ETSI TR 103 685 V1.1.1 (2020-11)

Lawful Interception (LI);
LI network function security

Reference
DTR/LI-00173

Keywords
lawful disclosure, lawful interception, virtualisation

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**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.

Introduction

The present document examines LI and LD network function security with a focus on virtualisation of computing and networking resources. It provides an overview of LI and LD aspects in a virtualised environment, examines the threat model and provides a list of provisions to address the identified threats. Finally, the provisions are categorized into security levels and summarized in a checklist for the purpose of evaluating the security of a LI and LD deployment in a virtualised environment.

1 Scope

The present document examines LI and LD network function security with a focus on virtualisation. It considers a broad definition of virtualisation i.e. including but not restricted to Network Functions Virtualisation. It focuses on threats and risks, provides applicable recommendations (although these are not meant to be exhaustive), and identifies areas where other standards present recommendations which are relevant to the threats and risks identified. The present document considers reuse of existing standards where applicable. It also considers a mixed deployment of physical and virtualised LI and LD implementations. It is restricted to LI and LD considerations only and does not look at wider considerations. Specifically, broader national security concerns are out of scope of the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.2] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".

[i.3] ETSI TS 133 127: "LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Lawful Interception (LI) architecture and functions (3GPP TS 33.127)".

[i.4] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.5] ETSI GR NFV-SEC 011: "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[i.6] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.7] ETSI TS 103 307: "CYBER; Security Aspects for LI and RD Interfaces".

[i.8] ETSI TS 103 221-2: "Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3".

[i.9] ETSI GS NFV-IFA 026: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification".

[i.10] ETSI GS NFV-EVE 005: "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework".

[i.11] NIST FIPS 140-2: "Security Requirements for Cryptographic Modules".

NOTE: Available at https://csrc.nist.gov/Projects/cryptographic-module-validation-program.

[i.12] ISO/IEC 11889-1:2015: "Information technology -- Trusted platform module library -- Part 1: Architecture".

[i.13] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.14] NIST SP800-90b: "Recommendation for the Entropy Sources Used for Random Bit Generation".

NOTE: Available at https://csrc.nist.gov/publications/detail/sp/800-90b/final.

[i.15] ISO/IEC 18031:2011: "Information technology -- Security techniques -- Random bit generation".

[i.16] NIST SP 800-88 Rev. 1: "Guidelines for Media Sanitization".

NOTE: Available at https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ADMF	Administration Function
CA	Certificate Authority
CC	Content of Communication
CPU	Central Processing Unit
CSP	Communication Service Provider
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DF	Delivery Function
DMA	Direct Memory Access
FIPS	Federal Information Processing Standard
GTP	GPRS Tunneling Protocol
GW	Gateway
HBRT	Hardware-based Root of Trust
HMEE	Hardware-Mediated Execution Enclave
HSM	Hardware Security Module
IAAS	Infrastructure As A Service
IOMMU	Input Output Memory Management Unit
IRI	Intercept Related Information
LD	Lawful Disclosure
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LICF	LI Control Function
LIPF	LI Provisioning Function
LN	Leaf Node
LRPG	Lawful Interception Routing Proxy Gateway
MAC	Mandatory Access Control
MANO	Management and Orchestration
MDF	Mediation and Delivery Function

MF	Mediation Function
MPLS	Multi-Protocol Label Switching
NAAS	Network As A Service
NE	Network Element
NF	Network Function
NFV	Network Functions Virtualisation
NFVI	NFV Infrastructure
NIC	Network Interface Controller
NIST	National Institute for Standards and Technology
PNF	Physical Network Function
POI	Point Of Interception
SDN	Software Defined Networking
SMF	Session Management Function
SN	Spine Node
SUPI	Subscription Permanent Identifier
SVR	Server and Virtual Machine
TCG	Trusted Computing Group
TF	Triggering Function
TOR	Top Of the Rack
TPM	Trusted Platform Module
UPF	User Plane Function
USB	Universal Serial Bus
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFCI	Virtual Network Function Component Instance
VPN	Virtual Private Network
WAN	Wide Area Network

4 Overview of LI, LD and virtualisation aspects

4.1 Generic LI reference model

Figure 4.1-1 provides a high-level LI architecture. The reference architecture shown is as defined for the 5G system (see 3GPP TS 33.127 [i.3]), but the major architectural elements may be considered to have wider applicability. The LI architectural elements can be implemented as virtual or physical network functions. The present document follows the convention of using the generic terms of Network Function (NF) and, when a distinction is necessary, Virtual Network Function (VNF) for those instantiated in a virtualised environment and Physical Network Function (PNF) for those instantiated on their own hardware platform. PNF are sometimes known as Network Elements (NE).

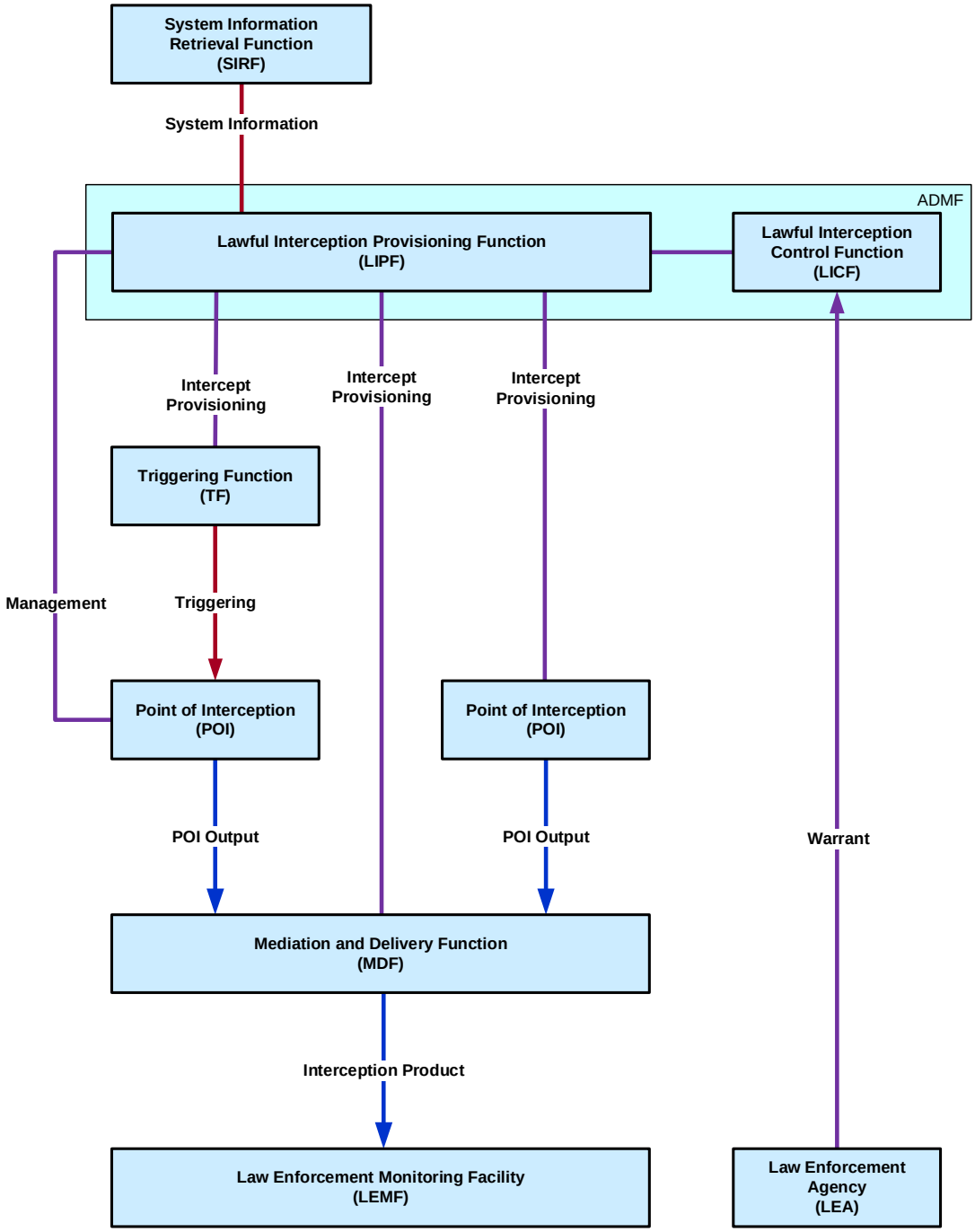

Figure 4.1-1: High-level generic view of LI architecture for 5G, from 3GPP TS 33.127 [i.3]

A description of each entity can be found in 3GPP TS 33.127 [i.3], but a summary is given below:

- ADMF (Administration Function) - Responsible for overall control of the LI network. In some architectures this is considered to be monolithic. In more recent LI architectures, it may be considered as consisting of two subcomponents:
  - LICF (LI Control Function) - Responsible for communication with the LEA and maintaining the authoritative record of LI tasking. As a result, the LICF may attract more stringent security requirements than the rest of the LI network.
  - LIPF (LI Provisioning Function) -Responsible for mediating communication between the LICF and the rest of the LI network, including provisioning and tasking POIs, TFs and MDFs.
- POI (Point Of Interception) - Responsible for performing LI as directed by either the ADMF or a TF.
- TF (Triggering Function) - Responsible for taking long-term identifiers as tasked by the ADMF and tasking other POIs to intercept on related dynamic short-term identifiers (triggering) e.g. a TF in a 5G SMF may a POI in a UPF to intercept particular GTP tunnels established in relation to a SUPI tasked by the ADMF.
- MDF (Mediation and Delivery Function) - Responsible for aggregating and converting the output from the POIs into a format that can be handed over to the LEMF.

Within an implementation of the LI architecture it is assumed that the VNF and PNF which can provide CC or IRI either embed, or interact with, a POI. Figure 4.1-2 provides a reference model in which POI are embedded. External POI are further discussed in clause 4.2.3.

