameter Event Messages.

5.3 INI3

INI3 carries CC data records from the CC-IIF to the MF.

Whichever encapsulation method is chosen, it should retain all the information available in the original packets (source and destination addresses as well as payload) and provide an identifier for correlating the packets with the IRI. The encapsulation mechanism chosen should provide an easy to implement mechanism that does not adversely impact the network elements, and should allow easy network engineering for both quality of service and security.

The following options can be considered along with their associated advantages and disadvantages:

- UDP encapsulation of original IP packets. The identifier for correlating the packets with IRI is the CC-IIF UDP port.
  - While simple this has the disadvantage of requiring the use of multiple UDP ports within the Mediation Function application, this can make the application less simple to implement as well as complicate security, firewall traversal, and encryption.
  - UDP is an unreliable protocol, so other mechanisms such as network engineering are needed to guarantee delivery of intercepted traffic.
- UDP encapsulation of original layer 2 packets. This method applies for layer 2 interception.
  - This can use either an explicit identifier for correlation of IRI and CC in the UDP packet, or it can use the UDP port method described above with its accompanying issues.
  - It is possible, even likely that the L2 information captured with the interception may not match the original L2 information sent by the target, this could be due to a change of media between the target and the interception point.

- In some instances where L2 protocols are used e.g. PPP the only identity available for use by the CCTF to provision the intercept may be at L2, in this case it is important that the full L2 header be available in the communication content for verification purposes.

- UDP is an unreliable protocol, so other mechanisms such as network engineering are needed to guarantee delivery of intercepted traffic.

- UDP encapsulation of the RTP payload. The CC is intercepted at layer 5. It does not apply for routers which intercept any type of IP traffic. The identifier for correlating the packets with IRI is the CC-IIF UDP port.

  - This method suppresses all the information available in original RTP, UDP and IP headers and does not detect that a RTP packet is lost or unordered, and does not allow reconstruction of the packet sequence.

  - UDP is an unreliable protocol, so other mechanisms such as network engineering are needed to guarantee delivery of intercepted traffic.

- Generation of RTP, UDP and IP headers for INI3 inside the CC-IIF. The CC is intercepted at layer 5. It does not apply for routers which intercept any type of traffic. This method may also be used in situations where interception is centralized e.g. a conference bridge and the underlying IP/UDP/RTP headers have been regenerated, perhaps for multiple call legs.

  - This method suppresses all the information available in original RTP, UDP and IP headers and does not detect that a RTP packet is lost or unordered between the CC-IIF and the target, or the other party of the multimedia session.

  - UDP is an unreliable protocol, so other mechanisms such as network engineering are needed to guarantee delivery of intercepted traffic.

- UDP encapsulation of the Original IP packets. There is an explicit identifier in the packet that is used to correlate the Communication content with the IRI. This identifier should be of sufficient length, say 4 bytes to not cause too much additional overhead, yet at the same time provide unique identifiers to scale to a large network.

  - Using an explicit identifier allows simple correlation of communication content with IRI even if there are multiple CC-IIF involved in the communication. It also allows one UDP port to be used by the MF application simplifying firewall traversal and encryption.

  - Encapsulating the whole of the IP/UDP/RTP headers in the delivery to the mediation function allows the detection of packet loss in the original communication, the RTP header contains a sequence number to allow this. The timestamp in the RTP header is also useful in reconstructing the time sequence for the communication.

  - Maintaining the IP/UDP headers from the target allow further verification of the communication e.g. with radius logs, and possible useful information for further investigation.

  - UDP is an unreliable protocol, so other mechanisms such as network engineering are needed to guarantee delivery of intercepted traffic.

- RTP and UDP encapsulation of original IP packets and higher layers in conjunction with an explicit identifier in the RTP packet, this explicit identifier can be placed in the stream identifier field (SSRC). RTP protocol, described in RFC 3550 [25], is practical to implement for network forwarding devices and is widely used in packet based networks. The CC Identifier may be placed in the SSRC field of the encapsulating RTP packet. The RTP header has a sequence number and a timestamp. The sequence number in conjunction with the stream identifier (SSRC) allows the MF to reconstruct the packet sequence if necessary, and so enables sequenced delivery from the MF to the LEMF, as well as detecting any packet loss in the CC. The timestamp allows the receiver to reconstruct the timing produced by the source. RTP is usually transported across UDP, and should not place any extra processing burden on the CC-IIF.

  - Using an explicit identifier allows simple correlation of communication content with IRI even if there are multiple CC-IIF involved in the communication. It also allows one UDP port to be used by the MF application simplifying firewall traversal and encryption.

- Encapsulating the whole of the IP/UDP/RTP headers in the delivery to the mediation function allows the detection of packet loss in the original communication, the RTP header contains a sequence number to allow this. The timestamp in the RTP header is also useful in reconstructing the time sequence for the communication.

- Maintaining the IP/UDP headers from the target allow further verification of the communication e.g. with radius logs, and possible useful information for further investigation.

- RTP encapsulation from the CC-IIF allows for detection of packet loss between the CC-IIF and the Mediation function however it does not provide for recovery of lost packets.

RTP or UDP can be used in conjunction with network Quality of Service guarantees to provide assured CC delivery to the MF. Packet based networks based on IP, provide Quality of Service guarantees using the Diffserv field (DS field), RFC 2474 [26]. The Diffserv Code Point, (DSCP, defined in the first 6 bits of the DS field) is used by Service Providers to select a Per Hop Behaviour (PHB) on each network node, each PHB is associated with a set of mechanisms that allow traffic differentiation, for example Class based Weighted Fair Queuing. Within the Diffserv Architecture RFC 2475 [27], this service differentiation allows delivery of multiple critical services for business and residential customers, and so has proved itself able to deliver high levels of service assurance on IP based networks. This value can be set on the CC-IIF for each individual intercept or more generally for all intercepted traffic and would allow prioritization of the intercepted traffic both in-band on the network and on an out of band management connection. Using RTP or UDP in conjunction with network Quality of Service allows the network provider to engineer the appropriate level of service required for CC delivery to the MF, and facilitate reliable delivery from the MF to the LEMF. RTP provides the additional benefit of being able to explicitly detect loss between the CC-IIF and the Mediation Function.

5.4 CC Trigger Interface (CCTI)

The CCTI carries CC trigger information from the IRI-IIF to the CCTF.

The CCTI shall notify the target activity to the CCTF, and shall provide the necessary parameters required by the CCTF to determine the location of the CC-IIF device associated to the target, control the CC-IIF, and filter the CC traffic.

The information passed from the IRI-IIF to the CCTF for the purpose of activation of LI shall include:

- A Lawful Interception Identifier (LIID) or a correlator to correlate IRI and CC for Handover.

- A CC filter specification which uniquely identifies the target inside the CC-IIF: this may be the IP address, and the port number associated with a target session or other identifiers that uniquely relate to the target. This information may not be known before the subject registers or set up a multimedia call, and so may require dynamic resolution during the call setup and duration.

If the CCTF has already identified the CC-IIF, specifically the IP address of the CC-IIF then this should be communicated over the interface. If the CC-IIF address is not provided by the CCTF then the CCTF must discover the CC-IIF address either dynamically e.g. on the network, or statically via a lookup table.

When the CCTF is collocated with MF, the CCTF information is imbedded inside INI2.

