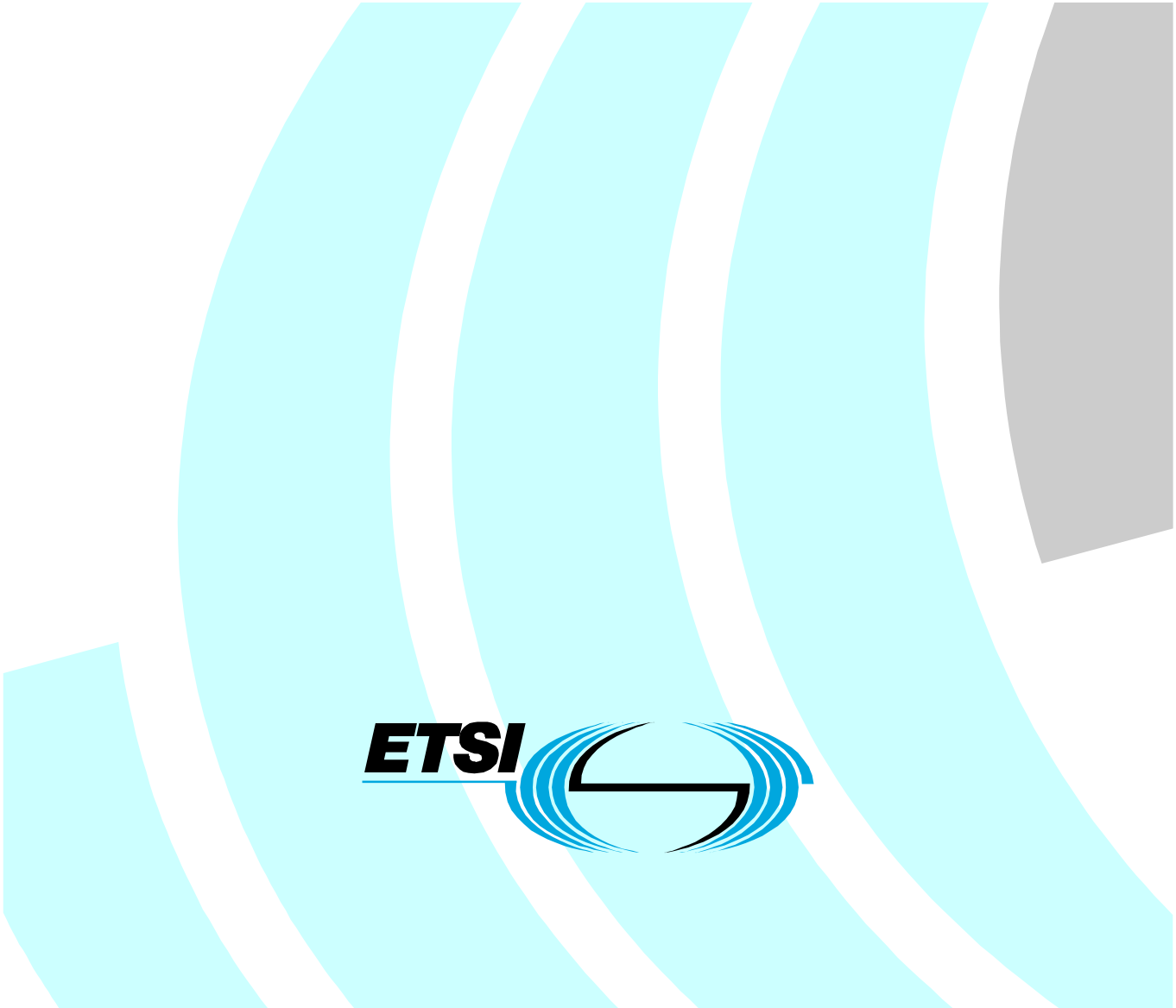
ETSI TS 187 005 V1.1.1 (2006-12)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception functional entities, information flow and reference points



Reference
DTS/TISPAN-07013-NGN-R1

Keywords
IP, Lawful Interception, security, telephony, VoIP

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2006.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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).

1 Scope

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 R1.

The present document specifies the stage 1 and stage 2 model for Lawful Interception (LI) of TISPAN NGN services as specified by TR 180 001 [5] and covering the following services explicitly:

- PSTN/ISDN emulation services (non IMS); and
- IMS based services.

