OIPF

Feature Package

Lawful Intercept for IPTV

[V1.0] – [2014-06-02]

Open IPTV Forum

Open IPTV Forum

Postal address

Open IPTV Forum support office address
650 Route des Lucioles – Sophia Antipolis
Valbonne – FRANCE
Tel.: +33 4 92 94 43 83
Fax: +33 4 92 38 52 90

Internet
http://www.oipf.tv

Disclaimer

The Open IPTV Forum accepts no liability whatsoever for any use of this document.

Copyright Notification

Contents

Figures

Foreword

The present Feature Package introduces Lawful Interception capability to the OIPF IPTV solution.

Introduction

IPTV services are subject to varying degrees of regulatory provisions, including regulations on lawful interception.

Unlike traditional broadcast TV content delivery, IPTV enables advanced interactivity between the user and the service, and enables additional services with the possibility for interaction between users. This allows the creation of innovative services, like user generated content (UGC), or Social TV services blending content delivery with bi-directional communications and social networking capabilities between IPTV users.

The communications aspect of additional IPTV-based services puts them on the radar of lawful interception (LI) regulations. While the LI requirements vary from country to country (in some cases requiring interception of specific communications services, while others make any information exchange carrying intelligence of any kind subject to possible legal interception), most jurisdictions around the globe mandate lawful interception capability. Thus, a general LI capability is necessary for enabling wide deployability of the OIPF-based IPTV solution.

Lawful interception is being standardized in several standization organizations, addressing specific regional and technology related requirements of the law enforcement agencies. The most comprehensive specifications to date are produced by the ETSI Technical Committee Lawful Interception (TC LI), which is also working on aligning and incorporating the specifications created by other standardization organizations.

The present Feature Package adopts the ETSI TC LI specifications as a basis of the OIPF LI solution and discusses the extensions required to address the specifics of IPTV.

1 References

1.1 Normative References

1.1.1 Standard References

[102 232-1]	ETSI TS 102 232-1 V3.6.1 (2014-02), “Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery”
[102 232-3]	ETSI TS 102 232-3 V3.3.1 (2013-10), “Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services”
[102 232-5]	ETSI TS 102 232-5 V3.2.1 (2012-06), “Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services”
[102 528]	ETSI TR 102 528 v1.1.1 (2006-10), “Lawful Interception (LI); Interception domain Architecture for IP networks”
[101 331]	ETSI TS 101 331 V1.4.1 (2014-02), “Lawful Interception (LI); Requirements of Law Enforcement Agencies”
[101 671]	ETSI TS 101 671 V3.12.1 (2013-10), “Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic”
[201 158]	ETSI ES 201 158 V1.2.1 (2002-04), “Telecommunications security; Lawful Interception (LI);Requirements for network functions”

1.1.2 Open IPTV Forum References

[OIPF_SVCS2]	Open IPTV Forum, “Services and Functions for Release 2” V1.0, October 2008.
[OIPF_REQS2]	Open IPTV Forum, “Service and Platform Requirements” V2.0, December 2008.
[OIPF_ARCH2]	Open IPTV Forum, “Functional Architecture - V2.3”, January 2014.
[OIPF_OVIEW2]	Open IPTV Forum, “Release 2 Specification, Volume 1 – Overview” V2.3, January 2014.
[OIPF_AVC2]	Open IPTV Forum, “Release 2 Specification, Volume 2 – Media Formats” V2.3, January 2014.
[OIPF_HAS2]	Open IPTV Forum, “Release 2 Specification, Volume 2a – HTTP Adaptive Streaming” V2.3, January 2014.
[OIPF_META2]	Open IPTV Forum, “Release 2 Specification, Volume 3 – Metadata” V2.3, January 2014.
[OIPF_PROT2]	Open IPTV Forum, “Release 2 Specification, Volume 4 – Protocols” V2.3, January 2014.
[OIPF_PROTEX2]	Open IPTV Forum, “Release 2 Specification, Volume 4a – Examples of IPTV Protocol Sequences” V2.3, January 2014.
[OIPF_DAE2]	Open IPTV Forum, “Release 2 Specification, Volume 5 - Declarative Application Environment” V2.3, January 2014.
[OIPF_PAE2]	Open IPTV Forum, “Release 2 Specification, Volume 6 - Procedural Application Environment” V2.3, January 2014.
[OIPF_CSP2]	Open IPTV Forum, “Release 2 Specification, Volume 7 - Authentication, Content Protection and Service Protection” V2.3, January 2014.
[OIPF_PROF2]	Open IPTV Forum, “Profile Specification” V2.0, January 2014.
[OIPF_TSO]	Open IPTV Forum, “Test Specification Overview” V1.0, November 2010.

