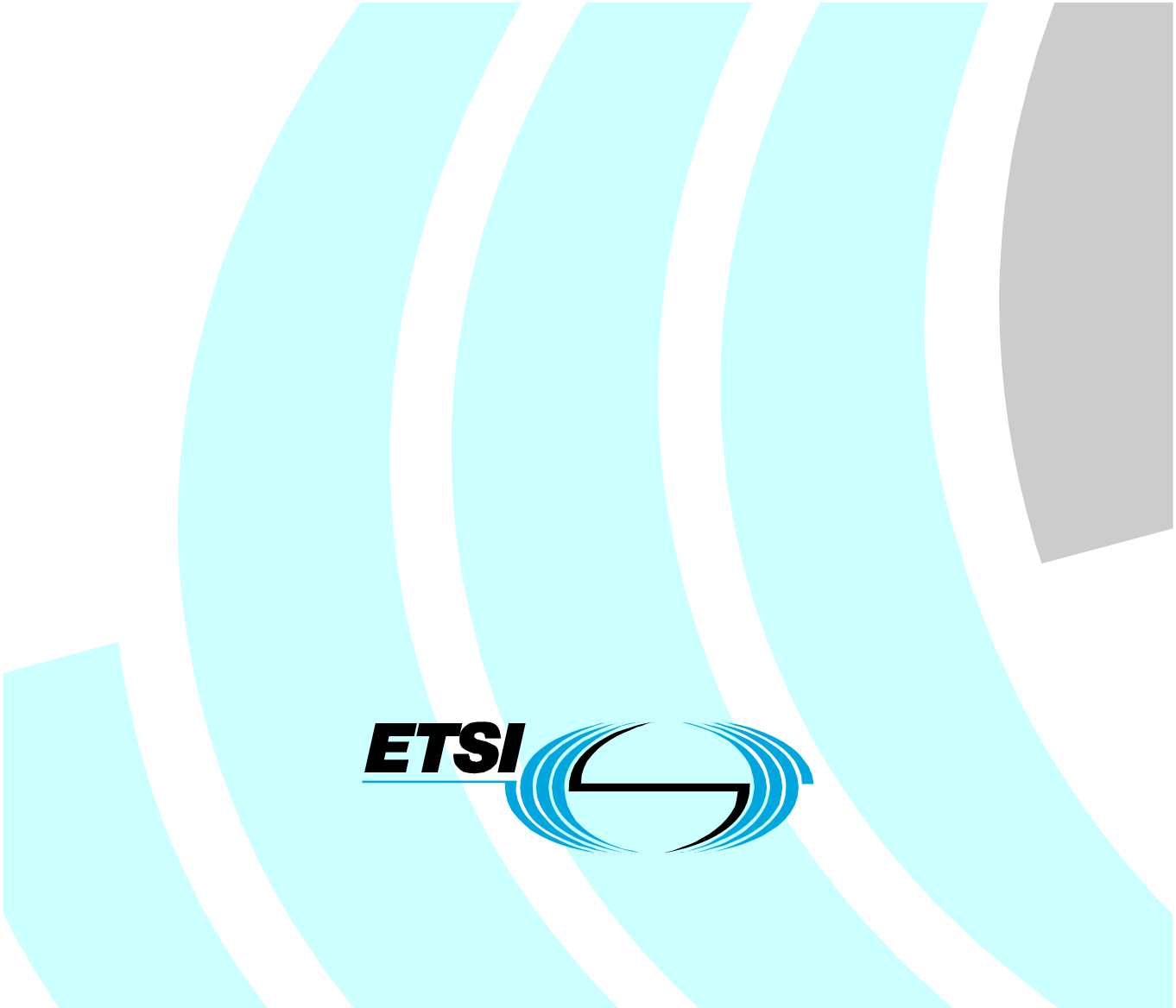
ETSI TS 187 005 V2.1.1 (2009-09)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 2 Lawful Interception; Stage 1 and Stage 2 definition



Reference
RTS/TISPAN-07031-NGN-R2

Keywords
IP, Lawful Interception, security, telephony

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 Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

The NGN is required to operate within a regulated environment. In Europe the privacy directive EC/2002/58 [i.1] applies and article 5 states:

1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2) Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3) Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/ 46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

SR 002 211 [i.2] identifies those aspects of standardization that are required to ensure compliance with the European Framework Directive. In some instances the right to privacy can be withheld as suggested in paragraph 2 of article 5 of the privacy directive [i.1] (see clause 5.1). Provisions for the lawful interception of traffic, and for retention of signalling data are allowed exceptions as defined in article 15(1) of the privacy directive:

1) Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in articles 5, 6, 8(1), (2), (3) and (4) and article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in articles 6(1) and (2) of the Treaty on European Union.

The obligations from the directive are placed on member states but may be met by the provision of specific capabilities in the NGN and for LI and DR these are as follows:

- An NGN operator should provide mechanisms to ensure the interception and handover of signalling of specific NGN users if required to by a lawful authority.
- An NGN operator should provide mechanisms to ensure the interception and handover of the content of communication of specific NGN users if required to by a lawful authority.
- An NGN operator should provide mechanisms to ensure the retention and handover of signalling of specific NGN users if required to by a lawful authority.

1 Scope

The present document specifies the stage 2 model for Lawful Interception (LI) of TISPAN NGN services as specified by TR 180 001 [i.3] (for release 1 specific capabilities) and TR 180 002 [i.5] (for release 2 specific capabilities).

The requirement for provision of lawful interception for all Communication Service Providers (CSP) is described in TS 101 331 [3] and the present document gives the stage 1 and stage 2 definition for provision of an interception capability in TISPAN NGN R2.

The provisions in the present document apply only when the target of interception is an NGN user identified as specified in TS 184 002 [7], and when the network supplying services on behalf of the CSP is an NGN as specified by TISPAN in TR 180 001 [i.3] (for release 1 specific capabilities), TR 180 002 [i.5] (for release 2 specific capabilities) and ES 282 001 [1].

A guide to the application of the handover specifications is given in informative annexes.

NOTE: Handover aspects are not specified in the present document but are described in TS 133 108 [9], ES 201 671 [2] and TS 102 232-1 [4], TS 102 232-5 [5], and TS 102 232-6 [6].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[2] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic".

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

[4] ETSI TS 102 232-1: " Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[5] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

[6] ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".

[7] ETSI TS 184 002: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

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

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

[10] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[11] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[12] ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Subsystem; Functional architecture".

[13] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

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

[15] European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications.

[16] International User Requirement (IUR).

NOTE: The IUR was provided as an annex to [15].

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.2] ETSI SR 002 211 (V1.1.1): "List of standards and/or specifications for electronic communications networks, services and associated facilities and services; in accordance with article 17 of Directive 2002/21/EC".

[i.3] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

[i.4] ETSI TR 102 528: "Lawful Interception (LI); Interception domain Architecture for IP networks".

[i.5] ETSI TR 180 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Release 2 definition".

[i.6] ETSI TR 102 661: "Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ES 201 671 [2] and the following apply:

Content of Communication (CC): information exchanged between two or more users of a telecommunications service, excluding intercept related information

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

corresponding party: correspondent of the target

Handover Interface (HI): physical and logical interface across which the interception measures are requested from Communications Service Provider (CSP), and the results of interception are delivered from a CSP to a law enforcement monitoring facility

interception: action (based on the law), performed by a CSP, of making available certain information and providing that information to a law enforcement monitoring facility

interception interface: physical and logical locations within the CSP telecommunications facilities where access to the content of communication and intercept related information is provided

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

intercept related information: 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

internal network interface: network's internal interface between the Internal Intercepting Function (IIF) and a mediation device

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

mediation device: equipment, which realizes the mediation function

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

target: interception subject

target identity: technical identity (e.g. the interception's subject directory number), which uniquely identifies a target of interception

NOTE: One target may have one or several target identities.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADMF	ADMinistration Function
AF	Administration Function
AGCF	Access Gateway Control Function
A-MGF	Access Media Gateway Function
ASF	Application Server Function
ASN.1	Abstract Syntax Notation 1

C-BGF	Core Border Gateway Function
CC	Content of Communication
CCCI	Content of Communication Control Interface
CCTF	Content of Communication Trigger Function
CCTI	Content of Communication Trigger Interface
CID	Communication Identifier
CIN	Communication Identity Number
CR	Change Request
CSP	Communications Service Provider
DF	Delivery Function
DR	Data Retention
FE	Functional Entity
GPRS	General Packet Radio Service
GSN	GPRS Support Node
HI	Handover Interface
HI1	Handover Interface Port 1 (for Administrative Information)
HI2	Handover Interface Port 2 (for Intercept Related Information)
HI3	Handover Interface Port 3 (for Content of Communication)
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
ID	IDentity
IIF	Internal Interception Function
IMS	IP Multimedia core network Subsystem
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
IUR	International User Requirement
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIAF	Lawful Interception Administration Function
LIID	Lawful Interception IDentifier
MF	Mediation Function
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NGN	Next Generation Network
NGN-R2	NGN Release 2
NID	Network IDentifier
P-CSCF	Proxy Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
PLMN	Public Land Mobile Network
PoI	Point of Interception
PSTN	Public Switched Telephone Network
RTCP	Real-time Transport Control Protocol
RTP	Real Time Protocol
S-CSCF	Serving Call Session Control Function
SDL	Specification and Description Language
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPDF	Service based Policy Decision Function
TDM	Time Division Multiplexing
T-MGF	Trunking Media Gateway Function
UPSF	User Profile Server Function
URL	Uniform Resource Locator

4 Interception in the NGN

4.0 Structure of analysis

The analysis presented in the present document is based on the recommendations for stage 2 of the method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN defined in ITU-T Recommendation I.130 [13]. The steps in expanding a stage 2 specification are listed below:

- Step 2.1: Derivation of a functional model from requirements stated in stage 1.
- Step 2.2: Information flow diagrams.
- Step 2.3: SDL diagrams for functional entities.
- Step 2.4: Functional entity actions.
- Step 2.5: Does not apply (see note).