The provisions in the present document apply only when the target of interception is an NGN user identified as specified in TS 184 002 [6], and when the network supplying services on behalf of the CSP is an NGN as specified by TISPAN in TR 180 001 [5] 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 [8], ES 201 671 [2] and TS 102 232 [4].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

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

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.

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

[2] ETSI ES 201 671 (V2.1.1): "Telecommunications security; Lawful Interception (LI); Handover Interface for the lawful interception of telecommunications traffic".

[3] ETSI TS 101 331 (V1.2.1): "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[4] ETSI TS 102 232 V1.4.1: " Lawful Interception (LI); Handover specification for IP delivery".

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

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

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

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

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

[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".

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.

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 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:

AF	Administration Function
CC	Content of Communication
CCCI	Content of Communication Control Interface
CCTF	Content of Communication Trigger Function
CCTI	Content of Communication Trigger Interface
CR	Change Request
CSP	Communications Service Provider
DF	Delivery Function
FE	Functional Entity
FFS	For Further Study
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)
IIF	Internal Interception Function
IMS	IP Multimedia Core Network Subsystem
INI	Internal Network Interface
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MF	Mediation Function
NGN	Next Generation Network
NGN-R1	NGN Release 1
PES	PSTN/ISDN Emulation Subsystem
PoI	Point of Interception
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
URI	Universal Resource Identifier
URL	Universal Resource Locator

4 Interception in the NGN

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.

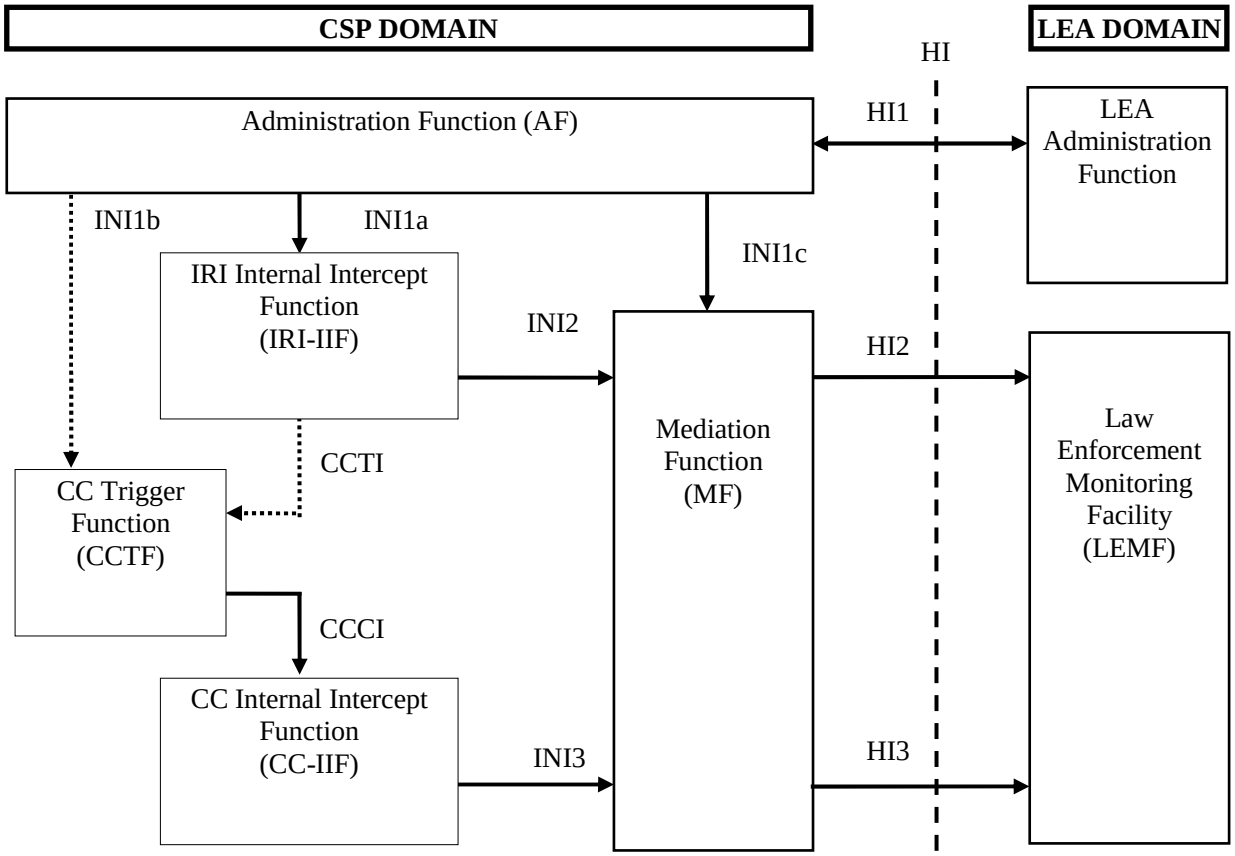
NOTE 1: A service offered to the NGN user may invoke many NGN-FEs.

