ETSI GR NFV-SEC 011 V1.1.1 (2018-04)

Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NFV-SEC011

Keywords
lawful interception, NFV, 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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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

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

Virtualised CSP networks are required to be able to support lawful interception and other mandatory regulatory requirements. Lawful Interception (LI) as detailed in ETSI GS NFV-SEC 004 [i.1], needs to be performed in a way that is transparent to both the targeted user and non-authorized CSP personnel. In addition, LI needs to be implemented in security domain isolation from other general CSP network functions.

In a virtualised network, many of the legacy "Security by Obscurity" and physical hardware based approaches for hiding Lawful Interception are no longer viable, either due to mobility of virtualised network functions or as a result of the common hypervisor/compute architecture on which virtualised networks are based. Therefore, the virtualised network functions need to provide equivalent transparency and security solutions compared to existing legacy hardware networks. In order to support this, it is necessary for both the NFV platform on which the virtualised function/application is running and the underlying hardware platform to provide a set of standard secure building blocks on which the virtualised network function/application can be implemented.

1 Scope

The present document provides a study of the virtual functions which are required to support LI in ETSI NFV based virtualised networks. The present document identifies the set of capabilities, interfaces, functions and components which can be utilized by the virtualised applications (VNFs) to provide Lawful Interception. The present document identifies top to bottom (Virtualised Application through NFV layer through hardware platform) LI architectures and identifies within the scope of ETSI NFV, capabilities, interfaces, functions and components required to support these architectures.

The present document has 3 primary objectives:

1) Identify and define 1 or more NFV reference LI architectures, including administration functions, virtual points of interception, mediation functions and other LI functions. This is intended to provide a common reference architecture which can be used to identify functional split across the Virtualised Network Functions application layer (e.g. 3GPP Network), NFV software platform layer (ETSI NFV) and Hardware Platform layer.

2) Identify potential NFV solutions which provide the capabilities, interfaces, functions and components to meet the identified LI architectures. This is intended to identify all of the elements and interconnection relationships needed to perform LI in a virtualised network. These will form the basis for future normative standardization in both ETSI NFV and other bodies such as 3GPP utilizing ETSI NFV to virtualise their network functions.

3) Document deployment scenarios examples for each of the identified reference LI architectures. This is intended to show specific examples for different types of interception (e.g. on switch/function vs probe based) in specific technology deployment scenarios (e.g. 3GPP).

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 GS NFV-SEC 004: "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications".

[i.2] 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".

[i.3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.4] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.5] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.6] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[i.7] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.8] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.9] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[i.10] ETSI GR NFV-SEC 016: "Network Functions Virtualisation (NFV); Security; Report on location, timestamping of VNFs".

[i.11] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 232-1 [i.2], ETSI TS 133 107 [i.9] and the following apply:

LI Virtual Machine (LI VM): dedicated virtual host containing a virtual Point of Interception

virtual point of interception: dedicated LI function which may be either a dedicated VNFCI within a VNFI or a separate VNFI in its own right targeting traffic from other VNFIs

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 232-1 [i.2], ETSI TS 133 107 [i.9] and the following apply:

ADMF	Administration Function
CA	Certificate Authority
DF	Delivery Function
HI	Handover Interface
HI1	Handover Interface 1
HI2	Handover Interface 2
HI3	Handover Interface 3
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Function
LI	Lawful Interception
LI VM	Lawful Interception Virtual Machine
LoA	Level of Assurance
LRPG	Lawful Interception Routing Proxy Gateway
MF	Mediation Function
POI	Point Of Interception
RD	Retained Data
SDN	Software Defined Network
SO	Security Orchestrator
TCF	Triggering Control Function
TTP	Trusted Third Party
vDF	virtualised Delivery Function
vMF	virtualised Mediation Function
vPOI	virtualised Point Of Interception

4 Problem Statement Lawful Interception in NFV

4.1 General

This clause outlines the overall challenges which should be addressed when considering how and where to deploy Lawful Interception functionality in an NFV environment. These challenges form the basis of the problem set which any LI architecture should be able to overcome, as detailed in subsequent clauses of the present document.

Details for the underlying LI requirements and internal LI VM functionality are given in ETSI GS NFV-SEC 004 [i.1] and ETSI TS 102 232-1 [i.2].

