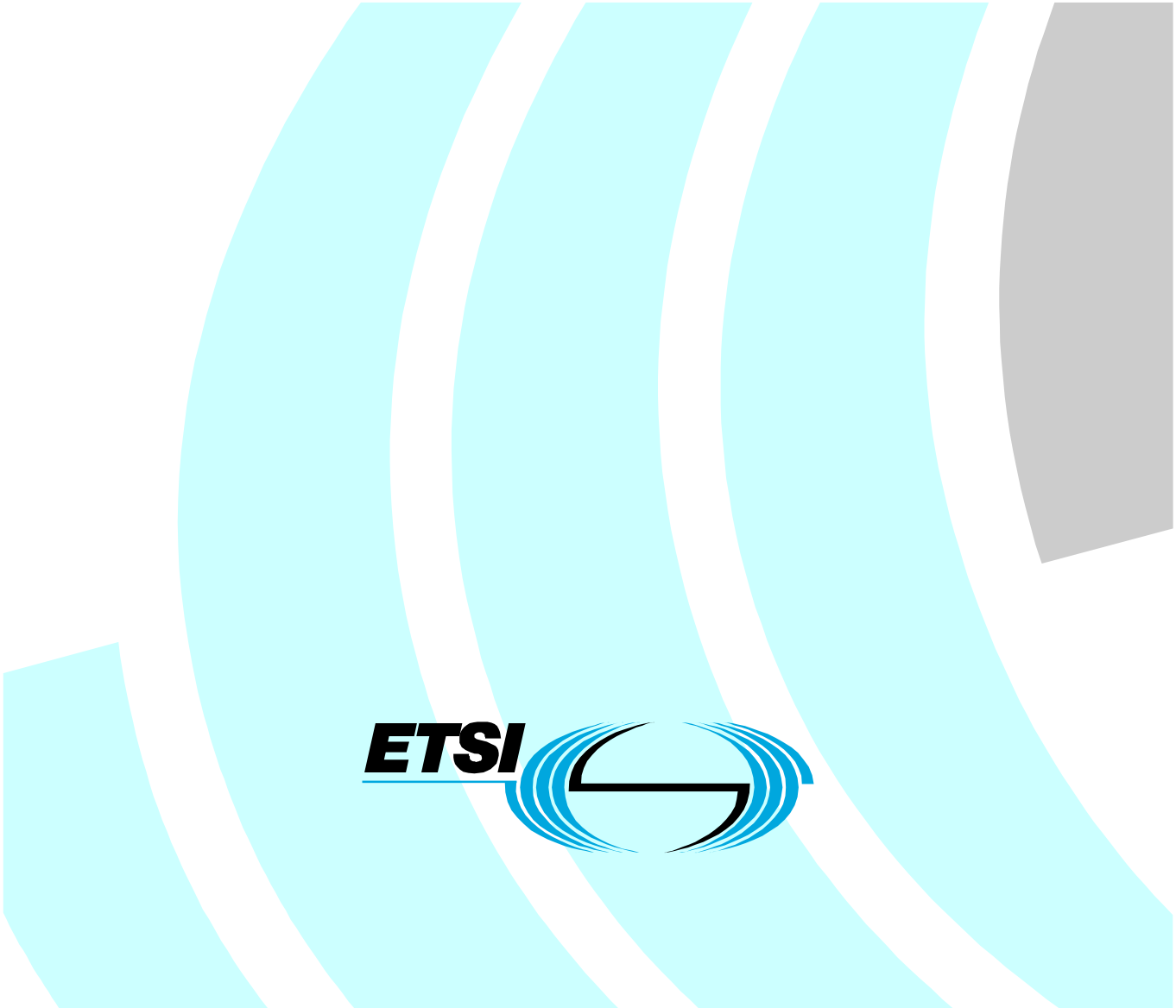
ETSI TS 102 227 V4.1.1 (2004-05)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception



Reference
DTS/ TISPAN-07002-TIPHON_R4

Keywords
IP, lawful interception, security,
telephony, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

The present document is a product in TIPHON™ Release 4 (see TR 101 301) of step D of the TIPHON™ development process described in TR 101 835.

The data definitions given in the present document are illustrative of the stage 3 requirement and are presented as ASN.1 for illustrative purposes.

1 Scope

The present document defines the intercept-related information to be derived from TIPHON™ release 4 networks, and its relationship to the LI framework.

The present document describes when messages are to be sent across the IRI reference point X2 and what they should contain.

The present document describes the information extracted from TIPHON™ systems and presented using the LI framework defined in [2] and [4].

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Capability Definition; Service Capabilities for TIPHON Release 4".

[2] ETSI TS 102 232 "Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery".

[3] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[4] ETSI TS 101 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[5] ETSI TS 101 882-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 1: Meta-protocol design rules, development method, and mapping guideline".

[6] ETSI TS 101 882-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 2: Registration and Service Attachment service meta-protocol definition".

[7] ETSI TS 101 882-3: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 3: TIPHON Simple Call service meta-protocol definition".

[8] ETSI TS 101 882-4: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 4: Media control Service meta-protocol definition".

[9] IETF RFC 3261: "SIP: Session Initiation Protocol ".

[10] ITU-T Recommendation H.248.1: "Gateway control protocol".