NOTE: Step 2.5 in ITU-T Recommendation I.130 [13] addresses the ISDN environment. The NGN specifications do not describe physical locations, but NGN Functional Entities (NGN-FEs). The present document gives examples of the allocation of Lawful Interception Functional Entities (LI-FEs) to NGN-FEs.

The primary points of the stage 1 requirements are stated in clause 4.0.1 as a starting point for the further development of stage 2.

The structure for LI within the NGN should be mapped to the structure for handover of telecommunications defined in ES 201 158 [14] and provisioned by each of ES 201 671 [2], TS 133 108 [9] and TS 102 232-1 [4].

4.0.1 Review of stage 1 requirements

The stage 1 analysis approach is defined in ITU-T Recommendation I.130 [13] and consists of the following steps:

- Step 1.1: Service prose definition and description.
- Step 1.2: Static description of the service using attributes.
- Step 1.3: Dynamic description of the service using graphic means.

For the purposes of the present document only step 1.1 is summarized.

4.0.1.1 Provision/withdrawal

The LI service shall always be provided.

4.0.1.2 Activation/deactivation

The LI service shall be activated upon issue of a valid interception warrant from an LEA. The LI service shall be deactivated when the interception warrant expires or as defined by the LEA.

4.0.1.3 Invocation and operation

The LI service shall be invoked on any communication from or to the target visible to the network.

4.0.1.4 Interrogation

Interrogation shall be possible only from an authorized user. Where audit records are maintained for the service (required by the IUR [16]) access shall be possible only from an authorized user.

An authorized user for the purposes of interrogation is one who is allowed by both LEA and the CSP to administer the LI interface.

4.0.1.5 Interaction with other services

There shall be no interaction.

NOTE: This means that the invocation of LI is not intended to alter the operation of any service and any resulting modification implies non compliance to the requirements of the present document.

4.1 LI architecture model

The architecture for lawful interception consists of a Point of Interception (PoI) for each of the signalling plane and the transport plane, collocated with an NGN Functional Entity (NGN FE) (the specific NGN FE varies with the service being intercepted), that delivers intercepted material to a Mediation Function (MF). The MF acts to mediate between the nationally specified handover interface and the internal interception interface of the NGN as specified in the present document.

The target is a specialist NGN user that receives service from the NGN.

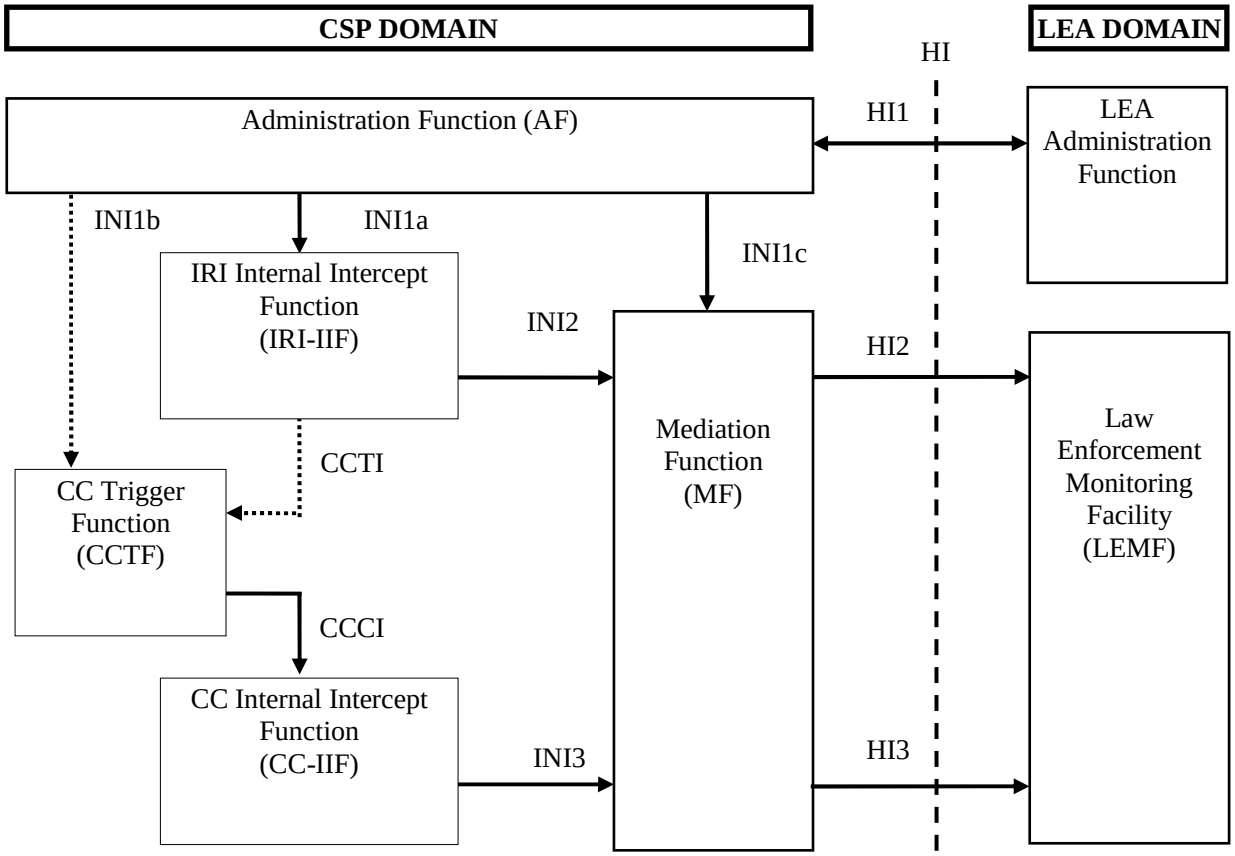
NOTE 1: A service offered to the NGN user may invoke many NGN-FEs.

NOTE 2: There are a number of terms used across ETSI to refer to the various functions outlined in the first paragraph of this clause (4.1). The MF is also known as a Delivery Function (DF) in 3GPP documents, the Internal Network Interception interfaces are also referred to in 3GPP as X interfaces.

The LI capability in the NGN shall always be available and shall be invoked on receipt of instruction from the Law Enforcement Agency or its authorizing agency. The functions of the LI capability shall only be visible to, and their operation shall only be invoked by, authorized parties within the NGN and shall not alter or be impacted by the operation of any other functional entity in the NGN.

4.2 LI reference model

The present document adopts the generic reference model for the interception domain from TR 102 528 [i.4], its internal intercept functions, IRI-IIF, CCTF, and CC-IIF, and the internal interfaces INI1, INI2, INI3, CCTI and CCCI as shown in figure 1.



NOTE: Interfaces INI1, INI1a, INI1b, INI1c, CCTI and CCCI, and functional entity CCTF are not fully defined in the present document but are shown in the figure for completeness.

Figure 1: Reference Model for Lawful Interception from TR 102 528 [i.4]

The reference model depicts the following functions and interfaces:

- Intercept Related Information Internal Intercept Function (IRI-IIF) generates signalling intercept material.
- Content of Communication Internal Intercept Function (CC-IIF) generates content intercept material.
- Content of Communication 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).
- Internal interface INI2 carries Intercept Related Information (IRI) from the IRI-IIF to the MF.
- Internal interface INI3 carries Content of Communication (CC) information from the CC-IIF to the MF.
- Content of Communication Trigger Interface (CCTI) carries trigger information from the IRI-IIF to the CCTF.
- Content of Communication Control Interface (CCCI) carries controls information from the CCTF to the CC-IIF.