5.5 CC Control Interface (CCCI)

The information passed from the CCTF to the CC-IIF for the purpose of activation of LI shall include:

- A Lawful Interception Identifier (LIID) or a correlator to correlate IRI and CC for Handover.
- A CC filter specification which uniquely identifies the target inside the CC-IIF: this may be the IP address, and the port number associated to a target session or other identifiers that uniquely relate to the target. This information may not be known before the subject registers or set up a multimedia call, and so may require dynamic resolution during the call setup and duration.
- Destination addresses of the MFs, for the delivery of the IRI and CC information from the IRI-IIF and CC-IIF
- Encapsulation and Transport parameters, for example transport parameters could include quality of service mappings that can be used by the underlying network for assured delivery.
- Optional Credentials to fulfil the security service requirements for the delivery to the MF.

The following options have to be considered.

5.5.1 Dedicated interface for the control of CC-IIF

A generic interface controls CC-IIF and provides the necessary parameters for every target services.

It is desirable that the active or provisioned intercept configuration on the network device should not be maintained in the case of a CCTF failure, and in the case where the CCTF has failed there also needs to be a mechanism to detect both failure and recovery and to reprovision the intercepts when the CCTF is available again.

One way that this can be achieved is by the use of a refresh mechanism between the CCTF and the CC-IIF. When an intercept is activated by the CCTF, a timeout value is associated with the intercept on the CC-IIF and a countdown timer is started. If the timer receives a refresh message from the CCTF this timer is reset, if no refresh message is received and the timer expires then the intercept is removed from the CC-IIF. If a failure of the device with the CCTF occurs, such that it is not able to supply the refresh to reset the timer, then the intercept will cease to exist after the timeout expires. Similarly, if the device performing the CC-IIF re-boots, then the intercept will not survive the re-boot unless the CC-IIF is capable of ascertaining that the intercept lifetime requirements will continue to be met.

In the case of a failure of the CC-IIF device, the responsibility for reprovisioning the intercepts is with the device performing the CCTF. In order for this to work, it must be possible for the CCTF to realize that there is a failure in the CC-IIF such that it must re-establish the intercepts. This may be in the form of an audit or interrogation (from the CCTF to the CC-IIF), or in the form of a heartbeat mechanism in the content stream sent to the MF, or both.

This method has the following characteristics:

- A generic CCCI interface controls the CC-IIF for every target services. Some devices like routers aggregate several type of traffic and services (i.e. internet access, VoIP, video, multimedia, Email…). Each service involves specific session, policy, or authentication protocols. There is no need to extend each of those protocols to control the CC-IIF for each of the target services.
- A central CCTF may control the capacity of CC-IIF when multiple IRI-IIF are associated with the same CC-IIF. For example, one router may provide CC-IIF for Internet access, VoIP, multimedia, and Email services. In this case, the CCTF should consolidate the interception filters for activation on the CC-IIF device for efficiency reasons and verify that the intercepted traffic of every target services does not exceed the device capacity.
- A dedicated interface should be encrypted with strong cryptographic authentication. It prevents detection by unauthorized entities. When CCTF is a trusted interception device, it prevents unauthorized activation of interception.
- A dedicated interface has the flexibility to provision the most appropriate INI3 encapsulation method, the optional credentials to fulfil the security service requirements. In an operational environment, there is a need for message extensions like Audit to detect unauthorized attempt to access the intercept capacity.

5.5.2 In-band control of CC-IIF

The CCCI is imbedded inside a session/policy/authentication control protocol defined between the CCTF device and the CC-IIF device for a specific target service.

One example of this method is the H.248 topology descriptor described in TS 133.107 [8] annex D.

ITU-T Recommendation H.248.1 [20] has the capability to control the duplication of media streams for multi-party conferences. A topology descriptor connects a one-way terminations to each termination of a Media Gateway, and duplicates the forward and backward target streams towards the MF.

It has the following characteristics:

- There is minimum impact on the Media gateway to support the H.248 topology descriptor for interception. It fits specifically well for Circuit Switch Handover Interface where the Media Gateway sends HI3 traffic. In this case, there is no need to encapsulate the INI3 traffic. For an IP Handover Interface, the Media Gateway may need to encapsulate the INI3 traffic with a format specific to the CC-IIF function.

- The same device (i.e. the MGC) controls both the Media Gateway and the CC-IIF functions. It simplifies the synchronization between the two functions.

- Combining LI control information with a general purpose control protocol has a major security weakness: It is very difficult to guarantee confidentiality of LI information when it is combined with another control protocol. Because the control protocol is also used for session, it often requires access via traces and debugging tools that provides information on intercepts to unauthorized users.

- There may not be a direct session control relationship between the IRI-IIF and that CC-IIF. The result is that the IRI-IIF will have to relay requests to some component that does have such a control relationship. The P-DCS-LAES header in RFC 3603 [31] is a SIP header extension that can be used for this purpose however there is no such equivalent for ITU-T Recommendation H.323 [21]. Ultimately this results in a significant increase in complexity: finding a component that can do the tap; scrubbing the signalling (e.g. P-DCS-LEAS header) so unauthorized components do not see the header, etc. For example, in some cases the header is passed in the session forward direction, then if nothing in that direction is unable to do the tap, it has to passed in the backward direction (e.g. with the response).

- In an operational environment, there is a need for extensions to an in band CCCI like auditing to detect unauthorized attempts to access the intercept capability, and LI traces. The associated information may be transported between the AF and the CC-IIF, impacting both the session/policy/authentication protocol, and the CCCI traffic.

- IRI-IIF cannot be a passive probe. If the service control device does not have all the security functions to prevent unauthorized creation and detection of intercepts, it may be appropriate to support CC-IIF inside a passive probe. A passive probe cannot modify the session/policy/authentication control protocols.

- When CC-IIF is used by multiple target services, there is no central function which controls the capacity of the CC-IIF.

Another option is to extend a session/policy/authentication protocol which does not have the capability to control the duplication of media streams for multi-party conferences (i.e. COPS, Radius, DHCP, Diameter). This approach has the following additional characteristics:

- The timing of the session/policy/authentication requests does not always line up with the timing for LI requests. This can lead to problems when a single request contains information elements for both session/policy/authentication control and LI (e.g. requiring the CC-IIF to parse and compare with previous requests to see which information elements have changed).

- When the model of combining existing session/policy/authentication control protocols with LI requests is used, a large number of protocols need to be extended with LI capabilities. With this approach, LI capabilities must be also extended to TGCP, SIP, H.323, Radius, DHCP, Diameter, and probably others in the future. This adds a tremendous complexity for each of these protocols, and each impacted device.

- The more network elements are involved with LI, the more difficult it is to secure the confidentiality of LI information, and protection against illegal interception. The model of combining session/policy/authentication control protocols with LI, results in intercept information being accessible via an increasing number of servers that are involved in session, policy and authentication control.

6 Security

This clause provides general information about security of Lawful Interception. Additional requirements may exist in particular regions or nations, in accordance with regulations or laws.

- Prevent detection by unauthorized entities: One requirement is to ensure that the intercept subject is unable to detect that they are being intercepted. The present document assumes a sophisticated subject:

  - Able to check IP addresses, use traceroute, which traces every layer 3 hop in the route, measure the round trip delay, etc.

  - Able to check if any unusual signalling is occurring on their Customer Premises Equipment (CPE).

  - Able to detect degradation or interruptions in service.

  Therefore, the intercept mechanism should not involve special requests to the CPE, re-routing of packets or end-to-end changes in IP addresses. Instead, content intercept should be done on a device along the normal content path (i.e. no re-routing has occurred) that is within the service provider's network.