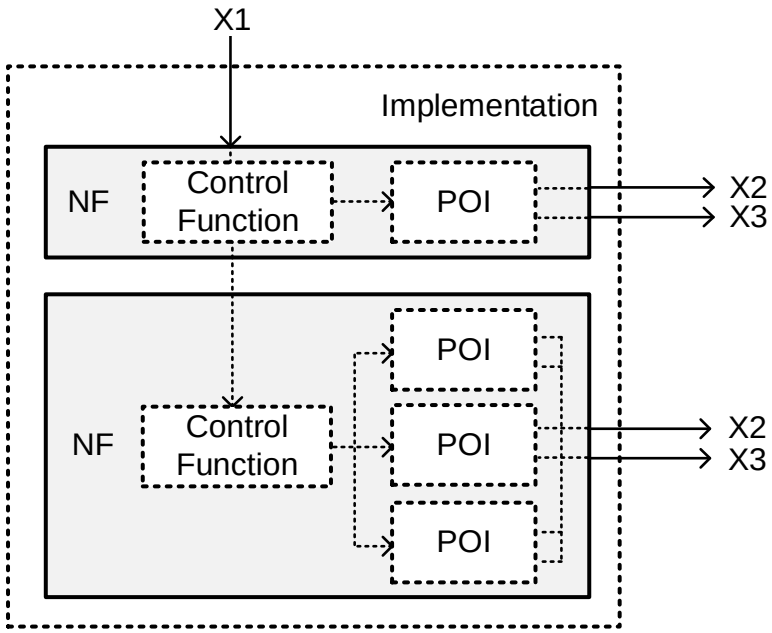

Figure 4.1-2: Implementation model with embedded POI, from ETSI TS 103 221-2 [i.8]

4.2 Reference model for LI lifecycle in a virtualised environment

4.2.1 Reference architecture for virtualised LI deployment

A simplified reference model for a virtualised LI deployment architecture is given in 3GPP TS 33.127 [i.3] and reproduced in figure 4.2.1-1.

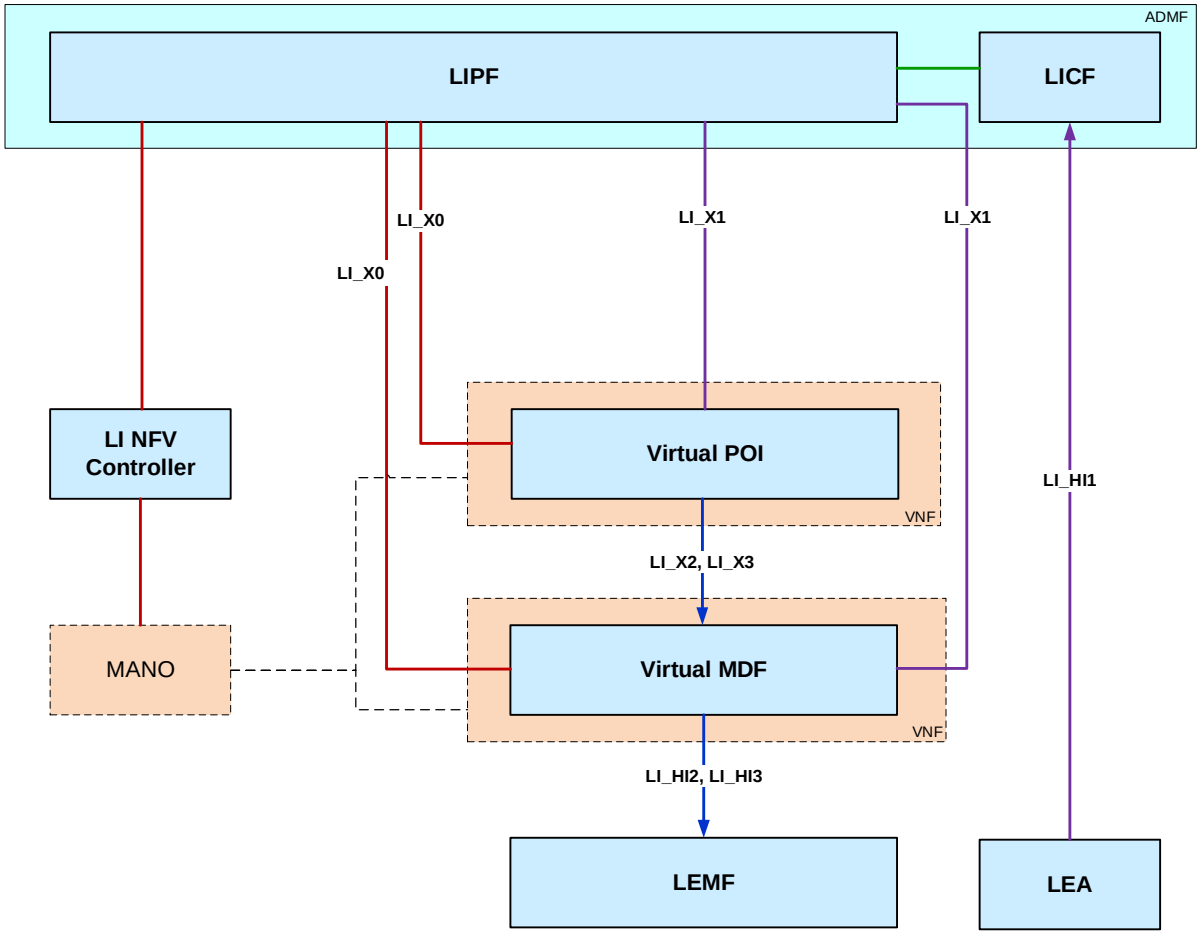

Figure 4.2.1-1: Simplified virtualised LI deployment architecture, from 3GPP TS 33.127 [i.3]

This architecture is defined for 3GPP networks but has wider general applicability.

LI functions, whether embedded within another NF or standalone, require their resources and lifecycle to be managed by MANO. However, additional measures are needed to ensure that MANO (and its administrators) cannot identify or interfere with the operation of LI functions. The LI NFV Controller is introduced to achieve this by mediating interactions between the ADMF/LIPF and the NFVI MANO such that the LI functions are correctly orchestrated without delegating control of the LI domain to the MANO. Once the VNF for an LI function has been instantiated by MANO, the LI NFV Controller is then responsible for notifying the ADMF/LIPF that the next stage of LI provisioning (e.g. provisioning of certificates for establishing onwards transport connections) can occur over interface LI_X0.

Figure 4.2.1-2 shows the process for instantiating a new VNF with an LI function (taken from 3GPP TS 33.127 [i.3]).

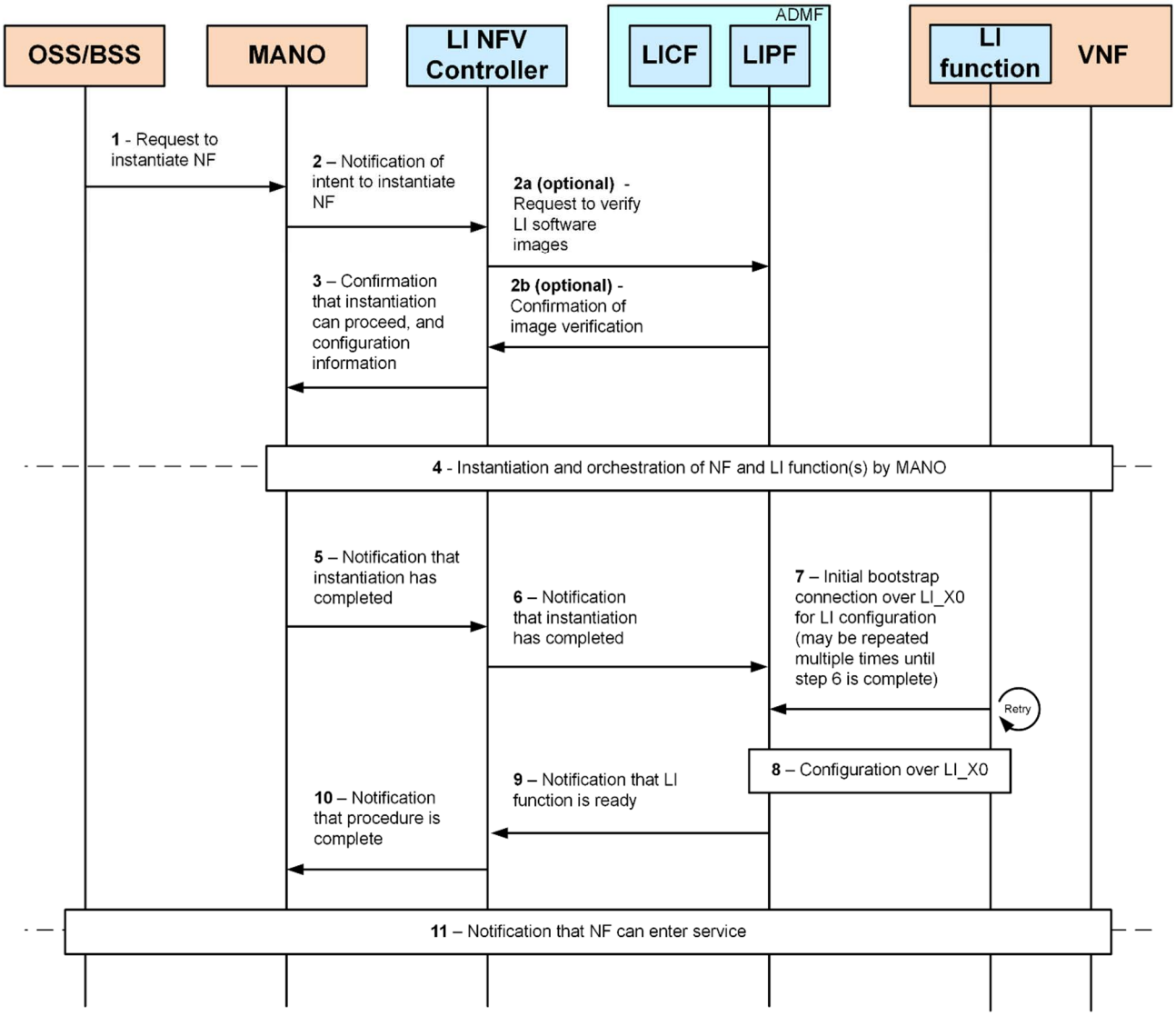

Figure 4.2.1-2: Simplified virtualised LI lifecycle architecture, from 3GPP TS 33.127 [i.3]

When an NF associated with LI is modified, the LI NFV controller is also required to manage to necessary interactions (e.g. via the mechanisms described in ETSI GS NFV-IFA 026 [i.9]) to ensure that the LI service continues to function. This may be managed by ensuring that the LI functions are appropriately scaled or relocated (or new LI functions instantiated) in order to allow them to align with changes made to the associated NFs. In some cases, it may also be necessary that the LI NFV controller can, subject to appropriate operator policy, prevent MANO from making such modifications, especially where the change might result in a sensitive function being moved outside of a particular jurisdiction.

When NFs and LI functions associated with them are terminated, the LI NFV Controller is responsible for informing the LIPF (and hence the LICF) of the removal of the NF. The LICF is responsible for ensuring that any necessary clean-up is performed e.g. revocation of the relevant certificates. In the event of the detection of abnormal behaviour in the LI service, the LIPF may also instruct MANO to terminate or quarantine the relevant NF.

