Draft **ETSI EG 201 781** V1.1.1 (2000-03)

Intelligent Networks (IN);
Lawful Interception

Reference
DEG/SPAN-061209

Keywords
IN, Security

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Important notice

This ETSI deliverable 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.

Copyright Notification

ETSI

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 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 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), and is now submitted for the ETSI standards Membership Approval Procedure.

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 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.

6   Functional IN architecture

6.1   Distributed functional plane model

The IN distributed functional plane (DFP) architecture has been used to describe the Functional IN architecture.

The IN DFP model is described in ITU-T Recommendation Q.1204 [6]. The diagram consists of **functional entities** - representing a unique group of functions in a single location and a subset of the total set of functions required to provide a service - and **relationships** - representing a set of information flows between a communicating pair of functional entities.

Following functional entities have been identified:

- Call control agent function (**CCAF)** [since CS-1];

- Call control function (**CCF**) [since CS-1];

- Service switching function (**SSF**) [since CS-1];

- Service control function (**SCF**) [since CS-1];

- Service data function (**SDF**) [since CS-1];

- Specialized resource function (**SRF**) [since CS-1];

- Service control user agent function (**SCUAF**) [since CS-2];

- Call unrelated service function (**CUSF**) [since CS-2];

- Intelligent access function (**IAF**) [since CS-2];

- Service creation environment function (**SCEF**) [since CS-1];

- Service management access function (**SMAF**) [since CS-1];

- Service management function (**SMF**) [since CS-1].

6.1.1   Capability Set 1 (CS-1) distributed functional plane model

Figure 1 identifies the IN DFP model for IN CS-1 as described in Q.1214. This diagram depicts the functional entities and relationships applicable to IN CS-1.
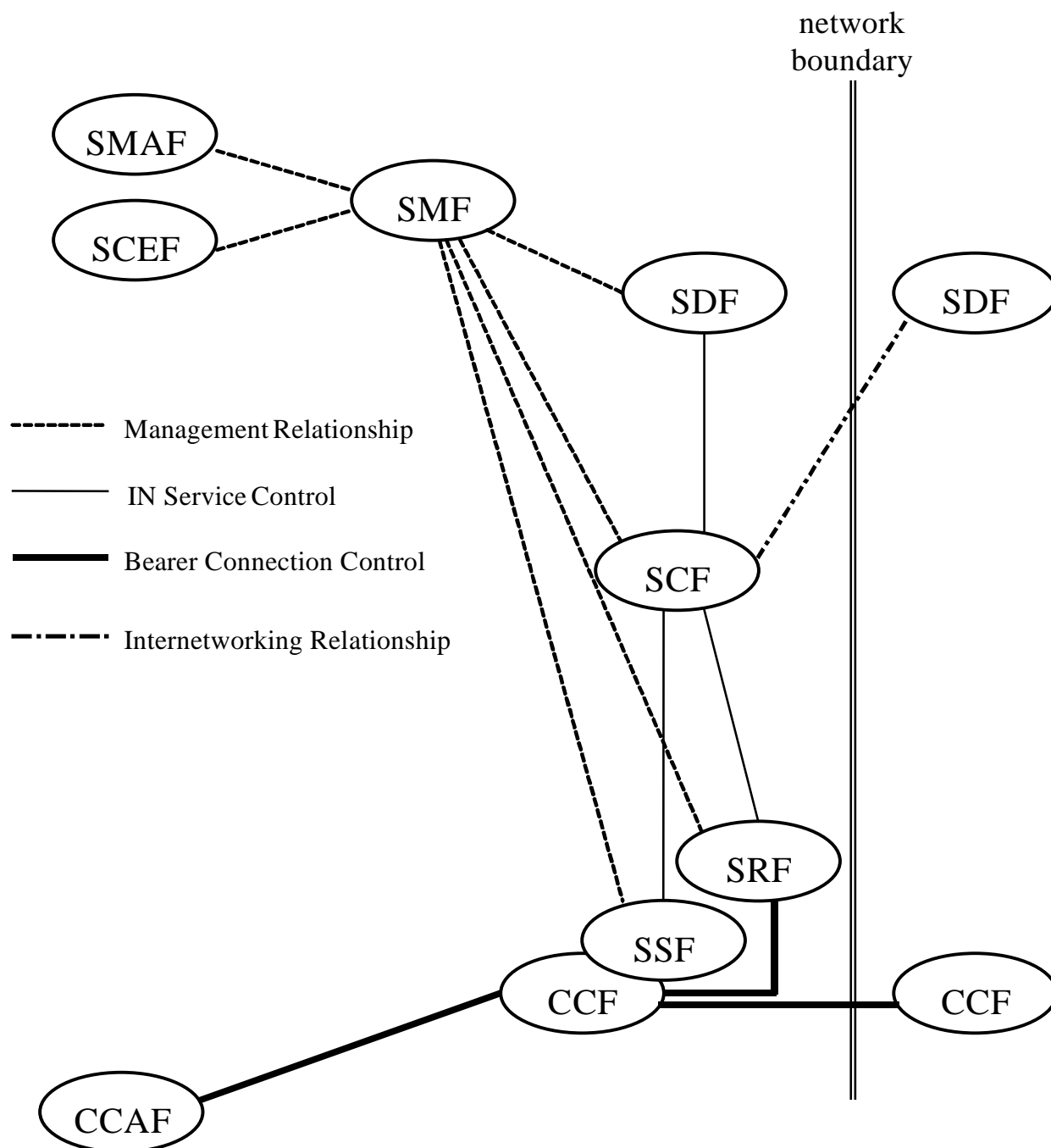
Figure 1: IN CS-1 DFP Architecture