1.2 Informative References

[RFC2119]	IETF, RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”

2 Conventions and Terminology

2.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Introduction”, are normative, unless they are explicitly indicated to be informative.

2.2 Terminology

2.2.1 Abbreviations

In addition to the Abbreviations provided in [OIPF_OVIEW2], the following abbreviations are used in this Volume.

Acronym	Explanation
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CC	Content of Communications
CID	Communication Identifier
CIN	Communication Identity Number
CSP	Communications Service Provider
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LI	Lawful Intercept
LIID	Lawful Interception Identifier
SNS	Social Network Service
UGC	User Generated Content
UNI	User Network Interface

3 Architecture

ETSI TC LI has specified a general solution for the lawful interception for IP-based services. The solution defines the conceptual architecture of the lawful interception domain, as well as the service-specific details of interception of various IP based services, including the general and service-specific interfaces for the intercept data delivery to the law enforcement agencies.

As IPTV is, generally speaking, another IP-based service, the general provisions of the ETSI TC LI standards also apply to the IPTV interception. The purpose of the present Feature Package is to determine the necessary extensions to the ETSI specifications to cover the specifics of the OIPF IPTV solution.

The conceptual Lawful Interception architecture for IP-based networks defined by ETSI and applicable to the OIPF IPTV LI solution is shown in Figure 3.1.