The reference model introduces the CCTF FE that may be used to in a number of configurations to allow for the provisioning of CC-IIF in an IP network. The location of the CCTF is not defined in the present document but considered configuration options are as follows:

- CCTF co-located with the LIAF: INI1b is internal to the AF and CCTF.
- CCTF co-located with the IRI-IIF: CCTI is internal to the IRI-IIF and CCTF.
- CCTF co-located with the IRI-IIF and CC-IIF: CCTI and CCCI are internal to the IRI-IIF, CCTF and CC-IIF.

- CCTF co-located with the MF: CCTI is merged with INI2.
- A stand alone CCTF: Both CCTI and CCCI are external interfaces.

A complete explanation of the functions and interface is found in clause 4 of TR 102 528 [i.4].

4.3 Result of interception

The CSP at the point of interception shall, in relation to each target service:

a) provide the content of communication;

b) remove any service coding or encryption which has been applied to the content of communication and the intercept related information at the instigation of the network operator/service provider;

NOTE 1: If coding/encryption cannot be removed through means which are available to the CSP for the given communication the content is provided as received.

c) provide the LEA with any other decryption keys whose uses include encryption of the content of communication, where such keys are available;

d) intercept related information shall be provided:

1) when communication is attempted;

2) when communication is established;

3) when no successful communication is established;

4) on change of status (e.g. in the access network);

5) on change of service or service parameter;

6) on change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on); and

7) when a successful communication is terminated;

NOTE 2: In the present document, service should be taken to include supplementary services.

e) intercept related information shall contain:

1) the identities that have attempted telecommunications with the target identity, successful or not;

2) the identities which the target has attempted telecommunications with, successful or not;

3) identities used by or associated with the target identity;

4) details of services used and their associated parameters;

5) information relating to status;

6) time stamps;

f) the conditions mentioned above also apply to multi-party or multi-way telecommunication if and as long as the target identity participates.

NOTE 3: Where the user has initiated and applied end to end encryption, the content is provided as received.

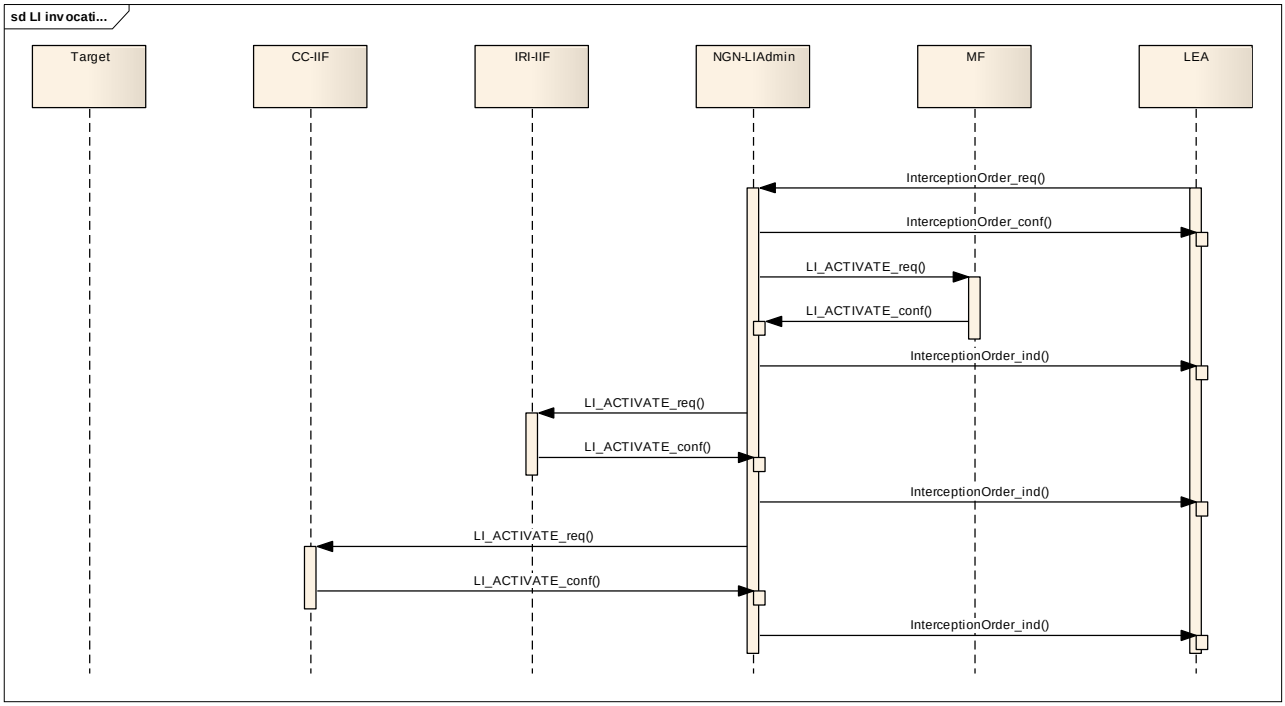
5A Stage 2 description of NGN LI

5A.1 Information flow sequences

5A.1.1 LEA control interactions and information flows

NOTE: The information flows described in this clause do not infer an implementation method. The related external interface (HI1 from ES 201 671 [2]) may be manual.

Figure 5A.1 shows the stimuli from the LEA and the responses from the NGN that are translated by the mediation function.



NOTE: The brackets indicated in each information flow indicate that parameters are contained in the message but are not expanded in the figure.

Figure 5A.1: External stimuli and information flow sequences for NGN LI

The LI_ACTIVATE_req information flow shall contain sufficient data to allow the NGN to validate the request and to make the required target activity data available to the MF. The returned information flow (LI_ACTIVATE_conf) shall contain a unique identifier for the interception applied within the network. Any subsequent information flows (LI_MODIFY_req/conf) shall refer to this unique identifier.

5A.1.1.1 LI_ACTIVATE_req

This information flow is sent from the Administrative function internally to the NGN functional entities (the PoIs) to request redirection of traffic (in T_TRAFFIC_ind and CT_TRAFFIC_ind information flows) and signalling (in TARGET_ACTIVITY_MONITOR_ind and TARGET_COMMS_MONITOR_ind information flows).

Table 5A.1: LI Activate request information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Invocation identifier	M	Used to allow the CSP to correlate the invocation of PoIs to the requested interception order.
Target identity	M	Uniquely identifies the target that the interception shall be invoked against. It shall be an identifier defined in TS 184 002 [7] and used in the serving NGN.
Services to be intercepted (see note)	M	A list of the specific services that are to be intercepted. By default all services will be intercepted.
NOTE: The NGN, in particular the IMS platform, does not offer specific services.		

Protocol constraints:

Response to = None.

Response expected = LI_ACTIVATE_conf.

5A.1.1.2 LI_ACTIVATE_conf

If the request is successful the Result element of the information flow shall be set to TRUE and the TLIInstanceid set. The TLIInstanceid shall thereafter be used as the NGN specific pointer to the interception. If the request is unsuccessful the Result element shall be set to FALSE and the TLIInstanceid shall not be returned. (I.e. the presence of the TLIInstanceid is conditional on the value of Result.)

Table 5A.2: LI Activate confirmation information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Invocation identifier	M	
Result	M	Indicates the success or failure of the activation.
Correlation and interception instance identifier	C	Provided if the interception invocation result is positive and allows the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.

Protocol constraints:

Response to = LI_ACTIVATE_req.

Response expected = None.

5A.1.1.3 LI_MODIFY_req

An interception may be modified many times in its life. Each modification is addressed using the reference identity (TLIInstanceid) and a sequential ModificationNumber. The modification may be one of a selection as shown in table 5A.3.

Table 5A.3: LI modify request information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Modification number	M	Sequential count of the modification at the particular PoI.
Modification type	M	Identifies the form of the modification, may be one of halt, reset, modification of expiry time and others.

Protocol constraints:

Response to = None.

Response expected = LI_MODIFY_conf.

5A.1.1.4 LI_MODIFY_conf

If the modification request is successful then Result shall be set to TRUE, else it shall be set to FALSE.

Table 5A.4: LI modify confirmation information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Modification number	M	Sequential count of the modification at the particular PoI.
Result	M	Indicates the success or failure of the modification.

Protocol constraints:

Response to = LI_MODIFY_req.

Response expected = None.

5A.1.1.5 LI_STATUS_ind

This information flow from the NGN PoIs to the administrative function reports changes in the status of the NGN PoI. This may indicate for example problems in the ability to provide interception.

Table 5A.5: LI status indication information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
System status	M	Identifies the current status of the invocation at the PoI.