4.2.2 Types of NFV environment

The present document considers two types of NFV environment:

- A high-trust NFV environment is one where the hypervisor and physical environment is under the control of the organization who is running the network functions on them. No VNFs from outside of the organization are permitted to run on the same hardware as that which is used to run VNFs belonging to the organization.

- A low-trust NFV environment is one where certain components (e.g. the hypervisor) are being managed outside the organization, or one where other VNFs are hosted on the same hardware which do not belong to the organization.

There is also a spectrum of possibilities between the two definitions above but the definition of a high-trust environment is one which fully falls into the first definition.

4.2.3 Embedded or external POI

There are two models to determining where Points of Interception (POI) are located (see 3GPP TS 33.127 [i.3], clause 8.5 for a fuller discussion):

- Embedded POI means that the VNF which is handling the communication also needs to handle LI. This is sometimes known as "on-switch" interception.
- External POI means that traffic is routed through an additional component which performs the LI separately from any existing network function. It may need access to look-up information or other details from the main network components, but it never asks for target-specific information (i.e. the target details do not leak outside the external POI).

External POI become increasingly difficult to achieve in an NFV or 5G environment, as they are adversely affected by encryption, anonymisation, multi-path communications, etc. In general, it will be much more effective to find ways to ensure that embedded POIs are sufficiently secure, rather than finding ways to ensure external POIs can function effectively.

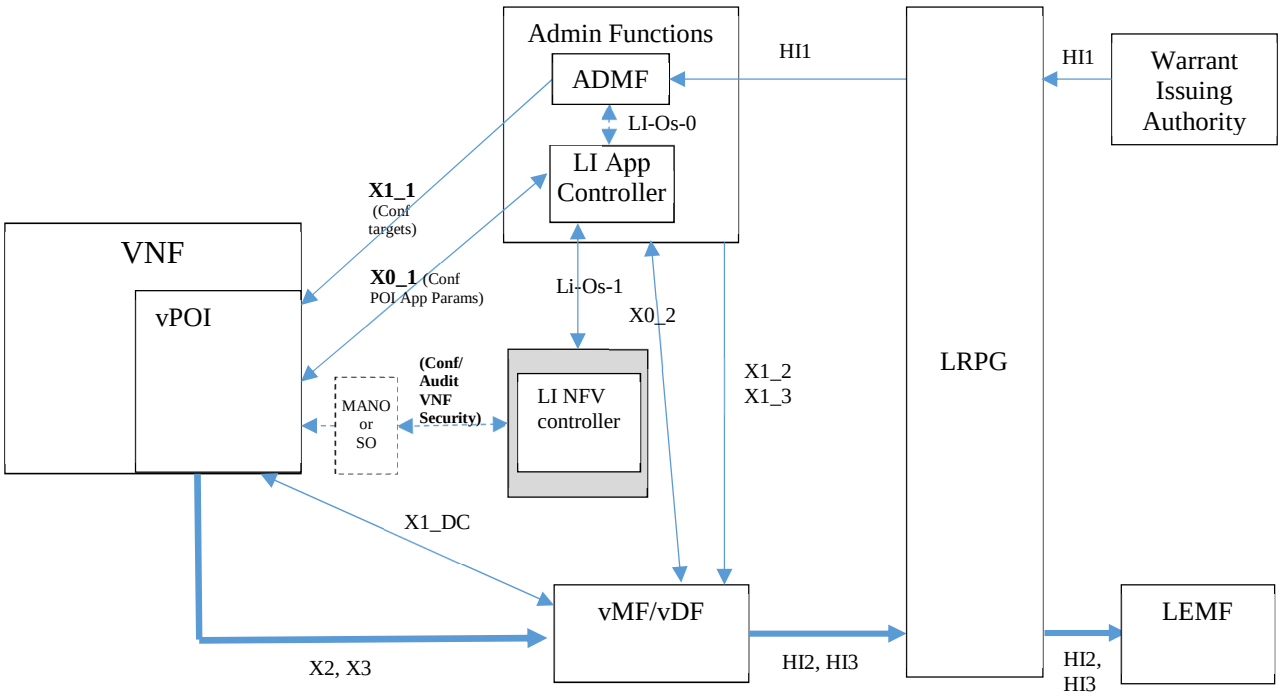

Figure 4.2.3-1: Simplified high level trusted virtualised LI Architecture, from ETSI GR NFV-SEC 011 [i.5]

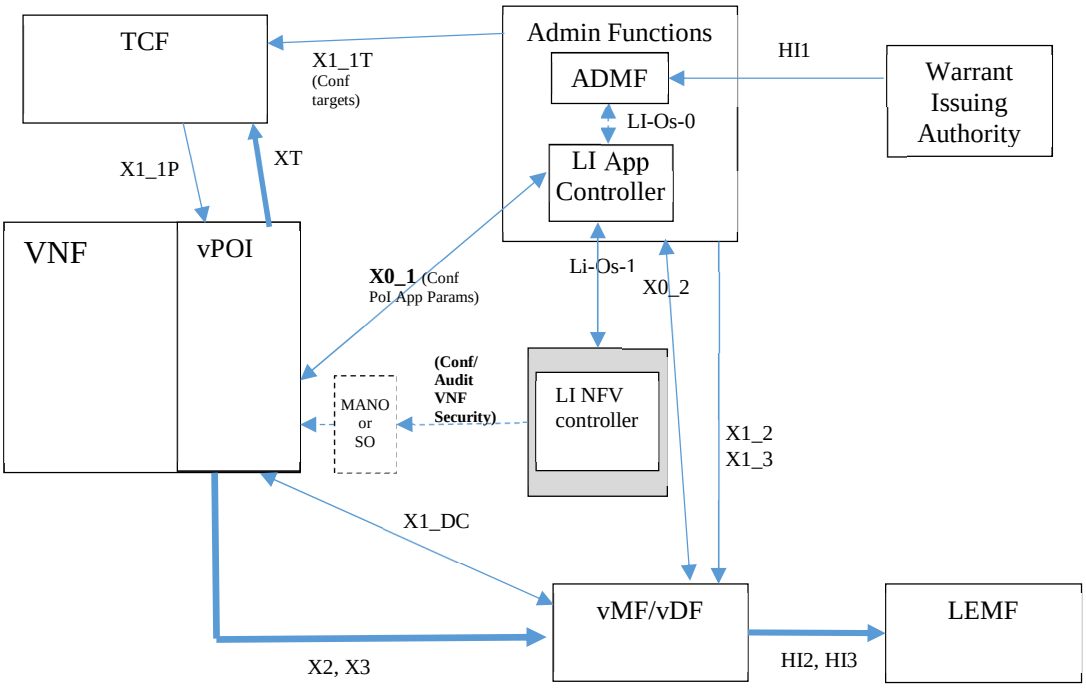

Figure 4.2.3-2: Simplified high-level low-trust virtualised LI architecture, from ETSI GR NFV-SEC 011 [i.5]

4.3 VNF scaling

For the purpose of scaling it is possible to add or remove hardware resources to a VNFCI, and to add or remove VNFCI to a VNF instance. The latter implies the existence of a data layer between the VNFCI, and potential operational data that can be saved in virtualised storage. These aspects have to be taken into account by the LI VNF developer for the security of the VNF.

Once instantiated, a NF can be composed of an arbitrary number of VNFC instances that do not necessarily reside on the same host. This introduces challenges to the proper operation of LI as illustrated in ETSI GR NFV-SEC 011 [i.5], clause 4.3.1.2, in particular regarding the location of vPOI and target data flow, as well as for certificate management.

4.4 Network virtualisation

MANO relies on the SDN Controller ETSI GS NFV-EVE 005 [i.10] to configure SDN resources and provide network connectivity. These resources can be PNF (e.g. dedicated switches) or VNF (e.g. virtual switches), for example ETSI GS NFV-EVE 005 [i.10], clause 4.3.3 identifies the following types of SDN resource:

- case a: physical switch or router;
- case b: virtual switch or router;
- case c: e-switch, software based SDN enabled switch in a server NIC; and
- case d: switch or router as a VNF.

Figure 4.4-1 illustrates the possible location of SDN resources in the virtualisation environment.

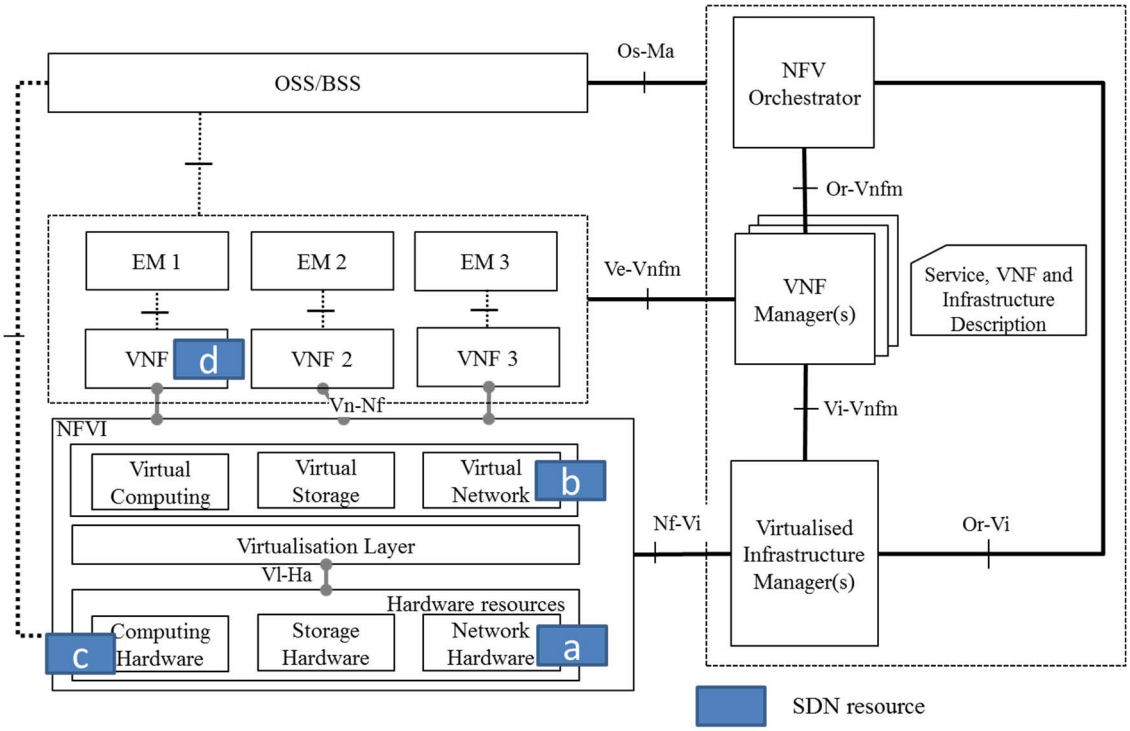

Figure 4.4-1: Possible SDN Resource Locations in the NFV Architectural Framework, from ETSI GS NFV-EVE 005 [i.10]

The SDN Controller can also be of different type as illustrated by figure 4.4-2. It can be embodied in a PNF residing aside the NFVI (case 5), a resource of the NFVI but not implemented as a VNF (case 3), a VNF running on top of the NFVI (case 2), or a function of the application layer or the VIM (cases 4 and 1).