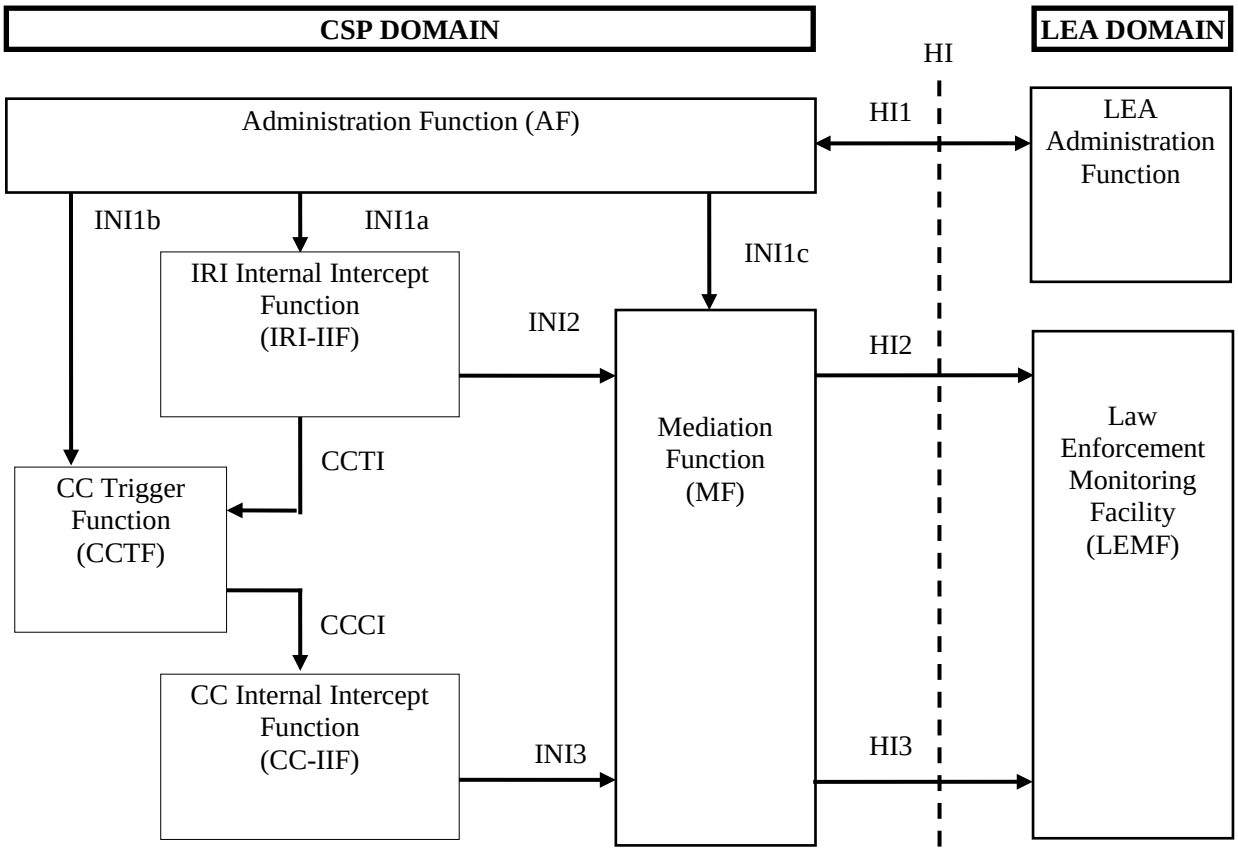

Figure 3.1: Reference Model for Lawful Interception (from ETSI TR 102 528 [102 528])

The reference model depicts the following functions and interfaces:

- Intercept Related Information Internal Intercept Function (IRI-IIF) generates signalling intercept material.
- Content of Communication Internal Intercept Function (CC-IIF) generates content intercept material.
- Content of Communication Trigger Function (CCTF) controls the CC-IIF.
- External interface HI2 carries Intercept Related Information (IRI) from the MF to the LEMF.

- External interface HI3 carries Content of Communication (CC) information from the MF to the LEMF.
- External interface HI1 carries intercept request information from LEA to the Lawful Interception Administration Function (AF).
- Internal interface INI1 carries provisioning information from the Lawful Interception Administration Function (AF) to the Internal Intercept Functions (IIF).
    - INI1a provisions Intercept Related Information Interception Function (IRI-IIF).
    - INI1b may (statically) provision CCs Control Function (CC-IIF).
    - INI1c provisions the Mediation Function (MF).
- Internal interface INI2 carries Intercept Related Information (IRI) from the IRI-IIF to the MF.
- Internal interface INI3 carries Content of Communication (CC) information from the CC-IIF to the MF.
- Content of Communication Trigger Interface (CCTI) carries trigger information from the IRI-IIF to the CCTF.
- Content of Communication Control Interface (CCCI) carries controls information from the CCTF to the CC-IIF.

The interfaces for LI in IP-based networks are defined in the ETSI TS 102 232 series of specifications.

3.1 Functional Entities

In the scope of the present Feature Package, the mapping of the LI functional entities onto the OIPF solution architecture components is discussed at the conceptual level. Definition of the exact locations of LI functional elements may be undesirable due to security requirements and should be left to the implementers' discretion. Based on this, the present Feature Package dwells on the generic LI architecture and keeps its main focus on the informational aspects of the interception, i.e., on the definition of the IPTV-specific handover interfaces.

The LI solution shown in Figure 3.1 is usually implemented as a stand-alone set of functional entities with as limited as possible integration with the functional architecture due to the operational and security requirements. The integration with the IPTV functional entities may be limited to the points where the service information and media flows have to be copied or observed for the purpose of creating the intercept material.

The functions requiring integration are the Internal Intercept functions IRI-IIF and CC-IIF.

No OIPF defined functional entities are impacted by the use of LI, which is implemented as a series of non-intrusive probes on existing reference points.