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 [9], 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, CCTF, CCTI and CCCI are not defined in the present document but are shown in the figure for completeness.

Figure 1: Reference Model for Lawful Interception from TR 102 528 [9]

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 102 058 [9].

4.3 Content of interception

The point of interception shall provide the following data when available in the intercepting network from the communication of the target:

- Date and time of interception.
- Identity of the target and the correspondents of the target.
- Location of the target if available.
- Activity of the target.

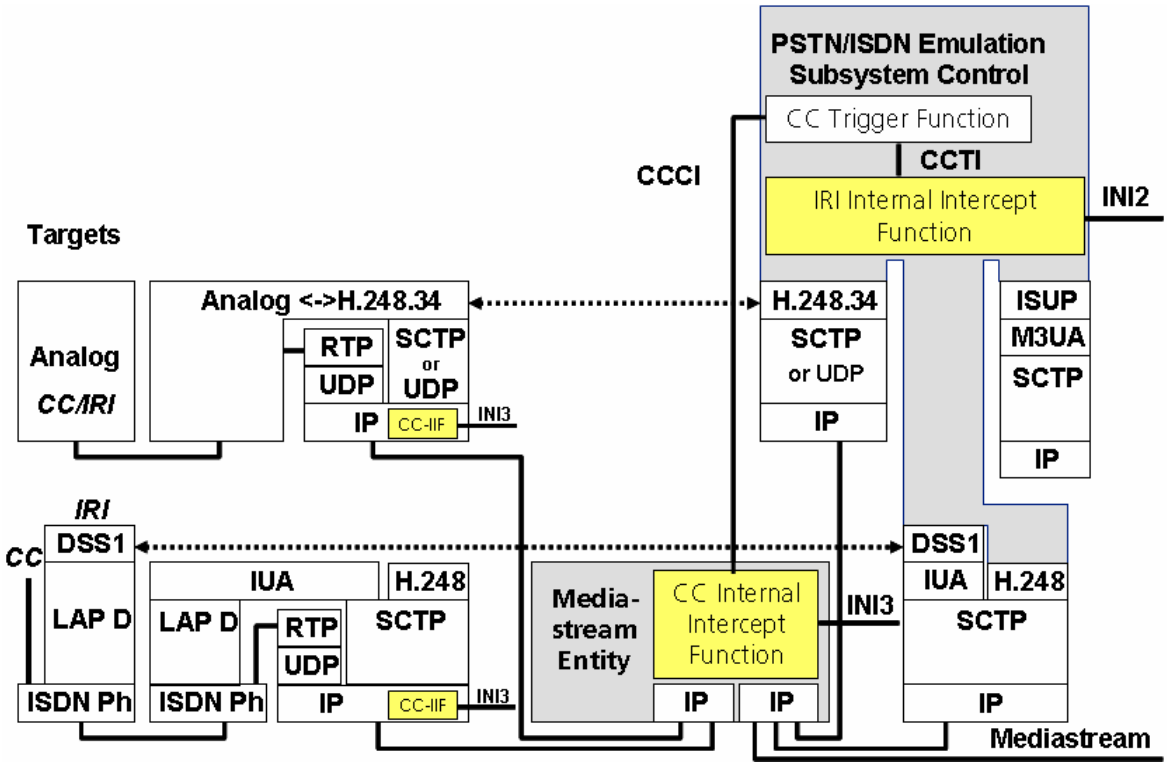
NOTE: Whilst each element of the interception may be described separately they may be delivered in combination, or may be delivered implicitly if no changes are reported (e.g. if location is not changed this knowledge may be delivered implicitly but when location is changed it may be explicitly reported).