4.2 Security

4.2.1 General

NFV does not necessarily introduce any new security challenges for lawful interception which did not otherwise exist in legacy networks. In fact, a properly implemented NFV network may actually provide better LI security than legacy networks which have historically provided security by obscurity. What NFV does in practice is remove the obscurity option and force implementers to secure LI properly.

Within the scope of the present document, LI architectures and solutions should trade-off security/detectability, against the actual ability to reliably perform LI in dynamic virtualised environments. The LI security details in this clause are intended as a guide only and are aimed at highlighting a number of the restrictions that LI requires that may not be familiar to those not familiar with legacy LI implementations. Detailed security threats, solutions and mitigation approaches are provided in ETSI GS NFV-SEC 004 [i.1], ETSI GS NFV-SEC 012 [i.7] and ETSI GS NFV-SEC 009 [i.3].

Specific consideration of LI security challenges in hybrid part legacy scenarios is given in clause 7.2.6.

4.2.2 Basic Trust and Default Security Stance

4.2.2.1 General

While ETSI GS NFV-SEC 012 [i.7] contains generic security requirements for sensitive functions, it is important to consider the fundamental LI specific security requirements that any NFV implementation requiring LI should be able to address.

4.2.2.2 The One Deity Complex

NFV and other IT cloud systems are typically built on the assumption that there is one root administrator who has absolute dominion over all software and resources in a system. Unfortunately that approach is not entirely compatible with LI, unless they are a member of the LI administration team that controls the rest of the network. While LI is always under the control of the CSP, most general network administration and support personnel will not be authorized to have control, knowledge or visibility of LI. Therefore it is necessary to be able to separate administration of LI from other network functions or processes. It is entirely reasonable for the primary root admin to have a role in initial enabling of LI when the network is initially built (or if LI needs to be retrofitted at a later date). However, once LI is enabled (with or without the main system root admin), LI from then on needs to be entirely invisible to the main network root admin and they should not be able to interfere with, inspect or monitor any aspect of LI unless they are specifically permitted to do so. This sets a very high bar but is the start point any NFV based LI implementation needs to start from.

For LI, the ADMF is considered to be the ruler of all other LI functions (with the exception of the LEA LEMF). All decisions and aspects of control ultimately sit with the ADMF (see clause 4.5).

4.2.2.3 Basic LI Security Stance

LI is generally considered to be a security sensitive issue and as such the knowledge of the existence of LI and LI target lists is typically subject to high security restrictions. Therefore, LI needs to be considered a highly sensitive network with all of the isolation and security requirements that such government systems require. However, given that if an LI system was considered government classified then the network to which it connects and all users would need to be subject to the same security restrictions.

That is clearly impractical for a public communications network. However, when considering how to implement LI securely in an NFV network, the start point should always be that LI is a high security, restricted system requiring absolute isolation and then design an implementation which sticks as close to that principle as possible within the limits of practicality for a public communications network.

Therefore, LI needs to be fully self-contained within a single legal jurisdiction (generally a single country), should not be visible or detectable to non-LI authorized entities (systems, processes or people), cannot rely on any information which would have to be specifically provided for an LI targeted communication which would otherwise not be available for a non-LI target communication. In general LI cannot be shared across operators and given the legal jurisdiction restriction, LI cannot be implemented in one country to provide LI capability for another.

4.2.2.4 System Trust and Isolation

By default, the LI Functions do not trust generic network resources or hardware which are not specifically dedicated to LI and under full audit control of the LI system. As such while placing LI encryption keys or target lists in hardware security modules mitigates some LI security requirements, unless these are specifically dedicated to LI, such hardware security modules would be considered untrusted. Therefore they are only a part of any overall LI security solution.

In order for LI to work, it needs to fundamentally exist to some degree within the main CSP NFV resources in order to gain access to target communications. However, while it needs to exist in the main network, only those aspects, processes or functions which need to be exposed should be exposed (e.g. LI VNFCI interfaces to send or receive LI data). Everything else should be fully secured using secure exclaves and other applicable security solutions as detailed in ETSI GS NFV-SEC 012 [i.7]. LI should be implemented in a logically separated trust domain. This is similar to basic NFV security isolation requirements for VNFs or slicing but for LI this needs to be implemented fully top to bottom (application layer through to the hardware) and not just NFV layer and above.