3.2 Reference Points

No OIPF reference points are impacted by this Feature Package and no additional reference points are required.

3.3 Signalling Flows

Signalling flows for LI handover interfaces are described in the ETSI TS 102 232 series of specifications.

4 Solution

As stated in section 3, the scope of the present Feature Package covers the definition of the lawful interception interfaces for delivery of the IPTV-specific intercept material. The solution approach is based on the analysis of the OIPF IPTV interception requirements against the interfaces defined by the ETSI TC LI for interception in IP-based networks. The result of this analysis is the identification of the extensions to the ETSI TC LI interface specifications required to support interception of IPTV services.

4.1 Media Formats

This Feature Package has no impact on existing service media formats. The LI handover interfaces preserve the media formats by wrapping them into an ASN.1 BER envelope as octet strings.

4.2 HTTP Adaptive Streaming

This Feature Package has no impact on the HTTP Adaptive Streaming functionality.

4.3 Content Metadata

No changes to the Content Metadata formats or processing are required. The intercepted metadata is wrapped into ASN.1 BER encoded messages as octet strings for the handover to the LEA.

4.4 Protocols

The LI capabilities are orthogonal to the service functions of the OIPF IPTV solution in the sense that the LI operation should not affect the operations of the IPTV solution. Thus, there shall be no impact from the LI on the OIPF functional interfaces and the protocols used for their realization. The LI solution, ideally, should be built as a stand-alone solution, with a limited number of interconnect points with the functional architecture, to minimize/eliminate the impact and also fulfil the LI security requirements.

The protocols for LI communications between the LEA and the IPTV service provider should be defined with the aim to be input into the appropriate ETSI specifications and subsequently maintained by ETSI. When such an ETSI specification is published, a future revision of the OIPF solution will then reference the ETSI IPTV LI specifications as normative.

The following sections describe the suggested IPTV extensions to the ETSI LI protocols.

4.4.1 OIPF interfaces and protocols from the LI perspective

The OIPF solution employs a variety of interfaces forming the control and the media planes for the operation of various IPTV services.

The OIPF IPTV solution’s main focus is on the UNI interface between the IPTV terminal (ITF) and the IPTV network. The OIPF architecture defines a set of UNI reference points and maps appropriate protocols and procedures to these points. The OIPF solution also decomposes the IPTV network, as well as the ITF, into sets of functional components with reference points defined between these components. For lawful interception, the main interest is the UNI.

4.4.1.1 Application session and transport control protocols

4.4.1.1.1 HTTP

HTTP is used across multiple UNI reference points for both managed and unmanaged IPTV service models. In some cases HTTP supports both the control and the media plane communications (e.g. Content Download, HTTP Adaptive Streaming). In other cases HTTP is used only for communicating the service and subscriber management data, while media are delivered by other means (e.g. Multicast content streaming).

This means that HTTP based communications for both control and media need to be intercepted as IRI and CC respectively.

The ETSI TS 102 232-3 specification [102 232-3] defines the interception at the access network level. The approach there is to intercept raw IP packets to and from the interception target. This obviously will deliver the required HTTP interception, as well (although putting an extra burden on the LEMF for filtering and interpreting the IPTV service control and media traffic). However, this model is not applicable to the unmanaged services model where there is no cooperation between the IPTV service provider and the access network provider.

To address this problem, the ETSI TS 102 232 specification has to be extended to cover the HTTP based communications interception data delivery.

4.4.1.1.2 SIP

The interface defined in [102 232-5] for the interception of IMS based services covers the needs for interception of SIP sessions. This interface should be re-used or replicated in the future ETSI IPTV intercept specification.

4.4.1.1.3 RTSP

OIPF defines 2 modes of RTSP operation (an additional RTSP use for performance monitoring on UNIS-18 is not a subject of the interception and is out of scope of the current specification).

The first mode uses RTSP for the communication session establishment and control in the OIPF solution model not relying on IMS. Interception of the RTSP-based sessions requires extending the ETSI TS 102 232 specifications.

