ETSI GS NFV-SEC 004 V1.1.1 (2015-09)

Network Functions Virtualisation (NFV);
NFV Security;
Privacy and Regulation;
Report on Lawful Interception Implications

Disclaimer

Reference
DGS/NFV-SEC004

Keywords
interception, NFV, privacy, regulation, security

ETSI

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

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

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

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://ipr.etsi.org).

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 Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

NOTE: Where the word "shall" appears in clauses 4 and 5 it has been taken from text originated in reference documents and offers a requirement against the operator of networks and services and in general does not place any additional technical constraints or conformance obligations on the NFV beyond those specified in the reference documents.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides a problem statement on implementing LI in NFV and identifies the necessary capabilities to be provided in NFV to meet the requirements outlined for telecommunications capabilities in general in ETSI TS 101 331 [i.2].

The present document identifies the challenges of providing LI in an NFV. The present document is intended to give guidance to the NFV community and to the wider LI community on the provision of LI in an NFV.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[i.2] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.3] ETSI TR 102 528: "Lawful Interception (LI) Interception domain Architecture for IP networks".

[i.4] ETSI TS 103 120: "Lawful Interception; Interface for warrant information; Q & D LI Agnostic".

NOTE: In draft stage at the time of publication.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 101 671 [i.1] and the following apply:

Content of Communication (CC): information exchanged between two or more users of a telecommunications service, excluding intercept related information

NOTE: This includes information which may, as part of some telecommunications service, be stored by one user for subsequent retrieval by another.

Handover Interface (HI): physical and logical interface across which the interception measures are requested from Communications Service Provider (CSP), and the results of interception are delivered from a CSP to a law enforcement monitoring facility

Intercept Related Information (IRI): collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (e.g. unsuccessful communication attempts), service associated information or data and location information

interception: action (based on the law), performed by a CSP, of making available certain information and providing that information to a law enforcement monitoring facility

interception interface: physical and logical locations within the CSP telecommunications facilities where access to the content of communication and intercept related information is provided

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

Internal Network Interface (INI): network's internal interface between the Internal Intercepting Function (IIF) and a mediation device

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

mediation device: equipment which realizes the mediation function

Mediation Function (MF): 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

target identity: technical identity (e.g. the interception's subject directory number), which uniquely identifies a target of interception

NOTE: One target may have one or several target identities.

3.2 Abbreviations

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

ADMF	ADMinistration Function
AF	Administration Function
CC	Content of Communication
CCCI	Content of Communication Control Interface
CC-IIF	Communications Content - Internal Interception Function
CCTF	Content of Communication Trigger Function
CCTI	Content of Communication Trigger Interface
CSP	Communications Service Provider
FE	Functional Entity
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)
IIF	Internal Interception Function
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
INI	Internal Network Interface
IP	Internet Protocol
IRI	Intercept Related Information
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIAF	Lawful Interception Administration Function
MANO	Management and Orchestration
MF	Mediation Function
NFV	Network Functions Virtualisation
PKC	Public Key Certificate
PoI	Point of Interception
SIP	Session Initiation Protocol
TC	Technical Comittee
VM	Virtual Machine

4 Requirements for Lawful Interception

4.1 General CSP obligations

The obligation to support LI applies irrespective of traffic type, signalling format or network configuration. The obligations are not specific to the NFV domain but rather apply to the end-to-end service.

There is a broad obligation to remove encoding provided by the CSP before material is handed over to the LEA, but if this cannot be done, the obligation to hand the material over still applies. This means that if the target is using some form of end-to-end encryption the intercepted material is handed over even if the clear text is not available.

There are two primary components for legacy LI acquisition and handover:

- Intercept Related Information (IRI), e.g. associated signalling and call/log record information.
- Content of Communication (CC), i.e. streaming traffic.

Where IRI and/or CC is acquired and handed over the CSP is obliged to indicate the time and location (virtual and geographic) of the Point of Interception (PoI) for CC and IRI information.