  A convenient CC-IIF is a router or switch at the edge of the service provider's network to which the intercept subject connects. One of the reasons for choosing the edge device is that it routes all the traffic between the target and every other subscriber. It is also unlikely there is L3 packet load sharing between the user and the edge device. If done in the core of the network per packet load balancing could mean multiple devices would need to be monitored and related to get all packets associated with a particular connection.

  Another possibility is to provide a special device along the path to provide the CC-IIF capabilities or to duplicate all traffic on one or more routes by means of passive splitters, cupper or fiber, and to process all duplicated traffic on a dedicated L3 switch or other device that allows for filtering of the target traffic.

NOTE: In the case where there is multi-homing (two or more routers connected to provide access for the CPE), intercept taps may have to be installed on more than one access router. If the CPE is multi-homed to multiple service providers, then the intercept will have to be installed on each service provider separately and the LEA will have to correlate the data.

- Prevent unauthorized activation of interception: Elements with access to intercept capabilities and related information should be carefully controlled and only accessed by authorized personnel.

  - When the interfaces to provision or control the IRI-IIF and CC-IIF are dedicated for LI, they should have strong cryptographic authentication to establish the identity of the principals, and correlate the identity of the principals with the action they are attempting to perform. Those interfaces should perform some sort of cryptographic message integrity checking such as, for example HMAC-MD5. Message integrity checking can also be used to counter replay attacks. The AF should be operated by authorized personnel only and only these personnel may have access to the INI1a, and INI1b and INI1c interfaces. The interception functions in the IRI-IIF and CC-IIF should only be provisioned via secured interfaces.

  - When the interfaces to control CC-IIF is shared with other protocols, it should be carefully designed to avoid unauthorized activation of interceptions in the CC-IIF.

- Information protection:

  - Non disclosure of target information:
    Target information and intercept states in the IRI-IIF and CC-IIF shall not be accessible to unauthorized personnel from any operational management station, via management protocols, Command Line Interfaces (CLI) and traces or dumps, and shall not be stored in Non Volatile Memory. If the IRI-IIF or CC-IIF device fails or re-boots, all intercept related information and states shall disappear and shall not be accessible by any means.

  - Non disclosure of IRI:
    Transmission of INI2 shall be done in a secure manner. The option for the IRI to be routed through the network independently of other traffic should be available, so that it is possible to forward traffic over secured network links independently of other traffic. In any case, IRI shall not be transmitted over the production network in "en-clair" form.

  - Non disclosure of CC:
    Transmission of INI3 shall be done in a secure manner. The option for the CC to be routed through the network independently of other traffic should be available, so that it is possible to forward traffic over secured network links independently of other traffic. In any case, CC shall not be transmitted over the production network in "en-clair" form.

  - Logging and auditing are used to detect unauthorized attempts to access the intercept capability. Log files may be controlled, retrieved and maintained by the AF in a secure manner. These log files should not be stored on the interception devices, to avoid being viewed or detected.

  - Measures must be taken to:

    - enable timely detection of system-, network- or software failures that may cause the interception system to over- or under collect data;

    - take appropriate action to prevent further over- or under collection; and

    - report on the anomaly to allow for corrective action.

7 Applying the reference model

Having defined a reference architecture, it is useful to examine the different ways in which the different functions may be mapped to service provider network elements. This provides verification of the architecture by showing that the various currently deployed LI solutions can be covered by the reference model. This clause will look at the different solutions and define the scope, characteristics and limitations of the solution.

Different solutions today include the following cases:

- The CCTF is collocated with the MF, an example of this would be a mediation device which is responsible for provisioning the intercept as well as receiving, correlating and handing over the IRI and CC information.

- The CCTF is collocated with the IRI-IIF, an example of this would be a MGC that would be responsible for providing IRI information to the MF, as well as provisioning intercepts on the CC-IIF, in this case a Media gateway via the CCCI interface.

- The CCTF, the IRI-IIF and the CC-IIF are collocated in the same device, an example of this would be a Session Border Controller which would be responsible for providing both IRI and CC information to the MF.

7.1 CCTF collocated with MF

7.1.1 Configuration

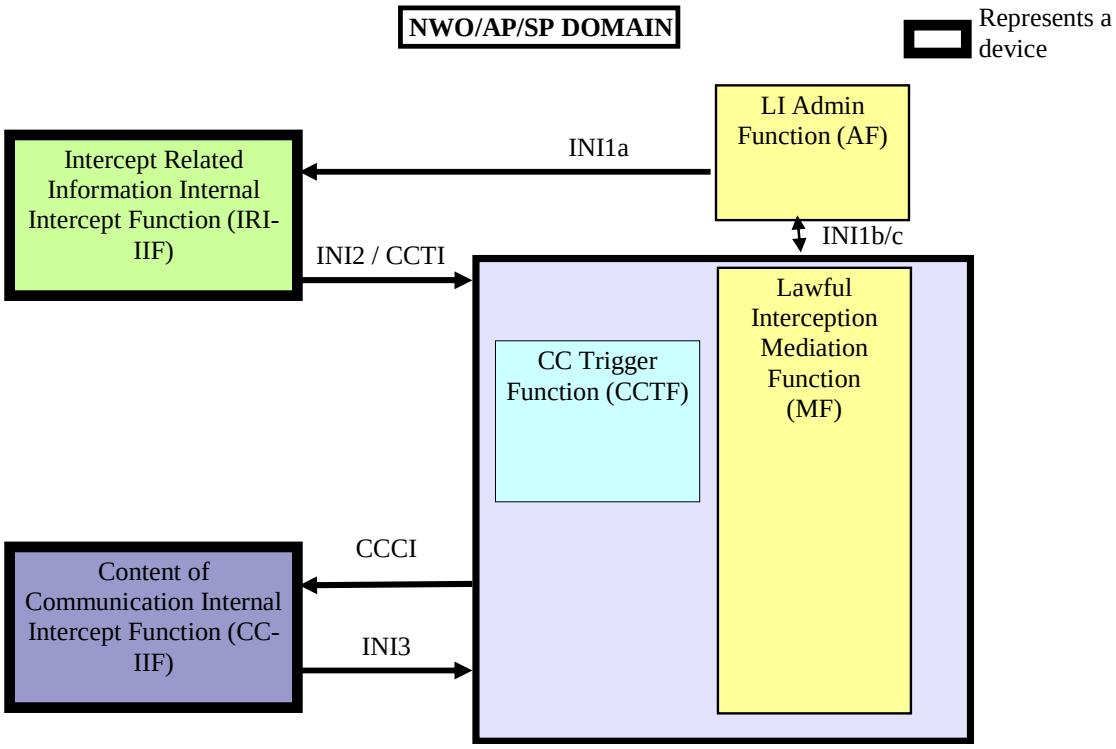


Figure 3: CCTF collocated with MF

7.1.2 Scope

This function placement applies for a number of service provider configurations:

- There is no in-band LI control protocol between the IRI-IIF and CC-IIF.
- The session, policy, authentication or control protocol between the IRI-IIF and the CC-IIF may not have the capability to control interception, or may not satisfy the security and visibility requirements for Lawful Interception.
- There may not be a direct session relationship between the IRI-IIF and the CC-IIF for every possible network scenarios and thus having a centralized function allows a common control layer for Lawful Interception.
- Some CC-IIF devices are stand-alone equipment which do not terminate the session, policy, or authentication protocol; in this case a specific out of band LI control is required.
- Some CC-IIF devices provide CC for multiple target services (i.e. a router integrating CC-IIFs for multimedia and data interception). In this case, the CCTF should consolidate the filters to activate in the CC-IIF devices and verify that the intercepted traffic for every target services does not exceed the device capacity. The Centralization of the capability with the MF facilitates this case.