6.1.2   Capability Set 2 (CS-2) distributed functional plane model

Figure 2 identifies the IN DFP model for IN CS-2 as described in 3/Q.1224 [17]. This diagram depicts the functional entities and relationships applicable to IN CS-2.
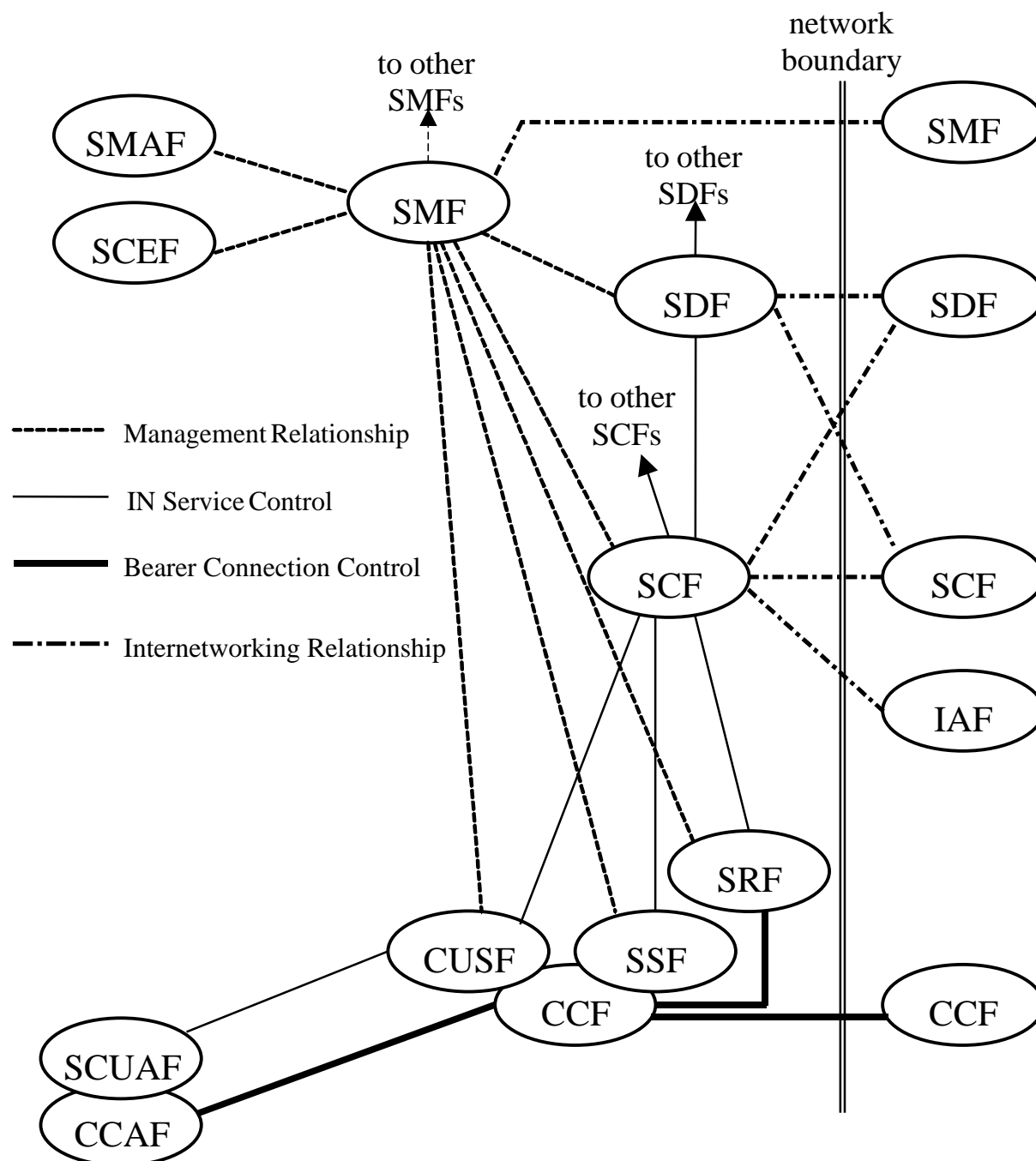
Figure 2: IN CS-2 DFP Architecture

6.2 Internetworking

Internetworking is the process in which several networks (potentially of different types, such as IN-structured, non-IN-structured, public and private) co-operate to provide a service. The need for internetworking capabilities results from the fact that the customer may want to access services which span multiple networks.

6.2.1 Capability Set 1 (CS-1) internetworking

IN CS-1 identified the SCF-SDF relationships for internetworking purposes. Neither distributed service logic, nor distributed service control is supported. Internetwork management interaction is not supported.

6.2.2 Capability Set 2 (CS-2) internetworking

IN CS-2 identifies the SCF-SCF, SCF-SDF, SCF-IAF, SDF-SDF and SMF-SMF relationships for internetworking purposes. Distributed service logic, but not distributed service control, is supported. Additionally, internetwork management interactions and distributed data handling processes are supported.

7 LI architecture

7.1 General

This clause details functions and interfaces, which are required to intercept a call, which invokes an IN service.

General aspects of this clause are contained in ITU-T Recommendation Q.1214 [11].

General LI related interfaces are according to the following model:
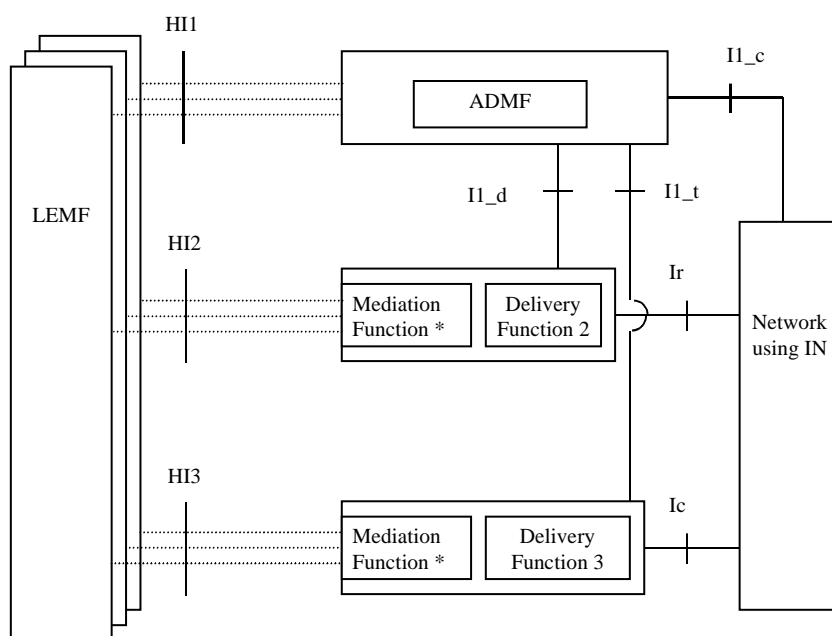
NOTE: The Mediation Function may be transparent, and may need to be adapted to a regional variant of the HI interface. The adaptation will be to HI1, HI2 and HI3 as defined in ES 201 671 [3].

Figure 3

The different interfaces are according to the following table:

Symbol	Defined in:
I1_c	7.3.3.2.6
I1_d	7.3.3.2.7
I1_t	7.3.3.2.8
Ir	7.3.3.2.3
Ic	7.3.3.2.4
It	7.3.3.2.1
Ii	7.3.3.2.2

The functional model takes this general model and provides details on network internal functions and required interfaces.

Generic Functional Plane Model

Figure 4: Lawful Interception for IN Services Functional Plane Model

7.2 Functions and procedures involved in LI for IN calls

The following subclauses provide details for functions and procedures involved in LI for IN.

7.2.1 LI Data Management

The sequence of actions to set up an intercept begins with the delivery of a lawful authorization across the HI1 interface. The information in the lawful authorization needs to be analysed and the relevant data distributed to the LI functions in the operator's network. This data will typically include the identification of the intercept subject by a meaningful key, e.g. dialled number (telephone number, credit card number), and the destination address of the mediation point for the call content and the Intercept related information. The LI Data Management function shall distribute the relevant information.

7.2.2 LI Data extraction

This function is invoked for every service invocation and whenever the services receives new information (service data, state change, etc.). The function extracts service specific information, which may be used by the LI Target detection function to determine, whether a specific call needs to be intercepted. This function is not involved in extracting the information, which will be reported to the LEA.

7.2.3   LI Target detection

Once the relevant data is set up in the network it will be necessary to identify any call involving the intercept subject that satisfies the intercept criteria. Hence there is a need for the service to provide the relevant data on every call to enable the detection of the intercept subject. This data needs to be analysed and compared against the "meaningful key" provided by the LI Data Management function. When all criteria are met the SCF or the SSF may arrange for interception to occur and the Intercept related information may be formatted and delivered to the mediation point. The LI Target detection function shall identify the need for LI to occur.

This function may also trigger when it receives an indication from another network element that an incoming call has been identified for interception. This function can then inhibit any further requests for CC interception and forward any relevant information to the IRI mediation point.