Since data needs to enter and leave the LI functions, implementations cannot simply assume that placing LI functionality inside secure enclaves is sufficient. LI security design should adequately protect the LI functions themselves and anything connected to them. Therefore, LI requires that the wider network in which it has been implemented also natively utilize many of the same fundamental security capabilities required for LI.

All key material and LI target lists should be protected in either secure enclaves or hardware security modules. Once any resources used for LI are no longer required all memory, storage (including hardware security modules) should be erased to government security standards to ensure no data is recoverable. LI should always fail safe such that under all error, crash or failure scenarios no LI data, keys or target lists can ever be exposed outside of the LI trust domain. LI information should be dead, not merely resting.

4.2.3 LI Function Visibility and Hiding

Securing and hiding LI functionality from other functions in an NFV environment is by far the largest initial challenge. Placing LI functions within the VNF environment exposes them to a variety of security and visibility risks. Placing them outside of the NFV environment comes with a different set of visibility risks, places significant constraints on VNF mobility, makes LI fragile to dynamic changes in the NFV environment and will only be possible in scenarios where the mandatory intra VNFI and inter VNFI encryption has been disabled. Disabling intra/inter VNFI encryption will expose the NFV platform to considerable Cyber risks and is therefore unlikely to be acceptable.

4.2.4 Data Egress and Communication

Beyond the basic security considerations for the virtualised LI functions themselves, LI functions require to be tasked with interception warrants and be able to transfer the resulting intercepted data between themselves and the LEA LEMF. In an NFV and SDN network, the HI and X interfaces generally need to start and end in virtualised functions. VPNs or other network paths used to route the LI data will be far more visible to the rest of the network than in legacy implementations. Current HI and X interface protocol security is generally designed to protect data between physically secure end points and in many cases using VPN and/or network links which use dedicated "hidden" infrastructure. Furthermore, in a fully NFV and SDN network, the LEMF end points will need to be fully visible to the NFV MANO and SDN controllers in order to ensure that intercept can be maintained as the network evolves (e.g. VNFI relocation, etc.).

4.3 Mobility and Location

4.3.1 Virtualised Function Location

4.3.1.1 General Location and Simple VNFs

After security, underlying mobility of the virtualised network (both logically and physically) is the biggest challenge for implementing LI in an NFV environment. The LI management functions needs to be able to figure out what the network architecture looks like at any point in time and where to place POIs (and therefore LI VMs) relative to the changing architecture in real-time. Furthermore, the LI management functions should be adapted to or able to monitor changes which impact LI VM placement, routing, interconnection or underlying VNF interconnectivity (and therefore target traffic routing) and make any necessary changes in real-time.

In terms of LI VM location, the LEMF/ADMF should be able to request assurance that the LI VMs and any other elements involved in the LI service are within the pre-defined location constraints which the NFV MANO layer has been given. For example, if a network has been implemented in 5 data centres, 4 in the jurisdiction of LEA and 1 outside, then the MANO needs to be able to attest to the ADMF/LEMF that the LI VMs (and any VNF from which they are taking target traffic) are running as pre-configured, in any of the 4 in jurisdiction data centres. It is this ability to attest this location geo fencing that is important and not necessarily whether LI VM process 12345 was for 20 ms on VM blade 66666, rack 7 sub-shelf 4, data centre A, address: 123 The Street, Long X:Lat Y.

In addition to the need to attest the location of LI VMs and their associated parent VNFIs, in many cases VNFIs with LI functionality need to obtain real-time target specific information from other peer VNFIs. Therefore, it is not a simple as needing to control and attest the location of single LI equipped VNFIs but rather groups of VNFIs. In such groups, the other non-LI VNFIs could be either directly or indirectly involved in supporting LI. For single vendor implementations where groups of VNFIs are directly involved in supporting LI, then it may be possible to group them directly via MANO using the software catalogues and VNFDs. However, more indirect scenarios where VNFIs may not be directly aware of LI are potentially more challenging to address (e.g. maintaining non-detectability when the non-LI VNFI scale or migrate).