7.1.3 Characteristics

- Security:
  - The CCCI is a secure, dedicated protocol controlled by a trusted device, operated by authorized personnel. It prevents unauthorized activation of interception. No intermediate entity is involved with LI information.
  - Strong protection of the CCCI and INI3. The CCCI should be encrypted and should control encryption of INI3.
- Flexibility:
  - A common CCCI for multiple target services.
  - Possibility to provision encapsulation methods with time stamps for INI3, secured interface to transmit INI3 and other options in the future.
  - A CCTF collocated with the MF allows to dynamically filter CC traffic when there is no direct session control relationship between the IRI-IIF and the CC-IIF.

7.2 CCTF collocated with IRI-IIF

7.2.1 Configuration

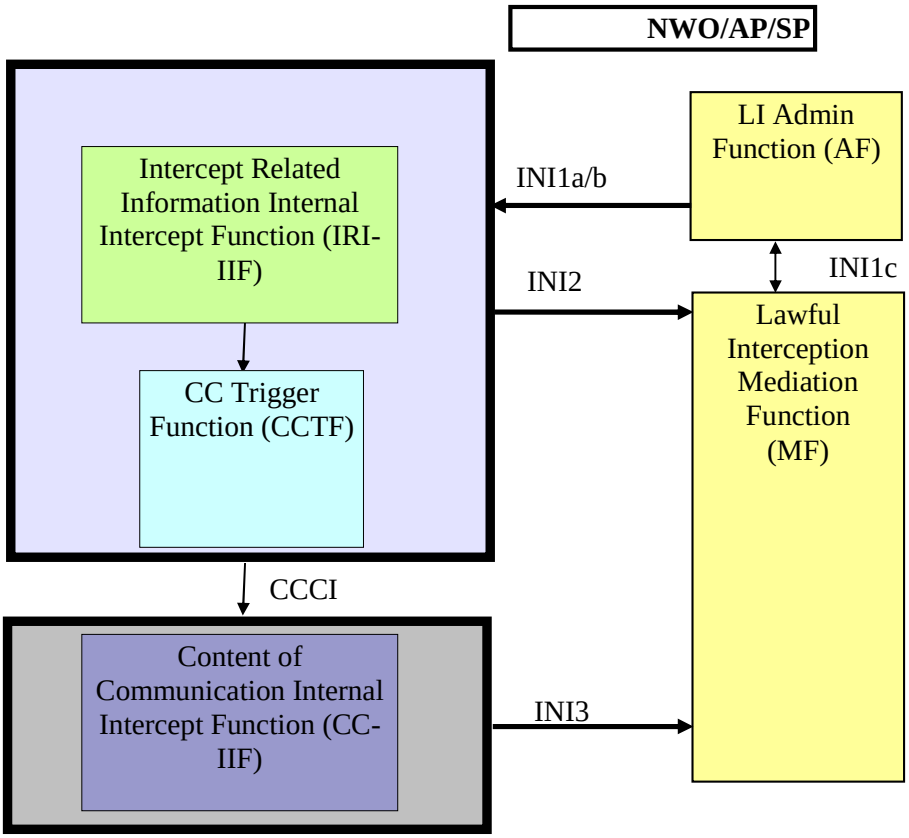


Figure 4: CCTF collocated with IRI-IIF

7.2.2 Scope

This function placement applies when IRI-IIF and CC-IIF devices process a single target service (e.g. MGC and Media Gateway for voice over IP) and there is an in-band LI control protocol between IRI-IIF and every possible CC-IIF devices (e.g. PES with monolithic softswitch).

7.2.3 Characteristics

- Security:
  - Control of CC in the CC-IIF is inherent to the signalling protocol between the IRI-IIF and CC-IIF.
- Flexibility:
  - No specific LI functions in the CC-IIF.

7.3 CCTF collocated with IRI-IIF and CC-IIF

7.3.1 Configuration

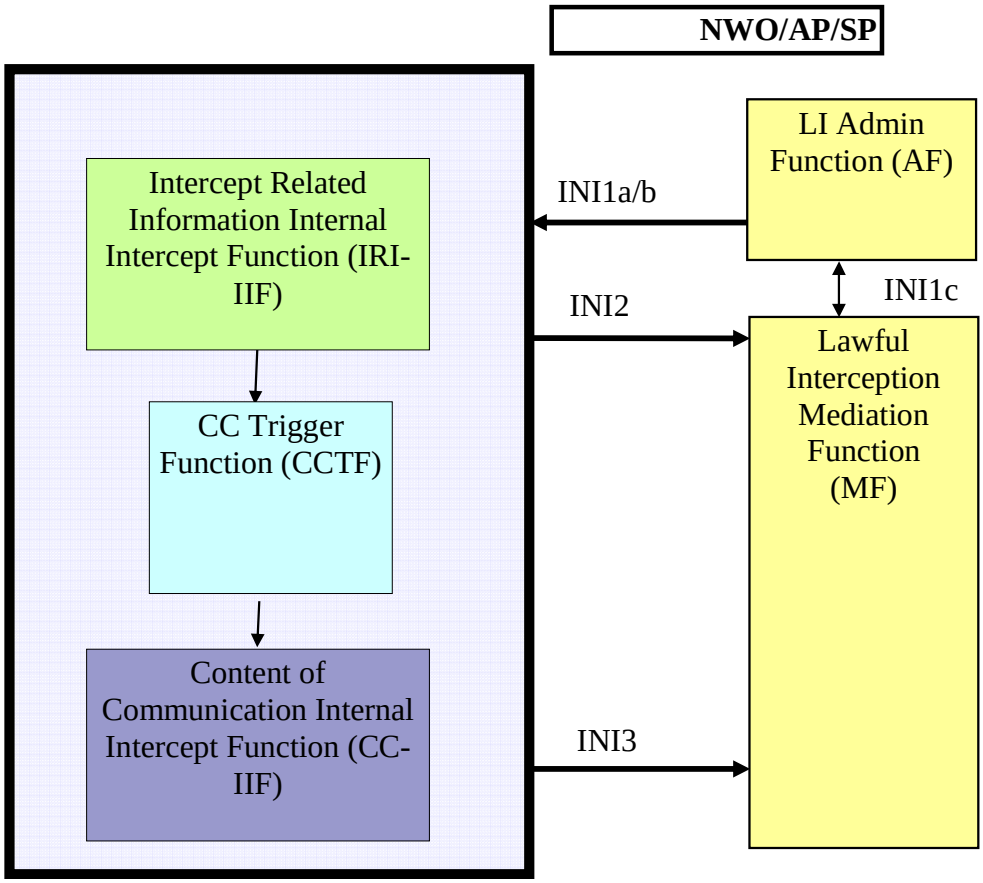


Figure 5: CCTF collocated with IRI-IIF and CC-IIF

7.3.2 Scope

The IRI-IIF, the CCTF and the CC-IIF are collocate in the same device.

7.3.3 Characteristics

CCTI and CCCI are internal interfaces.