In many jurisdictions, an array of retained data requirements associated with communications may also be required as part of the Lawful Interception obligations, but is outside the scope of the present document.

The present document acknowledges the legal basis for such activities by reference to the requirements established in ETSI TS 101 331 [i.2].

4.2 Root of trust in LI

In LI implementations the active components (i.e. the PoI for each of CC and IRI) act upon requests received from an LI administration function that acts as the root of trust for those components. In the wider NFV environment the instantiation and operation of virtualised components has a root of trust in a wider set of components that may include the orchestrator function, the hypervisor function, and the generalized MANO functions. The roots of trust for general NFV and for LI operations may be distinct but are required to interoperate such that LI functions can be instantiated as general NFV components.

4.3 Core requirements

The convention in LI is to have the operator (CSP) domain support 3 interfaces to the Law Enforcement Monitoring Facility:

- HI1 - For administration, normally maps to the internal interface INI1.
- HI2 - For transfer of intercept related information, normally maps to the internal interface INI2.
- HI3 - For transfer of the content of communication, normally maps to the internal interface INI3.

When considering the NFV environment the LI capability will most likely be implemented as a service that extends existing services under strict access control policy. The relatively formal requirements for LI in the NFV are as follows:

- The LI service capability shall always be provided.
- The LI service shall be activated upon issue of a valid interception order from an LEA. The LI service shall be deactivated when the interception warrant expires or as defined by the LEA.

NOTE 1: The details of the interception order and the validation of it are a national concern but guidance is given in ETSI TS 103 120 [i.4].

- The LI service shall be invoked on any communication authorized for interception from or to the target visible to the network.
- Interrogation shall be possible only from an authorized user. Where audit records are maintained for the service (required by the International User Requirement) access shall be possible only from an authorized user.
- An authorized user for the purposes of interrogation is one who is allowed and authorized by both LEA and the CSP to administer the LI interface.
- There shall be no interaction with other services.

NOTE 2: This means that the invocation of LI is not intended to alter the operation of any service and any resulting modification implies non-compliance to the requirements and breaks the primary requirement that the LI measure is only visible to authorized entities.

In rather more detail the CSP at the point of interception shall, in relation to each target service:

a) provide the content of communication;

b) remove any service coding or encryption which has been applied to the content of communication and the intercept related information at the instigation of the network operator/service provider;

NOTE 3: If coding/encryption cannot be removed through means which are available to the CSP for the given communication the content is provided as received.

NOTE 4: The semantic meaning has to always be transferred even if the exact syntax (encoding) is modified.

c) provide the LEA with any other decryption keys whose uses include encryption of the content of communication, where such keys are available;

d) intercept related information shall be provided:

   1) when communication is attempted;

   2) when communication is established;

   3) when no successful communication is established;

   4) on change of status (e.g. in the access network);

   5) on change of service or service parameter;

   6) on change of location (this can be related or unrelated to the communication or at all times when the apparatus is switched on); and

7) when a successful communication is terminated.

NOTE 5: In the present document, service should be taken to include supplementary services.

NOTE 6: For those protocols of type Representational State Transfer (REST) (e.g. SIP, HTTP) each transaction is considered as unique unless the signalling itself contains a means to link signals (e.g. session identity).

e) intercept related information shall contain:

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

2) the identities which the target has attempted telecommunications with, successful or not;

3) identities used by or associated with the target identity;

4) details of services used and their associated parameters;

5) information relating to status;

6) time stamps;

7) location of the target.

NOTE 7: The identity to be supplied should be that visible to the CSP and may take one or many forms including but not restricted to IMSI, IMEI, MSISDN, email address, SIP-identity.

f) the conditions mentioned above also apply to multi-party or multi-way telecommunication if and as long as the target is known to participate.

NOTE 8: Where the user has initiated and applied end-to-end encryption, the content is provided as received.