As a minimum, the ability to attest that LI VMs are running within the defined MANO placement rules will be required for all VNFIs. In some specific scenarios real, geographic location of specific LI VMs may be required. Attesting real world location LI VMs requires additional hardware beyond that implemented for traditional cloud service infrastructures and may therefore add significant cost if it was applied to all hosts and all VNFIs. Changes to hypervisor, firmware, MANO, OSs and VMs would also potentially be required to achieve full attestation of LI VMs.

Further guidance on location and associated timestamping is given in ETSI GR NFV-SEC 016 [i.10].

4.3.1.2 Multi VNFCI VNFs

Where a VNFI is composed of multiple VNFCIs and those VNFCIs are spread across multi hosts, location of the LI POIs becomes considerably more complicated. In legacy networks, large network elements have a single logical location. When those large functions become virtualised they will be implemented with potentially 100 s of physical hosts. Those hosts do not need to be in the same rack, data centre or physical location.

It is therefore necessary to consider which location used, attested or reported for LI purposes. The location of VNFCI running the vPOI within the VNF might be an obvious choice but there may be multiple vPOI VNFCI within a single VNFCI and left unrestricted the vPOI VNFCI could be in a different location to the VNFCI serving the actual target user data flow. Conversely the VNFCI handling the target user data flow may be a better choice (especially if that directly related to user location - see clause 4.3.2) but again there are likely to be more than 1 of those. Furthermore, some functions in virtualised networks may be purposely distributed.

The exact meaning, location and binding of the individual locations for each host relative to the each overall VNFI is outside the scope of ISG NFV. However, it will be necessary to ensure that sufficient location information (physical location or confirmation that the VNFCI is within the host allocation constraints attested by MANO), is made available for LI purposes.

4.3.2 Inferred Location of the Target

With exception of UE assisted (e.g. GPS) or other network enhanced location technologies, Lawful Interception does not typically obtain the actual location of the target subscriber. Instead the location is inferred from the location of network equipment to which it is attached. The accuracy of this location is therefore related to the technology used and density of the radio infrastructure to which the UE connects.

For legacy networks, in its simplest form location could be the postcode of a single standalone WLAN hotspot. In 3G/4G or other more complicated mesh technologies, the location derived from the infrastructure is associated with multiple elements in the network. For example, a CellID is a combination of the antenna mast ID and other parameters. Since the infrastructure does not change very often it is possible to derive accurate inferred location of the target.

With NFV, since the VNFs making up the service can change on a frequent basis, one or more elements of the information from which the CellID or other equipment associated location information is obtained may become dynamic. This may result in the location appearing to change rapidly for a static subscriber or indeed a highly mobile subscriber appearing to have a constant location as the VNFs move with user mobility. It may not be possible in some scenarios to obtain a location at all in some scenario, based on legacy static approaches.

Since the equipment ID, naming schemes, CellIDs or other equipment based location information are a VNF service level issue, it is not possible to precisely identify or mitigate all of the possible live deployment models. However, for the LEA to continue to rely on VNF associated location or identities to infer target location, the CSP will need to provide LEAs with near real-time network state information from which the equivalent to the static legacy network locations can be constructed.

4.3.3 VNF Migration

VNFI migration is not actually new. CSPs have a long history of deploying network functions in load balanced arrays or in hot standby configurations such that target traffic can migrate between multiple physical network functions. However, these elements are generally presented to the world as a single logical function, migrations are infrequent and they are in a small number of static locations.

There are two types of VNFI logical migration; Migration of the live service from one VNFI to another VNFI; and migration of the running VNFI from one set of hosts to another. These are shown in figure 4.3.3-1.