5 Interception of non-IMS PSTN/ISDN Emulation Subsystem (PES)

5.1 Architecture for interception of PES

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.

Figure 1 (in clause 4.2) identifies the generic architecture for LI. The specific provision of the CC-IIF and IRI-IIF in the NGN for PES services is as shown in figure 2. This architecture for LI applies to a PES whose architecture conform to ES 282 002 [13].



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

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, e.g. Border Gateway.

6 Interception of IMS

6.1 Architecture for interception of IMS

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.

Figure 1 (in clause 4.2) identifies the generic architecture for LI. The specific provision of the CC-IIF and IRI-IIF in the NGN for IMS services is as shown in figure 3. This architecture for LI applies to the IMS subsystem as described in ES 282 007 [11] and TS 182 012 [12].

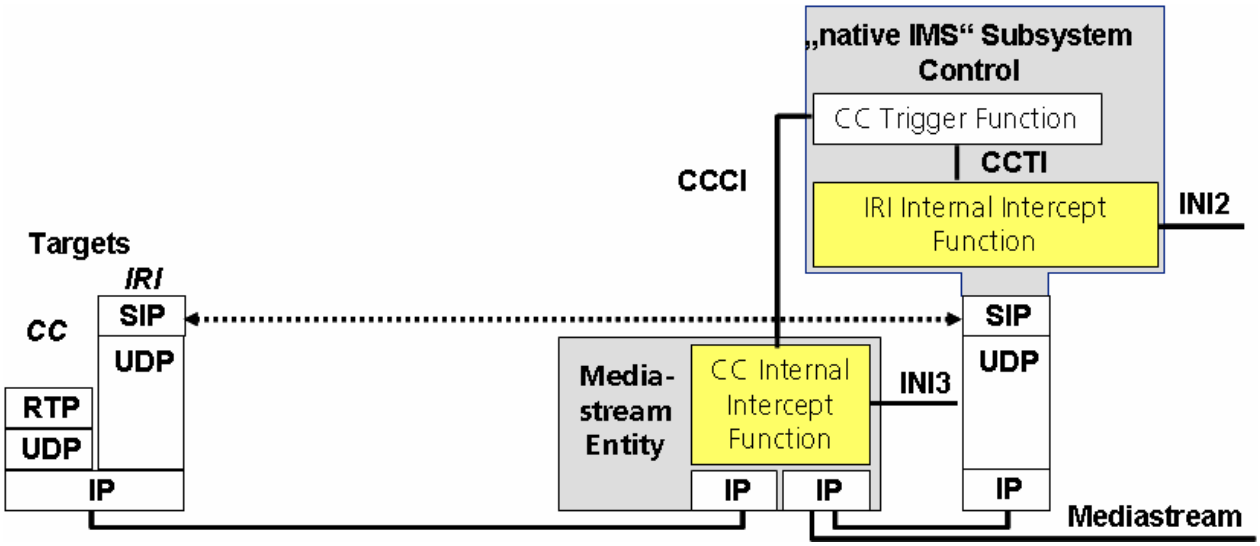


Figure 3: Reference architecture for interception in the IMS environment

6.2 Activation, deactivation and interrogation

The principles described in TS 133 107 [7] apply, with the exception that the list of target identities is restricted to be a SIP URI or a TEL URL.

6.3 Intercept Related Information

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 [7].

The stage 2 definition for interception of IMS found in TS 133 107 [7] shall apply for TISPAN NGN R1. Annex A specifies the parts of TS 133 107 [7] that apply.

NOTE 1: When IMS is providing a PES service the interception service identified above and defined in TS 133 107 [7] 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.

6.4 Content of Communication

Interception of the content of communications takes place at transport processing functional entities identified in the TISPAN NGN R1 architecture (ES 282 001 [1]). 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 at an A-MGF, C-BGF or MRFP takes place when the target of interception is a subscriber of the IMS network.

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.

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.

The instances in the network where the interception takes place (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.

7 Identification of target of interception

7.1 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.