This function may also be involved in non call related activities, which are subject to LI.

7.2.4   LI CC Delivery function

Once the intercept subject and intercept conditions have been identified the actual call content needs to be intercepted and delivered to the mediation point specified in the I1_c . It will be necessary to identify the identity of the call in relation to the lawful authorization and the intercept subject as part of the signalling associated with the call. It will also be necessary to establish a unique identity for the call so that it can be associated with the IRI. The content of the data sent to the Mediation function should be compatible with the HI3 interface.

7.2.5   LI IRI Delivery function

When the call content intercept is established the required information associated with the call needs to be recovered from the network. This may include one or all of the following; SSF, CCF, SCF and SDF. This data needs to be identified as being associated with the intercepted call and delivered to the destination specified by the I1_d. The content of the data sent to the Mediation function should be compatible with the HI2 interface.

In addition this function shall generate IRI in cases, where call independent data changes are done e.g. changes of subscriber profile data for UPT service.

7.2.6   Mediation Function

The mediation function is as described in ES 201 671 [3] and will transform the internal data format of the CC-IF and IRI-IF interfaces into the standard format required at the HI2 and HI3 interfaces to the LEMF. It may be transparent.

7.3   Distributed functional model

LI for IN shall be based on the above shown functional model.

This section provides information on the different interfaces and identifies, whether the interface needs standardization or not. The respective statement is based on analysis of implementation options as given in annex B.

7.3.1   IN functional model

The above Functional model applies to CS-1and CS-2. It uses the "Handover Interface for LI of Telecommunications Traffic" [3]. Unless stated otherwise all definitions of functions and interfaces are as defined in the respective documents.

7.3.2   Definition of functional entities related to LI of IN services

The following functional entities shall be implemented to support LI of IN services.

7.3.2.1   LI Management function

This function shall store HI1 data (HI1 Information) and shall provide access to that data for other functions in the functional plane. The function shall not provide access to any data across network boundaries.

It is an implementation detail, whether this function is co-located with SMF, CCF, SSF, SCF, or SDF.

7.3.2.2   LI Data extraction

This function shall be associated with an IN service. It shall extract data from the service subscriber profile information, invocation data and state information, which can subsequently be used to determine, whether LI interception shall be started.

The implementation and the data extracted may depend on the IN service, to which this function is associated.

It is an implementation detail, whether this function is co-located with SMF or SCF.

7.3.2.3   LI Target detection

This function shall determine from the data extracted by the LI Data extraction function if LI is required. It shall then inform the other LI functions to establish interception of the call.

7.3.2.4   LI CC Delivery function

When the conditions for LI have been identified by the target detection function this function shall set up the interception of the Call Content and deliver them to the mediation point specified in the related LI-CC Delivery data

7.3.2.5   LI IRI delivery function

Once the LI conditions have been established this function shall recover all relevant IRI data from the CCF/SSF and SCF/SDF and send them to the mediation point specified in the related LI-IRI Delivery data.

7.3.3   Interfaces

The following interfaces and associated interface data shall be used.

7.3.3.1   Interface data description

The following data shall be transported on the LI related interfaces.

7.3.3.1.1   LI-CC Delivery Data

This is the data associated with the lawful authorization which specifies where the Call Content is to be delivered and any additional information, e.g. LIID. The information is determined from the data transported on HI1. The information is sent over the I1_d Interface.

7.3.3.1.2   LI-IRI Delivery Data

This is the data associated with the lawful authorization which specifies where the Intercept Related Information is to be delivered and any additional information, e.g. LIID. The information is determined from the data transported on HI1. The information is sent over the I1_c Interface.

7.3.3.1.3   LI Target Data

This is the data required to identify the intercept subject of the lawful authorization and the key data associated with the service to initiate an intercept. The information is determined from the data transported on HI1. The information is sent over the I1_t Interface.

7.3.3.1.4   LI-trigger - Info

Any Data, which allows receiving LI-functions with sufficient access to HI1 Information to generate IRI and/or set-up CC.

7.3.3.1.5   LI-Active [optional]

This data contains a flag to indicate that the call is currently subject of interception and provides a unique identifier for the call, which can be associated with a lawful authorization.

7.3.3.1.6   CID

This is a unique call identifier as defined in [3].

7.3.3.2   Interface description

The following sections describe required interfaces by identifying data, which shall to be transported on the specific interface.

It is identified whether the interface shall support multiple entities of interface data.

7.3.3.2.1   Interface It

This interface shall transport LI-trigger - Info.

The LI-trigger information shall at least consist of two types of information:

- Identifier for the type of information;

- Actual Value.

    NOTE 1: The interface shall be capable of transporting multiple entities of LI-trigger - Info.

    NOTE 2: The need of standardization shall be considered.

7.3.3.2.2   Interface Ii

This interface shall transport LI-trigger - Info.

The LI-trigger information shall at least consist of three types of information:

- Identifier for the type of information, Fixed to identify that the Value contains the LIID;

- Actual Value, LIID to apply to this call;

- CID.

    NOTE 1: Several LIIDs may be active on one call. The interface shall therefore be capable to transport several entities of information.

    NOTE 2: The need of standardization shall be considered.

7.3.3.2.3   Interface Ir

This interface shall transport LI-IRI data.

The content is specific to the IN service. It should be compatible to the HI2 interface definition.

    NOTE: The need of standardization shall be considered.

7.3.3.2.4   Interface Ic

This interface shall transport LI-CC data. It shall transport all information, which is required to provide the HI3 information.

It should be compatible to the HI3 interface definition.

    NOTE: The need of standardization shall be considered.

7.3.3.2.5   Interface Ia

This interface shall transport LI-Active - Info.

The LI-Active information shall at least consist of four types of information:

- Indicator, whether LI shall be active on that call;

- Indicator, whether the call content (HI3 interface) is already captured;

- LIID of the LI, if LI shall be active on that call;

- CID.

The interface shall be capable of transporting multiple entities of LI-Active - Info.

It shall be foreseen, that this information can be discarded at network boundaries.

This is an optional interface, which is subject to national requirements and legal considerations.

> NOTE: The need of standardization shall be considered.

7.3.3.2.6   Interface I1_c

This interface shall transport LI CC Delivery data.

This interface is a network internal interface and does not require standardization.

7.3.3.2.7   Interface I1_d

This interface shall transport LI IRI Delivery data.

This interface is a network internal interface and does not require standardization.

7.3.3.2.8   Interface I1_t

This interface shall transport LI Target data.

This interface is a network internal interface and does not require standardization.

8   Security Aspects of LI for IN

For all actions related to Lawful Interception, the following general objectives have to be fulfilled: Confidentiality, Integrity, Availability, and Accountability (CIAA). This refers to all data entered into the LI system, stored in the LI system, or transmitted through the public network or to the Law Enforcement Agencies (LEAs). Confidentiality here includes the requirement to hide the fact of interception being performed.

8.1   Requirements

The security requirements stated in ETR 331 [1] and ES 201 158 [2] shall be fulfilled.

All functional entities and all interfaces concerned with LI need protection against unauthorized access and against disclosure or modification of stored or transmitted data. In the following, the related security requirements to the functional entities, data and interfaces concerned with LI in IN are given.

Functional Entities:

- **LI management function:** access control, accountability;

- **LI data extraction:** needs protection against modifications;

- **LI target detection:** confidentiality and integrity, access control;

- **LI CC delivery function:** same security requirements as for target detection;

- **LI IRI delivery function:** same security requirements as for target detection.