The second mode, used in the IMS-based solution, employs RTSP for the media stream control only, while the session control is performed by means of IMS SIP. In this mode, the RTSP operations are in the context of a SIP session and shall be included in the interception product for the SIP session. It means, that the intercepted RTSP packets shall be assigned the same LIID and CID as the related SIP session.

4.4.1.1.4 IGMP

While multicast content is generally not required to be intercepted, the solution should enable providing the respective IRI. Similar to the RTSP, the IGMP in the IMS-based solution is used in conjunction with a SIP session and should be intercepted as a part of the SIP session, sharing the LIID and CID.

4.4.1.2 Transport protocols

4.4.1.2.1 RTP

The handover interface for RTP-based content is defined in [102 232-5] and is sufficient for the IPTV CC delivery. The interface definition should be re-used in the future ETSI LI IPTV service specific specification.

4.4.1.2.2 HTTP

HTTP interception is described in 4.4.1.1.1.

4.4.1.2.3 MSRP

The handover interface for MSRP-based content is defined in [102 232-5] and is sufficient for the IPTV CC delivery. The interface definition should be re-used or replicated in the ETSI IPTV service specific details specification.

4.4.1.2.4 FLUTE

FLUTE is used for multicast data download and is currently out of scope of the present Feature Package.

4.4.1.2.5 UDP

The OIPF specifications enable content delivery over raw UDP. The ETSI LI IPTV handover interface specification should include the UDP-based content interception delivery.

4.4.2 ASN.1 Specification for IPTV IRI and CC

The following interface specification is based on the specifics of IPTV interception discussed in section 4.4.1. It is envisioned that this specification will be offered to ETSI TC LI as an extension to the interface defined in the ETSI TS 102 232. The ASN.1 definition below implies creation of an IPTV dedicated branch off the li-ps node in the ETSI TS 102 232 ASN.1 object tree. Alternatively, the definition below could be modified and merged into the branch for the IP Multimedia handover interface. (There is a precedent for including a non-IMS (H.323) protocol into the IMS handover specification).