4.4 PoI location attestation

The lawful authorization that invokes the lawful interception facilities has to identify the jurisdiction in which the authorization is valid, and the CSP has to ensure that the LI facilities operate within the same jurisdiction. The underlying hardware of any NFV is physically located in specific jurisdictions and whilst the VMs are intended to run on any viable hardware and not to have knowledge of which instance of the hardware they run on this knowledge has to be within the system and should be able to be reported to the LEA. Furthermore when LI is activated against a target, the system management (e.g. MANO) cannot instantiate any VM required to support LI for the user service outside the jurisdiction if the target is in the jurisdiction of the lawful authorization.

4.5 LI undetectability

Much of the data for the provision of LI is sensitive and should be protected from illicit exposure including transfer across jurisdictional borders. In particular the knowledge of targets of interception (often referred to as the target list) shall not be visible to any unauthorized party.

5 Analysis and recommendations

5.1 Overview

It should be noted that LI has often looked at the interception of communication between 2 parties, or at the communications initiating or terminating at a single party (the target). In this respect much of the terminology may be considered to be based on conventional circuit switching but that is an over-simplification. The aim in general is to ensure that whenever a target is involved in a communication that the knowledge of that communication, and the content of that communication, is also delivered to the facilities of the Law Enforcement Agency (typically referred to as Law Enforcement Monitoring Facility (LEMF)).

5.2 The LI service shall always be provided

This is straightforward. A functioning NFV deployment serving as a platform for the provision of services (through a CSP) has to have an LI service. What is much more difficult to answer is - where does the LI service sit in the NFV architecture and function suite? The main issue here is the identification of points of interception in the NFV. In theory any NFV node that is used to offer service to a customer and where any object is instantiated for a customer that is also a target then that object has to be considered as a point of interception.

There is also a geographic or jurisdiction concern for LI as in a fully virtualised environment with the potential to allocate resources anywhere globally there may be a requirement to restrict where services can be provided. This class of requirement is not specific to LI but also covers personal information and financial information. The main impact is that objects that are able to act as PoIs shall be able to report their location (either directly or through a management entity) in addition to the geographic location of the target. This knowledge of where the PoI and any supporting functions are located with respect to the jurisdiction may be critical and thus has to be treated as highly trusted data.

5.3 The LI service shall be activated upon receipt of a valid interception authorization from an LEA

This requirement underpins the access control for the LI service. Quite simply the always provided service cannot actually run unless there is a valid LEA request. The LEA request has not been fully defined in ETSI's TC LI as yet but there is work in progress to look at the use of digital signature based schemes for dissemination of warrants (or LI authorization certificates). If such warrants exist the signed authority may be used as part of the access control mechanism.

LI activation for IRI records may take the form of a publish/subscribe model. In this case when activated IRI data is forwarded to the subscriber where the only valid subscribers are of type "LEMF" and the authorization shall be from the LEA.

5.4 The LI service shall be deactivated when the interception authorization expires or as defined by the LEA

If solved as above the original authorization shall include an expiry time and as with any PKC based system the authorization certificate can be revoked (with revocation it is necessary to check that authorization remains valid whatever the model indicates that transmission of an IRI is required).

5.5 Interrogation shall be possible only from an authorized user

In this the term "interrogation" is used to mean identifying the state of the LI function. It is very unlikely that the administrator of a conventional hypervisor or orchestrator will be authorized as an interrogator who should be allowed to know that the LI function is activated, and against whom, as information that has to be strictly controlled. This is consistent with the requirement from clause 4 "An authorized user for the purposes of interrogation is one who is allowed and authorized by both LEA and the CSP to administer the LI interface". The use of some form of Role Based Access Control that can explicitly deny access to a super-user form is probably a pre-requisite. This goes even further as it also means many forms of analytic software that gather data on which functions are active will have to maintain the same level of access control.

5.6 What the PoI delivers

The requirements on what the Point of Interception delivers to the LEA/LEMF are quite clear from clause 4.3 and do not need to be repeated at length here. As LI is a lawfully authorized function (see above) then the CSP has to be confident that the information released is an accurate picture of the activity of the target. The CSP makes an attestation that the IRI and CC are accurate records of the activity of the target.