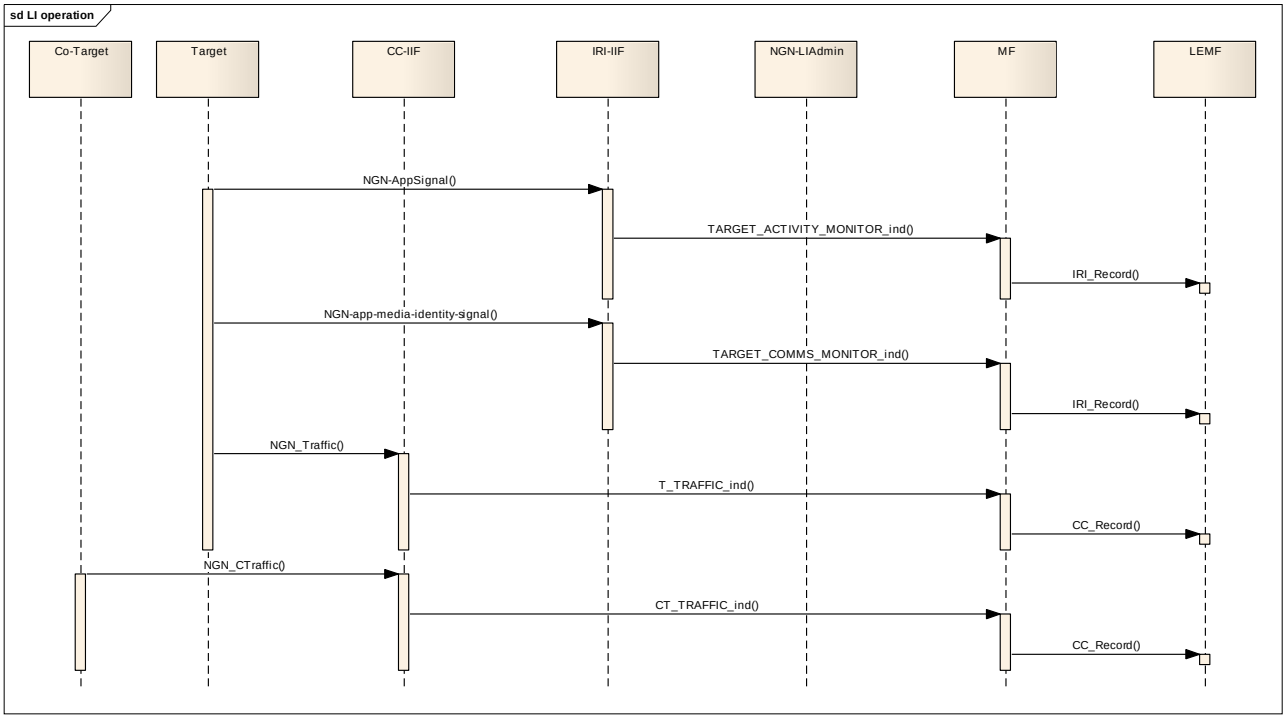
Protocol constraints:

Response to = None.

Response expected = None.

5A.1.2 Target signalling and traffic interactions and information flows

Figure 5A.2 shows an example of the transmission of traffic from the target connected to NGN. The principle captured applies to all target activity such as registration.



NOTE: The brackets indicated in each information flow indicate that parameters are contained in the message but are not expanded in the figure.

Figure 5A.2: Principle of interception information flow

The information flows that indicate the activity of the target (signalling or traffic) are described below.

5A.1.2.1 TARGET_ACTIVITY_MONITOR_ind

This information flow shall provide in summary form the activity of the target on the NGN to the MF. It shall have a header section indicating who, when and where, with a body section indicating the what of the target activity.

Table 5A.6: Target activity monitor indication information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Target location	M	The geographic or logical location of the target at the time of the activity being intercepted.
Target NGN public ID	M	
Target action	M	The actual activity of the target, including the content of any signalling information from the target.
Corresponding party information	C	If the activity of the target is sent to a known correspondent this information element contains the information about the correspondent known to the CSP.
Corresponding party NGN public ID	C	
NOTE: "Corresponding party information" and "Corresponding party NGN public ID" may be present multiple times.		

Protocol constraints:

Response to = None.

Response expected = None.

5A.1.2.1.1 Relation to Handover

The TARGET_ACTIVITY_MONITOR_ind information flow shall be delivered in the payload of an IRI-Record type across HI2.

5A.1.2.2 T_TRAFFIC_ind

This information flow carries an NGN traffic packet of the target to the MF.

Table 5A.7: Target traffic indication information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Traffic packet	M	A bit exact copy of the traffic sent by the target captured at the PoI.

Protocol constraints:

Response to = None.

Response expected = None.

5A.1.2.2.1 Relation to Handover

The T_TRAFFIC_ind information flow shall be delivered in the payload of a CC-Record type across HI3.

5A.1.2.3 CP_TRAFFIC_ind

This information flow carries a traffic packet of the corresponding party to the MF.

Table 5A.8: Corresponding party traffic indication information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Traffic packet	M	A bit exact copy of the traffic sent by the target's correspondent captured at the PoI.

Protocol constraints:

Response to = None.

Response expected = None.

5A.1.2.3.1 Relation to Handover

The CP_TRAFFIC_ind information flow shall be delivered in the payload of a CC-Record type across HI3.

5A.1.2.4 TARGET_COMMS_MONITOR_ind

This information flow is used to indicate the location and format of the communication content media flow. In the NGN this may be carried in the SIP-INVITE as part of the session description and confirmed in the 200 OK response. It identifies the logical location (by RTP/RTCP data) of the T_TRAFFIC_ind and CT_TRAFFIC_ind information flows. This information flow is sent on receipt of the SIP-INVITE containing the session description for the initiating party and on receipt of the 200 OK response for the receiving party and on any change of the media requested by either party.

NOTE: A single instance of interception may result in multiple TARGET COMMS MONITOR ind information flows being sent.

Table 5A.9: Target comms monitor indication information flow content

Information element	M/O/C	Description
Timestamp	M	Indicates the time at which the message was sent.
Correlation and interception instance identifier	M	Identifier to allow the LEA and CSP to uniquely identify the correlation of the point of interception and the invocation identifier.
Target CC details	M	Information as contained in the SDP (for SIP signalling) that defines the media stream component (e.g. RTP/RTCP). In addition this shall contain the identity of the CC-IIF for the target communication.
Corresponding party CC details	C	Information as contained in the SDP (for SIP signalling) that defines the media stream component (e.g. RTP/RTCP). In addition this shall contain the identity of the CC-IIF for the corresponding party communication. This is mandatory when sending the information flow for 200 OK responses.

Protocol constraints:

Response to = None.

Response expected = None.

5A.1.2.4.1 Relation to Handover

The TARGET_COMMS_MONITOR_ind information flow shall be delivered in the payload of an IRI-Record type across HI2.

5A.2 Data provision and encoding

5A.2.1 Identification of result of interception

The result of interception provided by the NGN shall be given a unique tag that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference. This tag shall be first returned in the LI_ACTIVATE_conf information flow and forms part of the subsequent header data in TARGET_ACTIVITY_MONITOR_ind and TARGET_COMMS_MONITOR_ind information flows, as well as being used in the LI_MODIFY information flows.

5A.2.2 Provision of identities/addresses

All identities used by the target or corresponding party in communication, successful or unsuccessful, shall be identified in the TARGET_ACTIVITY_MONITOR_ind information flow.

5A.2.3 Provision of details of services used and their associated parameters

The activity of the target shall be given in the TARGET_ACTIVITY_MONITOR_ind. The information element shall indicate the following:

- Relationship to a call or session:
  - Beginning of a call or session (e.g. Call Setup message).
  - Ending of a call or session (e.g. Call cleardown message).
  - Call or session related signalling (e.g. Call proceeding message).
  - Not related to call or session (e.g. Registration request).
- Direction of the information flow:
  - To the Target.
  - From the Target.
- Scope or topology of the call or session.
- Point to Point call or session (e.g. individual voice call).
- Point to MultiPoint call or session (e.g. multicast data transfer).
- Broadcast call or session (e.g. IPTV broadcast).

5A.2.4 Provision of those signals emitted by the target invoking additional or modified services

Signals that modify or invoke non-call related services shall be given in the same form as for services described in clause 5A.2.3 in the TARGET_ACTIVITY_MONITOR_ind data structure.

5A.2.5 Provision of time-stamps for identifying the beginning, end and duration of the connection

The header of TARGET_ACTIVITY_MONITOR_ind information flow shall contain a timestamp information element. This element shall be of a type recognized in the country or legislative area in which the interception is performed and which is available in the CSP domain.

5A.2.6 Provision of actual source, destination and intermediate public IDs in case of communication diversion

The following requirements apply to networks that support the communication diversion services.

The NGN public ID (as defined in TS 184 002 [7]) used by the NGN in communicating with the target shall be provided in the Target NGN public ID element, and if communication diversion is applicable, the NGN public ID(s) of the correspondent(s) of the target shall be provided in the Corresponding party NGN public ID element(s), if supported by the implementation of the protocol and the security and/or privacy and/or policy requirements of the involved NGN(s), of the TARGET_ACTIVITY_MONITOR_ind information flow.

The following scenarios are possible:

1) Communication Diversion by target.