The interface below applies to both IMS-based and non-IMS-based IPTV services interception.

```
-- ====================================
-- Description of the IPTV PDU
-- ====================================
IPTVPDU
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
iPTV(8) version1(1)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
IMPORTS
-- from TS 101 671
IPAddress
FROM HI2Operations
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version17(17)};
-- ============================
-- Object Identifier Definition
-- ============================
iPTVIRIObjId RELATIVE-OID ::= {li-ps(5) iPTV(8) version1(1) iRI(1)}
iPTVCCObjId RELATIVE-OID ::= {li-ps(5) iPTV(8) version1(1) cC(2)}
-- both definitions relative to:
-- {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2)}

-- ====================================
-- IP TV Communications Contents
-- ====================================
IPTVCC ::= SEQUENCE /* to be imported and included into 102 232-1 */
{
iPTVCCObjId [0] RELATIVE-OID,
iPTVCCContents [1] OCTET STRING,
-- Copy of the mediastream, i.e. all related RTP/RTCP, MSRP, UDP or HTTP packets
```



```
-- Each IPTVCC shall contain one intercepted packet
-- Protocol of the media packets is indicated by means of iPTVCCprotocol parameter
frameType [2] FrameType,
-- The availability of header information shall be signalled with the frameType parameter
streamIdentifier [3] OCTET STRING OPTIONAL,
-- Used to identify the media stream within the current CIN, typically in case of
-- multiple media streams communications
-- May be used to correlate each media stream with the relevant SDP media description of IRI
-- May contain c= and m= lines extracts for instance
iPTVCCprotocol [4] IPTVCCprotocol OPTIONAL
-- Used to identify the protocol of packets sent in iPTVCCContents (UDP, RTP, MSRP, HTTP, etc.)
-- Absence means iPTVCCContents contains RTP packets
}
FrameType ::= ENUMERATED
{
ipFrame(0),
-- All headers are present
udpFrame(1),
-- IP header is missing
rtpFrame(2),
-- UDP and IP headers are missing
httpFrame(3),
-- TCP and IP headers are missing
tcpFrame(4),
-- IP header is missing
artificialRtpFrame(5),
-- artificial RTP frame has been added
...
}
IPTVCCprotocol ::= ENUMERATED
{
rTP(0),
-- iPTVCCContents parameter contains RTP/RTCP packets
mSRP(1),
-- iPTVCCContents parameter contains MSRP packets
hTTP(2),
-- iPTVCCContents parameter contains HTTP packets
uDP(3),
-- iPTVCCContents parameter contains UDP packets
...
}
-- ========================================================
-- Intercept-related information for IP TV sessions
-- ========================================================
IPTVIRI ::= SEQUENCE /* to be imported and included into 102 232-1 */
{
iPTVIRIObjId [0] RELATIVE-OID,
iPTVIRIContents [1] IPTVIRIContents,
...
}
IPTVIRIContents ::= CHOICE
{
originalIPTVMessage [0] OCTET STRING,
-- Copy of the IP TV signalling packet including the original headers from IP layer up
sIPMessage [1] SIPMessage,
-- Copy of the SIP content and the source and destination IP address
rTSPMessage [2] RTSPMessage,
-- Copy of the RTSP content and the source and destination IP address
hTTPMessage [3] HTTPMessage,
-- Copy of the HTTP content and the source and destination IP address
iGMPMessage [4] IGMPMessage,
-- Copy of the IGMP content and the source and destination IP address
nationalIPTVIRIParameters [5] NationalIPTVIRIParameters
-- This parameter is used according to national regulations
...
}
SIPMessage ::= SEQUENCE
{
iPSourceAddress [0] IPAddress,
iPDestinationAddress [1] IPAddress,
sIPContent [2] OCTET STRING,
...
}
RTSPMessage ::= SEQUENCE
{
iPSourceAddress [0] IPAddress,
iPDestinationAddress [1] IPAddress,
rTSPContent [2] OCTET STRING,
...
}
HTTPMessage ::= SEQUENCE
{
iPSourceAddress [0] IPAddress,
iPDestinationAddress [1] IPAddress,
hTSPContent [2] OCTET STRING,
...
}
IGMPMessage ::= SEQUENCE
```



```
{
iPSourceAddress [0] IPAddress,
iPDestinationAddress [1] IPAddress,
iGMPContent [2] OCTET STRING,
...
}

NationalIPTVIRIParameters ::= SEQUENCE
{
countryCode [1] PrintableString (SIZE (2)),
-- Country Code according to ISO 3166-1,
-- the country to which the parameters inserted at the extensibility marker apply.
...
}
END -- end of IPTV PDU
```

4.4.3 Considerations on interception of IPTV Services

The following items are not in the scope of the present Feature Package but provided as input for future consideration.

4.4.3.1 User Generated Content

The LI feature use cases are mostly derived from the Social TV functionality which at the time of this writing is not fully defined in OIPF. Nevertheless, some of the related services are defined, although not specified by the OIPF. This pertains to the User Generated Content (UGC) services.

A UGC case requiring special consideration is the interception of the target UGC during content consumption by other users. This pertains to both the IRI and CC interception, as the content may be deposited at the service provider's storage facilities prior to the interception activation and, thus, not intercepted in the upload. This use case requires the ability to associate the Content ID with the User or Subscriber ID and may require an extension to the handover interface. The mechanism for providing such association is out of scope of the present Feature Package.

4.4.3.2 Blended services

Another example of innovative services requiring special consideration is the so called "blended services", where the overall services context is constructed from other services, such as watching a live TV content along with real-time chatting and/or AV conferencing in parallel. A special technique may be required to achieve synchronous interception of the partial services enabling the reconstruction of the actual user experience, necessary to interpret the intercepted material. Enhancements of the handover interface are likely required in this case but are not in the scope of the present Feature Package.