[11] ITU-T Recommendation H.323: "Packet-based multimedia communications system".

[12] ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[13] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[14] IETF STD 0007: "Transmission Control Protocol".

[15] IETR RFC 2126: "ISO Transport Service on top of TCP (ITOT)".

[16] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 671 [4] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 671 [4] and the following apply:

CC	Content of Communication
CCIF	Content of Communication Interception Function
IRI	Information Related to Interception
LEMF	Law Enforcement Mediation Function
LIAF	Lawful Intercept Administration Function
LIDF	Lawful Interception Delivery Function
LIF	Lawful Interception Function
SIP	Session Initiation Protocol

4 Background

The requirements for Lawful Interception of telecommunications are contained in TS 101 331 [16].

The building blocks for provision of the TIPHON™ Lawful Interception service are contained in TS 101 878 [1] as a set of service capabilities. The present document identifies how the service capabilities identified in TS 101 878 [1] are used in provision of the TIPHON™ Lawful Interception service. The present document also identifies how the meta-protocols defined in TS 101 882 provide data relating to interception and from the mappings and profiles of candidate protocols defined in TS 101 883 and TS 101 884 provide data content relating to interception.

The Lawful Interception service may be required in any or all functional groups within the TIPHON™ architecture.

NOTE: The present document is written with the assumption that within one Administrative Domain there will be only one functional group that implements Lawful Interception for a particular target entity.

The framework for lawful interception described in [2] defines aspects of the handover interface between a network operator and law enforcement agencies that are not specific to a particular network architecture or technology. This definition includes:

- identification of interception targets;
- identification of intercept access points;
- correlation between HI2 and HI3;
- time-stamping of intercepted events;
- session management on HI2 and HI3;
- reliability of handover interfaces;
- security of handover interfaces;
- mapping of handover information to physical interfaces.

5 Reference model for interception

5.1 Introduction

In figure 1 the overall reference model of TIPHON Lawful Interception is shown.

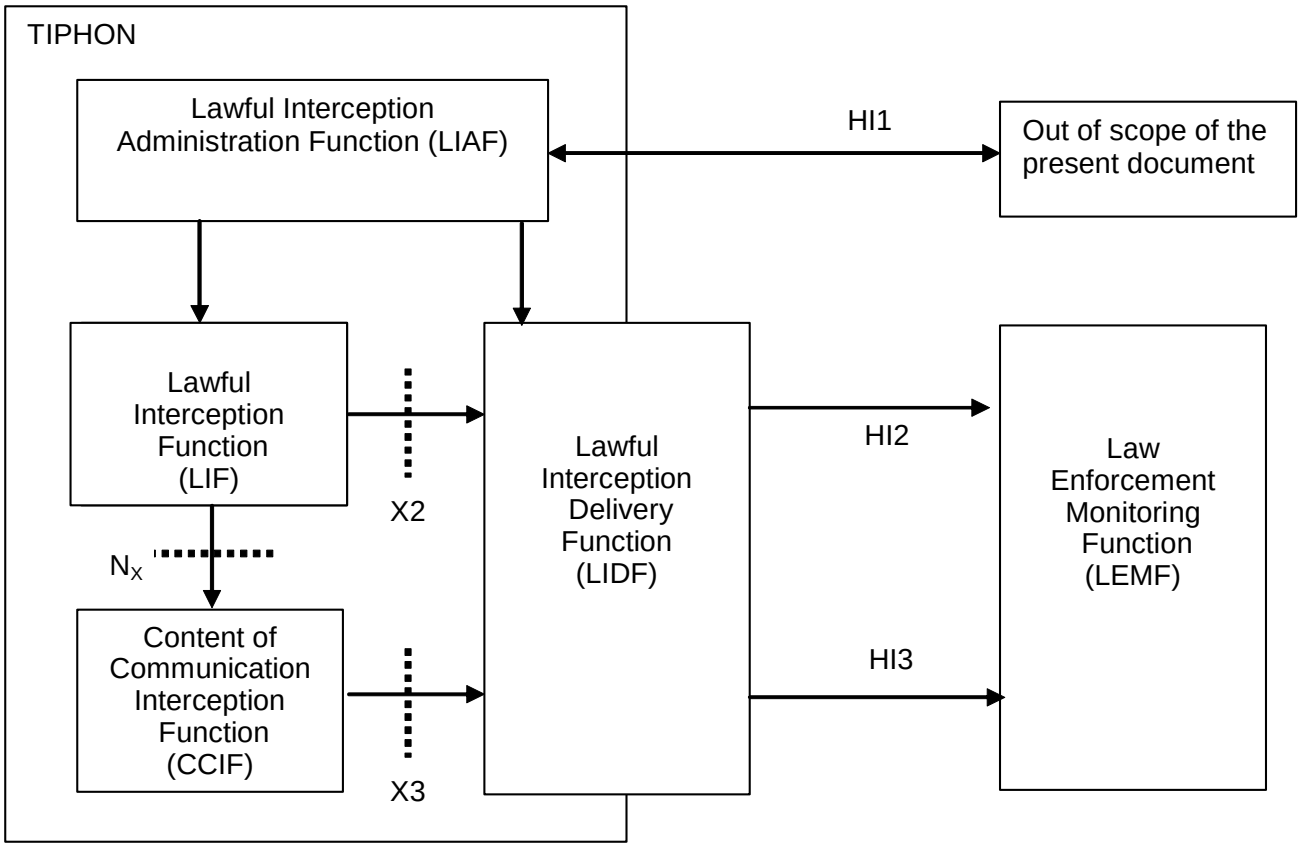


Figure 1: Reference model for lawful interception

Internal interface X2 carries Intercept Related Information (IRI) from the Lawful Interception function. Internal interface X3 carries Content of Communication (CC) information. The N_X interface carries control information to indicate where the CCIF should be activated and what address should be used to send the CC to the LIDF. The information carried across Nx may be appropriate for the Media Layer or Transport Layer implementations of the CCIF.