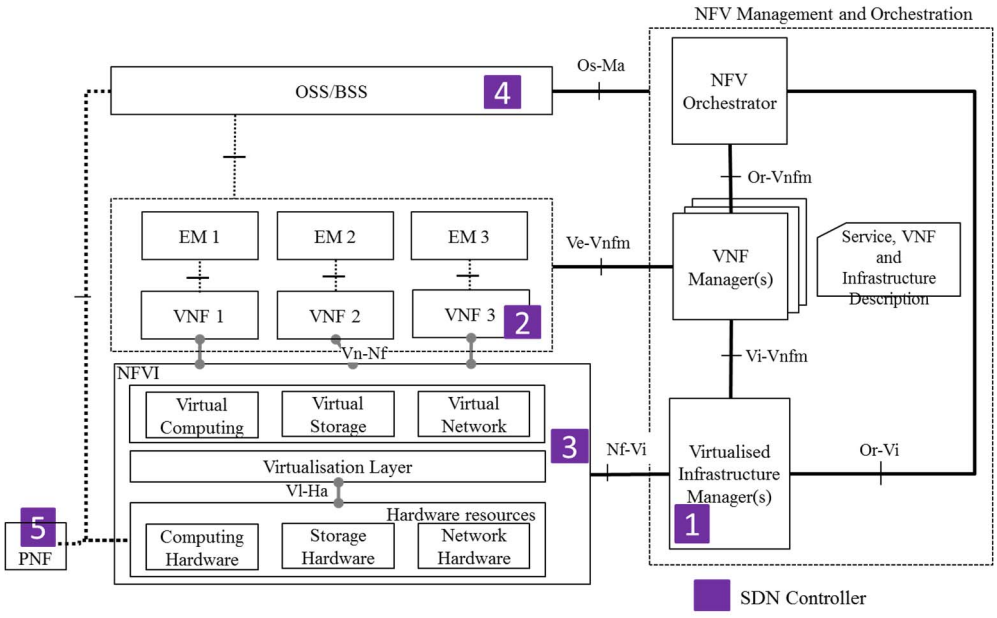

Figure 4.4-2: Possible SDN Controller Locations in the NFV Architectural Framework, from ETSI GS NFV-EVE 005 [i.10]

Within the virtualised environment there exists usually a hierarchy of SDN Controllers that are collectively responsible for connectivity but individually responsible for specific aspects. Figure 4.4-3 provides an example SDN Controller hierarchy matching an exemplary virtualisation stack. It should be noted that SDN Controllers can be responsible for connecting VNFC instances of a VNF instance together. In addition, in multi-tenant scenarios some SDN Controllers can be specific to a tenant, in particular at the application layer.

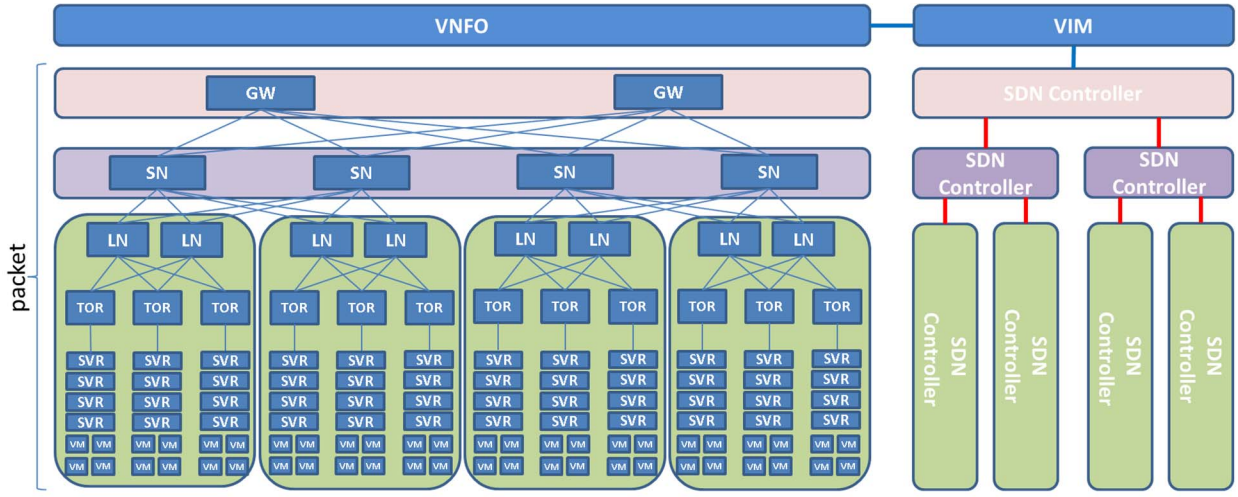

Figure 4.4-3: Typical Data Centre Structure, from ETSI GS NFV-EVE 005 [i.10]

NOTE: Abbreviations provided by ETSI GS NFV-EVE 005 [i.10] are GW - Gateway, SN - Spine Node, LN - Leaf Node, TOR - Top of the Rack, SVR - Server, and VM - Virtual Machine.

When the virtualised environment spans multiple physical locations (e.g. multiple datacentres), two categories of options exists for interconnection:

- using physical lines or functionally equivalent solutions such as MPLS tunnels or VPN (e.g. based on Network Domain Security) through a WAN; or
- using a WAN operator implementing a SDN WAN that is programmatically accessible to the operator's clients, which can be further refined depending on expected flexibility:
  - (option A) the WAN operator and the NFVI operator are in the same trust domain, the WAN operator serves a single client and exposes its SDN Controller to the client, this is illustrated in figure 4.4-4;
  - (option B) the WAN operator serves several NFVI operators, the WAN operator and the NFVI operators are in different trust domains, the WAN operators maintains its own SDN Controller and exposes a separate SDN Controller to each NFVI operator, this is illustrated in figure 4.4-5; and
  - (option C) the WAN operator serves several NFVI operators and does not maintain its own trust domain, each NFVI operator is provided an SDN Controller that has direct access to networking nodes.

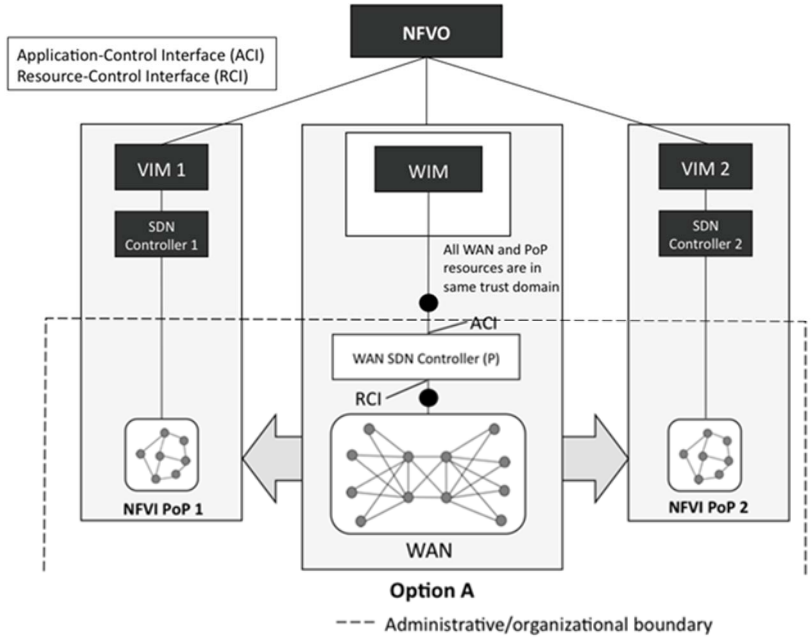

Figure 4.4-4: A Single SDN Controller for the WAN Resources, from ETSI GS NFV-EVE 005 [i.10]

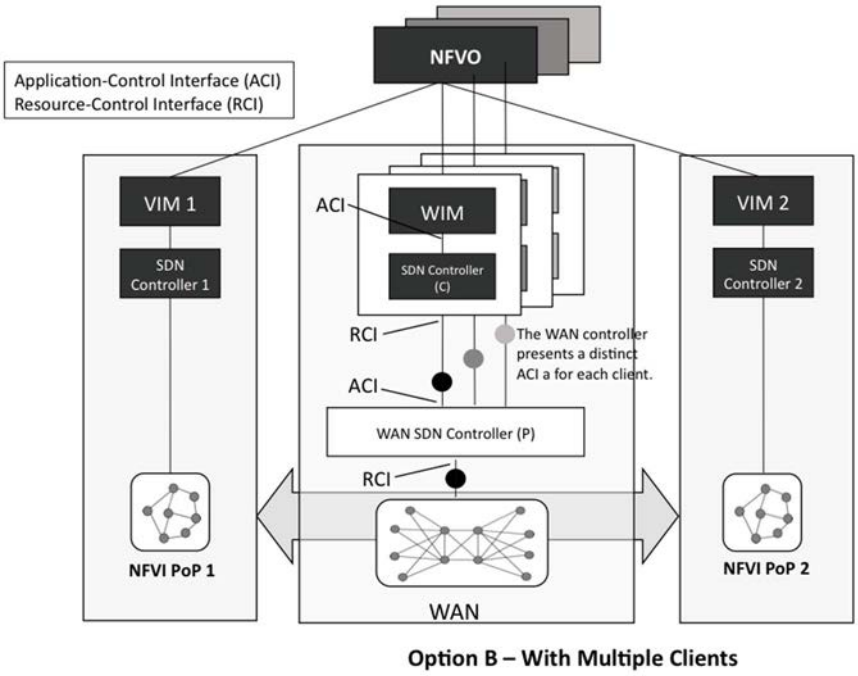

Figure 4.4-5: WAN SDN Controller accommodating multiple client SDN Controllers, from ETSI GS NFV-EVE 005 [i.10]

In general, the same security considerations for LI VNF and other VNF apply. From an LI perspective the LI Controller has to be able to ensure that the underlying connectivity between VNF/VNFC instances (and the establishment of connectivity) do not put the confidentiality and integrity of LI activities at risk. In the case of interconnection, not all SDN scenarios provide the same level of security assurance. Option A implies the NFVI and the WAN are in the same trust domain and provides the highest level of assurance. Option B can be an acceptable setup provided that LI operations cannot be inferred and interfered by SDN Controllers and networking nodes allocated to other clients. Option C provides little guaranty in this regard (in particular against interference to LI operations) and is not recommended.