EXAMPLE 1: If the NGN communicates with the target (Party-(x)) and the target has invoked communication diversion to Party-(x+1) then the interception record shall contain the public IDs of both Party-(x) and Party-(x+1). Similarly if Party-(x+1) has also invoked communication diversion to Party-(x+2) the interception record shall contain the public IDs of Party-(x), Party-(x+1) and Party-(x+2), if supported by the implementation of the protocols and the security and/or privacy and/or policy requirements of the involved NGN(s), and so on.

2) Forwarded communication terminated at target.

EXAMPLE 2: If the NGN communicates with the target (Party-(x)) and the communication has been previously diverted before reaching the target, then the interception record shall contain the public IDs of both Party-(x) and Party-(x-1), if supported by the implementation of the protocols and the security and/or privacy and/or policy requirements of the involved NGN(s). Similarly if the communication has been diverted before reaching Party-(x-1), then the interception record shall contain the public IDs of Party-(x), Party-(x-1) and Party-(x-2), if supported by the implementation of the protocols and the security and/or privacy and/or policy requirements of the involved NGN(s), and so on.

3) Communication from target forwarded.

EXAMPLE 3: If the NGN communicates with the target (Party-(x)) and the Party-(x+1) is diverting the communication, then the interception record shall contain the public IDs of both Party-(x) and Party-(x+1), if supported by the implementation of the protocols and the security and/or privacy and/or policy requirements of the involved NGN(s). Similarly if Party-(x+1) has also invoked communication transfer to Party-(x+2), the interception record shall contain the public IDs of Party-(x), Party-(x+1) and Party-(x+2), if supported by the implementation of the protocols and the security and/or privacy and/or policy requirements of the involved NGN(s), and so on.

5A.2.7 Provision of location information

Location information relating to the target should be provided in the header of every TARGET_ACTIVITY_MONITOR_ind information flow.

5 Interception in NGN subsystems

5.0 Allocation of LI-FEs to NGN-FEs

The Point of Interception shall be at premises of the CSP, i.e. IRI-IIF and CC-IIF shall reside in equipment under full control (physical access, etc.) of the CSP or CSPs (see note). The point of interception (as defined in clause 4) with respect to IRI, the IRI-IIF, should be implemented in the NGN-FE that hosts the service state machine. The point of interception (as defined in clause 4) with respect to CC, the CC-IIF, should be implemented in a mediastream entity.

NOTE: There may be separate CSPs for each of IRI-IIF and CC-IIF. This release does not specify the correlation of IRI-IIF and CC-IIF at the CCTF.

The following example scenarios (not exhaustive) are considered for deployment of LI in the NGN. All these examples assume that the target is subscribed to services offered by the CSP performing the interception. In particular, for the transit cases, the target has an account in a domain operated by the CSP performing the interception:

- Scenario 1: Interception at edge of NGN.
- Scenario 2: Interception at edge of NGN (alternative).
- Scenario 3: Interception in core of NGN.
- Scenario 4: Transit communication, IP case.
- Scenario 5: Transit communication, TDM case.

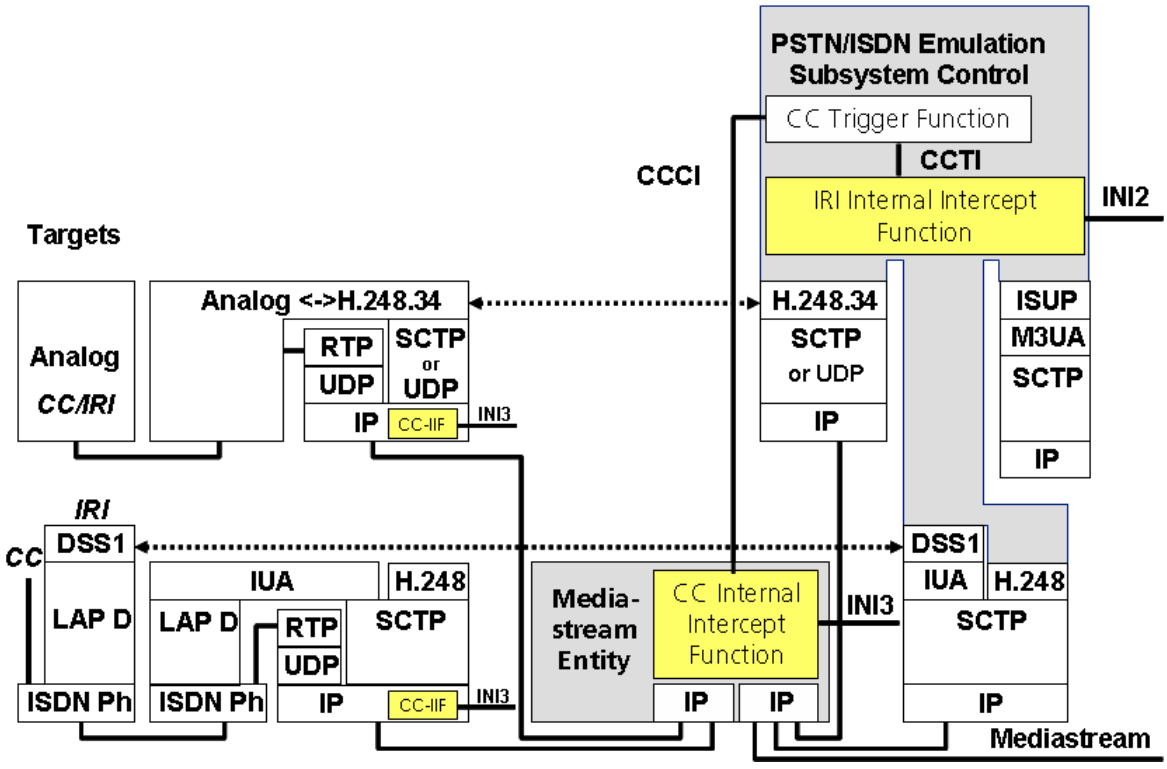
NOTE: In practical implementations several scenarios may need to be active at the same time. The combination of PoIs in multiple scenarios is not described in the present document.

Table 5.1: Examples of allocation of LI-FEs to NGN-FEs

LI-FE	Scenario 1	Scenario 2 (see note 3)	Scenario 3	Scenario 4	Scenario 5
LI-FE1, IRI-IIF	P-CSCF, AGCF (see note 2)	AGCF	S-CSCF	IBCF	MGCF
LI-FE2, CC-IIF	C-BGF	A-MGF	MRFP	I-BGF	T-MGF
LI-FE3, CCTF	SPDF	--	UPSF, ASF, MRFC	SPDF	--
LI-FE4, AF	ADMF	ADMF	ADMF	ADMF	ADMF
NOTE 1: The allocations of the LI-FEs to the NGN-FEs given in this table are examples and their choice is subject to implementation. LI-FEs could also be allocated to other NGN-FEs, and not all possible options need to be implemented. These scenarios are not exhaustive. NOTE 2: The use of the AGCF as a PoI for IRI is only valid for PES applications. NOTE 3: This scenario is PES specific.					

5.1 Architecture for interception of PES

The specific provision of the CC-IIF and IRI-IIF in the NGN for PES services where the NGN architecture conforms to ES 282 002 [10] is as shown in figure 2.



NOTE: Location of CC-IIF is subject to implementation and not all possible options need to be implemented.

Figure 2: Reference architecture for interception in the PES environment

5.2 Architecture for interception of IMS

The specific provision of the CC-IIF and IRI-IIF in the NGN for the IMS subsystem as described in ES 282 007 [11] and TS 182 012 [12] offering IMS services is as shown in figure 3.

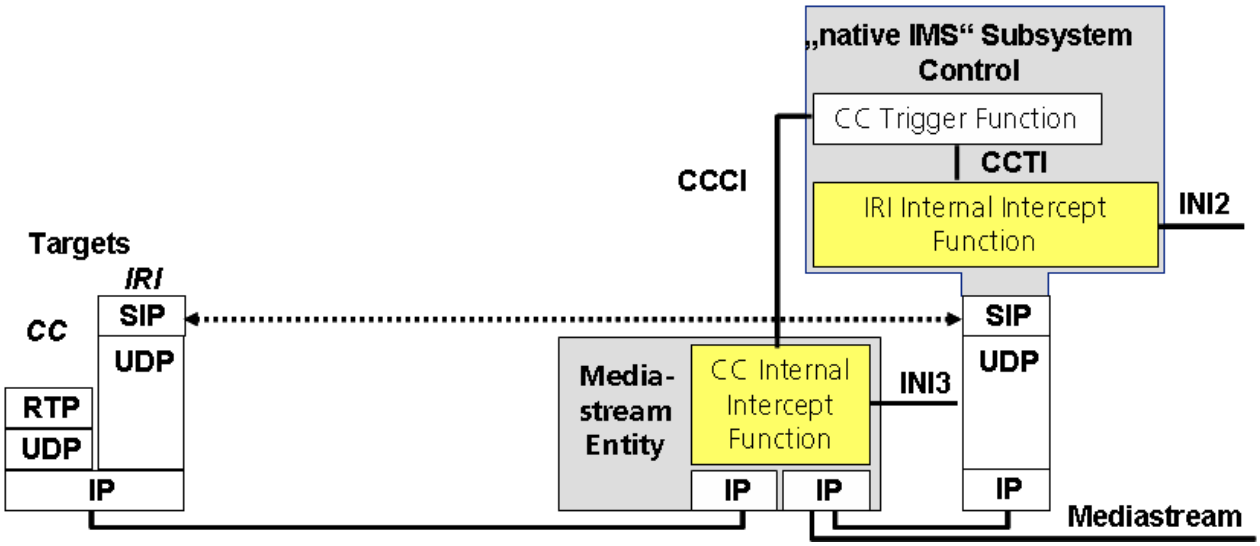


Figure 3: Reference architecture for interception in the IMS environment

5.3 Intercept Related Information (PoI IRI-IIF)

Communications to or from a targeted subscriber and communications initiated on behalf of a targeted subscriber are intercepted at the P-CSCF or S-CSCF as described in TS 133 107 [8].