5.2 Description of functional elements

5.2.1 Lawful Interception Function (LIF)

The purpose of the Lawful Interception function is to generate information related to calls or and other information involving interception targets identified by a Law Enforcement Authority (LEA) sessions, i.e. Information Related to Interception (IRI).

The IRI information is sent to the Lawful Intercept Delivery Function (LIDF) to be delivered to the LEMF over interface HI2.

5.2.2 Content of Communication Interception Function (CCIF)

The Content of Communication Interception Function (CCIF) shall cause the content of communication to be duplicated and passed to the Lawful Interception Delivery Function. The content may be duplicated within the Media Layer or within the transport layer and this may be achieved by any means such that the sender and recipient(s) are unaware of the copying process and cannot take steps that will reveal the copying process is taking place.

The content of communication is sent to the Lawful Interception Delivery Function and it is formatted in accordance with later clauses for delivery to the LEMF over interface HI3.

5.2.3 Lawful Interception Delivery Function (LIDF)

Within each administrative domains which contains one or more of the functional groups specified in TS 101 314 [3] there shall be an additional functional entity - the Lawful Interception Delivery Function. This function receives information from the Lawful Interception function(s) within the administrative domains and formats them to be passed on to the Law Enforcement Mediation Function (LEMF) using the interface design specified in the Handover specification for IP Delivery [2]. If there is more than one Lawful Interception function within an administrative domain the Lawful Interception Delivery Function shall manage the reporting state of the call so that information is sent to the LEMF as if it were from a single Lawful Interception function. In this case the LIDF shall ensure that the reported information elements represent a consistent and single view of the intercept.

5.2.4 Lawful Intercept Administration Function (LIAF)

In each administrative domain there exists a Lawful Interception Administration Function (LIAF) to manage requests for interception . This function ensures that the request from an LEA to send IRI and or CC information to an LEMF is acted upon. This function is not the subject of the present document and it listed here for completeness.

The information available at the LIAF includes:

NOTE: This list is adapted from clause 7.1 of TS 101 671 [4].

- Identification of the interception subject (Target Identity).
- The agreed lawful interception identifier (LIID).
- Start and end, or start and duration, of the interception.
- Kind of interception information, i.e. IR, CC or both.
- Destination address of the LEMF to which IRI information should be sent i.e. the HI2 destination address (if applicable).
- Destination address of the LEMF to which CC information should be sent i.e. the HI3 destination address (if applicable).
- Other details related to the intercept such as the value of options.
- A reference for authorization of the interception.
- Other information as required.

This information is placed in the lawful Interception Function, Lawful Interception Mediation Function and Content of Communications Interception Function as necessary by means that are not described in the present document.