4.5 Virtualisation hardware and software

Figure 4.5-1 provides a simplified view of the virtualisation hardware and software, considering its most important elements for the present document: CPU providing virtualisation instruction and security features (such as a trusted execution environment or hardware mediated execution enclave), hypervisor, virtual machines, TPM and vTPM. These elements are essential to ensure the trustworthiness and security of VNF instances running on top of the NFVI.

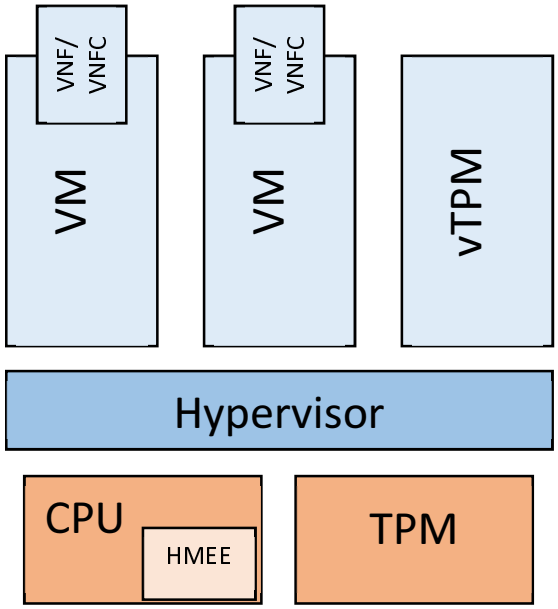

Figure 4.5-1: Simplified view of virtualisation hardware and software

5 Deployment scenarios

5.1 Deployment as physical network function (legacy deployment)

Legacy deployments are not in scope of the present document.

5.2 Deployment in a virtualised infrastructure

5.2.1 Single CSP

In this scenario, the CSP controls the entirety of the virtualised environment (NFVI, MANO, OSS/BSS and other applications and PNF). For example, the CSP hosts services within one or more datacentre it controls, and interconnection is provided over a WAN it controls.

This is the safest scenario as there is in principle reduced risks from third parties (as opposed to multitenancy scenarios). Third parties in this case are vendors providing the virtualisation stack and VNF. VNF vendors may not support a horizontal architecture where the VNF can run on a multi-vendor NFVI, and may instead provide their own virtualisation stack, requiring the CSP to integrate different vertical solutions. This can affect the security of CSP and of LI NFV.

5.2.2 Multi-tenant with one CSP controlling the virtualised environment

In this scenario CSP A controls the virtualised environment (NFVI, MANO) and provides virtualisation services to CSP B. CSP B may provide its own OSS/BSS, applications, VNF, and SDN Controller for the application layer.

This introduces a risk for CSP A as CSP B may introduce malicious VNF designed to capture or interfere with LI operations. On the other hand, CSP B does not control the NFVI and MANO which means it may prove difficult for CSP B to guarantee the trustworthiness of NFV instances and of the underlying network configuration.

5.2.3 Multi-tenant with no CSP controlling the virtualised environment

In this scenario both CSP A and B rent virtualisation resource from a third-party provider that controls the NFVI and MANO. In this case both CSPs are in the situation of CSP B in clause 5.2.2, and each may interfere with the operations of the other, as may the third-party provider.

5.3 Deployment in a mixed infrastructure

5.3.1 LI functions provided by PNF

It is possible that the CSP implements some LI functions using PNF in addition to VNF. Two categories of LI PNF can be considered:

- LI PNF that can easily reside on the edge of the NFVI, such as the ADMF and the DF.
- LI PNF that are closer to data flows, such as the POI, the TF and the MF.

The use of PNF in an otherwise virtualised environment can introduce risks in particular related to confidentiality as the PNF constitute a fixed point in an otherwise fully flexible network and service topology. This is particularly the case for the latter category of LI PNF.

5.3.2 Support functions instantiated as PNF

Even in a fully virtualised environment there may exist PNF relevant for security, due to the lack of VNF alternative. This is the case for HSM. When an HSM is shared across several VNF instances care has to be taken that the lifecycle of the HSM carefully follows that of the VNF instances for the management of cryptographic material, including secure deletion.

6 Threat model and risks

6.1 Generalities

The two high-level threats to LI/LD NF considered in the present document are:

- compromise of information, including data leakage and detection by unauthorized parties; and
- compromise of function, including misbehaviour of the NF and misconfiguration of the environment.

These threats can not only have an impact on the security posture of the CSP network, but also on the fulfilment of security requirements related to LI and LD. Security requirements for LI and LD are described in ETSI TS 101 331 [i.1] and ETSI TS 102 656 [i.2] (considering that LD closely resembles the case of retained data).

The security requirements for LI can be summarized as follows:

- Ensuring the availability and efficiency (real-time or near-real-time results) of the LI function.
- Ensuring that the LI function can be used by authorized persons and entities only.
- Ensuring the accuracy of CC and IRI.

- Ensuring non-disclosure to unauthorized persons or entities (confidentiality):
  - Concealment of LI implementation details at the CSP.
  - Confidentiality of target identities and target services.
  - Confidentiality of CC and IRI.
  - Controlled access to the LEMF.
  - Undetectability of LI activities by unauthorized persons, in particular communication parties, unauthorized personnel, and unauthorized third parties.
  - No alteration of operating facilities from an interception.
  - No alteration of quality of service from an interception.
- Ensuring auditability of the LI function (logging).
- Ensuring confidentiality and integrity of LI-related records.
- Being able to serve multiple LEA while following the non-disclosure requirements.

The security requirements for LD, adapted from the case of retained data, can be summarized as follow:

- Ensuring availability and efficiency of the LD service.
- Ensuring logging of requests allowing audits:
  - Ensuring confidentiality and integrity of LD-records.
- Ensuring non-disclosure to unauthorized persons or entities (confidentiality).
- Ensuring data quality, integrity and security of processing.
- Ensuring that the LD function can be used by authorized persons and entities only.
- Being able to serve multiple LEA while following the non-disclosure requirements.

NOTE: Integrity of records includes assurance for use of said records in evidence.

6.2 Threats related to Network Functions Virtualisation (NFV)

The present document notes the following threats related to NFV.

Threats to system availability:

- Ability to deny resource to the LI functions.
- Ability to deny LI functions themselves i.e. to fail to start the functions when requested.

Threats related to vulnerabilities to physical attacks:

- Ability to access memory. This includes in particular plug and play interfaces such as USB and hardware devices that use Direct Memory Access (DMA) on the host.

Threats related to the software environment:

- Ability to leverage a vulnerability present in commodity virtualisation software i.e. in a large number of NF, and thus to compromise NF in cascade.

Threats exist around attestation and loading code:

- Ability to introduce code which is not attested.
- Ability to attest code which is not genuine.

- Ability of the infrastructure or a NF to illegitimately instantiate an LI NF.

There are threats to LEA systems concerning locations and time:

- Ability to trick a VNF into thinking it is in a different physical place.
- Ability to trick the LI functionality into believing the time is different from the correct time.

Side-channels approaches present threats to law enforcement functionality:

- Ability to infer LI from analysis of resource usage, for example usage patterns of shared memory and storage resources.

Virtualisation presents additional threats to confidentiality and integrity:

- Ability to introspect i.e. look into LI functions or key management functions by a hypervisor (as discussed in ETSI GS NFV-SEC 009 [i.4]) or a function sharing the same physical resource.
- Ability to access or change stored data e.g. target lists or store of Retained Data.

NOTE: Data storage is a virtualised function itself and is not necessarily bound to the physical location of the NF.

- Ability to compromise or fake credentials e.g. untrusted host.
- Ability to access data from decommissioned NF. Secure clean-up is essential as threats to the confidentiality of data are presented by a failure to shut down and clean-up LI functions.

Cryptography issues can give rise to threats:

- Ability to adversely affect sources of entropy resulting in insecure communication or storage. Gathering of entropy at the level of the virtual machine (in order to seed a random number generator) can be challenging and requires a trusted source. NF that do not have their own CSPRNG will require a trusted source of randomness for which the virtualisation stack may not provide enough assurance. More information on these risks can be obtained from ETSI TS 103 307 [i.7].

Threats exist around placement of functions and isolation:

- Ability to place functions outside of determined boundaries e.g. in insecure places or the wrong side of jurisdictional boundaries.
- Failure to separate trust domains adequately leads to threat of attack from genuine parts of CSP network which are at a reduced security level compared to LI.

Finally, threats arise because of the difficulty of testing virtualised software in realistic conditions. For example, the virtualised software may be tested on a dedicated NFVI that is not comparable to an actual deployment.

6.3 Threats related to Software Defined Networking (SDN)

The present document notes the following threats related to SDN.

Threats related to availability:

- Ability to deny access to traffic (e.g. through the manipulation of routes, the injection of traffic resulting in a denial of service, or the compromise of an SDN function).
- Ability to route traffic around an NF.

Threats related to confidentiality:

- Ability to duplicate traffic to another location.

Threats related to integrity:

- Ability to alter or inject traffic.

Threats to specific aspects of law enforcement functionality:

- Ability to infer LI from analysis of resource usage, connection patterns and performance.
- Ability to infer LI from analysis of SDN flow rules and other configuration data (e.g. through memory scrapping of the SDN Controller or of another SDN function).
- Ability to route traffic from (or to) inappropriate jurisdictions.

7 Applicable security measures

7.1 Introduction

A range of security topics is put forward in this clause. For each topic, measures are put forward which are basic, extended or advanced.

The basic measures are designed to be strong but achievable industry-best-practice techniques. The extended measures could be more difficult to implement and sometimes includes cutting-edge techniques and practices. It is acknowledged that some of the advanced security practices are concepts which are theoretical or academic and it is not necessarily realistic to build them. There may be environments which have risk factors that cannot be mitigated by currently-available technology. It is therefore not recommended to perform LI (or other sensitive CSP functions) on such an environment.

The use of each measure should be considered in the context of individual deployments and the present document does not provide a *pass* or *fail*. The following points should be considered:

- the basic measures are recommended for all scenarios and are likely to be sufficient for an environment which is high-trust with a single CSP using the environment;
- as extra flexibility or sharing of resources is introduced to the deployment and architecture this would require use of extended measures; and
- the advanced measures are for the fullest and most flexible virtualisation architectures.

EXAMPLE 1: A basic response would include basic reporting of lifecycle events and other management events relating to LI-relevant nodes by the MANO components to security or LI monitoring systems.