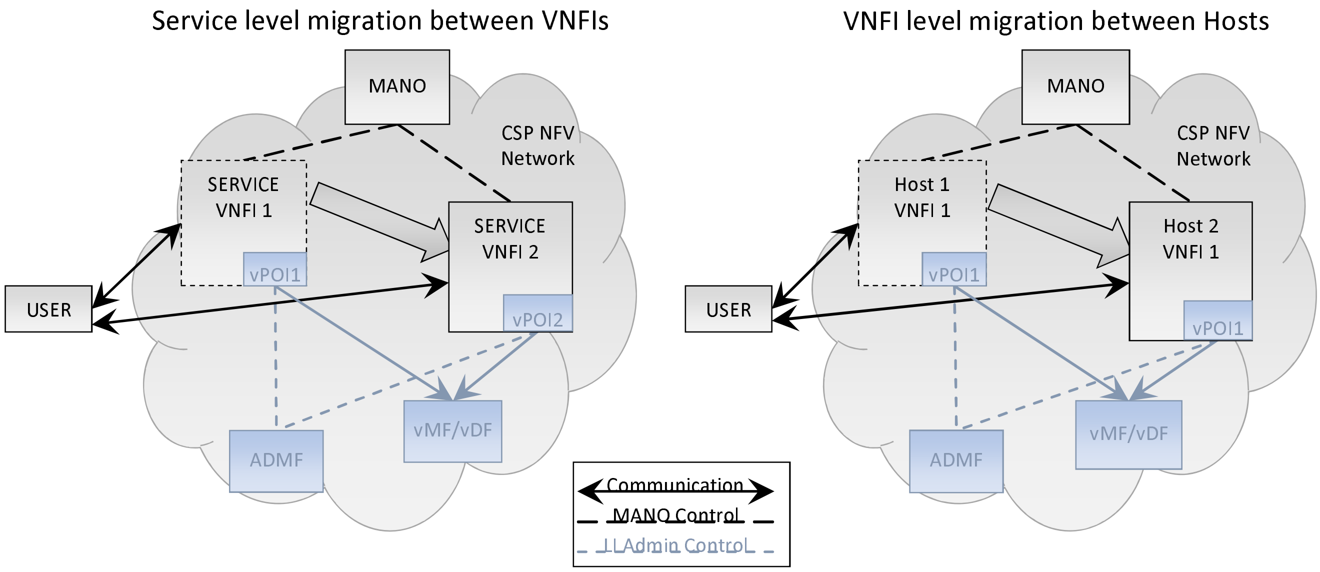

Figure 4.3.3-1: Simplified LI Migration for embedded vPOIs

In the case of a live service migration from one VNFI to another VNFI, while there are challenges in making sure the configured LI capabilities are available in the new VNFI before the service migrates, this is actually very similar to load balancing or other migrations which already occur in legacy networks. The frequency of migrations may be higher but NFV does not cause any significant new issues for LI that did not already exist in the legacy case. VNFI IDs are likely to change and it is therefore potentially easy for the LI systems to detect and correlate for these migrations.

In the case of the migration of a running VNFI from one set of hosts to another, this is potentially more difficult to handle. Firstly, the identifiers at the application level may not change, which may impact reported user location. Secondly it means that the location binding of hosts to VNFCI (as discussed in clause 4.3.1) should be performed continuously and not just at initial instantiation of the VNFCI.

Similar to migration of a whole VNFI, it is possible for one or more VNFCIs to migrate (or indeed the number of VNFCIs could change). The implications for LI are essentially the same as for a whole VNFI live migration, but the effects may be more difficult to detect and the effects on any on-going interception are likely subtler.

NOTE: The extent to which current hardware and MANO implementations support real-time live migrations is unclear and expected to be infrequent in the short - medium term. However, since LI location reporting capabilities may be difficult to retrofit, VNFI migration needs to be considered.

While migration of VNFs does not generally alter the functionality or intercepted traffic characteristics, scaling as discussed in clause 4.8 may cause similar impacts to the ability to maintain and operate LI in a virtualised network. If scaling results in new VNFCIs in substantially different locations to that of existing VNFCIs or scaling results in exceeding the capacity of the existing LI POI VNFCI then the effects of migration and scaling can be considered to be similar from an LI perspective. Both migration and scaling should therefore be considered together in any implementation.

4.3.4 User Mobility

In a static legacy network, as a user moves through the radio environment of a mobile technology (e.g. 4G) or physically moves from one physical Ethernet connection to another, the UE moves between different physical elements of the network. Those changes result in inferred or actual location information changes as reported to law enforcement.

With NFV deployments, the movement of 1 or more users may impact the logical structure of the VNFIs serving those users. The higher the overall level of user mobility the larger the changes which may occur on the network side to adapt the network to maintain optimum user experience.

For LI, the relationships between physical user mobility and the corresponding changes in information reported to the LEA may become more dynamic. User mobility may cause a higher degree of vPOI migration than for an equivalent level of mobility in a legacy network. This makes issues such as LI dimensioning more difficult to achieve without reserving higher levels of spare resources.