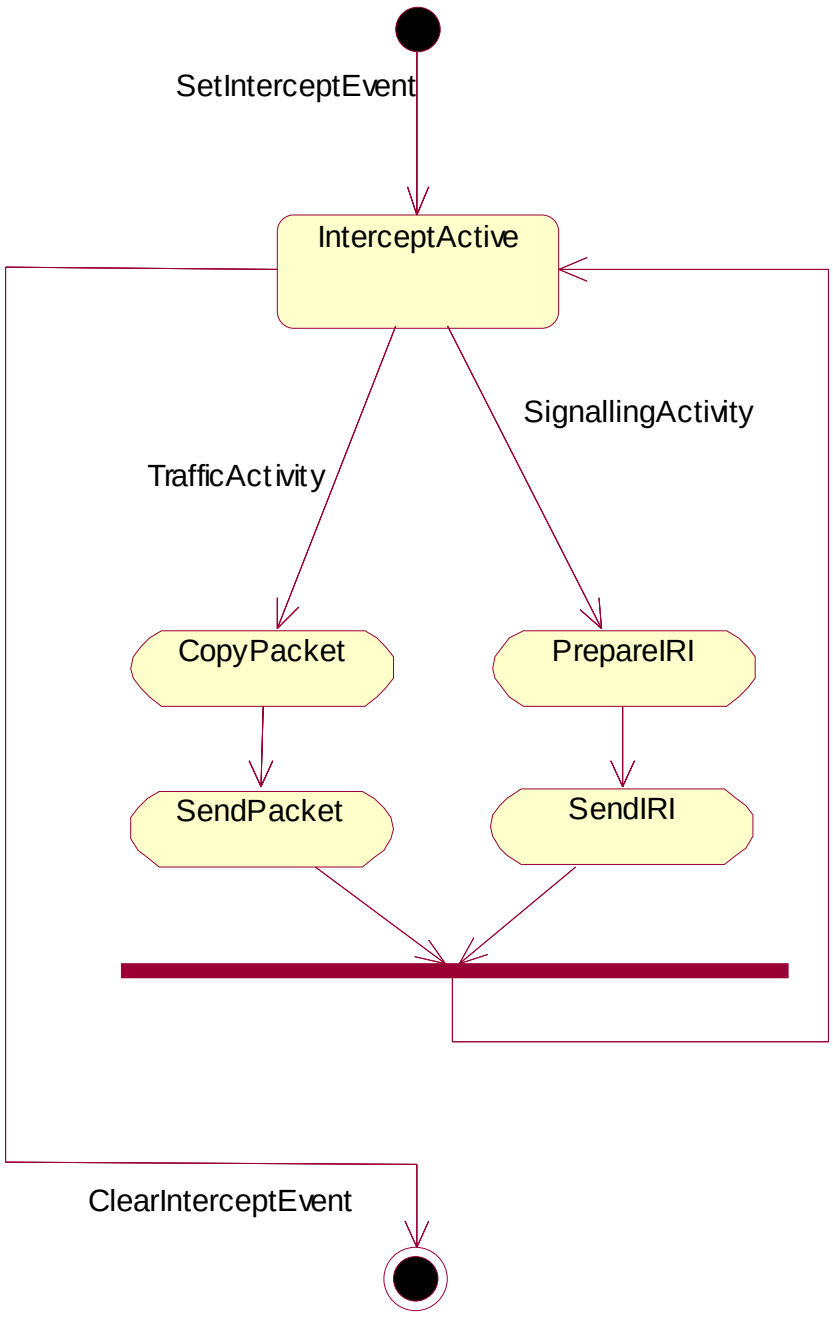


Figure 2: Simplified interception activity diagram

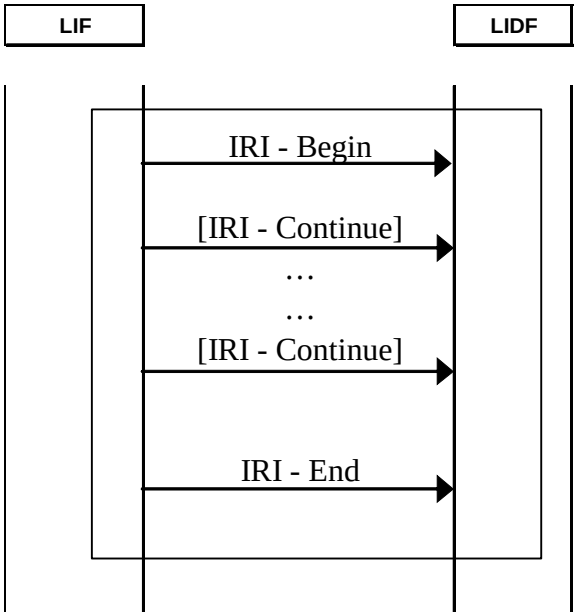
6 Interception of signalling

6.1 Interception protocol at interface X2

There are four kinds of record type used across X2, which are:

- begin-record;
- continue-record;
- end-record;
- report-record.

The first three of these record types form an IRI-transaction. A message sequence chart of the IRI protocol is shown in figure 3.



NOTE 1: The bordered area of the chart indicates an IRI-transaction
NOTE 2: The LIDF is often termed "mediation function"

Figure 3: IRI protocol sequence chart

The use of each IRI record types is defined by table 1.

Table 1: Use of IRI Record Types

Record Type	When record type is used
Begin	First event of a communication attempt, opening the IRI transaction
Continue	Any time during a communication or communication attempt within the IRI transaction
End	The end of a communication or communication attempt, closing the IRI transaction
Report	Used in general for non-communication related events

All signals in a TIPHON environment can be classified using set theory as below (see also figure 4):

$anySignal \in \{AllSignals\}$

$\{TransactionSignals\} \subset \{AllSignals\}$

$\{BeginSignals\} \subset \{TransactionSignals\}$

$\{EndSignals\} \subset \{TransactionSignals\}$

$\{ContinueSignals\} \subset \{TransactionSignals\}$

The sets {*BeginSignals*}, {*EndSignals*} and {*ContinueSignals*} in general should have no intersections, i.e. *anySignal* should only be a member of one of these sets.

NOTE: In some protocols, e.g. SIP, the set of message types is very small and the same message type may belong to more than one set but in such cases the content of the message determines to which set the message belongs. In other protocols, e.g. DSS1, the message type itself determines to which set the message belongs.

The logical processing model of interception is shown below:

IF $AnySignal \in \{BeginSignals\}$ THEN "prepare IRI-Begin record".

IF $AnySignal \in \{EndSignals\}$ THEN " prepare IRI-End record".

IF $AnySignal \in \{ContinueSignals\}$ THEN " prepare IRI-Continue record".

IF $AnySignal \notin \{TransactionSignals\}$ THEN " prepare IRI-Report record".