EXAMPLE 2: An extended response would be the use of HMEE (hardware mediated execution environments) such as SGX (or similar). It should be noted that already this is difficult commercially as these are not necessarily supported by off-the-shelf OS or MANO components such as OpenStack®.

NOTE: The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. ETSI is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

EXAMPLE 3: An advanced response would be the use of run-time attestation which would provide a check regarding whether code had been altered at run-time. This could be very difficult to implement.

7.2 VSP - Virtualisation Stack Protection

This clause covers measures to protect the virtualisation stack in hardware and software. Specifically, the goal is to protect the VNF (LI NF) within the virtualisation stack.

VSP-01 - BASIC - Trust domains: Ensure that trust domains are defined. The system should manage (e.g. define, enforce) the security policies for each trust domain independently. The system should ensure that there is a dedicated LI trust domain, but it is also important that the other trust domains are managed correctly.

VSP-02 - BASIC - Inter VM communications: Ensure that communications between various component VMs within a single VNF use encryption. They might be physically hosted in different places and the communications between them might be insecure. See also clause 7.5 of the present document.

VSP-03 - BASIC - Functions not on bare metal: Sensitive functions should not be run on bare-metal (i.e. they should run on type-1 hypervisors). This advice applies until it is possible to demonstrate adequate isolation procedures for use of bare-metal technology for cloud-native applications. Additionally, there are concerns about the ability to keep patches up-to-date with bare metal computing.

VSP-04 - EXTENDED - Isolation and confidentiality: Techniques should be used to protect sensitive processes and databases as described in clauses 7.4 and 7.5 of the present document.

VSP-05 - BASIC - Hardware-based root of trust: A hardware-based root of trust should be used, with the features defined in ETSI GS NFV-SEC 012 [i.6], clause 5.1, item 1 and clause 8.10. It should be possible to restrict the booting procedure by preventing the running of workloads if assistance from the HBRT is not available or the HBRT currently does not contain valid cryptographic material. The intent of this requirement is to stop VNFs/VNFCIs being loaded onto possibly compromised hardware and to allow appropriate mitigations to be put in place (see ETSI GS NFV-SEC 012 [i.6], clause 5.2).

NOTE: This particular use of the HBRT is known as platform attestation. The HBRT can also be used for validation of software assets as specified in SCM-03 and SCM-07, including pre-execution check of VNFs/VNFCIs.

VSP-06 - BASIC - Key management system: The host system should implement a key management system with the features defined in ETSI GS NFV-SEC 012 [i.6], clause 5.1, item 2.

VSP-07 - BASIC - No direct access to memory: The host system should be able to deny direct access to memory to particular hardware resources (ETSI GS NFV-SEC 012 [i.6], clause 8.12).

VSP-08 - BASIC - Access control to host memory: The host system should implement hardware memory access controls (IO-memory management, e.g. IOMMU, VT-d, AMD-Vi) (ETSI GS NFV-SEC 012 [i.6], clause 8.12).

VSP-09 - BASIC and **EXTENDED - Prevent memory inspection:** In order to protect against memory inspection of LI sensitive data, security measures such as dedicated administrator roles and access control to memory for VMs and hypervisors should be followed.

VSP-10 - EXTENDED - Prevent hypervisor breakout: The NFVI should provide security isolation to minimize the impact of and detect hypervisor/VM breakout.

VSP-11 - BASIC - Patch policies: The NFVI and VNFs should be patched regularly i.e. every 14 days for critical bugs, 90 days for others.

VSP-12 - BASIC - Prevent VNF breakout: The system should try to prevent and detect attacks that breakout from an attacked VNF through the virtualisation layer to any other VNF or any other location.

VSP-13 - EXTENDED - Infrastructure lock-down: The infrastructure should be locked-down to avoid enabling unnecessary attack vectors and to make it easier to monitor whether a network is behaving appropriately. This includes techniques such as physical host isolation and attestation, as well as management of host services.

7.3 IR - Incident Response

This clause describes incident detection and response using information from the virtualisation stack.

IR01 - BASIC - Logging policies: Logging should be enabled, for example as described in provision CSC 6 of ETSI TR 103 305-1 [i.13], clause 4.6.

IR02 - BASIC - Post-incident analysis: Post-incident analysis needs to include checking logs (traffic logs and logs from applications), integrity checks (physical components, software and file systems), checks for modifications to systems (applications data, hosting service data or any permissions modification). Checks should be made to any human reports of unusual system behaviour.

IR03 - BASIC - Post-incident response: Consider a post-incident response plan, for example as described in provision CSC 19 of ETSI TR 103 305-1 [i.13], clause 4.19.

7.4 ISOL - Isolation through leveraging the virtualisation stack

This clause looks at techniques which leverage the virtualisation stack to allow for isolation (e.g. MANO, SDN).

ISOL-01 - BASIC - Isolation by design: It is important to demonstrate that, from the earliest stages of the design process, isolation of sensitive components has been major consideration. The isolation requirements need to be evident in planning overall system design, with evidence that these considerations are extending in a coherent way through to all the subcomponents of the design.

ISOL-02 - EXTENDED - Security of sensitive data: Techniques should be used to protect sensitive databases. The list of targets is the most sensitive information for LI, together with any keys for encryption used to secure information that identifies any target (i.e. tasking, or delivered traffic containing identifiers). Such databases should be stored in a Hardware Security Module (certified e.g. according to NIST FIPS 140-2 [i.11]) or Trusted Platform Module (see ISO/IEC 11889-1 [i.12] based on the TCG TPM Library), that is made available to NFs within the NFVI in a secure manner.

ISOL-03 - EXTENDED - Security of sensitive processes: Techniques should be used to protect sensitive processes i.e. those which use the target selectors to create target traffic (up to the point that it is encrypted for secure delivery). Sensitive processes should take place in a Trusted Platform Module (see ISO/IEC 11889-1 [i.12] based on the TCG TPM Library) or Hardware-Meditated Execution Enclave (HMEE). The HMEE should conform to the statements in ETSI GS NFV-SEC 009 [i.4], clause 6.16 and also consider ETSI GS NFV-SEC 012 [i.6], clause 8.9.

ISOL-04 - EXTENDED - Workload isolation: Functions which share memory between workloads should be able to be prohibited in the manner described in ETSI GS NFV-SEC 012 [i.6], clause 6.2.

ISOL-05 - EXTENDED - Prohibition of binary image caching: The features in ETSI GS NFV-SEC 012 [i.6], clause 6.2 regrading prohibiting binary image caching should be considered.

ISOL-06 - BASIC - Isolation through software defined traffic rules: Limit both incoming and outgoing traffic in an efficient and scalable way through software defined traffic.

ISOL-07 - EXTENDED - Separation of physical hosts: Physical hosts should be physically and logically segregated, and virtual workloads should be configured such that the impact of one physical host being compromised is limited to the smallest set of virtual networks and workloads possible.

7.5 CM - Confidentiality Measures

This clause includes measures beyond those in clause 7.4 of the present document for ensuring confidentiality (communication security, secure storage, secure deletion, in-memory encryption). It includes both data-at-rest and data-in-transit. Many of these techniques will be ineffective without the measures in clause 7.4 of the present document (isolation of sensitive functions).

CM-01 - BASIC - Review list of cryptographic algorithms: Ensure that old ciphers are removed from available choices. This is true for non-virtualised environments but can be particularly important in virtualised environments where physical controls are not possible. Specifically:

- In general, by default, a very limited and modern set of ciphers should be used.
- In exceptional cases then a lower tier of less modern ciphers may be used on a case-by-case basis but these should not be used without justification.
- However, ciphers should not be used where they have known, published compromises.

CM-02 - BASIC - Intra-NFV communication security: Consider that there will be vulnerable communications links even within a given virtualised function whenever that function can be split between different physical components. Data-in-transit security should encompass data in transit within a given function wherever there is a possibility that the function is not wholly in a secured environment.

CM-03 - BASIC - Inter-guest communication security: Ensure that communications between container or between pods, or other forms of virtualised guests, are demonstrably secured, even when they are local or using the same kernel. It should be possible to demonstrate that sensitive data has been isolated and secured. Internal/local techniques for transmitting data should not be used if it is not possible to assure these processes, i.e. it may be necessary to revert to more traditional approaches if those are the only ones that can be reliably assured.

CM-04 - BASIC - Secure deletion of data: Ensure data is deleted securely, being particularly careful wherever physical storage resources could be re-used by functions from a third party. This is not always possible to verify and instead it may be sufficient to ensure that data is deleted using the secure delete command. It is also possible to consider the use of full-disk encryption.

CM-05 - BASIC - Proper termination point for encryption: Encryption for data in transit should be terminated as close as possible to the function using the connection. Specifically, encryption should be terminated within the correct container rather than alongside it (i.e. not in a "sidecar"). When a function moves (e.g. a container moving to a new compute node), it should be clear that the termination of the encryption moves with it.

CM-06 - BASIC - LI Certificate Authority: Look carefully at situations where there are different requirements for the CA that is needed for LI-sensitive functions compared to the requirements for CAs for other purposes. If there is a conflict between these two requirements sets, then two separate CA should be established, with the LI CA being kept separate and managed separately (e.g. with extra controls on the security clearance of those involved).

CM-07 - BASIC - Hardware-based protection of data-at-rest: Consider use of HSM and TPM (see clause 7.4) for protection of data-at-rest.

CM-08 - BASIC - Evolution of platform capabilities: Consider secure management of keys, cryptographic algorithms and security services offered by the platform to ensure ability of evolution, security strengthening, and countermeasure deployment (see ETSI GS NFV-SEC 012 [i.6], clause 5.2).

CM-09 - BASIC - Host entropy: The host system should meet a minimum entropy standard such as that described in NIST SP800-90b [i.14]. The designed and actual entropy obtained should be measurable (see ETSI GS NFV-SEC 012 [i.6], clause 6.4).

BASIC - Host random number generator: The host system should implement a Random Number Generator for cryptographic purposes, meeting the requirements of ISO/IEC 18031 [i.15].

7.6 BESP - Interaction of bespoke hardware with a virtualised environment

This clause contains measures related to the interaction of bespoke hardware with a virtualised environment (i.e. LI/LD PNF vs. NF).

BESP-01 - BASIC - Prevent attacks from a vulnerable PNF: The system design should consider vulnerabilities in which a PNF could be used as a starting point for an attack against VNFs, potentially taking advantage of legacy security used by PNFs and not understood by VNFs.

BESP-02 - BASIC - Prevent attacks from a vulnerable VNF: The system design should consider vulnerabilities in which a VNF could be used as a starting point to forward malicious messages to a PNF which has not been secured against attacks of that nature.