Interfaces:

- **CC-INI:** confidentiality and integrity of CC (same security requirements as for non-IN calls);

- **IRI-INI:** confidentiality and integrity of IRI (same security requirements as for non-IN calls);

- **It:** confidentiality and integrity (sensitive data transmitted through network!);

- **Ii:** confidentiality and integrity (sensitive data transmitted through network!);

- **Ir:** confidentiality and integrity of IRI (same security requirements as for non-IN calls);

- **Ic:** confidentiality and integrity of CC (same security requirements as for non-IN calls);

- **Ia:** confidentiality and integrity (sensitive data transmitted through networks!).

NOTE: The data sent through this interface may make it possible to track down the target. This interface is, however, optional and subject to national requirements and legal considerations.

- **I1_c:** confidentiality and integrity;

- **I1_d:** confidentiality and integrity;

- **I1_t:** confidentiality and integrity.

8.2 Solutions

The specification of security mechanisms is out of scope of the present document. It depends on the implementation of the Intelligent Network and of the LI functionality. It depends especially on the location of the LI related functional entities and interfaces.

A general directive should be: any implementation of LI in Intelligent Networks has to be checked if confidentiality and integrity of personal data and LI data are ensured.

Annex A (informative):
Lawful Interception Principles for Intelligent Networks

A.1   Introduction

This annex outlines the basic principles of Lawful Interception in an IN enabled Network. This will include discussions of the following principles:

- IN specific issues for LI;

- Identification of Interception subjects and target identities;

- Possible Interception trigger points.

First it is clarified who can be the interception subject and their target identity in an IN call. Thereafter some triggering methods with their general characteristics and associated issues are outlined.

A.1.1   Background

To understand the relevance and impacts of the outlined methods it is important to understand the purpose of IN. The IN architecture was invented in order to rapidly provide a flexible way of inventing and deploying value added services to users, it was built to be independent of the switching and transport layer.

IN services are being run on the Intelligent Network Platform. The functional entities are described in chapter 6 of the present document. Typical examples of functions that may involve IN are Number Portability and CLI-Validation. Examples of value added services are Freephone, Premium Rate, Universal Personal Telecommunication etc.

As IN based services can be developed by individual service providers and operators it is not possible to standardize the services. Hence the present document can only provide a framework based on IN principles to enable the interception of IN calls and can not prescribe how to intercept particular services.

A.2   Intercepted Target Identities

The intercepted subject in an IN call may further be defined on a call case basis by the following target identities:

1) a calling party;

2) the virtual dialable subscription number, originating call;

3) the virtual dialable subscription number, terminating call;

4) the virtual non-dialable subscription number;

5) the actual destination(s) to which the call is routed.

A.3   Triggers/Activation of interception

Three types for triggers for interception of IN calls are described in this annex:

Access, Number and SCF Based triggering.

A.3.1   Access Based trigger

Access Based triggering is a typical implementation of Lawful Interception for PSTN/ISDN calls. In general IN services have no knowledge of the network access points. Hence it is assumed that this type of interception would be carried out by the PSTN/ISDN Interception function rather than the IN interception function. However some supplementary information has to be sent to the LEMF (e.g., new destination number or calling line identity provided in the Connect operation, etc.)

For further details on interception of PSTN/ISDN calls, refer to ES 201 671 [3].

A.3.2   Number Based trigger

A number based triggering means that the E.164 numbers related to the call (see note) are examined and verified against the list of intercepted target identities. This means that all IN calls can be intercepted, in which the said E.164 number of the target appears e.g. Freephone Numbers, Personal Numbers etc. This method can be used by PSTN/ISDN calls as well as IN calls.

   NOTE: With the E.164 numbers related to a call, at least CPN, CdPN, OCN, RDN are meant.

Implementation option B.1 in annex B uses this method.

The number based intercept triggering function (LI) triggers on numbers, not the access. That is why the LI can handle originating, terminating and transit calls in the same way. The numbers examined by LI are at least the common numbers, here described with their ISUP terms:

- Called Party Number (CdPN);

- Calling Party Number (CPN);

- Originally Called Party Number (OCN);

- Redirecting Number (RDN).

A.3.3   Service Based trigger

For Service based triggering the Service Control Function (SCF) or Service Data Function (SDF) may store the LI list of intercepted target identities. The LI list may be interpreted as one of the following: e.g. a list in the SCF may be used, or a mark in the service subscriber profile may be used.

This means that all IN calls can be intercepted, when the SCF instructs the SSF set up interception of the specific call. E.g. Freephone Numbers, Personal Numbers, Calling Cards etc.

Implementation options B.2 to B.7 in annex B use this method.

A.4   Issues

This section identifies some of the key issues considered in the creation of the present document.

1) In order to implement interception of IN calls additional functionality may be required in the IN entities.

2) Any LI data sent over INAP is visible to all parties with the capability to monitor SS7 traffic, for example Fraud management personnel. The INAP operation/parameter carrying the LI data could be encrypted. However, this method has a security issue, since not many calls would have to be made before it is possible for previously mentioned SS7 monitoring personnel to uniquely determine who is the intercepted target. It is also possible to use an alternative signalling path specifically for LI data.

3) There is a need to minimize the impact on the IN standards, if LI Data is to be included in some existing/new INAP operation.

4)   Network redirection algorithms, e.g. Optimal routing, could automatically route calls via alternative network nodes and bypass the original SSP which triggered the IN service. Hence the call may also bypass the interception point if it is associated with this SSP.

5)   In principle if any signalling parameters are altered by an IN service the change should be notified to the LEMF. For example if UPT is interpreted as a diverted call in IN, the Calling Party number can be exchanged for the UPT number. Thus the UPT outgoing call may also be captured by the Number Based method. The ETR 164 [15] regarding handling of Calling Party Number in the INAP-ISUP interaction has to be taken into account.

A.4.1   Subscriber controlled input:

It is possible for IN services subscribers to control aspects of the services directly from the users terminal, e.g. Call diversion destination number. This interaction can be enabled by the Specialized Resource Function (SRF), the Service Management Function, etc. When required this information needs to be intercepted and transferred to the LEA via the Handover Interface, refer to ES 201 671 [**3**].

This may mean that the following methods can be applied:

1)   via the HI3 by direct interception of In-band signalling on the call connection;

2)   via the HI2 interface after the IN-Service application has processed the service control input from the subscriber. This information may be service specific.

Annex B (informative):
Implementation options for the generic functional model

This annex identifies some implementation possibilities for the generic functional model. For the detailed options the characteristics are identified.