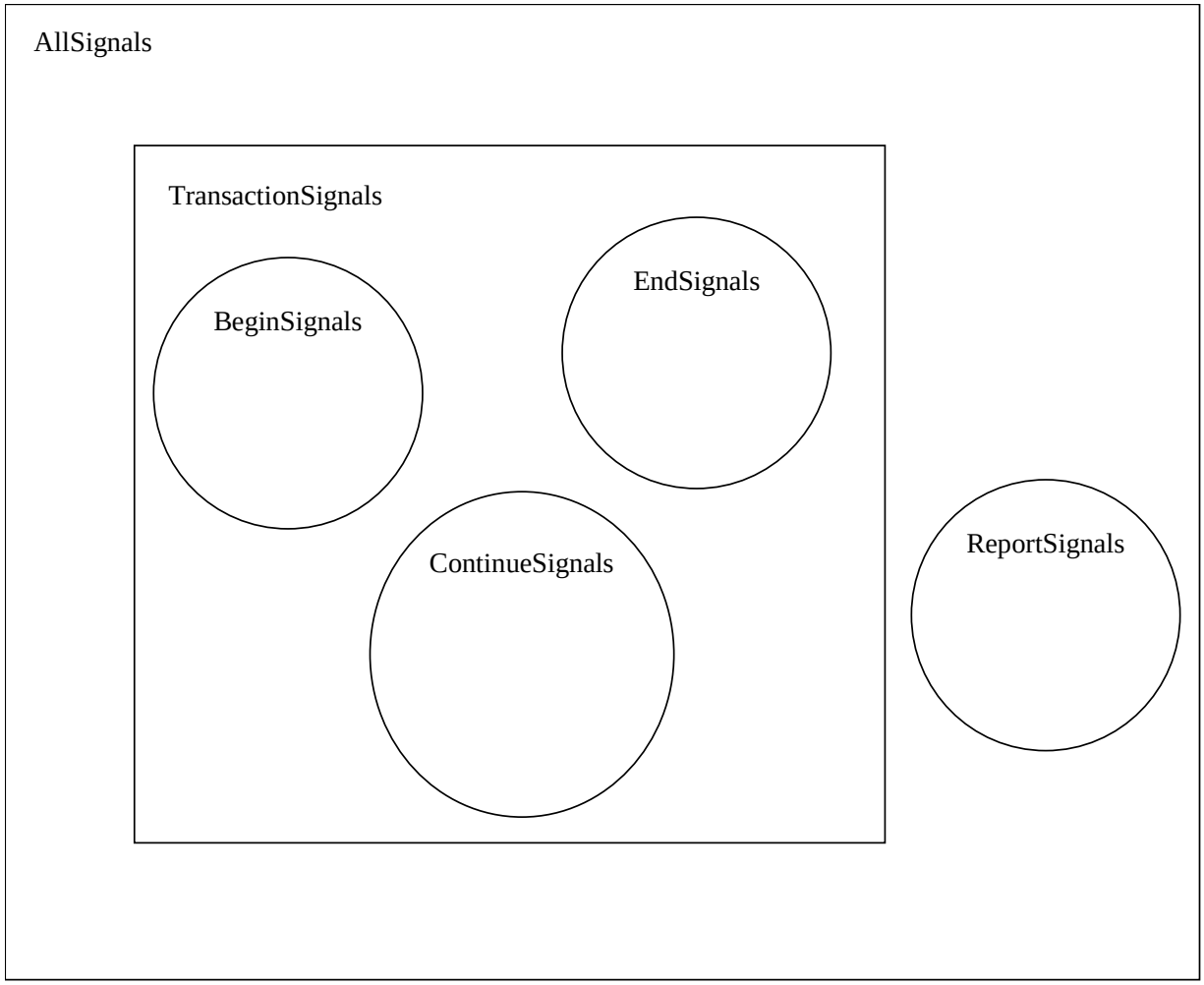


Figure 4: Ven diagram showing signal sets

6.2 Definition of IRI records

6.2.1 Begin record

The begin record is a confirmed flow internal to the system being intercepted.

6.2.1.1 Begin record request

Table 2: IRI Begin-record request

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF to which IRI data is to be sent
LIID	M	Lawful Interception Identifier
Correlation Number	M	Identifies this session of communication with the target
Protocol compatibility	M	Version of Meta-protocol for use by the LIDF
Direction	M	Original signal, either "towards target", or "from target"
Call Control Information	O	Note 1
Bearer Control Information	O	Note 1
Copy Flow Information	O	Information about the duplicated media flow on X3
SIP Information	O	Note 2
ITU-T Recommendation H.323 information [11]	O	Note 2
ITU-T Recommendation H.248.1 information [10]	O	Note 2
NOTE 1: At least one of Call Control Information and/or Bearer Control Information MUST be present. Information Elements should not be repeated if previously sent on the same correlation Number. NOTE 2: This Information is included if end to end information is sent but not represented in the meta-protocol information or if the administration requires it.		

If the IRI begin-record is sent as soon as the simple call service state machine moves from the "idle" state, then it occurs before the *route_response* has identified the destination. Full information on the media flow (and hence its mapping to the X3 flow) is not available until after a response from the media control layer has been received. The copy flow information is therefore shown as optional in the begin-record, but if omitted from the begin-record, it must be sent in a continue-record when it becomes available. Subsequent modification of the media paths is reported by sending new copy flow information.