Annex A:
Service scenarios

A.1 IP Multimedia services

This clause will look at some of the issues surrounding the interception of IP Multimedia calls, taking local voice services as a specific service example. The reference model from figure 2 will be applied with the use of a common set of interfaces that are independent of the call signalling protocols in use.

There are a variety of architectures in use for IP Multimedia (e.g., centralized versus distributed) as well as various protocols (SIP, H.323, MGCP, H.248).

NOTE 1: In the case where the intercept subject accesses the network via a non-IP endpoint (e.g., TDM), the detectability issue is less acute (e.g., re-routing of packets to intercept them in a special device is a possible option), since the intercept subject does not have access to the IP addresses or to traceroute.

However, in the case of local services, this is a much more difficult problem. The intercept for a call originating and terminating on-net (i.e., a call that is IP Multimedia end-to-end) has to be intercepted along its normal route in order to be undetectable. In addition, the call-forwarding feature that is often provided as a local service feature makes interception even more difficult: If call forwarding is invoked, a call that was intended to terminate on the intercept subject may be forwarded anywhere in the network resulting in the media stream bypassing the original CC-IIF (since in IP Multimedia, the media stream goes directly from end-to-end). Also, since call forwarding can often be set up on a call-by-call basis, the location of the CC-IIF will often not be known until the call is set up.

In case the intercept subject under surveillance is being provided with a local voice service by the same provider that also provides the network access (e.g., controls the edge router or switch). This is an important assumption, since in IP Multimedia the entity providing call control (e.g., SIP server, MGC of H.323 gatekeeper) can be totally separate from the entity providing network access (e.g., operates edge routers).

Suppose that a subscriber that subscribes to a local (e.g., residential) voice service is a target for a lawfully authorized surveillance. Part of the system providing these services is a subscriber database that includes addressing information about the subscriber as well information on what features are in effect (e.g., call forwarding). Some call control entity accesses that database in order to provide local services. For example, if the subject has call forwarding invoked, that fact (and where to forward the call) is indicated in the subscriber database. A call arriving at the call control entity that "owns" that subscriber can then take the appropriate action (e.g., forward the call).

The call control entity that "owns" the target subscriber (which could be an H.323 gatekeeper, a SIP proxy or a MGC) is the IRI-IIF. The AF provisions the IRI-IIF with INI1 which defines the intercept parameters (e.g., subject identification information such as the telephone number and address of the MF). Once provisioned, it passes the IRI to the MF for every call or session initiated by the target. In the scenario being discussed, the IRI-IIF typically remains in the signalling path throughout the call, even in the call-forwarding case. Part of the IRI it passed to the MF is the media signalling information (i.e., SDP or H.245), which includes endpoint IP address and port information for the media (content) streams. Armed with this media address information, the AF can determine the CC-IIF and make the request via INI1. The request identifies the voice stream to be intercepted based on information received in the call signalling (i.e., IP addresses and UDP port numbers).

NOTE 2: The CC-IIF in the case of IP Multimedia could be an edge router or a PSTN gateway (e.g., a call from the PSTN forwarded to the PSTN). SIP, H.323, MGCP or H.248 call signalling protocols could be used. However, the INI1 provisioning interface, is not dependent on the type of call signalling protocol used; nor is the encapsulation format and transport protocol of INI3. The same reference model (figure 2) with the same interfaces can be used for lawfully authorized surveillance, regardless of the signalling protocol and regardless of the type of service being provided (Note that even though a local voice service was used in this example, other voice services could use the same model and interfaces).

Figure A.1 depicts the message exchange between a Target End Point, the remote IP Multimedia End Point, CC-IIF, IRI-IIF, AF/MF and LEA/LEMF during a SIP session establishment:

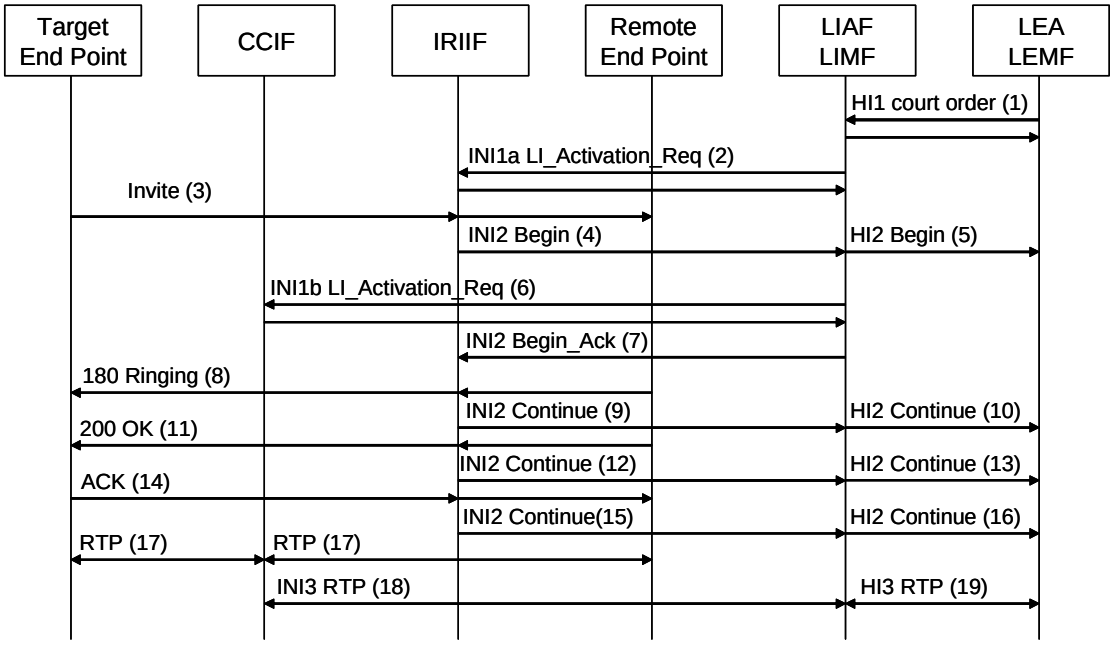


Figure A.1: Basic IP Multimedia message exchange

The following list describes the sequence of messages shown in figure A.1:

1) The LEA delivers a court order to the network administrator who operates the LI Administration Function.

2) The AF sends an INI1a LI_Activation_Request to provision the IRI-IIF with the target IRI filter.

3) The target End Point sends a SIP Invite to a SIP proxy which routes the Invite to the remote End Point. The SIP Invite is intercepted by the IRI-IIF. The SIP Invite contains a Session Descriptor Protocol (SDP) which describes the Target Endpoint IP address and UDP port used to send and receive the RTP stream during the session.

4) The IRI-IIF sends an INI2 Begin to the MF.

5) The MF forwards a HI2 Begin to the LEMF.

6) The AF sends an INI1b LI_Activation_Request to provision the CC-IIF with the target CC filter (IP address and UDP ports for the RTP stream).

7) The MF acknowledges the INI2 Begin from the IRI-IIF.

8) The remote End Point sends a SIP 180 ringing message to a SIP proxy which routes it to the remote End Point. The SIP 180 ringing message is intercepted by the IRI-IIF. The SIP 180 ringing contains a Session Descriptor Protocol (SDP) which describes the remote End Point IP address, the UDP port used to send and the UDP port to receive the RTP stream during the session.

9) The IRI-IIF sends an INI2 Continue to the MF.

10) The MF forwards a HI2 Continue to the LEMF.

