SLOVENSKI STANDARD
SIST-V ETSI/EG 201 781 V1.1.1:2003

01-november-2003

Inteligentno omrežje (IN) - Zakonito prestrezanje

Intelligent Network (IN) - Lawful interception

Ta slovenski standard je istoveten z: EG 201 781 Version 1.1.1

ICS:

33.040.35	Telefonska omrežja	Telephone networks

SIST-V ETSI/EG 201 781 V1.1.1:2003 en

ETSI EG 201 781 V1.1.1 (2000-07)

ETSI Guide

Intelligent Networks (IN);
Lawful Interception

Reference

DEG/SPAN-061209

Keywords

IN, security

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://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

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://www.etsi.org/ipr).

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 ETSI Guide (EG) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

1 Scope

The present document lays down architectural requirements for the lawful interception of IN services. Those requirements shall be fulfilled to allow the Network Operator, an Access Provider or a Service Provider (NWO/AP/SvP) to implement an interception order from a Law Enforcement Agency (LEA) and to provide the handover interface to the LEA which is described in other documents. The provision of lawful interception is a requirement of national law, which is usually mandatory for the operation of any telecommunication service.

The present document specifies the generic flow of information and generic interfaces, which are focussing on IN capability set CS1and CS2 services. Future services should follow the guidelines where possible.

CS3, CS4 and CAMEL are not examined in this version of the document but may be included in future versions.

The present document does not specify how these generic flows of information and generic interfaces shall be used to intercept a specific IN service. There will normally be several implementation methods available by using the generic interfaces. Details for a service, which affects the way interception is already carried out shall be negotiated between the NWO/AP/SvPs and the responsible regulatory authority on a national basis.

Where applicable, this guide is based on other ETSI standards or ITU-T Recommendations in the area of telecommunication services. The reader should be familiar with the referenced standards/recommendations, including the ITU Recommendations, which are endorsed by many of the referenced ETSI standards.

It is not intended to define enhancements of specific interfaces like HI2 and HI3 in the present document. This work shall be covered by other ETSI documents.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETSI ETR 331: "Definition of user Requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

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

[3] ETSI ES 201 671: "Telecommunications Security; Handover Interface for Lawful interception of telecommunications traffic".

[4] ETSI ETR 330: "Guide to the legal and regulatory environment".

[5] ITU-T Recommendation X.881: "Information technology - Remote operations: OSI realisations - Remote Operations Service Element (ROSE) service definition".

[6] ITU-T Recommendation Q.1204: "Intelligent Network Distributed Functional Plane Architecture".

[7] ITU-T Recommendation Q.1211: "Introduction to Intelligent Network Capability Set 1".

[8] ITU-T Recommendation Q.1221: "Introduction to Intelligent Network Capability Set 2".

[9] ITU-T Recommendation Q.1231: "Introduction to Intelligent Network Capability Set 3".

[10] ITU-T Recommendation Q.1241: "Introduction to Intelligent Network Capability Set 4".

[11] ITU-T Recommendation Q.1214: "Distributed Functional Plane for Intelligent Network CS-1".

[12] ETSI EN 301 140-5: "Intelligent Network (IN); Intelligent Network Application Protocol (INAP); Capability Set 2 (CS2); Part 5: Distributed Functional Plane (DFP) [ITU-T Recommendation Q.1224 (1997) modified]".

[13] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[14] European Union Council Resolution on the Lawful Interception of Telecommunications (17 January 1995).

[15] ETSI ETR 164: "Integrated Services Digital Network (ISDN);Intelligent Network (IN);Interaction between IN Application Protocol (INAP) and ISDN User Part (ISUP) version 2".

[16] ETSI ETS 300 374-1: "Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1); Core Intelligent Network Application Protocol (INAP); Part 1: Protocol specification".

[17] ITU-T Recommendation Q.1224: "Distributed functional plane for intelligent network Capability Set 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1], [2] and [3] and the following apply:

accountability: principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation

access provider: access provider 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 have been expanded to include reference to an access provider, where appropriate.

activation/deactivation: procedures for activation, which is the operation of bringing the service into the "ready for invocation" state, and deactivation, which is the complementary action, are described in this clause. For some services there may be a specific user procedure to allow activation and deactivation as necessary, whilst for others the service is permanently activated on provision and thus no procedure is provided (see [5])

availability: avoidance of unacceptable delay in obtaining authorized access to information or IT resources

call: any temporarily switched connection capable of transferring information between two or more users of a telecommunications system. In this context a user may be a person or a machine

call identifier: number, generated automatically by the internal interception function for each call or call leg of a intercept subject identity

confidentiality: avoidance of the disclosure of information without the permission of its owner

content of communication: information exchanged between two or more users of a telecommunications service, excluding intercept related information. This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another

handover interface: physical and logical interface across which the interception measures are requested from network operator / access provider / service provider, and the results of interception are delivered from a network operator / access provider / service provider to a law enforcement monitoring facility