7.2 IMS services

IMS service users shall be identified by either a SIP-url or a tel-url [6].

8 Security considerations

The guidelines for security identified in TS 101 331 [3] apply. The provision and actions of the interception measure should be confidential and not discoverable, or alterable, by unauthorized parties.

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

For the stage 2 definition of the interception of IMS and generic IP subsystem parts of TS 133 107 [7] apply normatively in the context of TISPAN NGN. This annex summarizes those parts of TS 133 107 [7] 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-R1 interception.

Clause	Applicability in TISPAN NGN R1
1	
2	
3	
4	Figure 1d applies
5	
6	Does not apply
7	Does not apply
7A	Applies in full
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)
8	
9	Does not apply
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 document)
NOTE: Annexes E and F do not exist in TS 133 107 [7].	

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 [8].

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 133.108 and how they should apply in TISPAN NGN.

This annex summarizes those parts of TS 133 108 [8] 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 normative specification for NGN-R1 interception.

Clause	Applicability in TISPAN NGN R1
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	
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	Applies in full
Annex J	Does not apply
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 [8] 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

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

NOTE 2: The endorsements stated are indicative and further work is required to fully analyse the data and operations in TS 102 232 [4] 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 R1
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
Annex F (informative):	GPRS HI3 Interface	
Annex G (informative):	LEMF requirements – handling of unrecognized fields and parameters	

Clause	Title	Applicability in TISPAN NGN R1
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. Interception of communications in transit are shown in figures E.4 and E.5.

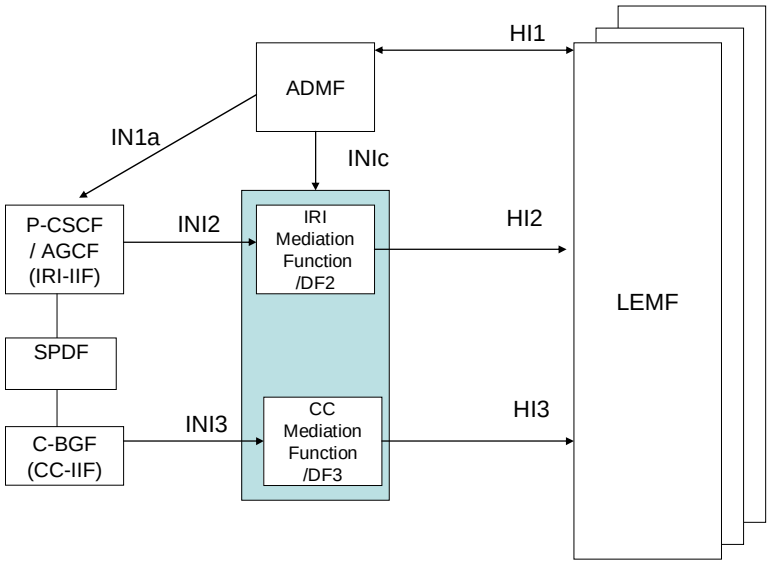


Figure E.1: Interception at the edge (case 1)

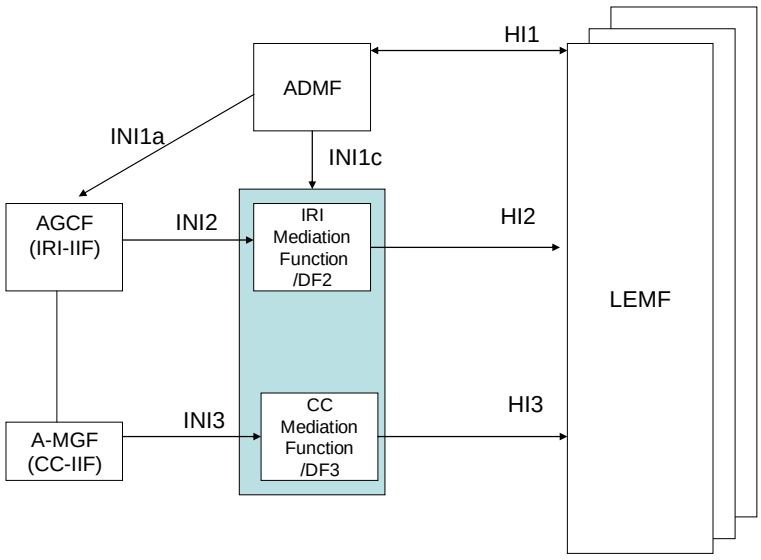


Figure E.2: Interception at the edge (case 2)