11) The remote End Point answers the call and sends a SIP 200 OK message to a SIP proxy which routes it to the remote End Point. The SIP 200 OK message is intercepted by the IRI-IIF.

12) The IRI-IIF sends an INI2 Continue to the MF.

13) The MF forwards a HI2 Continue to the LEMF.

14) The target End Point sends an ACK message to a SIP proxy which routes the Invite to the remote End Point. The SIP ACK is intercepted by the IRI-IIF.

15) The IRI-IIF sends an INI2 Begin to the MF.

16) The MF forwards a HI2 Continue to the LEMF.

17) The target End Point sends and receives RTP packets with the remote End Point. This RTP streams are intercepted by the CC-IIF.

18) The CC-IIF sends the INI3 RTP packets to the MF.

19) The MF forwards the HI3 RTP packets to the LEMF.

A.2 Data services

The same model (figure 2) can also be used for data services. In this case the IRI-IIF could be a server performing authentication, authorization, and accounting services (e.g. Radius) or simple authorization (e.g. DHCP server) for services, and assigning IP addresses to the target. If a potential IRI-IIF does not have the available INI1 and INI2 interface support, an external probe located in the path between the target and the server can be used to obtain the IRI.

The IRI in the case of a data service could include:

- The time that the user registered or de-registered for the service.
- Addressing information (i.e., given the user identity, what IP address or other information is available that could be used in interface (d) to do the content tap).

Once suitable addressing information is available to the CCTF, the CCTF provisions the CC-IIF using CCCI.

Clearly the IRI are different for data than they are for voice services. However, the INI1 is typically the same (an edge router).

Figure A.2 depicts the message exchange between a Target CPE, the remote client or server, CC-IIF, IRI-IIF, AF/MF and LEA/LEMF during a data connection establishment with Radius authentication.

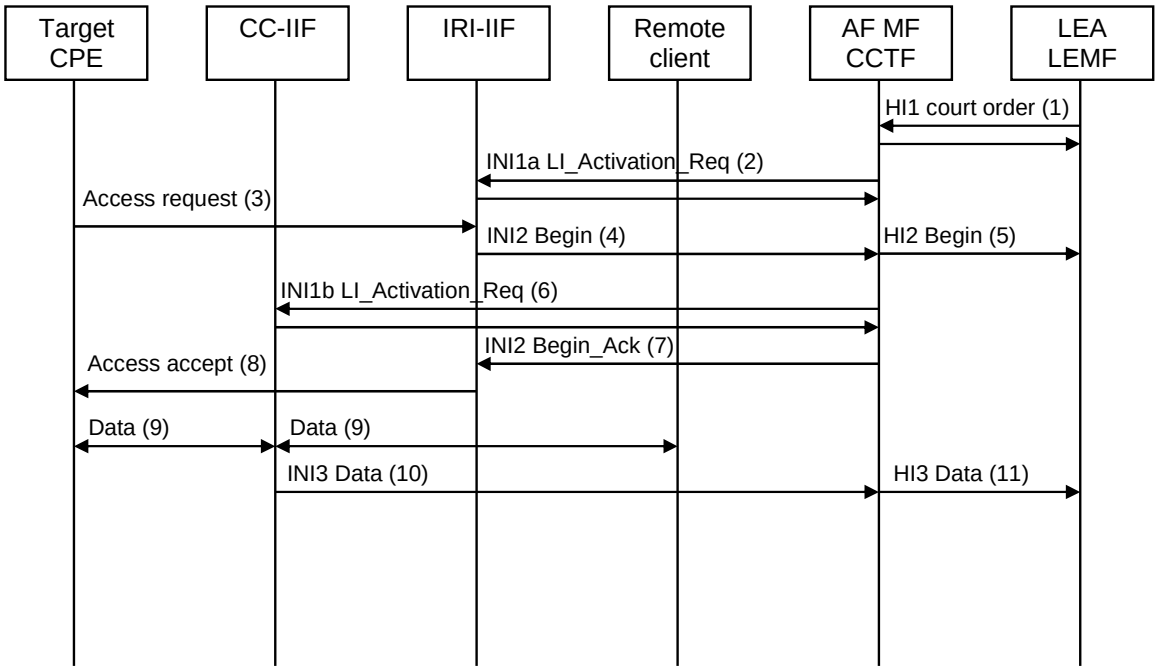


Figure A.2: Basic data connection message exchange

The following list describes the sequence of messages shown in figure A.2:

1) The LEA delivers a court order to the network administrator who operates the LI Administration Function.

2) The AF sends an INI1a LI_Activation_Request to provision the IRI-IIF with the target IRI filter.

3) The target CPE sends user name and password to a Radius client which sends an Access Request to a Radius server. The Access Request is intercepted by the IRI-IIF.

4) The IRI-IIF sends an INI2 Begin to the MF.

5) The MF forwards a HI2 Begin to the LEMF.

6) The AF sends an INI1b LI_Activation_Request to provision the CC-IIF with the target CC filter (IP address of the target).

7) The MF acknowledges the INI2 Begin from the IRI-IIF.

8) The Radius Server sends an Access Accept to Radius client.

9) The target CPE sends and receives IP packets with the remote client or server. These IP packets are intercepted by the CC-IIF.

10) The CC-IIF sends the INI3 data packets to the MF.

11) The MF forwards the HI3 data packets to the LEMF.

Annex B:
Deployment scenarios

This annex describes a number of common deployment scenarios for IP multimedia services. It discusses the network configuration, and the characteristics for the following deployment scenario:

1) IRI-IIF integrated in Call Agent, CC-IIF integrated in aggregation router, CCTF collocated with MF.

2) IRI-IIF integrated in Call Agent, CC-IIF integrated in Media Gateway, CCTF collocated with MF.

3) IRI-IIF and CCTF integrated in Call Agent, CC-IIF integrated in Media Gateway.

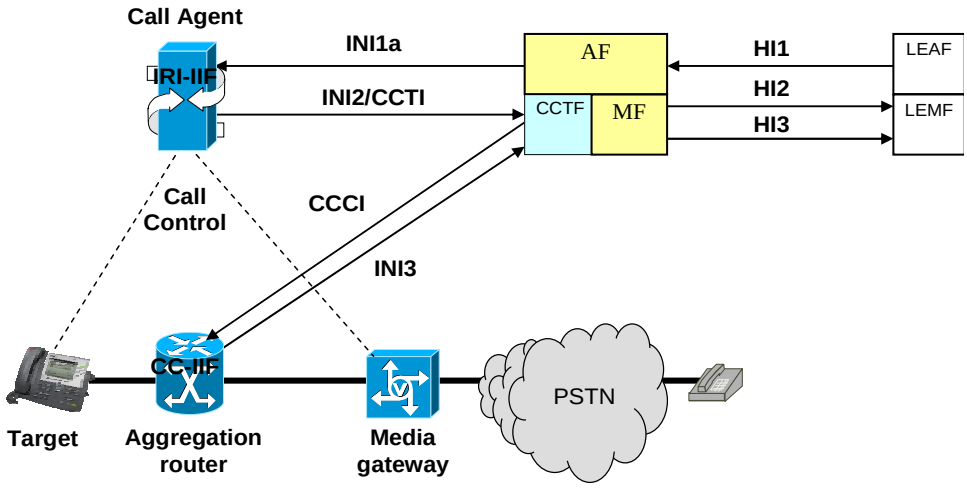
4) Stand-alone IRI-IIF, CC-IIF integrated in aggregation router or aggregation router, CCTF collocated with MF.