BESP-03 - BASIC - Authenticated and approved communications between NF: LI functions should be configured so that NFs can only communicate with NFs which they are specifically authorized to communicate with (irrespective of whether the NF is a PNF or a VNF). The default should be for two NFs not to trust one another and to block communication.

7.7 ACIM - Access Control and Identity Management

This clause relates to access control and identity management as it relates to virtualisation i.e. excluding access control and identity management for physical resources.

ACIM-01 - BASIC - Access control to LI selectors databases: Ensure that databases containing LI selectors have appropriate access control and interfaces are not exposed beyond the places that this is necessary. This is clearly also true for non-virtualised environments, but is even more important if virtualisation facilitates access to the database.

ACIM-02 - BASIC - Protection of key and certificate stores: Ensure key and certificate stores have a level of protection suitable for the capability of the key or certificate.

ACIM-03 - BASIC - LI and root function interaction: When creating account permissions, ensure that the interaction of the root function and the LI function are carefully managed. Where root functions can create and delete LI functions, ensure that the consequences of this are understood.

ACIM-04 - BASIC - Limitation of LI privileges: It is important that various management and support functions do not get LI privileges (this should be carefully assessed where certain functions are overseas). LI privileges can only be made available to those with the right clearance. This will need sufficiently granularity in the roles to cover the eventualities. Ensure that where system dumps are shared with support functions, that they do not contain LI-sensitive material.

ACIM-05 - BASIC - Role management: There should exist a table of all roles and all the access privileges each role has been given (i.e. all the functions they are allowed to run). Users should not be allowed customized roles or profiles. Each function should be assessed to determine whether it exposes any LI capabilities, i.e. explicitly (because it is an LI function) or accidentally (e.g. because it allows a user to see material on the X1 interface), noting that NFV introduces many more paths for accidental access. There should be a clear process whereby it is established which roles have the ability to see LI-sensitive material, and the processes by which people are granted access to these roles. Administration responsibilities should be split between a global administrator role and delegated administrator roles, where the global administrator role should only be used to manage permissions of delegated administrator roles, and delegated administrator roles should each be limited to the minimal set of administration duties possible. Access to and use of administrator roles should be logged and only be possible from attested devices and by using multi-factor authentication.

ACIM-06 - EXTENDED - Mandatory Access Control: Mandatory Access Control (MAC) should be used. It is noted that examples in this space include: SELinux or Mandatory Integrity Control (Windows®). Access control policies should be applied to processes attempting access to LI-sensitive files and network resources. Privilege levels should be set to minimize the damage that could be caused by an authorized process which was compromised.

NOTE: SELinux in an open source project, Mandatory Integrity Control is a product of Microsoft Corporation. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

ACIM-07 - BASIC - Protection of credentials: The host system should ensure that all authentication credentials are presented in an encrypted fashion. The host system should not store any authentication credentials in clear text or unencrypted.

ACIM-08 - BASIC - User account management: The host should disable all non-essential functions for user accounts (e.g. administrative privilege, change root capabilities, input/output (physical and virtual)) and for service ("non-user") accounts (e.g. shell access, remote login, input/output (physical and virtual)).

7.8 PERF - Ensuring performance of the LI/LD solution

This clause considers measures for ensuring the performance of the LI/LD solution (availability, timeliness). It includes measures which combat deliberate attacks (such as denial of service attacks) and also non-deliberate problems.

PERF-01 - BASIC - Pruning of monitoring feeds: Ensure that performance monitoring feeds do not contain sensitive LI information.

PERF-02 - BASIC - Security monitoring: Ensure security monitoring is in place to alert security monitoring systems to denial of service attacks. Ensure security monitoring systems report appropriately to LI systems whenever LI functions are potentially affected.

PERF-03 - BASIC - Performance monitoring: Ensure performance monitoring solutions are in place and are receiving information from appropriate levels of the NFV stack e.g. NFVO-level components in MANO but also the lower-level VIM. Ensure that performance monitoring solutions are appropriate linked to LI monitoring and security centres to provide information on LI-affecting issues.

PERF-04 - BASIC - Safeguard LI performance: Ensure that mitigations taken by performance management systems prioritize the performance of LI-related components and systems.

PERF-05 - BASIC - Ensure resource availability to LI processes: the system should manage the utilization, traffic distribution, and overload control of the NFs and sub-NFs to ensure availability for LI processes. Network functions should not be allowed to continue if there is insufficient availability for LI processes (this should not apply only to targets, otherwise it would be clear who was a target).

PERF-06 - BASIC - Redundancy: The system should be deployed in such a way as to provide isolation and redundancy to increase the resiliency and defence against a single point of failure. MANO functions should include internal health checks to detect potential intrusion and take protective action.

7.9 OM - Operational Measures

This clause includes organizational measures such as contact points, personnel controls, operational policies and physical access control adapted to LI and LD.

OM-01 - BASIC - Physical separation according to security level: In situations where users can access both high-security and low-security systems, ensure that there is appropriate physical separation between systems to avoid confusion or transfer of data between the systems.

OM-02 - BASIC - Security controls: Consider logical controls as well as physical controls i.e. two-factor authentication or time-based controls.

OM-03 - BASIC - Physical security controls for hardware: Industry best-practice techniques are required for the underlying hardware security, wherever the hardware is based. These include the physical controls and alarms as listed in ETSI GS NFV-SEC 009 [i.4], clause 6.4, to cover any hardware which is or may be running LI-sensitive functions or LI-sensitive storage. Also consider the requirements on alarms from ETSI GS NFV-SEC 012 [i.6], clause 8.3.

OM-04 - BASIC - Security controls for personnel: Industry best-practice techniques are required for personnel checks wherever LI functions may be present. This will include the administration of the hosting service, VIM, SDN and VNF catalogue.

OM-05 - BASIC - General and LI management: It is important to make a distinction between general administration/security management and the LI-specific and LI-sensitive management. Either *all* security management has to be cleared for LI access, or it has to be possible to create separate roles for general security management and LI management. If so, it needs to be ensured that general security management will not be able to create new LI manager accounts (which would defeat the point).

OM-06 - EXTENDED - Secure wipe capabilities: The host system should provide secure wipe capabilities meeting at least those specified in NIST SP 800-88 Rev. 1 [i.16] which can be used at the time of deprovisioning for any files associated with a workload. It should be possible for authorized external services to confirm completion of the secure wipe operation. Storage which is in the process of a secure wipe should not be reallocated until that operation is successfully completed.

OM-07 - BASIC - Debug options off by default: The host system should be booted with debug options off by default. The host system should make a record when debug options are turned on. This record should be unalterable without a power off or reboot of the host system.

OM-08 - EXTENDED - Local restriction to debug options: Consider using a capability that makes it impossible to turn on debug options for the host system. When this capability is provided, the host system needs to have an interface to provide authorized external services with information about this capability. The host system should have an interface to provide authorized external services with information about the state of its debug options, including historical state since boot. The host system should provide a mechanism to report to authorized external services when a change in debug status occurs.

OM-09 - BASIC - LI and jurisdiction: The system should ensure LI functions and LI target lists remain within a single legal jurisdiction. This includes protection against data leakage, data encryption at rest and in transit, security policies restricting the location of sensitive data, and secure deletion of memory and storage resources.

OM-10 - EXTENDED - Network time source: The system should provide a protected and trusted network time source. These should be sufficient to mitigate clock-tampering issues such as tampering of security logs, expiry of used certificates or UEs getting out of sync with the network. If an attack manipulates the network timing source or VNF clock, the network can be compromised.

7.10 AU - Audit

This clause considers audit capabilities for data integrity and authenticity protection. It includes the ability of security or audit monitoring functions to collect and check (on an ongoing basis) audit functions or log files. It includes measures that assure that certain isolated areas could only have been accessed by those with permission to do so.

AU-01 - BASIC - Audit logs security: Any audit logs should be securely stored. The logs should have integrity checking using hashes which are securely stored (e.g. consider - for EXTENDED only - in a TPM or HSM see clause 7.4). Consider creating a chain of entries which provides ongoing assurance against tampering or modification.

AU-02 - EXTENDED - Secure logging: The features of the logging system should conform to the statements in ETSI GS NFV-SEC 012 [i.6], clause 8.1.

AU-03 - BASIC - Audit logs permissions: Consider using permissions to ensure that certain parties can add but not modify the audit logs, and others (the auditors) can read *but not write to* the audit log. See also ETSI GS NFV-SEC 009 [i.4], clauses 6.8 and 6.9.

AU-04 - BASIC - Pruning of log files: Ensure that log files do not contain sensitive information, or if they do then ensure they are separate and sufficiently protected. Specifically, there should be dedicated LI-based logging which is separate from generic logging.

AU-05 - EXTENDED - System configuration record: A record should be maintained of all installed and/or running software, configurations and versions, which should include debug status of any component of the host system.

AU-06 - EXTENDED - Secure software management record: A time-stamped, confidentiality-protected and integrity-protected record and history of changed/updated software with reasons for changes should be maintained, which should be protected from unauthorized access.

AU-07 - BASIC - Authorized users and accounts: A record should be maintained with a list of authorized users and accounts for each host (see ETSI GS NFV-SEC 012 [i.6]).

AU-08 - BASIC - Query mechanism for software version: The host should provide a means by which current versions of software and configurations can be queried by an authorized party.

AU-09 - ADVANCED - Prevention of LI detection by analytics: Consideration should be given to the wider analytics that may be used on logging in future e.g. via Machine Learning. These could inadvertently spot LI activity even if they are not exposed directly to LI logging. For example, it is possible that Artificial Intelligence security analytics could spot anomalies due to LI because of the absence of data for certain tasks or processes, rather than because data was logged for those processes.

7.11 SCM - Supply Chain Management

This clause considers measures related to supply chain management and assurance of LI/LD NF and of other assets (e.g. catalogue management, attestation). It only considers aspects relating to virtualisation i.e. it has a focus on short-term verification or assurance of assets rather than longer-term contractual concerns. As described in the scope of the present document, this clause does not cover broader national security concerns in relation to supply chains or vendors.

SCM-01 - BASIC - Examine product composition: Care should be taken around consolidated products i.e. where multiple services are provided by one product. In particular, it is not recommended that products are used which combine security functions (e.g. a firewall) with other telecommunications functions.

SCM-02 - EXTENDED - Remote attestation service: The host system should support the use of a service providing remote attestation as defined in ETSI GS NFV-SEC 012 [i.6], clause 6.1. The statements regarding "bare metal" deployments in that clause should be considered.