Annex A (informative): Architectures and structures for LI in networks composed from VNFs

As noted at the beginning of clause 4.1, the obligation to support LI applies irrespective of traffic type, signalling format or network configuration. Thus LI applies when all or part of the network configuration is implemented using VNFs. Where a network function is virtualised the corresponding LI function should also be virtualised such that the flexibility of the virtualisation is maintained.

A legacy LI model could be mapped to a set of virtualised PoIs, virtual X interfaces and virtual ADMF and MFs. In following the model of the dynamic NFV environment therefore each of these LI-VNFs need to be deployed, maintained and terminated during the entire lifecycle and remain compliant to the legal and security requirements established for LI.

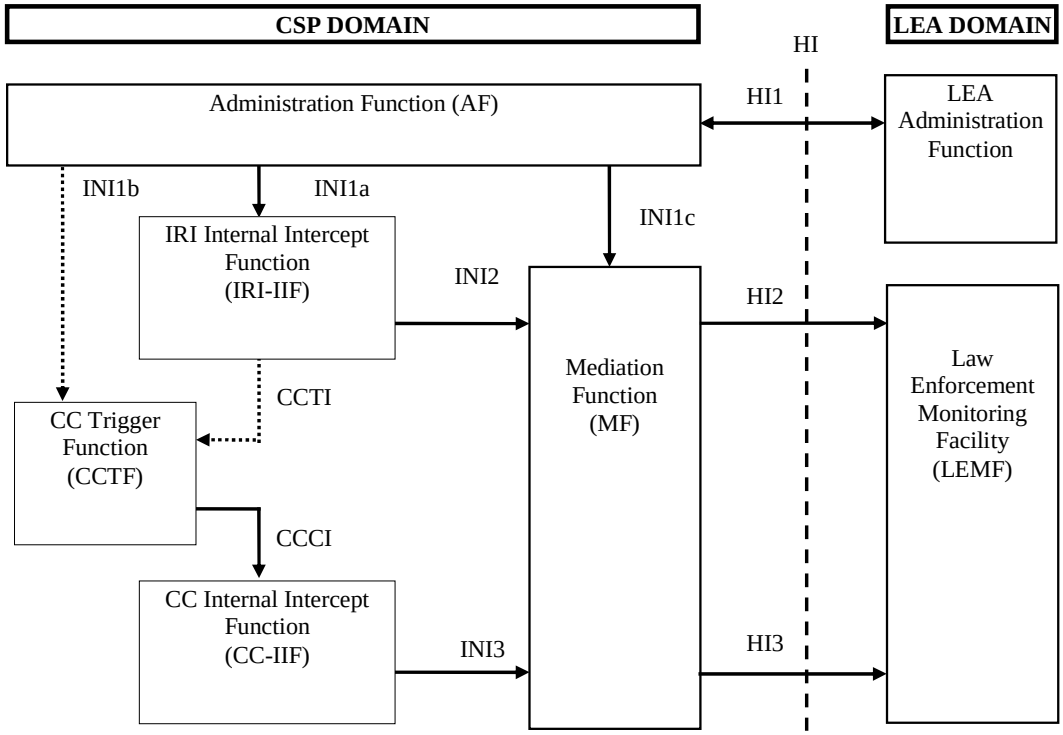

Figure A.1: Reference Model for IP Network LI from ETSI TR 102 528 [i.3]

The reference model identifies 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.
- Internal interface INI1 carries provisioning information from the Lawful Interception Administration Function (AF) to the Internal Intercept Functions (IIF).
- 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 reference model introduces the CCTF FE that may be used to in a number of configurations to allow for the provisioning of CC-IIF in an NFV installation. The location of the CCTF is not defined in the present document but considered configuration options are as follows:

- CCTF co-located with the LIAF: INI1b is internal to the AF and CCTF.
- CCTF co-located with the IRI-IIF: CCTI is internal to the IRI-IIF and CCTF.
- CCTF co-located with the IRI-IIF and CC-IIF: CCTI and CCCI are internal to the IRI-IIF, CCTF and CC-IIF.
- CCTF co-located with the MF: CCTI is merged with INI2.
- A stand alone CCTF: Both CCTI and CCCI are external interfaces.