5) IRI-IIF integrated in Call Agent, stand-alone CC-IIF, CCTF collocated with MF.

6) IRI-IIF, CCTF and CCTF integrated in SBC.

B.1 IRI-IIF integrated in Call Agent, CC-IIF integrated in aggregation router, CCTF collocated with MF

B.1.1 Configuration



NOTE 1: IRI-IIF is a line side softswitch, proxy, gatekeeper or Application Server.
NOTE 2: CC-IIF is the first aggregation router connected to the target.

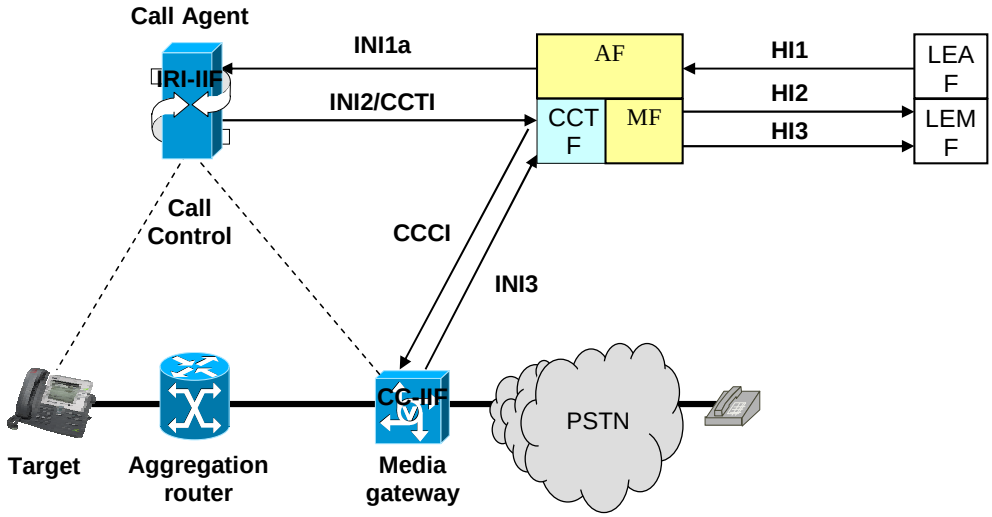
Figure B.1: IRI-IIF integrated in Call Agent, CC-IIF integrated in Aggregation router, CCTF collocated with MF

B.1.2 Scope

- Line side Multimedia IP or PSTN Simulation Services (residential and business).
- Dynamic filter of media streams on a session by session basis.

B.2 IRI-IIF integrated in Call Agent, CC-IIF integrated in Media Gateway, CCTF collocated with MF

B.2.1 Configuration



NOTE 1: IRI-IIF is a line side softswitch, proxy, gatekeeper or Application Server.
NOTE 2: CC-IIF is a Media Gateway.

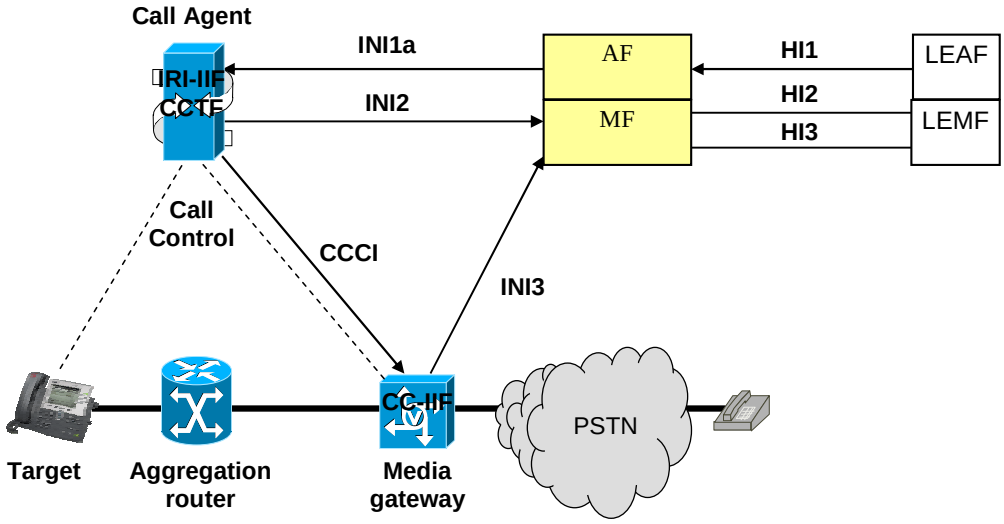
Figure B.2: IRI-IIF integrated in Call Agent, CC-IIF integrated in Media Gateway, CCTF collocated with MF

B.2.2 Scope

- Line side VoIP / PSTN Simulation Services (residential and business).
- PSTN Emulation Services.
- VoIP transit.

B.3 IRI-IIF and CCTF integrated in Call Agent, CC-IIF integrated in Media Gateway

B.3.1 Configuration



NOTE 1: IRI-IIF is a MGC.
NOTE 2: CC-IIF is a Media Gateway.

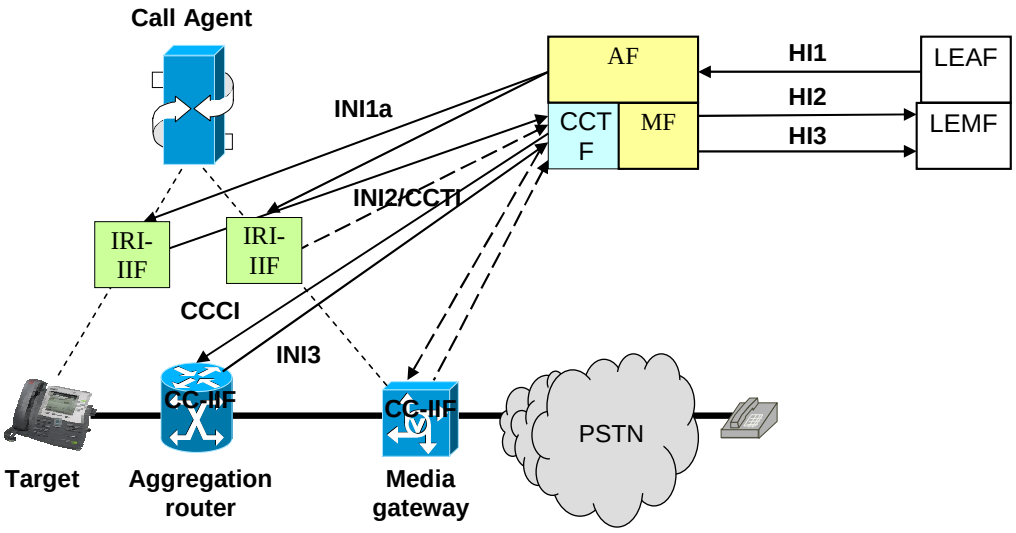
Figure B.3: IRI-IIF and CCTF integrated in Call Agent, CC-IIF integrated in Media Gateway

B.3.2 Scope

- PSTN Emulation Services.
- VoIP transit.

B.4 Stand-alone IRI-IIF, CC-IIF integrated in aggregation router or aggregation router, CCTF collocated with MF

B.4.1 Configuration



NOTE 1: IRI-IIF is a probe.
NOTE 2: CC-IIF is an aggregation router or Media Gateway.