NOTE 1: When IMS is providing a PES service the interception service identified above and defined in TS 133 107 [8] still applies. In addition, the AGCF may be used as an alternative point of interception.

NOTE 2: If the IMS is used for the support of transit communication and national LI requires their interception then the interception of communications in transit may take place at the IBCF or MGCF depending on the characteristics of the interconnected networks involved in the communication.

5.4 Content of Communication (PoI CC-IIF)

Interception of the content of communications takes place at transport processing functional entities identified in the TISPAN NGN architecture (ES 282 001 [1] and ES 282 002 [10]). Transport processing entities that may provide the CC-IIF are:

- An Access Media Gateway Function (A-MGF).
- A Core Border Gateway Function (C-BGF).
- An Interconnect Border Gateway Function (I-BGF).
- A Trunking Media Gateway Function (T-MGF).
- A Multimedia Resource Function Processor (MRFP).

NOTE 1: Interception may take place at an A-MGF, C-BGF or MRFP when the target of interception is a subscriber of the IMS or PES.

NOTE 2: If the IMS is used for the support of transit communication and national LI requires their interception then the interception of communications in transit may take place at the I-BGF or T-MGF depending on the characteristics of the interconnected networks involved in the communication.

NOTE 3: The use of MRFP as interception point only for those services already including it in the normal traffic path (e.g. call conferencing, messaging services, multimedia announcements) assures the security (especially confidentiality) requirements of LI as defined in TS 101 331 [3] and in TR 102 661 [i.6].

When the interception of communication contents takes place at a C-BGF or I-BGF, interactions between the IRI-IIF and the CC-IIF takes place through the SPDF or the MF. The SPDF or the MF plays the role of a CCTF as identified in clause 4.3.

When the interception of communication contents takes place at an A-MGF or T-MGF, the AGCF or MGCF plays the role of the IRI-IIF, and the CCTF (as identified in clause 4.3) is located in the AGCF, MGCF or MF.

When the interception of communication contents takes place at an MRFP, the associated MRFC and an Application Server Function collectively, or the MF, play the role of a CCTF. The ASF controls the MRFC via the S-CSCF. In order to ensure that the Application Server gets involved in the communications subject to interception, the Administration Function (ADMF) provisions the S-CSCF with the address of the Application Server or creates an appropriate Initial Filter Criteria in the targeted subscriber's profile in the UPSF.

6 Identification of target of interception

6.1 ISDN/PSTN services

In the context of PSTN/ISDN emulation and services, the target shall be identified in the service domain by a globally unique E.164 identity.

NOTE: The PES offers seamless ISDN/PSTN service to existing core network customers who will remain identified by their E.164 identity that may be mapped to a system unique SIP-identity.

6.2 IMS services

IMS service users shall be identified by either a SIP-url or a tel-url [7].

7 Security considerations

The security guidelines for assurance of the CSP environment in intercepting target signalling and traffic and its handover given in TS 101 331 [3] should be followed.

Annex A (normative): Endorsement statement for TS 133 107

NOTE: Only the 3GPP Release 7 documents apply for mapping to NGN Release 2.

For the stage 2 definition of the interception of IMS and generic IP subsystem parts of TS 133 107 [8] apply normatively in the context of TISPAN NGN. This annex summarizes those parts of TS 133 107 [8] that apply in the context of TISPAN NGN LI.

NOTE: Where no specific endorsement statement is given the text in the endorsed document is considered to have only background relevance and not to form part of the normative specification for NGN-R2 interception.

Clause	Applicability in TISPAN NGN R2
1	
2	
3	
4	Figure 1d applies
5	
6	Does not apply
7	Does not apply
7A	See note 1
7A.1	Does not apply (refers only to GSNs)
7A.2	Applies in full
7A.3	Applies in full with extensions defined in the present document
7A.4	Applies in full
7A.5	Does not apply (service defined only for cellular network)
7A.6	Applies in full
8	
9	Does not apply
10	
Annex A	Does not apply
Annex B	Does not apply
Annex C	
Annex D	Does not apply
Annex G	Does not apply (informative annex showing history of CRs applied to the referred to document)
NOTE 1: Considered to have only background relevance and not to form part of the normative specification. NOTE 2: Annexes E and F do not exist in TS 133 107 [8].	

Annex B (informative): Endorsement statement for TS 133 108

NOTE 1: This annex is provided for information pending a full stage 3 mapping from TISPAN NGN to TS 133 108 [9].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 133 108 [9] and how they should apply in TISPAN NGN.

This annex summarizes those parts of TS 133 108 [9] that apply in the context of TISPAN NGN LI.

NOTE 3: Where no specific endorsement statement is given the text in the endorsed document is considered to have only background relevance and not to form part of the specification for NGN-R2 interception.

Clause	Applicability in TISPAN NGN R2
1	
2	
3	
4	
4.1	
4.2	
4.3	
4.4	
4.4.1	Applies in full
4.4.2	
4.5	Applies in full
4.5.1	Applies in full
4.5.2	Applies in full
4.5.3	Applies in full
5	Does not apply
6	
7	
7.1	
7.1.1	
7.1.2	
7.1.3	Correlation to the relevant CC is necessary
7.2	
7.3	
7.4	
7.5	Yes / for correlation ASN.1 parameter correlation had to be used
7.5.1	Yes / for correlation ASN.1 parameter correlation had to be used
7.6	
8	
Annex A	
Annex B	Requires detail study of ASN.1 to confirm applicability. May not apply
B.1	May not apply
B.2	May not apply
B.3	May not apply
B.3a	May not apply
B.4	May not apply
B.5	May not apply
B.6	May not apply
Annex C	
Annex D	
Annex E	
Annex F	
Annex G	
Annex H	
Annex J	Does not apply

Clause	Applicability in TISPAN NGN R2
Annex K	Does not apply (informative annex showing history of CRs applied to the document)
NOTE:	Whereas the scope of the present document is interception in the NGN domain the scope of TS 133 108 [9] is handover for the PLMN, the data emanating from the PLMN is described and covers a range of capabilities more specific than those of the NGN (although the NGN is a superset of the capabilities that form the PLMN).

Annex C (informative): Endorsement statement for TS 102 232 and its subparts

C.1 Endorsement statement for TS 102 232-1

NOTE 1: This annex is provided for information pending a full stage 3 mapping from TISPAN NGN to TS 102 232-1 [4].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 102 232-1 [4] and how they should apply in TISPAN NGN.

C.2 Endorsement statement for TS 102 232-5

NOTE 1: This annex is provided for information pending a full stage 3 mapping from TISPAN NGN to TS 102 232-5 [5].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 102 232-5 [5] and how they should apply in TISPAN NGN.

C.3 Endorsement statement for TS 102 232-6

NOTE 1: This annex is provided for information pending a full stage 3 mapping from TISPAN NGN to TS 102 232-6 [6].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 102 232-6 [6] and how they should apply in TISPAN NGN.

Annex D (informative): Endorsement statement for ES 201 671

NOTE 1: This annex is provided for information pending a full stage 3 mapping from TISPAN NGN to ES 201 671 [2].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in ES 201 671 [2] and how they should apply in TISPAN NGN.