6.2.1.2 Begin record response

Table 3: Begin record response

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; A string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Response	M	Accepted, Error detected, Cease transmission, resume transmission
Suspend duration	O	When Cease transmission is sent the expected duration for suspension, in seconds. See note.
NOTE: When Cease Transmission is required the duration should apply for all information flows for record types Begin, Continue and End		

6.2.2 Continue record

6.2.2.1 Continue record request

Table 4: Continue record request

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; A string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Protocol compatibility	M	Integer representing version of Meta-protocol for use by the LIDF
Direction	M	Original signal ; 0 = towards target, 1 = from target
Call Control Information	O	Note 1
Bearer Control Information	O	Note 1
Copy Flow Information	O	Information about the duplicated media flow on X3
SIP Information	O	Note 2
ITU-T Recommendation H.323 information [11]	O	Note 2
ITU-T Recommendation H.248.1 information [10]	O	Note 2
NOTE 1: At least one of Call Control Information and/or Bearer Control Information MUST be present. Information Elements need not be repeated if previously sent on the same correlation Number. NOTE 2: This Information is included if end to end information is sent but not represented in the meta-protocol information or if the administration requires it.		

6.2.2.2 Continue record response

Table 5: Continue record response

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; A string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Response	M	Accepted, Error detected, Cease transmission, resume transmission
Suspend duration	O	When Cease transmission is sent the expected duration for suspension, in seconds (see note)
NOTE: When Cease Transmission is required the duration should apply for all information flows for record typesBegin, Continue, End, and Report.		

6.2.3 End record

6.2.3.1 End record request

Table 6: End record request

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; a string parameter
Correlation Number	M	Identifies this session of communication with the target
Bearer ID	M	Bearer ID for the attempted connection
Timestamp	M	
Protocol compatibility	M	Integer representing version of Meta-protocol for use by the LIDF
Direction	M	Original signal ; 0 = towards target, 1 = from target
Call Control Information	O	Note 1
Bearer Control Information	O	Note 1
SIP Information	O	Note 2
ITU-T Recommendation H.323 information [11]	O	Note 2
ITU-T Recommendation H.248.1 information [10]	O	Note 2
NOTE 1: At least one of Call Control Information and/or Bearer Control Information MUST be present. Information Elements need not be repeated if previously sent on the same correlation Number. NOTE 2: This Information is included if end to end information is sent but not represented in the meta-protocol information or if the administration requires it.		

6.2.3.2 End record response

Table 7: End record response

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; a string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Response	M	Accepted, Error detected, Cease transmission, resume transmission
Suspend duration	O	When Cease transmission is sent the expected duration for suspension, in seconds. See note.
NOTE: When Cease Transmission is required the duration should apply for all information flows for record typesBegin, Continue, End, and Report.		

6.2.4 Report record

6.2.4.1 Report record request

Table 8: Report record request

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; A string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Protocol compatibility	M	Integer representing version of Meta-protocol for use by the LIDF
Direction	M	Original signal ; 0 = towards target, 1 = from target
Registration Information	O	Registration meta-protocol information elements

6.2.4.2 Report record response

Table 9: Report record response

Information element name	Mandatory/Optional	Description
LEMF ID	M	Identity of the LEMF, as a string, to which IRI data is to be sent
LIID	M	Lawful Interception Identifier; A string parameter
Correlation Number	M	Identifies this session of communication with the target
Timestamp	M	
Response	M	Accepted, Error detected, Cease transmission, resume transmission
Suspend duration	O	When Cease transmission is sent the expected duration for suspension, in seconds. See note.
NOTE: When Cease Transmission is required the duration should apply for all information flows for record types Begin, Continue, End, and Report.		

6.2.5 Concrete protocols

The ability to report concrete protocol information in the IRI is provided to prevent information being lost in mapping to meta-protocol format. Subject to national requirements to the contrary, not all messages received are copied to the IRI. Information elements from the concrete protocol shall be reported except:

a) Information elements from concrete protocols that only duplicate or repeat information reported via the meta-protocol should not be reported.

b) Information elements used solely for transport functions of the concrete protocol should not be reported.

c) Information elements that are conveyed only between nodes within the network and cannot be observed by users should not be reported.

d) Repeated information elements within concrete protocols should not be reported, provided that it was reported when it first arrived, or if it was subsequently changed.

NOTE 1: To avoid loss of information both the arrival of a concrete protocol signalling message, and the information it contains, must be reported. The message will typically contain a mixture of information that must be reported, and information that should not be reported. It is therefore not appropriate to insist that the entire signalling message is reported via the IRI.

Concrete protocol IRI shall report information elements from signalling messages, with the addition of a message identity parameter that identifies the most recent signalling message. This has the consequence that repeated information elements are reported only once. If the national option to send all concrete protocol information is not in force information elements that duplicate meta-protocol information shall be omitted.

NOTE 2: This technique avoids the need to recreate the entire signalling message in implementations where the concrete protocols are mapped to a proprietary internal representation.

When changes of state occur that cause a connection to be established that includes the target as either the originator or recipient (or if the originators intention was that the recipient was the target) of the media flow the LIF shall send the LEMF destination information across reference point N_X and cause the media flow to be copied. The LIF will determine by request from the Lawful Interception Delivery Function (LIDF) what IP address and port should be associated with the flow. The LIF will report this association immediately upon determining that a media flow has been requested, i.e. in the begin record or a continue record where a second connection is requested.

7 Interception of content of communication

7.1 Internal delivery of content of communication across interface X3

NOTE: The interception methods described here apply only when IP is used for streaming media.