B.1   SCP with no LI related functionality

For this option, it is assumed, that no LI related functionality will be implemented in an SCP. The assumed mapping of the functional components to physical entities will be as given in the following diagram:
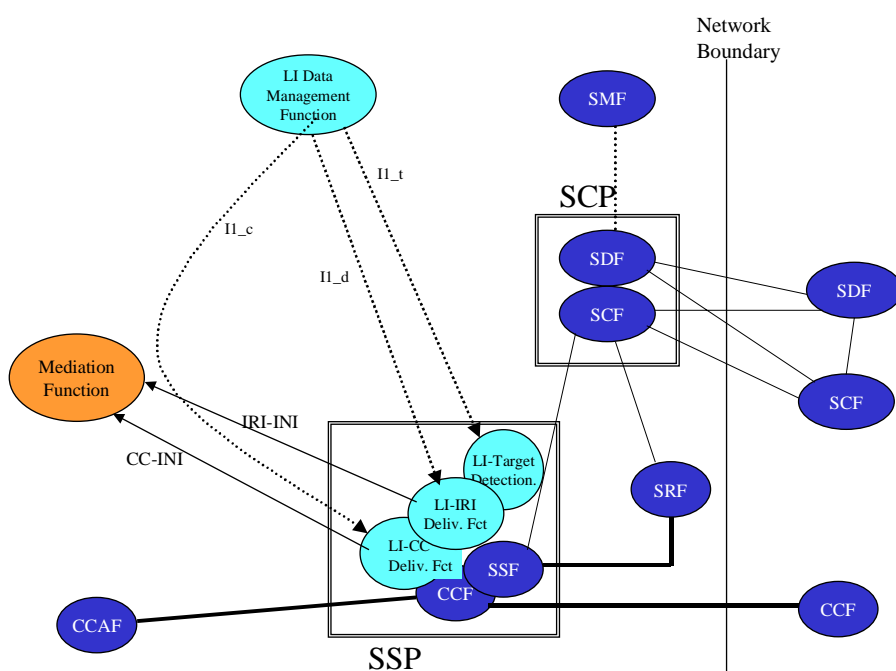
Figure B.1

B.1.1   Characteristics

Correlation (note 1)	HI2 and HI3 coming from **different** CCF/SSF may not be correlated (only time as indicator)
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Not available
Multiple IN from different CCFs	May result in multiple HI3 delivery. Other effects: see correlation
Calls spanning several networks	May result in multiple HI3 delivery. Other effects: see correlation (note 2)
Standardization	No Work required
Effected Network entities	All SSPs
Effect on New IN-Service deployment	Yes, all SSPs need SW and/or data changes
NOTE 1:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.
NOTE 2:	Each Network needs to receive HI1 data.

B.2   Limited LI functionality in SCP

For this option, it is assumed, that LI related functionality in the SCP will not have access to monitoring order details. The SCP will be able to extract LI-trigger information, but will not start LI and will not provide IRI. The assumed mapping of the functional components to physical entities will be as given in the following diagram:
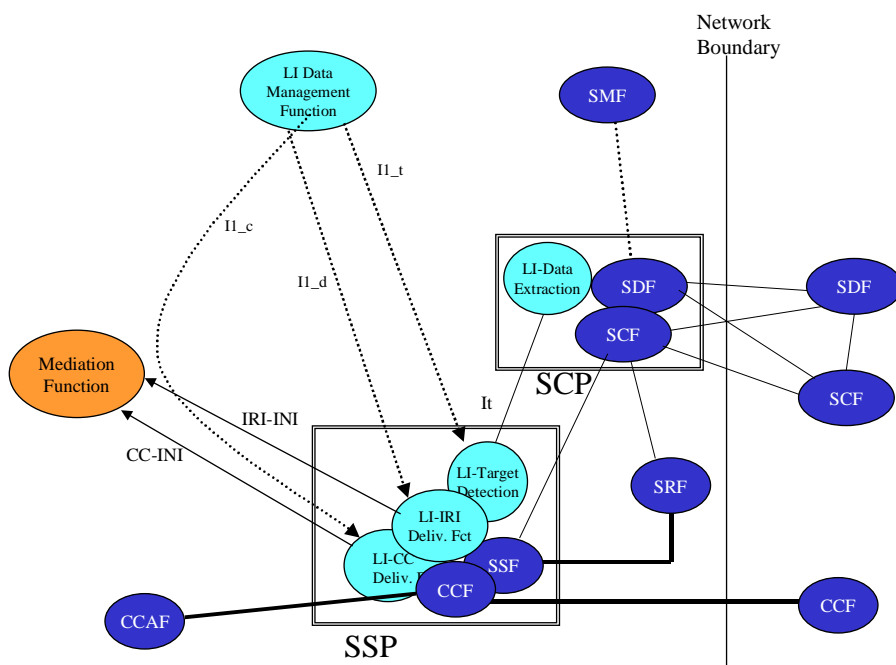

Figure B.2

B.2.1   Characteristics

Correlation (note)	HI2 and HI3 coming from **different** CCF/SSF may not be correlated (only time as indicator).
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Not available
Multiple IN from different CCFs	May result in multiple HI3 delivery. Other effects: see correlation
Calls spanning several networks	May result in multiple HI3 delivery. Other effects: see correlation Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the It interface
Effected Network entities	All SSPs and SCPs
Effect on New IN-Service deployment	Yes, all SSPs need SW and/or data changes Yes, all SCPs need modifications
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.

B.3   LI functionality in SCP, NO LI related signalling between CCFs

For this option, it is assumed, that LI related functionality in the SCP will have access to monitoring order details. It is assumed that CID is not supported by the Ii interface. The assumed mapping of the functional components to physical entities will be as given in the following diagram:

Figure B.3

B.3.1   Characteristics

Correlation (note)	HI2 and HI3 coming from **different** CCF/SSF may not be correlated (only time as indicator) IRI coming from SCF/SDF/SMF may not be correlated.
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Will be available, but possibly not correlated (see correlation)
Multiple IN from different CCFs	May result in multiple HI3 delivery. Other effects: see correlation
Calls spanning several networks	May result in multiple HI3 delivery. Other effects: see correlation Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the Ii interface
Effected Network entities	All SSPs and SCPs will be effected
Effect on New IN-Service deployment	Yes, all SCPs need SW and/or data changes No effect on the SSPs
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.

B.4   LI functionality in SCP, LI related signalling between CCFs

For this option, it is assumed, that LI related functionality in the SCP will have access to monitoring order details. Intercepted calls will be rerouted by normal IN behavior to a specified switch, which then handles LI. In addition it is assumed, that no CID is available on the Ia interface. The assumed mapping of the functional components to physical entities will be as given in the following diagram:

