

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/0f477d2f-db08-486e-a12c-fe47fa9843b0/etsi-ts-187-005-v2.1.1-2009-09>



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

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/chaicor/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 2009.
All rights reserved.

DECT[™], **PLUGTESTS**[™], **UMTS**[™], **TIPHON**[™], the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered 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.

LTE[™] is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	9
4 Interception in the NGN.....	11
4.0 Structure of analysis	11
4.0.1 Review of stage 1 requirements.....	11
4.0.1.1 Provision/withdrawal	11
4.0.1.2 Activation/deactivation	11
4.0.1.3 Invocation and operation.....	11
4.0.1.4 Interrogation.....	11
4.0.1.5 Interaction with other services	12
4.1 LI architecture model	12
4.2 LI reference model	12
4.3 Result of interception	14
5A Stage 2 description of NGN LI.....	15
5A.1 Information flow sequences	15
5A.1.1 LEA control interactions and information flows	15
5A.1.1.1 LI_ACTIVATE_req.....	16
5A.1.1.2 LI_ACTIVATE_conf.....	16
5A.1.1.3 LI_MODIFY_req.....	16
5A.1.1.4 LI_MODIFY_conf.....	17
5A.1.1.5 LI_STATUS_ind.....	17
5A.1.2 Target signalling and traffic interactions and information flows	18
5A.1.2.1 TARGET_ACTIVITY_MONITOR_ind.....	18
5A.1.2.1.1 Relation to Handover.....	19
5A.1.2.2 T_TRAFFIC_ind.....	19
5A.1.2.2.1 Relation to Handover.....	19
5A.1.2.3 CP_TRAFFIC_ind	19
5A.1.2.3.1 Relation to Handover.....	19
5A.1.2.4 TARGET_COMMS_MONITOR_ind.....	20
5A.1.2.4.1 Relation to Handover.....	20
5A.2 Data provision and encoding	20
5A.2.1 Identification of result of interception	20
5A.2.2 Provision of identities/addresses.....	20
5A.2.3 Provision of details of services used and their associated parameters	21
5A.2.4 Provision of those signals emitted by the target invoking additional or modified services	21
5A.2.5 Provision of time-stamps for identifying the beginning, end and duration of the connection	21
5A.2.6 Provision of actual source, destination and intermediate public IDs in case of communication diversion	21
5A.2.7 Provision of location information	22
5 Interception in NGN subsystems.....	22
5.0 Allocation of LI-FEs to NGN-FEs	22
5.1 Architecture for interception of PES	23
5.2 Architecture for interception of IMS	23
5.3 Intercept Related Information (PoI IRI-IIF)	24

5.4	Content of Communication (PoI CC-IIF).....	24
6	Identification of target of interception.....	25
6.1	ISDN/PSTN services.....	25
6.2	IMS services.....	25
7	Security considerations.....	25
Annex A (normative):	Endorsement statement for TS 133 107.....	26
Annex B (informative):	Endorsement statement for TS 133 108.....	27
Annex C (informative):	Endorsement statement for TS 102 232 and its subparts.....	29
C.1	Endorsement statement for TS 102 232-1.....	29
C.2	Endorsement statement for TS 102 232-5.....	29
C.3	Endorsement statement for TS 102 232-6.....	29
Annex D (informative):	Endorsement statement for ES 201 671.....	30
Annex E (informative):	ISDN/PSTN LI reference configurations.....	32
Annex F (informative):	Selection of handover interface.....	35
Annex G (informative):	Bibliography.....	36
G.1	ETSI Specifications.....	36
G.2	3GPP specifications.....	36
G.3	ITU-T specifications.....	37
G.4	IETF specifications.....	37
G.5	ISO specifications.....	37
G.6	ANSI specifications.....	37
Annex H (informative):	Change history.....	38
History	39

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/0f477d2f-db08-486e-a12c-fe47fa9843b0/etsi-ts-187-005-v2.1.1-2009-09>

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.