3GPP TR 33.848 V0.14.0 (2022-10)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Security Aspects;

Study on Security Impacts of Virtualisation

(Release 18)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

<keyword[, keyword]>

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [7](#__RefHeading___Toc116919883)

Introduction [7](#__RefHeading___Toc116919884)

1 Scope [8](#__RefHeading___Toc116919885)

2 References [8](#__RefHeading___Toc116919886)

3 Definitions, symbols and abbreviations [9](#__RefHeading___Toc116919887)

3.1 Definitions [9](#__RefHeading___Toc116919888)

3.2 Symbols [10](#__RefHeading___Toc116919889)

3.3 Abbreviations [10](#__RefHeading___Toc116919890)

4 Virtualisation Background, Concepts and Assumptions [11](#__RefHeading___Toc116919891)

4.1 Introduction [11](#__RefHeading___Toc116919892)

4.2 Architecture [11](#__RefHeading___Toc116919893)

4.3 Virtualisation of 3GPP Network Functions [12](#__RefHeading___Toc116919894)

4.4 General NFV security issues [12](#__RefHeading___Toc116919895)

4.4.1 Access to VNFs via virtualisation layer [12](#__RefHeading___Toc116919896)

4.4.2 Sharing of private keys between VNFs [12](#__RefHeading___Toc116919897)

4.4.3 Isolation [13](#__RefHeading___Toc116919898)

4.4.4 Vulnerabilities of physical hosts [13](#__RefHeading___Toc116919899)

4.4.5 Secure Administration [13](#__RefHeading___Toc116919900)

4.5 Limited Virtualisation vs Full Virtualisation [13](#__RefHeading___Toc116919901)

5 Key Issues [14](#__RefHeading___Toc116919902)

5.1 Introduction [14](#__RefHeading___Toc116919903)

5.2 Key Issue 1: Establishment of trust domains for Network Functions [14](#__RefHeading___Toc116919904)

5.2.1 Key issue detail [14](#__RefHeading___Toc116919905)

5.2.2 Security threats [14](#__RefHeading___Toc116919906)

5.2.3 Potential security requirements [14](#__RefHeading___Toc116919907)

5.3 Key Issue 2: Confidentiality of sensitive data [15](#__RefHeading___Toc116919908)

5.3.1 Key issue detail [15](#__RefHeading___Toc116919909)

5.3.2 Security threats [15](#__RefHeading___Toc116919910)

5.3.3 Potential security requirements [15](#__RefHeading___Toc116919911)

5.4 Key Issue 3: Availability of Network Functions [15](#__RefHeading___Toc116919912)

5.4.1 Key issue detail [15](#__RefHeading___Toc116919913)

5.4.2 Security threats [15](#__RefHeading___Toc116919914)

5.4.3 Potential security requirements [16](#__RefHeading___Toc116919915)

5.5 Key Issue 4: Common Software Environment [16](#__RefHeading___Toc116919916)

5.5.1 Key issue detail [16](#__RefHeading___Toc116919917)

5.5.2 Security threats [16](#__RefHeading___Toc116919918)

5.5.3 Potential security requirements [16](#__RefHeading___Toc116919919)

5.6 Key Issue 5: Data Location and Lifecycle [17](#__RefHeading___Toc116919920)

5.6.1 Key issue detail [17](#__RefHeading___Toc116919921)

5.6.2 Security threats [17](#__RefHeading___Toc116919922)

5.6.3 Potential security requirements [17](#__RefHeading___Toc116919923)

5.7 Key Issue 6: Function Isolation [17](#__RefHeading___Toc116919924)

5.7.1 Key issue detail [17](#__RefHeading___Toc116919925)

5.7.2 Security threats [18](#__RefHeading___Toc116919926)

5.7.3 Potential security requirements [18](#__RefHeading___Toc116919927)

5.8 Key Issue 7: Memory Introspection [18](#__RefHeading___Toc116919928)

5.8.1 Key issue detail [18](#__RefHeading___Toc116919929)

5.8.2 Security threats [18](#__RefHeading___Toc116919930)

5.8.3 Potential security requirements [19](#__RefHeading___Toc116919931)

5.9 Key Issue 8: Test Isolation and Assurance [19](#__RefHeading___Toc116919932)

5.9.1 Key issue detail [19](#__RefHeading___Toc116919933)

5.9.2 Security threats [19](#__RefHeading___Toc116919934)

5.9.3 Potential security requirements [20](#__RefHeading___Toc116919935)

5.10 Key Issue 9: Trust domain and Slice Isolation [20](#__RefHeading___Toc116919936)

5.10.1 Key issue detail [20](#__RefHeading___Toc116919937)

5.10.2 Security threats [20](#__RefHeading___Toc116919938)