Figure B.4: IRI- Stand-alone IRI-IIF, CC-IIF integrated in aggregation router or aggregation router, CCTF collocated with MF

B.4.2 Scope

- Line side Multimedia / PSTN Simulation Services (residential and business).
- PSTN Emulation Services.
- VoIP transit.

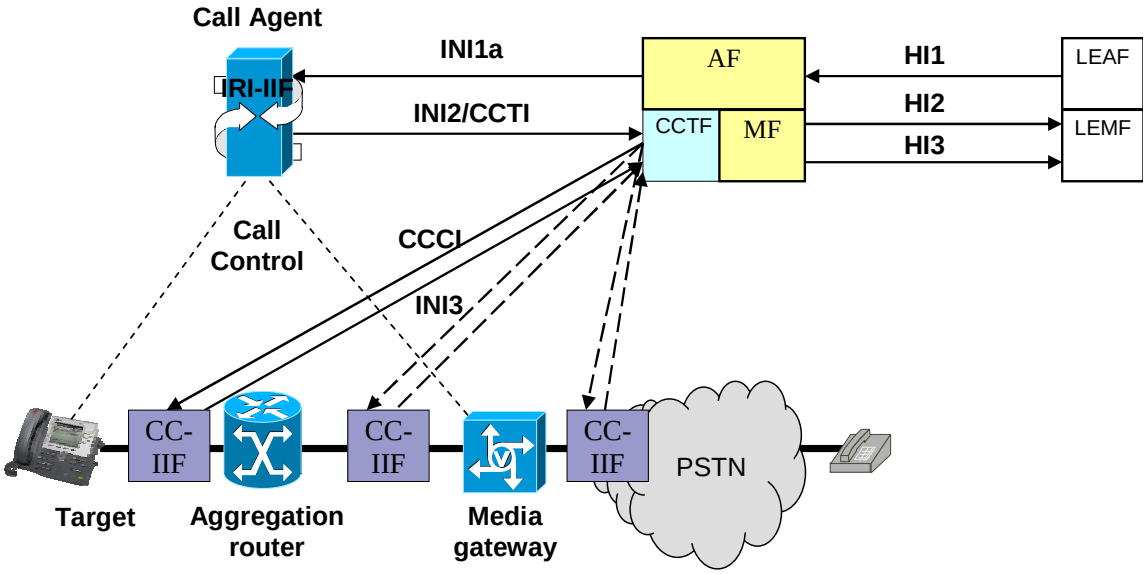
B.4.3 Characteristics

For IP Multimedia interception, this option has a number of limitations:

- When the target receives a call with Calling Line ID Restriction, the line side signalling protocol will not contain the Calling Line ID. This information must be provided to the LEA.
- When the target forwards or transfer his calls towards another number, the signalling traffic will not reach the target device. One or more stand-alone IRI-IIF must then be able to monitor and correlate signalling at all possible locations in the network where the call could be transferred. Depending on the network scenario, the protocol may be SIP, H.323, SS7 (TDM or Sigtran), with MGCP or H.248.
- When signalling is encrypted, the stand-alone IRI-IIF must have access to the encryption key which introduces a significant security hole.

B.5 IRI-IIF integrated in Call Agent, stand-alone CC-IIF, CCTF collocated with MF

B.5.1 Configuration



NOTE 1: IRI-IIF is a line side softswitch, proxy, gatekeeper or Application Server.
NOTE 2: CC-IIF is a probe.

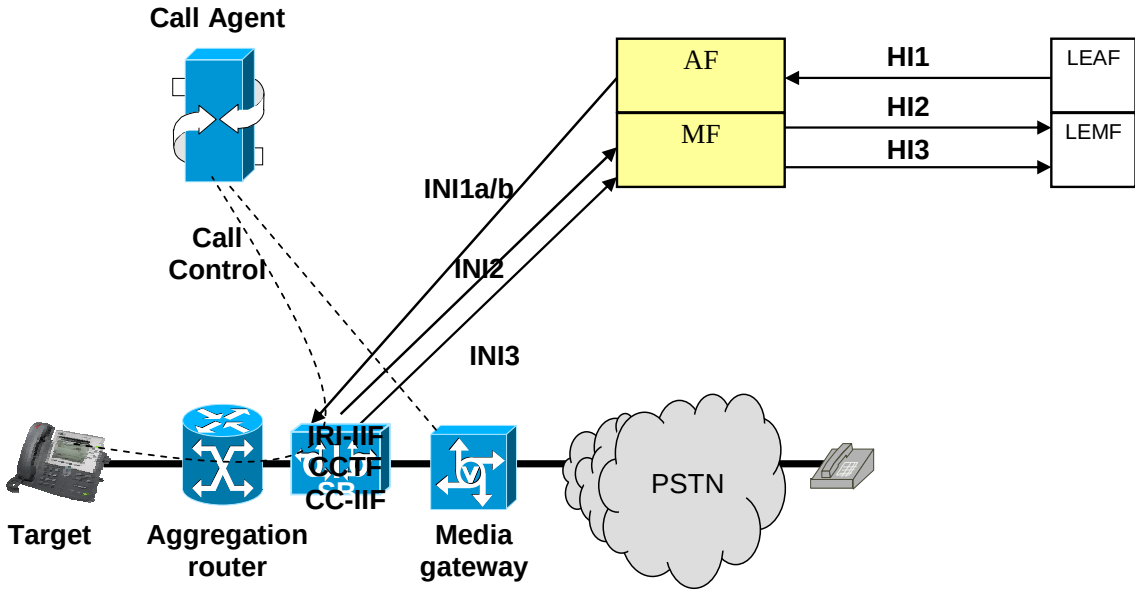
Figure B.5: IRI IRI-IIF integrated in Call Agent, stand-alone CC-IIF, CCTF collocated with MF

B.5.2 Scope

- Line side Multimedia / PSTN Simulation Services (residential and business).
- PSTN Emulation Services.
- VoIP transit.

B.6 IRI-IIF, CCTF and CC-IIF integrated in a device

B.6.1 Configuration



NOTE: IRI-IIF, CC-IIF and CCTF are collocated in a SBC.

Figure B.6: IRI IRI-IIF, CCTF and CC-IIF integrated in a device

B.6.2 Scope

Line side Multimedia / PSTN Simulation Services (residential and business).

B.6.3 Characteristics

- Line side protocol may not contain Calling Line ID. No signalling for transferred calls.
- No interception of transferred calls to PSTN.
- SBC must be installed for every subscriber to avoid detection by target.

Annex C:
Examples of CCCI

C.1 Dedicated CCCI using SNMPv3 MIBs

An example of dedicated CCCI interface using SNMP v3 is described in TS 101 909-20-2 [29] annex B.

The MIB is contained in archive ts_1019092002v010201p0.zip which accompanies the TS 101 909-20-2 [29] document.

C.2 In-band CCCI using H.248

An example of in-band CCCI using H.248 is described in TS 133 107 [8] annex D: Information flows for Lawful Interception invocation at the MGW using H.248.

Annex D:
Change Request history

Status of the present document Interception domain Architecture for IP networks		
Date	**Version**	**Remarks**
September 2006	1.1.1	First publication of the TS after approval by ETSI/TC LI#13 (6-8 September 2006, Stockholm). Version 1.1.1 prepared by Maurice Duault (Circo) (rapporteur v1.1.1).

History

Document history		
V1.1.1	October 2006	Publication