HI1 Information: data received over the HI1 Interface

identity: system-unique tag applied to a user

IN call: call, which involves the IN layer. It may involve a virtual subscriber, but it may also only involve an operator network function, like Number Portability

IN service: service, which uses IN technology

Integrity: avoidance of the unauthorized modification of information

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

NOTE 3: In the present document the term interception is not used to describe the action of observing communications by a law enforcement agency (see below).

intercept related information: collection of information or data associated with telecommunication services involving the intercept subject identity, 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 Subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

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

invocation and operation: these terms describes the action and conditions under which the service is brought into operation; in the case of a lawful interception this may only be on a particular call. It should be noted that when lawful interception is activated, it shall be invoked on all calls (Invocation takes place either subsequent to or simultaneously with activation.). Operation is the procedure which occurs once a service has been invoked. *Remark:* The definition is based on [5], but has been adopted for the special application of lawful interception, instead of supplementary services

law enforcement agency: 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: enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject

lawful authorization: permission granted to a LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator / access provider / service provider. Typically this refers to a warrant or order issued by a lawfully authorized body

lawful interception: see interception

lawful interception identifier: identifier, generated by the law enforcement agency, which relates to a specific lawful authorization. It is used as an alias for the intercept subject identity

LI list: list with intercept subject identities

LI data: information (e.g. prefix, INAP operation, parameter in some INAP operation etc.) that enables the execution (start, duration and end) of the intercept warrant in the switching layer. This LI data is to be sent on a call by call basis, as opposed to only when the intercept period starts and ends

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

mediation device: equipment, which realizes the mediation function

mediation function: 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

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

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

service provider: natural or legal person providing one or more public telecommunications services whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network. A service provider needs not necessarily run his own network

Service subscriber: natural or legal person who subscribes to a service offered by a service provider

Subscriber Controlled Input: customer control activity, either through the PSTN/ISDN network, or the data communication network, to the IN layer

target identity: technical identity (e.g. the interception's subject directory number), which uniquely identifies a intercept subject. One intercept subject may have one or several intercept subject identities

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

"Virtual" subscriptions: subscription not connected to a physical line card in a switch. Typically an IN service subscription, e.g. Freephone. The service can be reached through signalling from more than one switch

"Virtual Dial-able" subscriptions: these virtual subscriptions may be designed for incoming calls only. Thus another party may not call to them. These are called "dialable" subscriptions. Examples are Freephone and Premium Rate services

"Virtual Non-dial-able" subscriptions: these virtual subscriptions may be designed for outgoing calls only, thus they may not be called to, by another party. These are called "non-dialable" subscriptions. Examples are Prepaid, Account and Credit Card Calling services

3.2 Abbreviations

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

ADMF	Administration function
AP	Access Provider
BCSM	Basic Call State Model
CC	Content of Communication
CCAF	Call control agent Function
CCF	Call Control Function
CID	Call Identifier
CPN	Calling Party Number
CS-x	Capability Set x
CUSF	Call Unrelated Service Function (out-channel interaction)
DFP	Distributed Functional Plane
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)
IAF	Intelligent Access Function
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
iPIWF	Internet protocol interworking Function
iPSCF	Internet protocol service control Function
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception Identified – it uniquely identifies a LI-order within all networks
NWO	Network Operator
OCN	Originally Called Party Number
RDN	Redirecting Number
SCEF	Service creation environment Function

SCF	Service Control Function
SCP	Service Control Program
SCUAF	Service Control User Agent Function
SDF	Service Data Function
SMAF	Service Management Access Function
SMF	Service Management Function
SRF	Service Resource Function
SS7	Signalling System 7
SSF	Service Switching Function
SvP	Service Provider
SW	Software
TCAP	Transaction Capabilities Application Part
UPT	Universal Personal telecomunication

4 Introduction

IN technology provides the capability to easily define and implement new IN-services. Although there are general requirements for LI of telecommunication e.g. [3] and [14], IN specific requirements are nowhere laid down. Since IN services can be developed by service providers and/or operators it is required to provide means which enable the developer of an IN service to comply with obligations to provide LI support.

The present document captures requirements, which need to be fulfilled to make LI support of IN services possible.

The fulfilment of these requirements will make it also possible to provide LI support as an IN service.

5 General Requirements for Lawful Interception

5.1 Introduction

This clause presents the Law Enforcement Agency (LEA) requirements, with the LEA as the user, in relation to the lawful interception of telecommunications. These requirements are subject to national law and international treaties that should be interpreted in accordance with the applicable national policies. Service, network and access providers may co-operate to meet LEA requirements. Handover interfaces, to the LEA, shall be configured in accordance with appropriate ETSI Standards or with national requirements. A handover interface should be in accordance with ES 201 671 [3].

5.2 General LEA Requirements

General requirements for lawful interception of the law enforcement agencies can be found in ETR 331 [1] which is based on a European Council Resolution [14].

5.3 Requirement for Network Functions

General requirements for lawful interception from the network point of view can be found in ES 201 158 [2].

5.4 IN Specific Requirements

Every IN service shall support LI; exceptions may be agreed between the IN service provider and the relevant national authorities.