Figure B.4

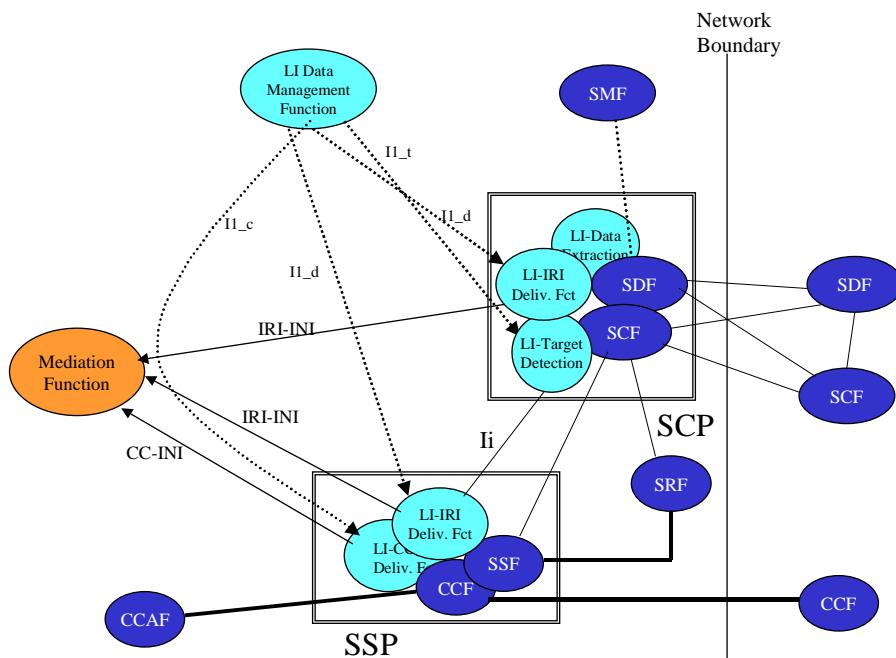## B.4.1   Characteristics

Correlation (note)	HI2 and HI3 coming from **different** CCF/SSF may not be correlated (only time as indicator) IRI coming from SCF/SDF/SMF may not be correlated.
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Will be available
Multiple IN from different CCFs	May result in multiple HI3 delivery. Other effects: see correlation
Calls spanning several networks	May result in multiple HI3 delivery. Other effects: see correlation Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the Ia interface
Effected Network entities	All SCPs, in addition the SSPs which deliver CC-INI and IRI-INI
Effect on New IN-Service deployment	Yes, all SCPs need SW changes, in addition all SSPs which deliver CC-INI and IRI-INI may be effected
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.

B.4.2   Limitations

This implementation architecture may result in loss of LI (CCC) in cases, where the IN disconnects and re-establishes call halves after the setup of the CCC links.

B.5   LI functionality in SCP, related signalling between CCFs

For this option, it is assumed, that LI related functionality in the SCP will have access to monitoring order details. It is assumed that all Interfaces are fully supported. The assumed mapping of the functional components to physical entities will be as given in the following diagram:

Figure B.5

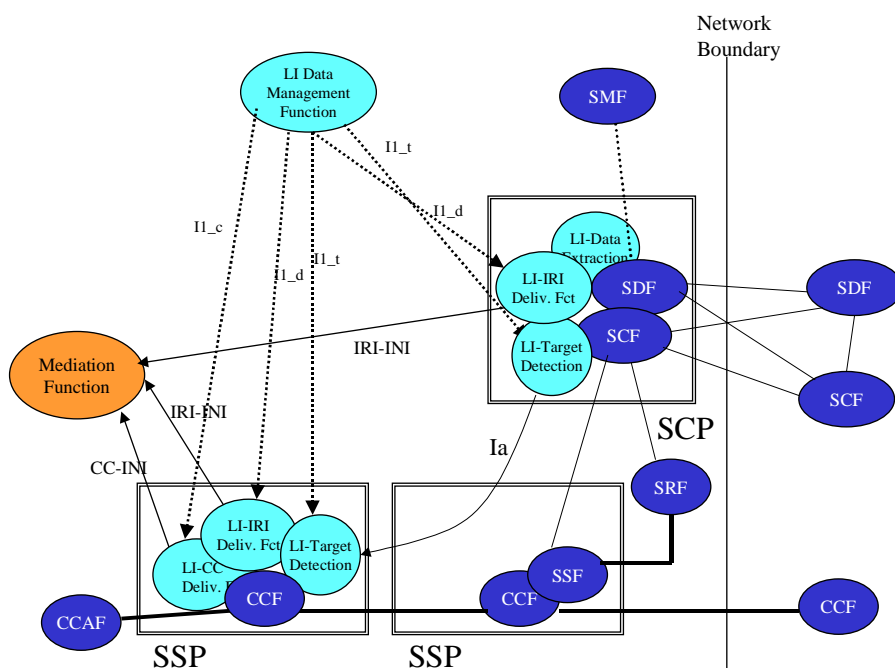## B.5.1   Characteristics

Correlation (note)	Available
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Will be available
Multiple IN from different CCFs	May result in multiple HI3 delivery. Depending whether LI active information is transferred
Calls spanning several networks	May result in multiple HI3 delivery. Depending whether LI active information is transferred Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the Ia and Ii interface
Effected Network entities	All SSPs and all SCPs
Effect on New IN-Service deployment	Yes, all SSPs need SW and/or data changes Yes, all SCPs need modifications
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order

B.6   LI functionality in LI Service Application on SCP

For this option, it is assumed, that LI related functionality is implemented in a new LI service, written in IN style to run on all the SCPs. The LI service employs a new Intelligent Peripheral device, "LI Gateway" which provides an interception point for the Call Content. This gateway also contains all the LI Delivery data. Hence the SSP has no LI specific components.

It is assumed that all Interfaces are fully supported. The assumed mapping of the functional components to physical entities will be as given in the following diagram:
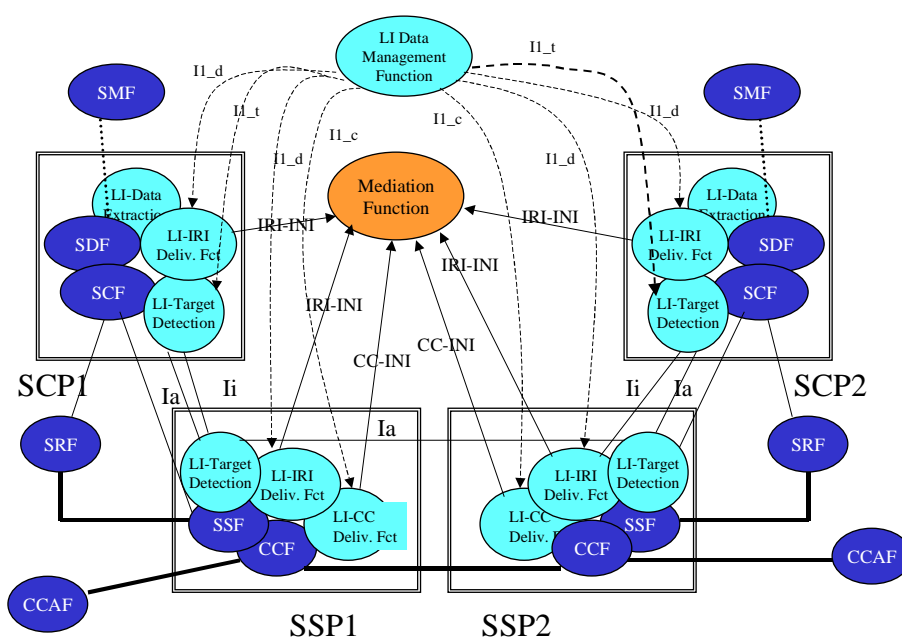

Figure B.6

B.6.1   Characteristics

Correlation (note)	Limited, see below
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Will be available
Multiple IN from different CCFs	May result in multiple HI3 delivery. Depending whether LI active information is transferred
Calls spanning several networks	May result in multiple HI3 delivery. Depending whether LI active information is transferred Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the Ic Interface
Effected Network entities	A NEW entity is introduced (LI-Gateway) All SCPs require to run the LI-Service
Effect on New IN-Service deployment	Yes, all SCPs
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.

B.6.2   Limitations

This implementation architecture may result in loss of LI (CCC) in cases, where the IN disconnects and re-establishes call halves after the setup of the CCC links.

Correlation is only available, if the identifier used to provide correlation information is generated in a centralized Network application, to which the LI service has access.