7.1.1 Carriage of IP packets

When a copy flow request has been made in respect of a Media or Transport flow a copy of the media shall be sent to the LIDF. The source and destination address and ports shall be set in accordance with the information sent across the N_X reference point. The bit rate used for the copy flow shall be equal to or greater than that of the original flow.

The transport addresses may cause the transport plane to route the packets via the LIDF. The packets shall be conveyed by the transport plane to the LEMF. Provision of confidentiality mechanisms is outside the scope of the present document.

Media flows using a RTP/UDP/IP protocol stack shall have the header fields in the copy flow set as indicated in the clauses that follow.

7.1.1.1 RTP header

All fields in the RTP header shall be copied from the media flow packet.

7.1.1.2 UDP header

Table 10: UDP header data source

Header element name	Disposition
Source port	Set as directed via Nx
Destination Port	Set as directed via Nx
Length	Update to match copy packet with modified fields
Checksum	Update to match copy packet with modified fields

7.1.1.3 IPv4 header

Table 11: IPv4 header data source

Header element name	Disposition
Version	Set to ensure transmission to LEMF
Internet header length	Update to match copy packet with modified fields
Type of Service	Copy from media flow
Total Length	Update to match copy packet with modified fields
Identification	Copy from media flow
Flags	Copy from media flow
Fragment Offset	Copy from media flow
Time to live	Set to ensure transmission to LEMF
Protocol	Copy from media flow
Header Checksum	Update to match copy packet with modified fields
Source address	Set as directed via Nx
Destination address	Set as directed via Nx
Options - end of option list	Copy from media flow
Options - no operation	Copy from media flow
Options - security	Copy from media flow
Options - loose source route	Remove (note)
Options - strict source route	Remove (notes 1 and 2)
Options - record route	Copy from media flow
Options - internet timestamp	Copy from media flow
NOTE 1: These are removed to ensure they do not interfere with correct routing of the copy packet to the LEMF. NOTE 2: Since fields are either copied or removed, the copy packet size is never larger than the original media packet, and so there is no requirement for additional bandwidth for the copy flow, or danger of the copy flow exceeding network MTU.	

7.1.1.4 IPv6 header

Table 12: IPv6 header data source

Header element name	Disposition
Version	Set to ensure transmission to LEMF
Traffic Class	
Flow label	
Payload length	Update to match copy packet with modified fields
Next header	Update to match copy packet with modified fields
Hop limit	Set to ensure transmission to LEMF
Source address	Set as directed via Nx
Destination address	Set as directed via Nx
Extension Header - Hop-by-Hop Options	Remove (note)
Extension Header - Routing	Remove (note)
Extension Header - Fragment	Copy from media flow
Extension Header - Destination Options	Copy from media flow
Extension Header - Authentication	Copy from media flow
Extension Header - Encapsulating Security Payload	Copy from media flow
NOTE: These are removed to ensure they do not interfere with correct routing of the copy packet to the LEMF. Since fields are either copied or removed, the copy packet size is never larger than the original media packet, and so there is no requirement for additional bandwidth for the copy flow, or danger of the copy flow exceeding network MTU.	

```
CopyFlowType ::= SEQUENCE
{
-- Describes the relationship between the original user-user media flow and
-- the copied flow sent over HI3. Flows may be started, stopped, or modified
-- at any point during the call.

    BearerID                    VisibleString,
    copyFlowAction              CopyFlowActionType,
    hi3Destination              IPAddressType,
    hi3Source                   IPAddressType,
    originalDestination         IPAddressType,
    originalSource              IPAddressType
}

CopyFlowActionType ::= ENUMERATED
{
    createFlow,
    modifyFlow,
    deleteFlow
}

CopyFlowStatisticsType ::= SEQUENCE
{
-- Periodic report of statistics generated by the CCIF about a copy flow
-- Used by the LEMF to detect disruptions to the copy flow between CCIF and LEMF
    bearerID                    VisibleString,
    packetCount                 INTEGER,
    octetCount                  INTEGER,
    checksum                    INTEGER
}
```

Annex A (normative): Reporting of concrete protocols in IRI

A.1 Overview

The internal IRI contains knowledge of the actual protocol used by the target. This annex describes how the protocols in use by the target are reported over and above the meta-protocol report.

A.2 SIP

SIP [9] is a text based protocol whose syntax is defined in ABNF. It has a simple top-level structure as shown in the BNF fragment below.

```
SIP-message =  Request / Response
Request     =  Request-Line  *( message-header )  CRLF  [ message-body ]
Response    =  Status-Line   *( message-header )  CRLF  [ message-body ]

The SIP IRI defined below follows this structure to permit reporting of individual information
elements.
SipInformationType ::= SEQUENCE
{
    requestLine     OCTET STRING               OPTIONAL,
    statusLine      OCTET STRING               OPTIONAL,
    messageHeader   SEQUENCE OF OCTET STRING   OPTIONAL,
    messageBody     OCTET STRING               OPTIONAL
}
```

All information elements from SIP messages shall be reported except where they duplicate information reported via the meta-protocol, or are simply repeats of information already reported. Information elements that are transited by the functional element without interpretation must be reported.