4.5 Declarative Application Environment

No changes to this functionality are required for this Feature Package.

4.6 Procedural Application Environment

No changes to this functionality are required for this Feature Package.

4.7 Authentication, Content Protection and Service Protection

No changes to this functionality are required for this Feature Package.

5 Testing

The LI acceptance testing is usually conducted on the ad-hoc basis between the service providers and LEAs. Thus, no OIPF involvement in testing/certification is required or expected.

5.1 Conformance Testing

5.2 Interoperability Testing

Appendix A. Requirements

This section lists all the requirements of the OIPF Solution. Requirements of actual implementations may vary by jurisdiction; not all requirements listed in this section may apply to all jurisdictions.

For the description of use cases from which the requirements below were derived, refer to the OIPF-CR-REQ-291-R07-LI_for_IPTV_FP_Requirements document.

A.1 Reuse of Generic Solution

The OIPF LI solution shall be seen as a service-specific extension of the generic LI solution for IP-based networks currently in use in the industry. It means, the OIPF LI solution shall use the generic LI solution as a basis, and build upon it to also fulfil the service-specific requirements for IPTV.

The most comprehensive and widely adopted (in Europe and worldwide) LI solution is provided by ETSI. The generic LI requirements and the ETSI LI solution for IP-based networks are specified in references [101 331], [201 158], [101 671] and [102 232-1]. The IMS-specific LI solution extensions are provided in [102 232-5].

Therefore, the base requirement for the OIPF LI solution is:

LI-1. The OIPF LI solution shall be compliant with the ETSI LI solution defined in the following specifications:

[101 331] ETSI TS 101 331

[201 158] ETSI ES 201 158

[101 671] ETSI TS 101 671

[102 232-1] ETSI TS 102 232-1

[102 232-5] ETSI TS 102 232-5

The rest of the present section is a list of generic LI requirements, which is, mostly, a summary of the requirements provided in [101 331]. These requirements will be fulfilled by adopting the generic ETSI LI solution as a basis for the OIPF LI solution. Next section A.4 then introduces the requirements that are specific to IPTV services, and notably blended services that combine IPTV with user-generated content and social TV functionality.

A.2 Service Control Requirements for LI service

The following requirements typically apply to an LI solution. The OIPF LI Solution shall support them:

LI-1-1. Provision/withdrawal.

The LI service shall be always provided, there is no explicit provision/withdrawal required.

LI-1-2. Activation/deactivation.

The LI service shall be activated upon issuing of a valid interception warrant from a LEA. The LI service shall be deactivated when the interception warrant expires or as defined by the LEA.

LI-1-3. Invocation and operation.

The LI service shall be invoked on any communication from or to the LI target. The LI service shall also be invoked when a content related to the LI target is accessed (e.g. LI target-generated content uploaded and stored in the SP storage facilities, regardless of whether the LI service was active when the target-generated content was uploaded.)

LI-1-4. Interrogation.

Interrogation shall be possible only from an authorized (by LEA and by SP) user.

LI-1-5. Interaction with other services.

There shall be no interaction, i.e., the invocation of LI shall not alter the operation of any service.

A.3 General Requirements

LI-1-6. The OIPF LI solution shall ensure that:

a) the entire content of communication associated with an intercept target can be intercepted during the period of the intercept warrant;

b) any content of communication associated with an intercept target which is routed to technical storage facilities or is retrieved from such storage facilities can be intercepted during the period of the intercept warrant;

c) the delivery of the intercept related information (IRI) is reliable;

d) the delivery of the content of communication (CC) is reliable;

e) the service provider does not monitor or permanently record the results of interception;

f) LI is undetectable by the intercept target;

g) LI is undetectable by other users;

h) mechanisms are in place to prevent unauthorized personnel from performing or knowing about intercepts;

i) the service provider is able to do multiple simultaneous intercepts on a single intercept target. The fact that there are multiple intercepts should be transparent to the LEAs.