Clause	Title	Applicability in TISPAN NGN R2
1	Scope	
2	References	
3	Definitions and abbreviations	
3.1	Definitions	
3.2	Abbreviations	
4	General requirements	
4.1	Basic principles for the Handover Interface	Applies in full
4.2	Legal requirements	Applies in full
4.3	Functional requirements	Applies in full
5	Overview of Handover Interface	Applies in full
5.1	Handover Interface port 1 (HI1)	No: national implementation
5.1.1	Manual interface	No: national implementation
5.1.2	Electronic interface	No: national implementation
5.2	Handover Interface port 2 (HI2)	Applies in full
5.3	Handover Interface port 3 (HI3)	Applies in full
6	Specific identifiers for LI	Applies in full
6.1	Lawful Interception Identifier (LIID)	Applies in full
6.2	Communication Identifier (CID)	Applies in full
6.2.1	Network Identifier (NID)	Applies in full
6.2.2	Communication Identity Number (CIN) - optional	Applies in full
7	HI1: Interface port for administrative information	
7.1	Information for the activation of lawful interception	Applies in full
7.2	LI notifications towards the LEMF	No: national implementation
8	HI2: Interface port for Intercept Related Information	
8.1	Data transmission protocols	
8.1.1	Application for IRI (HI2 information)	
8.2	Types of IRI records	
9	HI3: Interface port for Content of Communication	
10	Performance and quality	
10.1	Timing	
10.2	Quality	
11	Security aspects	Advisable
11.1	Security properties	Advisable
11.2	Security mechanisms	Advisable
12	Quantitative aspects	national matter
Annex A (normative)	Circuit switched network handover	Applies in full
Annex B (normative)	Packet switched network handover	Applies in full
Annex C (normative)	HI2 Delivery mechanisms and procedures	
C.1	ROSE	
C.2	FTP	
Annex D (normative)	Structure of data at the Handover Interface (ASN.1)	
Annex E (informative)	Use of subaddress and calling party number to carry correlation information	National matter

Clause	Title	Applicability in TISPAN NGN R2
Annex F (informative)	GPRS HI3 Interface	
Annex G (informative)	LEMF requirements - handling of unrecognized fields and parameters	
Annex H (informative)	IP Multimedia Subsystem (IMS) handover	
Annex I (informative)	Latest ASN.1 module versions	No
Annex J (informative)	Bibliography	
Annex K (informative)	Change Request history	No

Annex E (informative): ISDN/PSTN LI reference configurations

The figures contained in this annex identify a number of reference configurations for lawful interception in TISPAN NGN networks. Interception configurations for communications to or from a targeted TISPAN NGN subscriber are shown in figures E.1, E.2 and E.3. Interceptions of communications in transit are shown in figures E.4 and E.5.

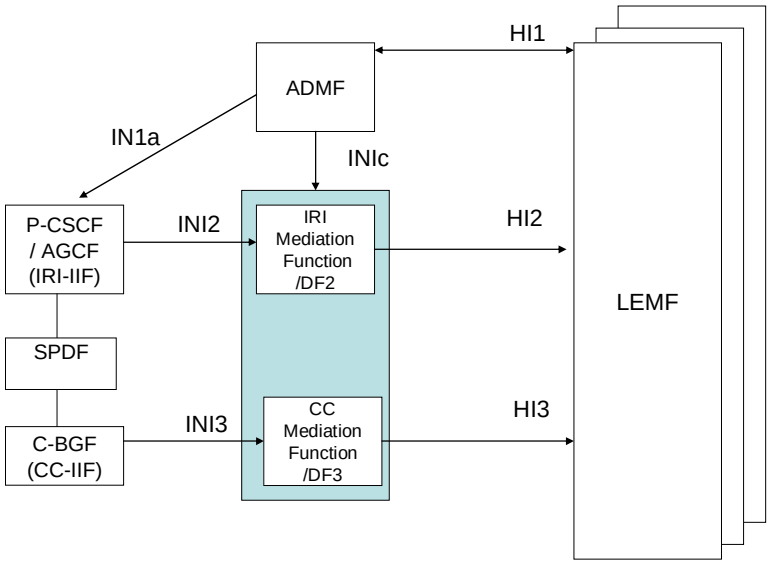


Figure E.1: Interception at the edge (case 1)

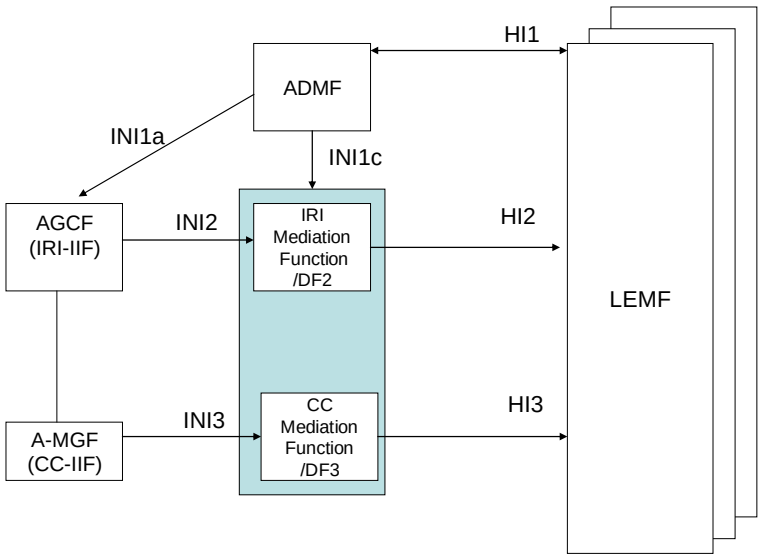


Figure E.2: Interception at the edge (case 2)

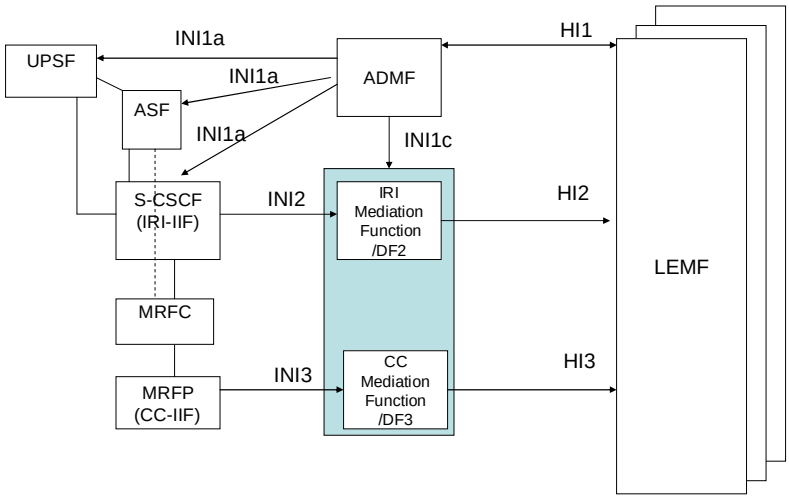


Figure E.3: Interception in the core

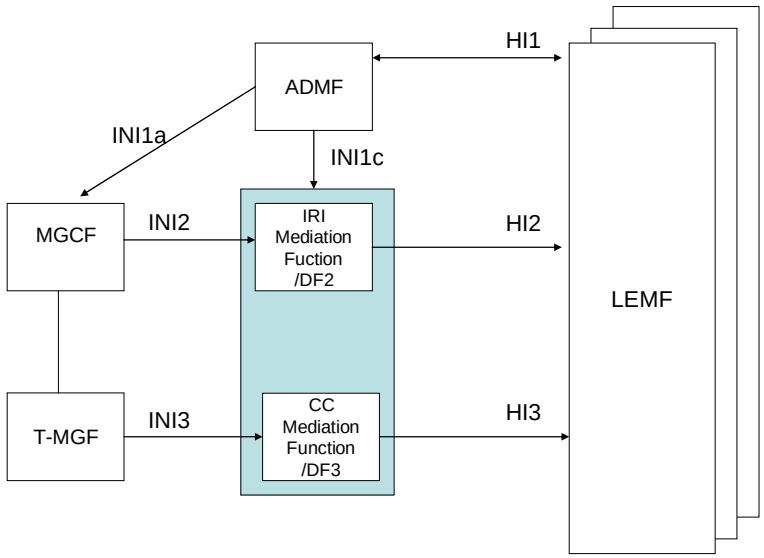


Figure E.4: Interception of communications in transit (TDM case)

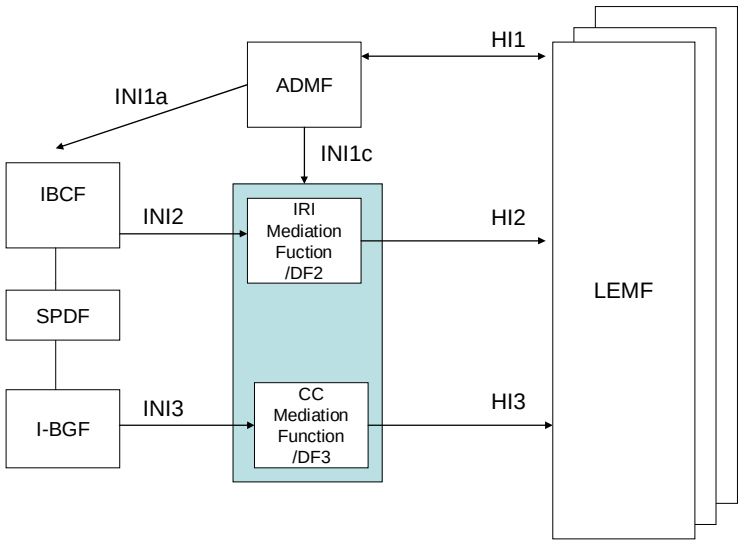


Figure E.5: Interception of communications in transit (IP case)