A.3 H.323

H.323 uses a number of protocols [11], [12],[13]. The concrete protocol reporting scheme for H.323 identifies the protocol from which the information is derived by setting the value of information element H323InformationType:

```
H323InformationType ::= CHOICE
{
    h225RasInformation      H225RasInfoType,
    h225_q931Information    H225_q931InfoType,
    h245Information         H245InfoType,
    ...
}

H225RasInfoType ::= RasMessage                      -- from H.225.0

H225_q931InfoType ::= SEQUENCE
{
    q931Information     OCTET STRING    OPTIONAL,   -- from Q.931
    h225Information     H323-UU-PDU     OPTIONAL    -- from H.225.0
}

H245InfoType ::= MultimediaSystemControlMessage     -- from H.245
```

Messages that only have meaning within a single link, and do not influence call state (e.g. H.245 master/slave negotiation in a gatekeeper routed call) need not be reported.

The definitions above may be extended in future to permit reporting of messages from associated specifications such as H.235.

A.4 H.248

ITU-T Recommendation H.248.1 [10] uses both text and ASN.1 encoding. Since authentication headers and transaction handling are only significant on a single link, reporting of messages takes the form of the "action request" and "action reply" definitions.

```
H248InformationType ::= CHOICE
{
    h248TextInformation     [0] H248TextInfoType,
    h248BinaryInformation   [1] H248BinaryInfoType
}

H248TextInfoType ::= CHOICE
{
    actionRequest   [0]     OCTET STRING,
    actionReply     [1]     OCTET STRING
}

H248BinaryInfoType ::= CHOICE
{
    actionRequest   [0]     OCTET STRING,
    actionReply     [1]     OCTET STRING
}
```

Information that has already been reported via the meta-protocol, or which simply repeats information already reported may be omitted from the IRI. Information transited by the functional element without interpretation must be reported.

Annex B (informative): Handover considerations

Quote from TS 102 232 [2]:

"R1) The interface shall be able to handover communications content in the form of:

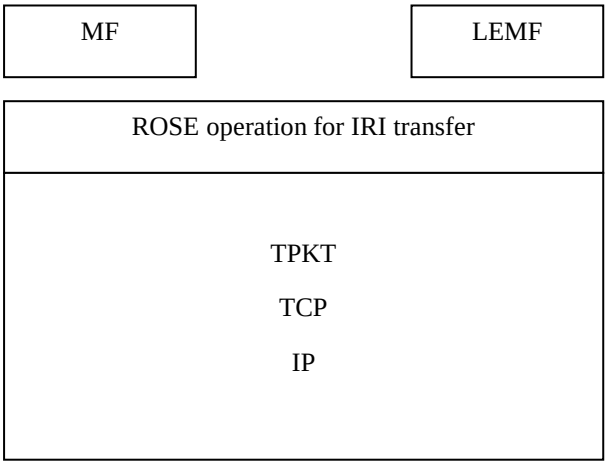
- *one or more datagrams (as per RFC 0791 [14] or RFC 2460 [22]);*
- *one or more application level PDUs (e.g. messages conforming to RFC 2821 [24] or RFC 2822 [25]).*

R2) The interface shall be able to handover:

- *intercept-related information associated with the CC noted above;*
- *intercept-related information which is not associated with CC (i.e. the interface should support IRI-only interception; see ES 201 671 [3], clause 7.1.4)."*

The IP handover specification defined by [2] containing the requirements stated above is restricted in scope to the provision of handover functionality for those packets conforming to a restricted list of IETF RFCs.

It is not clear how TS 102 232 [2] can be used to handover those IRI records defined in TS 201 671 [4] which make use of the ROSE operation over an SS7 stack. The proposal contained in this annex allows replacement of the SS7 stack for carriage of the defined ROSE operation by the widely implemented TCP stack and the TPKT protocol. This extends the capability of handover as below where TPKT+TCP+IP replaces the SS7 stack.



The ROSE operation defined in TS 201 671 [4] assumes use of the SS7 stack for transport. Where provision of an SS7 stack is inappropriate, for example in an IP network, ISO Transport Service on top of TCP (ITOT) [15], also referred to as TPKT, as defined in RFC 1006 and later updated by RFC 2126 [15] may be used as an alternative. This annex identifies the mode of operation required in using TPKT/ITOT as an alternative to the SS7 stack.

- Protocol class 0 defined in RFC 2126 shall be supported.

Annex C (informative): Management of X3 interface

The X3 interface is internal to the TIPHON system but acts to carry the content of communication from CCIF to LIDF. In order to ensure operation a number of actions have to occur and this annex suggest the form of information required to ensure successful operation of the X3 interface by provision of signalling across the Nx interface.

C.1 Address and port allocation for X3

This management flow prepares the X3 interface such that copies of Content of Communication can be sent in a timely manner. The operation determination of destination IP addresses and Ports in advance of a call event starting communications with a target. The allocation of the destination addresses that are available for use is depicted as a separate information flow.

Annex D (informative): Bibliography

ETSI TR 101 301: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Release Definition".

ETSI TR 101 835: "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); Project method definition".

IETF RFC 3219: "Telephony Routing over IP (TRIP)".

ETSI TS 101 883: " Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Technology Mapping; Implementation of TIPHON architecture using H.323".

ETSI TS 101 884: " Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Technology Mapping; Implementation of TIPHON architecture using SIP".

History

Document history		
V4.1.1	May 2004	Publication