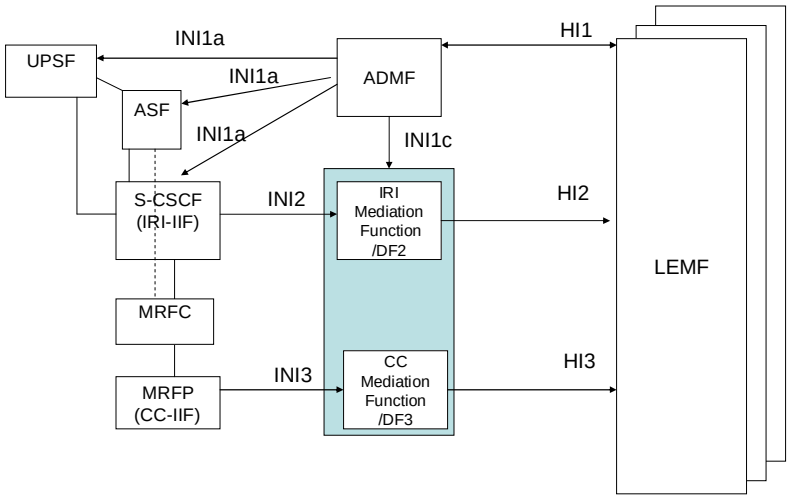


Figure E.3: Interception in the core

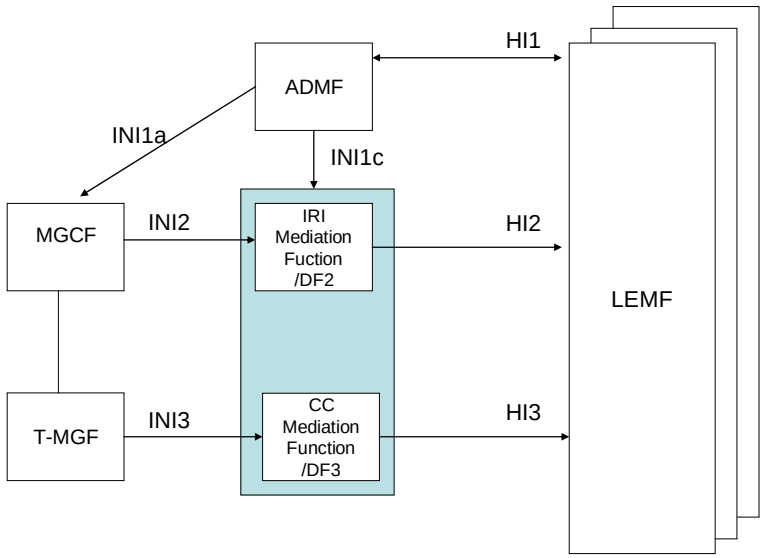


Figure E.4: Interception of communications in transit (TDM case)

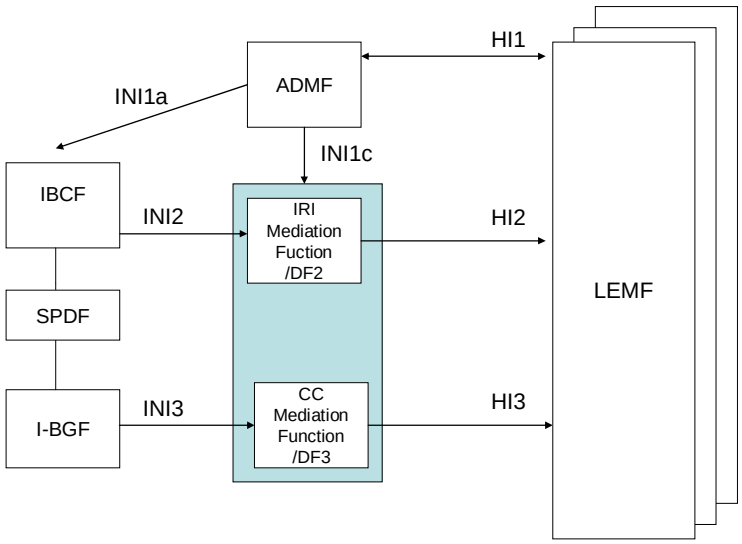


Figure E.5: Interception of communications in transit (IP case)