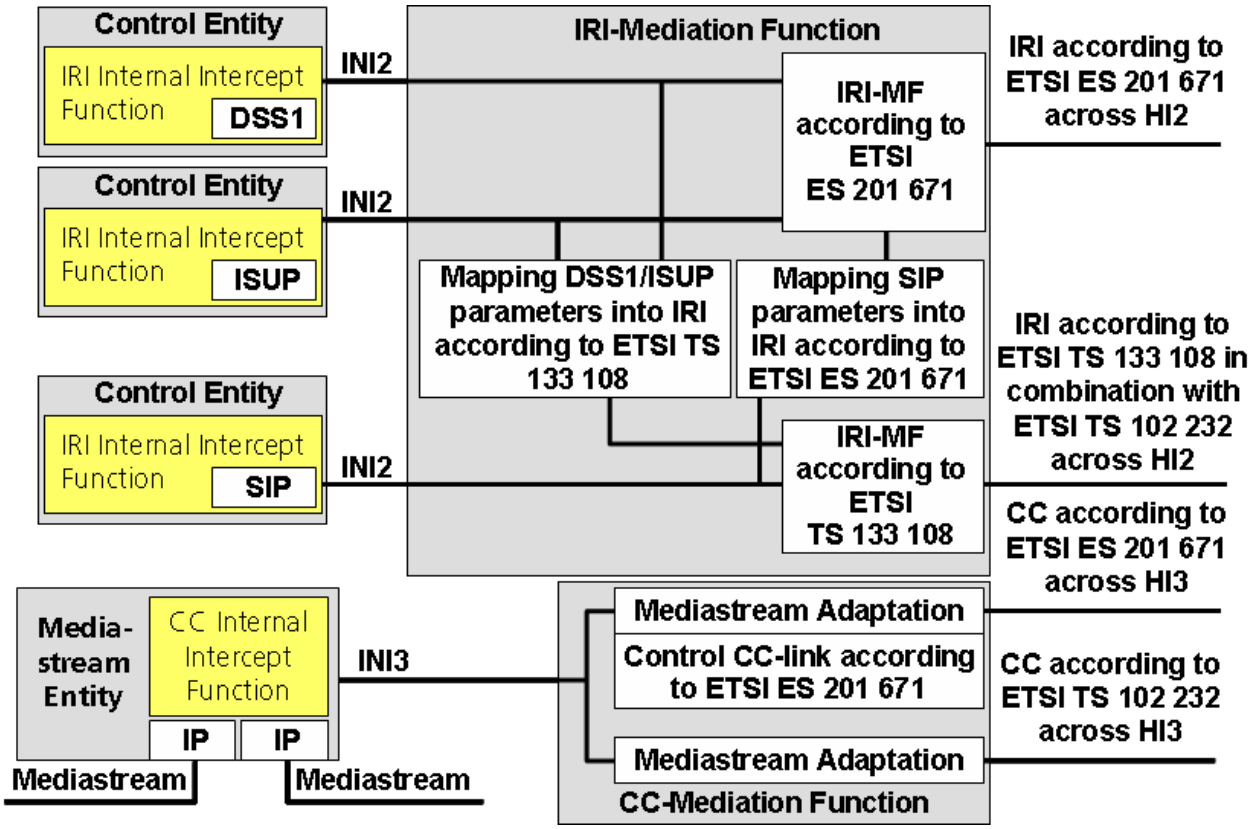
Annex F (informative): Selection of handover interface

Handover of intercepted material should be made by reference to one or more of the following specifications:

- ES 201 671 [2]: Handover Interface for the lawful interception of telecommunications traffic.
- TS 133 108 [9]: Handover interface for Lawful Interception.
- TS 102 232-1 [4]: Handover specification for IP delivery.

NOTE: National specifications may be used instead of any of the ETSI specifications cited above.

Figure F.1 illustrates configurations of mediation function to map the Handover Interface to the intercepted data that are subject to bilateral agreement between Network Provider and LEA.



NOTE 1: CS interception formats from the NGN may map to CS capabilities in TS 133 108 [9] but there may be a requirement for extensions to TS 133 108 [9] in some instances.
NOTE 2: IMS interception formats from the NGN may map to IMS capabilities in TS 133 108 [9] but there may be a requirement for extensions to TS 133 108 [9] in some instances.
NOTE 3: SIP interception formats from the NGN map to IMS capabilities in TS 133 108 [9] but there may be a requirement for extensions to TS 133 108 [9] in some instances.

Figure F.1: Reference Model for LI Mediation Function

Annex G (informative): Bibliography

G.1 ETSI Specifications

[A] ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface".

[B] ETSI EN 300 403-1 (V1.3.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

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

[D] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

[F] ETSI TS 101 671: "Handover Interface for the lawful interception of telecommunications traffic".

[G] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".

G.2 3GPP specifications

[H] 3GPP TS 29.002: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Application Part (MAP) specification".

[I] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing, and identification".

[J] 3GPP TS 23.107: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service QoS concepts and architecture".

[K] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[L] 3GPP TS 24.008: "3GPP Technical Specification Group Core Network; Mobile radio interface Layer 3 specification, Core network protocol; Stage 3".

[M] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[N] 3GPP TS 32.215: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain)".

[O] 3GPP TS 33.106: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".

[P] 3GPP TS 23.032: "3rd Generation Partnership Project; Technical Specification Group Core Network; Universal Geographical Area Description (GAD)".

[Q] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

G.3 ITU-T specifications

[R] ITU-T Recommendation Q.763: "Signalling System No. 7 - ISDN User Part formats and codes".

[S] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[T] ITU-T Recommendation X.680: "Abstract Syntax Notation One (ASN.1): Specification of Basic Notation".

[U] ITU-T Recommendation X.681: "Abstract Syntax Notation One (ASN.1): Information Object Specification".

[V] ITU-T Recommendation X.682: "Abstract Syntax Notation One (ASN.1): Constraint Specification".

[W] ITU-T Recommendation X.683: "Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 Specifications".

[X] ITU-T Recommendation X.690: "ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[Y] ITU-T Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".

[Z] ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

G.4 IETF specifications

[AA] IETF STD 0005 (RFC 0791): "Internet Protocol".

[AB] IETF STD 0007 (RFC 0793): "Transmission Control Protocol".

[AC] IETF STD 0009 (RFC 0959): "File Transfer Protocol (FTP)".

[AD] IETF RFC 1006: "ISO Transport Service on top of the TCP".

[AE] IETF RFC 2126: "ISO Transport Service on top of TCP (ITOT)".

[AF] IETF RFC 2806: "URLs for Telephone Calls".

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

G.5 ISO specifications

[AH] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

G.6 ANSI specifications

[AI] ANSI/J-STD-025-A: "Lawfully Authorized Electronic Surveillance".

Annex H (informative): Change history

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
23-9-08	18bTD019r1	1	-	C	Result of interception in clause 4.3	2.0.7	2.0.8
23-9-08	18bTD303r1	2	-	D	Removal of annex H	2.0.7	2.0.8
5-11-08	19WTD133r1	3	-	C	Change of data definitions from ASN.1 to tables and short textual descriptions	2.0.7	2.0.8
5-11-08	19WTD134r1	4	-	C	MSC changes	2.0.7	2.0.8
5-11-08	19WTD136r1	5	-	C	Annex scenario changes	2.0.7	2.0.8
5-11-08	19WTD207r1	6	-	C	Changes agreed in principle by joint meeting of WG7 and SA3-LI in August 2008	2.0.7	2.0.8
5-11-08	19WTD224	7	-	D	Tidying of references and editorial spell checks	2.0.7	2.0.8
5-11-08	19tTD241r1	8	-	D	Cleanup the wording, references and remove duplications	2.0.8	2.0.9
24-3-09	WG7-05-004 21WTD291	9	-	F	The “physical locations” in the draft have to be replaced by “NGN-FEs”, and in the scenarios, the allocations of LI-FEs to NGN-FEs have to be marked as examples	2.0.9	2.0.10
24-3-09	WG7-05-005	10	-	F	Editorial consistency	2.0.9	2.0.10
24-3-09	WG7-05-006r1	11	-	D	Adoption of term "corresponding party" instead of "co-target"	2.0.9	2.0.11
24-3-09	WG7-05-007	12	-	D	Clarification of intercept material handed over in IRI payload	2.0.9	2.0.11
18-3-09	WG7-05-029	13	-	F	Inclusion of End Session IRI event as Result of Interception	2.0.10	2.0.11
					Publication	2.0.11	2.1.1

History

Document history		
V1.1.1	December 2006	Publication
V2.1.1	September 2009	Publication