SCM-03 - ADVANCED - Component measurement: Attestation is a core component of ensuring trust in a chain of components. The hashes of various components in the boot sequence should be measured and stored securely e.g. in a TPM or HSM (see clause 7.4). Each time the boot sequence is completed, the hashes should be checked to match the required values. Other parameters may be measured and should be checked to be within appropriate boundaries (see ETSI TS 102 656 [i.2], clause 4.4.5.1 for further details).

SCM-04 - EXTENDED - Requirements for attestation: It should be possible to attest the hardware layer, virtualisation layer, and VNF layer prior to the operation of a VNF.

SCM-05 - ADVANCED - Run-time integrity: Local agents should be present to perform integrity-checking of running processes and periodic checking of executable and binary file integrity. The issues around the vulnerability of agents (ETSI GS NFV-SEC 012 [i.6], clause 6.3) should be considered.

SCM-06 - EXTENDED - Run-time integrity extended requirements: Further processes for software integrity protection are provided in ETSI GS NFV-SEC 009 [i.4], clause 6.21.

SCM-07 - EXTENDED - Pre-installation and pre-execution checks: The host system should verify the provenance and integrity of all instances and versions of software components before installing them (refusing to install all software which fails verification against the policies held by the host system). The host system should verify the integrity of software components before execution. See ETSI GS NFV-SEC 012 [i.6], clause 8.14.

SCM-08 - EXTENDED - Software catalogue: Software catalogues holding LI VNF images should be integrity protected.

SCM-09 - EXTENDED - Third party hosting: Smaller CSPs may be run as a tenant in an IAAS or NAAS model (i.e. not operating their own virtualisation host infrastructure). If so, requirements around third party hosting should be followed. This includes confidentiality protection of sensitive information, the ability of the third party hosting environment to help CSP meet legal and regulatory requirements and the ability to attest the third party environment.

Annex A:
Checklist for Communication Service Providers

A.1 Introduction

The present annex provides a summary of the security requirements identified in clause 7 along with a methodology for Communication Service Providers (CSPs) to select security requirements that are relevant to the deployed configuration. In clause A.4, a pro forma checklist is provided to help CSPs evaluate the security of their deployment.

A.2 Categorization

The type of security measures which are applicable will depend on the risk associated with the type of NFV deployment under consideration.

The present document puts forward an informal categorization process for risks and for security measures. This categorization process is only an informal guide. The formal approach would be to assess the threats and establish in each case how to mitigate any risks which were incompatible with the security requirements in clause 6.2 of the present document.

The present document works based on an informal categorization into three levels: BASIC, EXTENDED, and ADVANCED:

- the BASIC security measures are recommended except where there is a reason for that topic not to be applicable;
- the EXTENDED security measures are recommended where there are any minor threats/risks beyond the traditional configuration; and
- the ADVANCED security measures are recommended to mitigate any major threats/risks.

The following areas would contribute to the type of measures which are required:

- The type of environment - whether it is a high-trust or low-trust as defined in clause 4.2.2 of the present document. The high-trust environment (falling fully into the "high-trust" definition in the first bullet) is one which requires only basic responses. If there is management or use of resources from third parties which are known or trusted to the CSP - this would imply that extended security measures are required. Any involvement of unknown or untrusted third parties - this would add a major risk and implies that advanced measures are required.
- The choice of architectures in clause 4.4 of the present document. Option A has the NFVI and the WAN in the same domain and does not (in itself) imply that measures beyond BASIC are required. Option B introduces a risk that LI operations can be deduced and affected by SDN controllers and therefore EXTENDED measures would be required to address these risks. As described in clause 4.4 of the present document, option C contains very significant risks and highly sophisticated mitigations would be required to prevent interference in LI operations.
- The deployment scenario in clause 5 of the present document. The single CSP infrastructure (clause 5.2.1 of the present document) requires basic responses. The multi-tenant infrastructure requires extended measures if the other CSP(s) are known and trusted, and otherwise it requires advanced security measure, as does the scenario in clause 5.2.3 of the present document.

A.3 Checklist

A checklist can be created using the following process:

- All BASIC requirements should be considered for all deployments. In some cases, there may be reasons why they are not appropriate, in which case they should not be followed.
- Check the type of environment (high-trust or low-trust) as defined in clause 4.2.2 of the present document to assess whether any EXTENDED measures would be required to mitigate issues from low-trust environments.
- Similarly, the choice of architecture in clause 4.4 should be noted to see if EXTENDED measures are required to prevent interference in LI operations based on risks from options B or C.
- The deployment scenario in clause 5 should be checked with multi-tenant infrastructures requiring EXTENDED or ADVANCED measures as described in clause A.1 of the present document.

A.4 Checklist pro forma

The pro forma checklist below is provided as an example for the CSP to evaluate LI network function security of a specific deployment against the provisions identified in clause 7. The fields are defined as follow:

- **Reference:** the identifier of a given provision, as defined in clause 7.
- **Level:** the security level the same provision applies to, as defined in clause 7.
- **Title:** the name of the same provision, as defined in clause 7.
- **Selected:** indicates whether the CSP has selected this provision as part of the risk analysis according to clause A.2.
- **Fulfilled:** indicates whether the selected provision is fulfilled by the deployment considered.
- **Justification:** indicates a reference to a document providing justification to the result obtained in the 'fulfilled' field.

Table A.4.1: Applicable security measures for LI network function security

Applicable security measures for LI network function security					
Reference	**Level**	**Title**	**Selected (y/n)**	**Fulfilled (y/n)**	**Justification (ref.)**
7.2 VSP - Virtualisation Stack Protection					
VSP-01	BASIC	Trust domains			
VSP-02	BASIC	Inter VM communications			
VSP-03	BASIC	Functions not on bare metal			
VSP-04	EXTENDED	Isolation and confidentiality			
VSP-05	BASIC	Hardware-based root of trust			
VSP-06	BASIC	Key management system			
VSP-07	BASIC	No direct access to memory			
VSP-08	BASIC	Access control to host memory			
VSP-09	BASIC EXTENDED	Prevent memory inspection			
VSP-10	EXTENDED	Prevent hypervisor breakout			
VSP-11	BASIC	Patch policies			
VSP-12	BASIC	Prevent VNF breakout			
VSP-13	EXTENDED	Infrastructure lock-down			
7.3 IR - Incident Response					
IR-01	BASIC	Logging policies			
IR-02	BASIC	Post-incident analysis			
IR-03	BASIC	Post-incident response			
7.4 ISOL - Isolation through leveraging the virtualisation stack					
ISOL-01	BASIC	Isolation by design			
ISOL-02	EXTENDED	Security of sensitive data			

Applicable security measures for LI network function security					
Reference	**Level**	**Title**	**Selected (y/n)**	**Fulfilled (y/n)**	**Justification (ref.)**
ISOL-03	EXTENDED	Security of sensitive processes			
ISOL-04	EXTENDED	Workload isolation			
ISOL-05	EXTENDED	Prohibition of binary image caching			
ISOL-06	BASIC	Isolation through s			
ISOL-07	EXTENDED	Separation of physical hosts			
7.5 CM - Confidentiality Measures					
CM-01	BASIC	Review list of cryptographic algorithms			
CM-02	BASIC	Intra-NFV communication security			
CM-03	BASIC	Inter-guest communication security			
CM-04	BASIC	Secure deletion of data			
CM-05	BASIC	Proper termination point for encryption			
CM-06	BASIC	LI Certificate Authority			
CM-07	BASIC	Hardware-based protection of data-at-rest			
CM-08	BASIC	Evolution of platform capabilities			
CM-09	BASIC	Host entropy			
CM-10	BASIC	Host random number generator			
7.6 BESP - Interaction of bespoke hardware with a virtualised environment					
BESP-01	BASIC	Prevent attacks from a vulnerable PNF			
BESP-02	BASIC	Prevent attacks from a vulnerable VNF			
BESP-03	BASIC	Authenticated and approved communications between NF			
7.7 ACIM - Access Control and Identity Management					
ACIM-01	BASIC	Access control to LI selectors databases			
ACIM-02	BASIC	Protection of key and certificate stores			
ACIM-03	BASIC	LI and root function interaction			
ACIM-04	BASIC	Limitation of LI privileges			
ACIM-05	BASIC	Role management			
ACIM-06	EXTENDED	Mandatory Access Control			
ACIM-07	BASIC	Protection of credentials			
ACIM-08	BASIC	User account management			
7.8 PERF - Ensuring performance of the LI/LD solution					
PERF-01	BASIC	Pruning of monitoring feeds			
PERF-02	BASIC	Security monitoring			
PERF-03	BASIC	Safeguard LI performance			
PERF-04	BASIC	Ensure resource availability to LI processes			
PERF-05	BASIC	Redundancy			
7.9 OM - Operational Measures					
OM-01	BASIC	Physical separation according to security level			
OM-02	BASIC	Security controls			
OM-03	BASIC	Physical security controls for hardware			
OM-04	BASIC	Security controls for personnel			
OM-05	BASIC	General LI management			
OM-06	EXTENDED	Secure wipe capabilities			
OM-07	BASIC	Debug options off by default			
OM-08	EXTENDED	Local restriction to debug options			
OM-09	BASIC	LI and jurisdiction			
OM-10	EXTENDED	Network time source			
7.10 AU - Audit					
AU-01	BASIC	Audit logs security			
AU-02	EXTENDED	Secure logging			
AU-03	BASIC	Audit logs permissions			
AU-04	BASIC	Pruning of log files			
AU-05	EXTENDED	System configuration			
AU-06	EXTENDED	Secure software management record			
AU-07	BASIC	Authorized users and accounts			
AU-08	BASIC	Query mechanism for software version			
AU-09	ADVANCED	Prevention of LI detection by analytics			
7.11 SCM - Supply Chain Management					
SCM-01	BASIC	Examine product composition			

Applicable security measures for LI network function security					
Reference	**Level**	**Title**	**Selected (y/n)**	**Fulfilled (y/n)**	**Justification (ref.)**
SCM-02	EXTENDED	Remote attestation service			
SCM-03	ADVANCED	Component measurement			
SCM-04	EXTENDED	Requirements for attestation			
SCM-05	ADVANCED	Run-time integrity			
SCM-06	EXTENDED	Run-time integrity extended requirements			
SCM-07	EXTENDED	Pre-installation and pre-execution checks			
SCM-08	EXTENDED	Software catalogue			
SCM-09	EXTENDED	Third party hosting			

Annex B: Bibliography

- ETSI TS 133 126: "LTE; 5G; Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Lawful Interception requirements (3GPP TS 33.126)".
- ETSI GS NFV-SEC 010: "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".
- ETSI TR 101 567: "Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)".
- ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

Annex C:
Change History

Date	Version	Information about changes
November 2020	1.1.1	First publication after approval by ETSI TC LI#55e

History

Document history		
V1.1.1	November 2020	Publication