B.7   LI functionality in SCP, NO LI related signalling between CCFs

For this option, it is assumed, that LI related functionality in the SCP will have access to monitoring order details. It is assumed that CID is not supported by the Ii interface. In addition it is assumed, that there will be no IRI-delivery function implemented in the SCP. The assumed mapping of the functional components to physical entities will be as given in the following diagram:
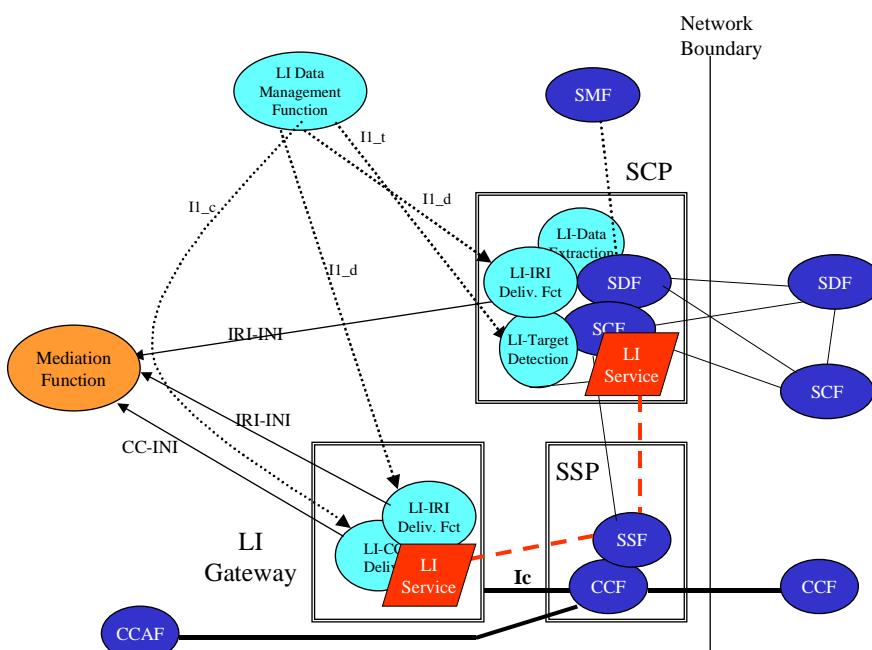
Figure B.7

B.7.1   Characteristics

Correlation (note)	HI2 and HI3 coming from **different** CCF/SSF may not be correlated (only time as indicator)
Multiple LI on one subscriber	Possible, identified as for non-IN calls
Simultaneous calls of monitored subscriber	Possible, identified as for non-IN calls
Non call related IRI (e.g. profile changes)	Will be available, but possibly not correlated (see correlation)
Multiple IN from different CCFs	May result in multiple HI3 delivery. Other effects: see correlation
Calls spanning several networks	May result in multiple HI3 delivery. Other effects: see correlation Note: each Network needs to receive HI1 data.
Standardization	Requires standardization of the Ii and Ir interface
Effected Network entities	All SSPs and SCPs will be effected
Effect on New IN-Service deployment	Yes, all SCPs need SW and/or data changes No effect on the SSPs
NOTE:	Correlation refers to correlation between the different IRI information sent from different SSPs for one call. It does **not** refer to the correlation of the IRI to the respective court order. Missing correlation in this sense will especially be a problem, if more than one call is active at the same time for the same court order.

Annex C (informative):
Interface Data Description

C.1   Common Data Types

The following data types are already defined in other standardization documents, and therefore, they are not redefined here:

Reference	Title of document	Data type
ES 201 671 v.1.1.1 (1999-07) [3]	Telecommunications Security; Hand-over interface for Lawful Interception of telecommunications traffic	CallIdentifier LawfulInterceptionIdentifier
ETS 300 374-1 ed.1 (1994-09) [16]	Intelligent Network (IN); Intelligent Network Capability Set 1 (CS1); Core Intelligent Network Application Protocol (INAP); Part 1: Protocol specification	ServiceKey LegID

The following common data types are needed for the Lawful Interception (LI) activity:

-- FurherSpecOfTypeOfInterception Type

FurtherSpecOfTypeOfInterception ::= BIT STRING {
                    iRI (0),
                    cC (1),
                    stereo (2),   -- Default: mono
                    optionA (3)   -- Default: Option B
                    }
-- Explanation: iRI and cC provide the information, whether IRI and CC are requested.
--   Stereo indicates indicates, whether the cC needs to be delivered in stereo or mono mode
--   optionA indicates, that Option A shall be used, where option A and B exist.

-- LeaRequirementsList Type

 -- This parameter is used to pass information concerning the LI function to be started in the receiving side.
 -- It is assumed that only the sending side is able to decide if the LI function has to be started or not.

LeaRequirementsList ::= SET OF (SIZE 1..3)   -- max. 3, see ES 201671, A.3
                    SEQUENCE {   -- see ES 201 671, 7.1
                    lawfulInterceptionIdentifier   [0] LawfulInterceptionIdentifier,
                    furtherSpecOfTypeOfInterception   [1]
FurtherSpecOfTypeOfInterception,
                    hI2DestAddress   [2] LemfAddress **OPTIONAL**,
                    hI3DestAddress   [3] LemfAddress **OPTIONAL**,
                    otherNetwork-dependantParam   [4] **BIT STRING** {
                                locationInformation (0)
                                -- others to be defined
                                }
                    }
-- Explanation: lawfullInterceptionIdentifier: see ES 201 671, A.9

-- LemfAddress Type

LemfAddress ::= CHOICE {
                    e164-Number   [0] **OCTET STRING (SIZE 1..25),**
                    x25-Number   [1] **OCTET STRING (SIZE 1..25),**

ETSI

```
                 iP-Address              [2] OCTET STRING (SIZE 1..25),
                 otherAddress            [3] OCTET STRING (SIZE 1..25)
                                            -- e.g. individual agreed address
                 }
```

-- LiAssociatedData Type

```
LiAssociatedData ::= CHOICE {
                 triggerInformation      [0] TriggerInformation,
                 leaRequirements         [1] LeaRequirementsList
                 }
```

-- LiCorrelationID

   -- The definition below is exactly the same as used in the TCAP protocol for the TCAP Transaction
Identifier.

```
LiCorrelationID ::= IMPLICIT OCTET STRING (1..4)
```

-- INServiceSpecificHi2Data Type

 -- This parameter is used as a container to send HI2 information from the SCP to the LEMF via the SSP

```
INServiceSpecificHi2Data ::= OCTET STRING (SIZE 1..64)
```

-- SignallingPartyId Type

```
SignallingPartyId ::= ENUMERATED  {
                 unknown  (0 ),
                 aParty  (1 ),
                 bParty  (2 )
                 }
```

-- TriggerCriteria Type

```
TriggerCriteria ::= ENUMERATED  {
                 unknown  (0 ),
                 IsLIID  (1 ),
                 IsCreditCardNr  (2 )
                 InbandDN (3)
                 }
```
 -- This type shall be expanded as new Trigger Criteria Types are identifed
 -- Numbers from 0 to 1000 shall be allocated by a standardization body
 -- Numbers from 1001 to 9999 shall be allocated by a national regulatory agencies
 -- Numbers above 10000 shall be mutually agreeable between operators

-- Explanation: This type identifies the type of triggerinformation, which is send.

-- TriggerInformation Type

 -- This parameter is used to pass information concerning the target identification. It is assumed that
 -- the receiving side is able to decide autonomously if the LI function has to be started or not.

```
TriggerInformation ::= SEQUENCE  {
                 triggerCriteria         [0] TriggerCriteria DEFAULT IsLIID,
                 criteria                [1] GenericDigits,
                 callIdentifier          [2] CallIdentifier OPTIONAL
                 }
```

C.2   It Interface

The data element sent on this interface shall be the TriggerInformation.