LI-1-7. The solution shall support the ability to intercept telecommunications relating to the interception targets operating permanently within a telecommunications system (e.g. a subscriber or account).

LI-1-8. The solution shall support giving all results of interception provided at the handover interface a unique identification relating to lawful authorization.

LI-1-9. The solution shall support protection of integrity and confidentiality of the intercepted communications.

A.3.1 Result of interception

The OIPF LI solution shall enable:

LI-1-10. Providing the content of communication and related information;

LI-1-11. Removing any service coding or encryption which has been applied to the content of communication and the intercept related information at the instigation of the service provider;

LI-1-12. Providing the LEA with any other decryption keys whose uses include encryption of the content of communications, where such keys are available for SP (in case the coding/encryption cannot be removed by the SP);

NOTE: Where the user has initiated and applied end to end encryption, the content is provided as received.

LI-1-13. Providing the intercept related information (IRI), when:

a) communication is attempted;

b) communication is established;

c) no successful communication is established;

d) there is a change of status (e.g. in the access network);

e) there is a change of service or service parameter;

f) there is a change of location;

g) a successful communication is terminated;

LI-1-14. Providing the intercept related information (IRI) containing:

a) the identities that have attempted telecommunications with the target, successful or not;

b) identities used by or associated with the target;

c) details of services used and their associated parameters;

d) information relating to status;

e) time stamps.

A.4 IPTV Specific Interception Requirements

A.4.1 Communication services

LI-2. The OIPF LI solution shall support interception of communication services provided by the IPTV service provider, including but not limited to A/V, textual, graphical communications and presence information.

A.4.2 Content Services

LI-3. The OIPF LI solution shall support interception (IRI and CC) of the target-generated content during the content contribution (streaming or uploading) to the service provider storage facilities.

LI-4. The OIPF LI solution shall support interception (IRI and CC) of the target-generated content during the real-time (i.e. live) content contribution and delivery to other users.

LI-5. The OIPF LI solution shall support interception (IRI and CC) of the target-generated content during the content delivery, including the case when the content was deposited to the service provider storage facilities prior to the interception activation.

LI-6. The OIPF LI solution shall support interception (IRI and CC) of the content created by other users during the content delivery (streaming or downloading) to the target.

LI-7. The OIPF LI solution shall support interception of information (IRI) generated and delivered by an IPTV service on behalf of the target to other users, e.g., notifications on user-generated content availability or updates.

LI-8. The OIPF LI solution shall support interception of information (IRI) generated and delivered by an IPTV service on behalf of other users to the target, e.g., notifications on user-generated content availability or updates.

LI-9. The OIPF LI solution shall enable delivery of the content metadata as part of the intercept product (IRI) for target-generated content during the content contribution or delivery.

LI-10. The OIPF LI solution shall enable interception (IRI) of target-generated content metadata when the metadata is modified by the target or retrieved by other users.

LI-11. The OIPF LI solution shall enable delivery of the content metadata as part of the intercept product (IRI) for content generated by other users during content delivery to the target.

LI-12. The OIPF LI solution shall enable delivery of the content metadata as part of the intercept product (IRI) for service provider content (on-demand or linear) delivered to the target.

***Note: Generally, no CC delivery is required for the service provider content**.*

A.4.3 SNS User Comments

LI-13. The OIPF LI solution shall enable intercepting data and metadata generated by a target pertaining to content, regardless of the type of content. This shall include comments on the content in any form, such as A/V, textual or graphical.

LI-14. The OIPF solution shall enable inclusion of information generated by the service into the intercept product related to a target-generated comment, such as the temporal position of the user-generated comments and, if a target is able to put comments in a particular location overlaid on the content, their spatial positions relative to the viewed content.

LI-15. The OIPF LI solution shall support interception of comments generated by other users and consumed by a target.

A.4.4 General

LI-16. The OIPF LI solution shall support interception (IRI) of all changes in services and service parameters generated by the target, such as subscriptions to personal or service provider channels, creation of personal channels, specifications of content distribution policies for target-generated content, etc.

