

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TP TR 101 750 V1.1.2:2004](https://standards.iteh.ai/catalog/standards/sist/f8eaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004)

<https://standards.iteh.ai/catalog/standards/sist/f8eaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004>

ETSI TR 101 750 V1.1.2 (2002-01)

Technical Report

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Studies into the Impact of lawful interception

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TP TR 101 750 V1.1.2:2004](https://standards.iteh.ai/catalog/standards/sist/f8eaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004)

<https://standards.iteh.ai/catalog/standards/sist/f8eaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004>



Reference

RTR/TIPHON-08001a

Keywords

IP, network, security, 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TP TR 101 750 V1.1.2:2004

<https://standards.iteh.ai/catalog/standards/sist/f8eaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004>

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, send your comment to:

editor@etsi.fr

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 2002.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	5
3.1 Definitions	5
3.2 Abbreviations	8
4 General introduction.....	8
5 User (LEA) requirements for Lawful Interception.....	9
5.1 General requirements	9
5.2 Result of interception	10
5.3 Location information.....	10
5.4 Time constraints	11
5.5 Non disclosure	11
5.6 Information transmission and information protection requirements	11
5.7 Internal security.....	12
5.8 Unchanged state of service, etc.	12
5.9 Technical interface(s) and format requirements	12
5.10 Independence of the Network Operator/Access Provider/Service Provider	13
5.11 Temporary obstacles to transmission	13
5.12 Identification of the identity to be intercepted.....	13
5.13 Multiple interception measures	14
6 TIPHON scenarios and role model	14
6.1 TIPHON scenarios	14
6.2 Functional block diagram.....	14
7 Further work.....	16
History	17

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 SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The present document has been produced by ETSI Project TIPHON of the European Telecommunications Standards Institute (ETSI) in close alliance with the ad-hoc group for TIPHON Security of ETSI Technical Committee Security (TC-SEC) and the Lawful Interception Working Group of TC-SEC.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

[SIST-TP TR 101 750 V1.1.2:2004
https://standards.iteh.ai/catalog/standards/sist/f8eaaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004](https://standards.iteh.ai/catalog/standards/sist/f8eaaf7a-2954-4d08-b5a9-8fb84a4aff63/sist-tp-tr-101-750-v1-1-2-2004)

1 Scope

The present document describes the user (Law Enforcement Agencies) requirements for Lawful Interception and the impact in a TIPHON Implementation. It provides an abstract of the requirements [6], [3] and outlines a study on the impact of Lawful Interception for TIPHON compliant systems.

The provision of lawful interception on the SCN part of a TIPHON network is already generally addressed and is not considered in the present document. The present document does consider lawful interception in an IP network.

NOTE: The present document is a pre-study to identify the impact of lawful interception and therefore should lead to a subsequent document which specifies a TIPHON system compliant mechanism to permit the provision of lawful interception according to national law and appropriate standards.

The provision of lawful interception is a requirement of national law, which is usually mandatory. From time to time, a network operator/access provider/service provider shall be required, according to a lawful authorization, to make available results of interception, relating to specific target identities, to a specific Law Enforcement Agency.

2 References

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

- [1] ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".
- [2] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".
- [3] ETSI ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".
- [4] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".
- [5] ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of technical issues".
- [6] Official Journal of the European Communities 96/C329/01: "Council Resolution of 17 January 1995 on the lawful interception of telecommunications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

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

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

NOTE 2: The definitions from ETR 331 [3] have been expanded to include reference to an access provider, where appropriate.

(to) buffer: temporary storing of information in case the necessary telecommunication connection to transport information to the LEMF is temporarily unavailable

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

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

content of communication: 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.

Gatekeeper (GK): H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, Gateways and MCUs

NOTE: The Gatekeeper may also provide other services to the terminals, Gateways and MCU such as bandwidth management and locating Gateways. (See also ITU-T Recommendation H.323 [4]).

Gateway (GW): H.323 Gateway (GW) is an endpoint on the network which provides for real-time, two-way communications between H.323 terminals on the packet based network and other ITU terminals on a switched circuit network, or to another H.323 Gateway

NOTE: Other ITU Terminals include those complying with recommendations H.310 (H.320 on B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.234 (GSTN), H.234M (Mobile) and V.70 (DSVD). (See also ITU-T Recommendation H.323 [4]).

H.323 Terminal: endpoint on the network which provides for real-time, two-way communications with another H.323 Terminal, Gateway, or Multipoint Control Unit (MCU)

NOTE: This communication consists of control, indications, audio, moving colour video pictures, and/or data between the two terminals. A terminal may provide speech only, speech and data, speech and video, or speech, data and video. (See also ITU-T Recommendation H.323 [4]).

handover interface: physical and logical interface across which the results of interception are delivered from a network operator/access provider/service provider to an LEMF

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

intercept related information: collection of information or data associated with telecommunication services involving the TI, specifically call associated information or data (e.g. unsuccessful call attempts), service associated information or data (e.g. service profile management by subscriber) and location information

interception (or Lawful Interception): action (based on the law), performed by a network operator/access provider/service provider, of making available certain information and providing that information to an LEMF

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

interception interface: physical and logical locations within the access provider's/network operator's/service provider's telecommunications facilities where access to the content of communication and intercept related information is provided

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

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations

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

internal intercepting function: point within a network or network element at which the content of communication is made available

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

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

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

lawful authorization: permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/access provider/service provider

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

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

mediation device: mechanism which passes information between a network operator/access provider/service provider and a handover interface

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

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

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

NOTE: Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

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

result of interception: information relating to a target service, including the content of communication and intercept related information, which is passed by an access provider or network operator or service provider to an LEA

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

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

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

Service Provider (SP): natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network

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

Target Identity (TI): identity associated with a target service (see below) used by the interception subject

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

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

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

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

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