C.3   Ii Interface

-- LiRequest Type

LiRequest ::= SEQUENCE {
        partyInfo   [0] LegID,
        liAssociatedData   [1] LiAssociatedData
        }

Explanation of the data elements :

partyInfo is used to tell the receiving side which party has to be considered as the LI target. A typical example is the follow-on call configuration; if the target is the controlling leg, all following calls have to be intercepted continuously. If the target is the passive leg, the interception is stopped for following calls with different called parties.

liAssociatedData contains the associated information to launch the LI activity. Two options are possible, depending on the agreement between the SCP and the SSP:

- the receiving side can always decide autonomously if LI has to be started for the current call. This means that the LI data are stored on **both**, the sending side and the receiving side of the interface;

- the sending side (SCP or SSP) indicates to the other side all the associated information (LIID, LEMF address, etc.). This means that the LI data are stored **only** on the sending side of the interface.

C.4   Ia Interface

-- LiInfo Type

LiInfo ::= SEQUENCE {
        liRequired   [0] **BOOLEAN**,
        cCcaptured   [1] **BOOLEAN,**
        callIdentifier   [2] CallIdentifier,
        signallingPartyId   [3] SignallingPartyId **DEFAULT** unknown,
        lawfulInterceptionIdentifier   [4] LawfulInterceptionIdentifier,
        leaRequirements   [5] LeaRequirementsList **OPTIONAL**
        }

C.5   Ir Interface

The data element sent on this interface shall be the INServiceSpecificHi2Data.

C.6   Ic Interface

The information sent on this interface shall be the bearer content.

C.7   LI data on the SCP-SSP interface

C.7.1   LI data over the INAP protocol

The INAP protocol is used only as a transport mechanism to convey LI data. From the point of view of the INAP definition, only an LI dedicated container shall be specified, as described below:

> -- LiContainer Type

LiContainer {PARAMETERS-BOUND : bound} ::= **OCTET STRING (SIZE(**
bound.&minLIDataLength..
bound.&maxLIDataLength))

Thus, the impact of the Lawful Interception activity on the INAP protocol definition shall be limited to the following type of specification :

> -- extensionLiContainer

extensionLiContainer **EXTENSION** ::= {
&ExtensionType   LiContainer,
&criticality   CriticalityType,
&id   local: x or global: with ETSI object identifier (to be assigned by SPAN3)

}

-- In case the SSP/SCP has received this parameter, the LI activity for that call is started.
-- Extension is applicable to any INAP operation where the extension parameter has been defined.

Clearly, one major advantage is that the proposed evolution has to be applied only once to the INAP protocol specification.

The criticality of this new extension parameter (abort/ignore) shall be left under the customer responsibility, since the value of this option is directly related to the application context definition.

In principle, any INAP operation could be used to carry the LI data; in general, the principle is to use always "the next INAP operation to be sent", since the LI data is completely independent of the INAP interface.

However, a given implementation could limit the LI data to some INAP operations only. The following INAP operations are considered as the minimum subset using this new parameter to launch the LI activity, either in the SSP or in the SCP:

- Connect;

- Continue With Arguments;

- Initial DP;

- Initiate Call Attempt;

- Request Report BCSM Event.

This set of INAP operations allows to cover almost all the possibilities of dialogue between the SCF and the SSF, including the phases where the SSF is waiting for instructions from the SCF.

The LI activity request should be taken into account immediately in the SSP (respectively the SCP), after receipt of an INAP operation carrying the parameter LiContainer.

The acceptability of the LiContainer parameter at both ends of the INAP interface can be easily handled via the application context name mechanism, and its associated negotiation procedures.

The INAP protocol can be used to send two different types of LI data, as follows:

- Information related to LI triggering in the receiving side, as described for the Ii interface.

- IN service specific information to be sent from the SCP to the LEMF (HI2 data), via the SSP. When using this option, the HI2 interface is not needed in the SCF. The latter sends its specific information to the SSP who generates the corresponding HI2 message, adding the common information as the lawful interception identifier, the call identifier, the time stamp (a single source for time stamp), etc. This option allows also to be fully inline with the principle of "single point of contact for multi-entity services".

Thus, the container LiContainer can be redefined internally for LI purposes, as follows (this definition is not more related to the INAP protocol, even if the latter is used as the transport mechanism) :

```
-- LiData
```

LiData ::= CHOICE {
          liRequest   [0] LiRequest,
          inServiceSpecificHi2Data   [1] InServiceSpecificHi2Data
          }

C.7.2   LI data over a separate communication channel

When using a separate communication channel to carry the LI data, a correlation value is needed to associate the LI activity information to the communication having triggered the IN service logic.

As the INAP protocol is carried over TCAP, the most natural correlation identifier is the TCAP transaction identifier, whose value is well-known at both sides of the INAP interface : the SCF and the SSF. The main advantage of this choice is to re-use an existing identifier, and therefore, to avoid handling a supplementary correlation value, which has to be generated, recognized, protected, etc.

The service key value can also be used in order to solve any possible ambiguity with TCAP transaction identifiers, especially in the case where one SSP is connected to several SCPs.

Thus, the arguments of the message carrying the LI activity request can be defined as follows:

```
-- LiActivity
```

LiActivity ::= SEQUENCE {
          serviceKey   [0] ServiceKey,
          liCorrelationID   [1] LiCorrelationID,
          liData   [2] LiData
          }

It has to be noted that the LiData parameter is re-using exactly the same definition as in the case of the INAP protocol, as described in the preceding section. In both cases, this parameter is carrying exactly the same content.

For transport purposes, the LiActivity parameter can then be encapsulated using a normal ROSE Invoke component. The ROSE operation class is 5 ("Asynchronous, outcome not reported"), since neither a result nor an error component is expected.

Next, the ROSE component can now be carried also by a dedicated TCAP dialogue, since its definition is totally independent of the transport mechanism.

One major advantage of this type of solution is that there is no impact on the INAP interface. This can be especially important in the Camel Phase 2 environment, where the Continue With Arguments operation is not specified. A Camel IN server which has to request for LI activity, could be obliged to use either the Connect operation or the Request Report BCSM Event operation, as the Continue operation has no parameter.

As the LI information is carried separately, security and confidentiality issues can be handled independently of the INAP interface, and according to specific LI needs.

It has to be noted also that the only relation between both communication channels is a TCAP transaction identifier, which is a non-permanent type of information. Moreover, by definition, this correlation value is volatile, as its value is re-allocated for each dialogue between an SSF function and the triggered IN service logic.

Annex D (informative):
Topics for future work

D.1   Mutual legal assistance between LEAs

User requirements for a future mutual legal assistance between the LEAs of different countries are not covered and are for future studies.

D.2   Interworking with other countries

Interworking with other countries than those following the present document is for further study.

D.3   Interworking with other protocols

Interworking with other protocols is for further study.

D.4   CS-3

Changes and modification resulting from CS-3 are for further study.

D.5   CS-4

Changes and modification resulting from CS-4 are for further study.

D.6   CAMEL

Changes and modification resulting from CAMEL are for further study.

History

Document history		
V1.1.1	March 2000	Membership Approval Procedure MV 20000519: 2000-03-21 to 2000-05-19