A complete explanation of the functions and interface is found in clause 4 of ETSI TR 102 528 [i.3]. The base architecture model from ETSI TR 102 528 [i.3] as above is extended for the NFV with the multi-operator model for Dynamic Triggering given in figure A.2.

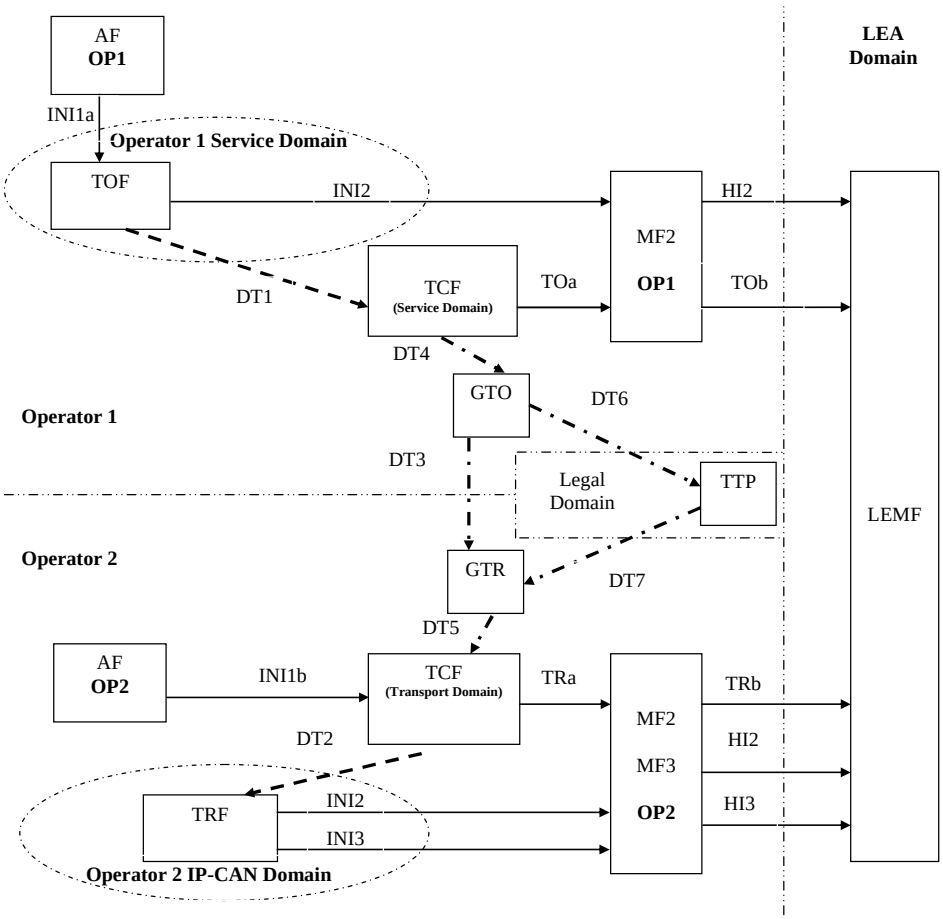

Figure A.2: Dynamic Triggering Multiple Operator Reference Model [i.5]

The models above can also be seen in the 3GPP specifications for LI with some changes of terminology although no changes in core functionality.

Annex B (informative): Authors & contributors

The following people have contributed to this specification:

Rapporteur:

Mr Scott Cadzow, Cadzow Communications Consulting Ltd.

Annex C (informative): Bibliography

- ETSI TS 102 677: "Lawful Interception (LI); Dynamic Triggering of Interception".

History

Document history		
V1.1.1	September 2015	Publication