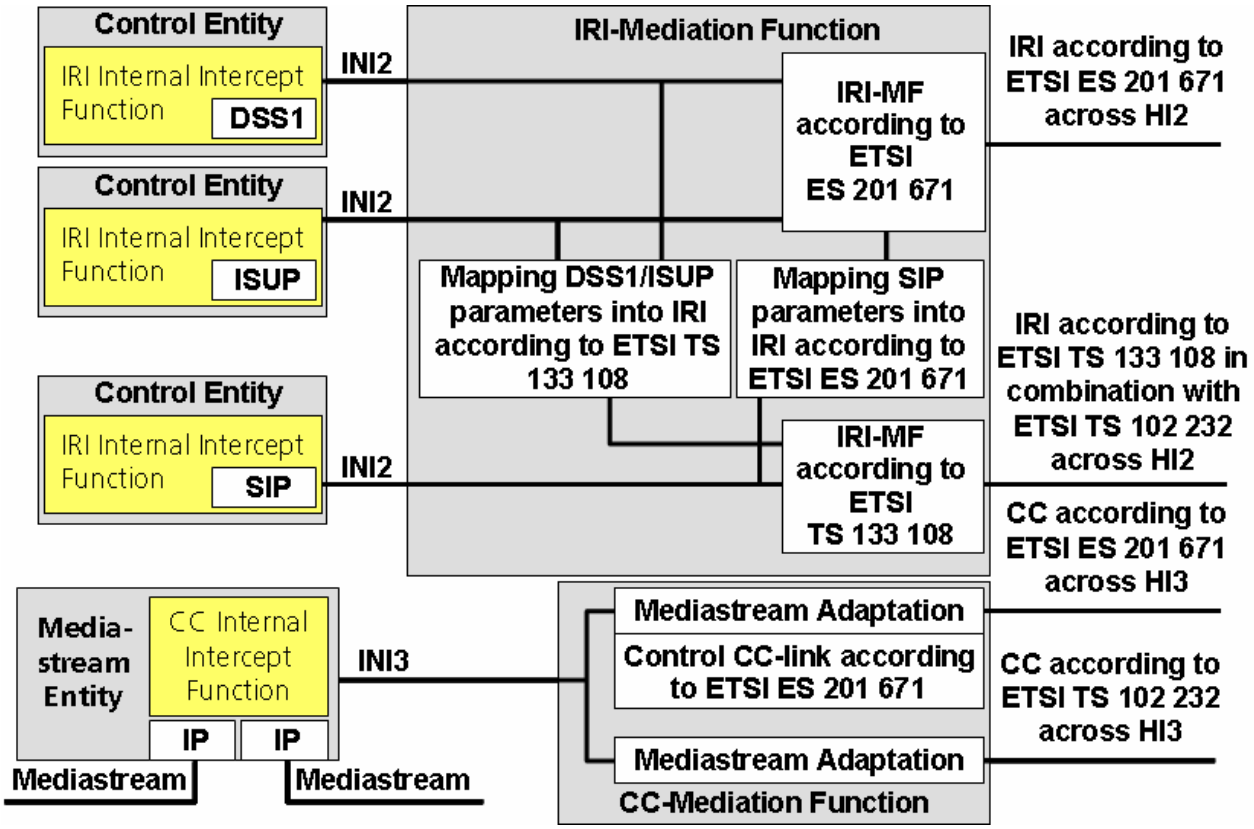
Annex F (informative): Selection of handover interface

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 [8]: Handover interface for Lawful Interception.
- TS 102 232 [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 but there may be a requirement for extensions to TS 133 108 in some instances.
NOTE 2: IMS interception formats from the NGN may map to IMS capabilities in TS 133 108 but there may be a requirement for extensions to TS 133 108 in some instances.
NOTE 3: SIP interception formats from the NGN map to IMS capabilities in TS 133 108 but there may be a requirement for extensions to TS 133 108 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".

History

Document history		
V1.1.1	December 2006	Publication