5.10.3 Potential security requirements [20](#__RefHeading___Toc116919939)

5.11 Key Issue 10: Single Administrator Domain [21](#__RefHeading___Toc116919940)

5.11.1 Key issue detail [21](#__RefHeading___Toc116919941)

5.11.2 Security threats [21](#__RefHeading___Toc116919942)

5.11.3 Potential security requirements [21](#__RefHeading___Toc116919943)

5.12 Key Issue 11: Where are my Keys and Confidential Data [21](#__RefHeading___Toc116919944)

5.12.1 Key issue detail [21](#__RefHeading___Toc116919945)

5.12.2 Security threats [22](#__RefHeading___Toc116919946)

5.12.3 Potential security requirements [22](#__RefHeading___Toc116919947)

5.13 Key Issue 12: Where the is my function [22](#__RefHeading___Toc116919948)

5.13.1 Key issue detail [22](#__RefHeading___Toc116919949)

5.13.2 Security threats [22](#__RefHeading___Toc116919950)

5.13.3 Potential security requirements [22](#__RefHeading___Toc116919951)

5.14 Key Issue 13: Attestation at 3GPP Function level [23](#__RefHeading___Toc116919952)

5.14.1 Key issue detail [23](#__RefHeading___Toc116919953)

5.14.2 Security threats [23](#__RefHeading___Toc116919954)

5.14.3 Potential security requirements [23](#__RefHeading___Toc116919955)

5.15 Key Issue 14: VNF Host Spanning [24](#__RefHeading___Toc116919956)

5.15.1 Key issue detail [24](#__RefHeading___Toc116919957)

5.15.2 Security threats [24](#__RefHeading___Toc116919958)

5.15.3 Potential security requirements [24](#__RefHeading___Toc116919959)

5.16 Key Issue 15: Encrypted Data Processing [24](#__RefHeading___Toc116919960)

5.16.1 Key issue detail [24](#__RefHeading___Toc116919961)

5.16.2 Security threats [25](#__RefHeading___Toc116919962)

5.16.3 Potential security requirements [25](#__RefHeading___Toc116919963)

5.17 Key Issue 16: Mixed Virtual and Legacy PNF Deployments [25](#__RefHeading___Toc116919964)

5.17.1 Key issue detail [25](#__RefHeading___Toc116919965)

5.17.2 Security threats [25](#__RefHeading___Toc116919966)

5.17.3 Potential security requirements [26](#__RefHeading___Toc116919967)

5.18 Key Issue 17: Software Catalogue Image Exposure. [26](#__RefHeading___Toc116919968)

5.18.1 Key issue detail [26](#__RefHeading___Toc116919969)

5.18.2 Security threats [26](#__RefHeading___Toc116919970)

5.18.3 Potential security requirements [27](#__RefHeading___Toc116919971)

5.19 Key Issue 18: The Startup Paradox [27](#__RefHeading___Toc116919972)

5.19.1 Key issue detail [27](#__RefHeading___Toc116919973)

5.19.2 Security threats [27](#__RefHeading___Toc116919974)

5.19.3 Potential security requirements [27](#__RefHeading___Toc116919975)

5.20 Key Issue 19: Time Manipulation [27](#__RefHeading___Toc116919976)

5.20.1 Key issue detail [27](#__RefHeading___Toc116919977)

5.20.2 Security threats [28](#__RefHeading___Toc116919978)

5.20.3 Potential security requirements [28](#__RefHeading___Toc116919979)

5.21 Key Issue 20: 3rd Party Hosting Environments [28](#__RefHeading___Toc116919980)

5.21.1 Key issue detail [28](#__RefHeading___Toc116919981)

5.21.2 Security threats [28](#__RefHeading___Toc116919982)

5.21.3 Potential security requirements [28](#__RefHeading___Toc116919983)

5.22 Key Issue 21: VM and Hypervisor Breakout [29](#__RefHeading___Toc116919984)

5.22.1 Key issue detail [29](#__RefHeading___Toc116919985)

5.22.2 Security threats [29](#__RefHeading___Toc116919986)

5.22.3 Potential security requirements [29](#__RefHeading___Toc116919987)

5.23 Key Issue 22: MANO Single Point of Failures [29](#__RefHeading___Toc116919988)

5.23.1 Key issue detail [29](#__RefHeading___Toc116919989)

5.23.2 Security threats [29](#__RefHeading___Toc116919990)

5.23.3 Potential security requirements [30](#__RefHeading___Toc116919991)

5.24 Key Issue 23: IP layer vs Application layer Security [30](#__RefHeading___Toc116919992)

5.24.1 Key issue detail [30](#__RefHeading___Toc116919993)

5.24.2 Security threats [30](#__RefHeading___Toc116919994)

5.24.3 Potential security requirements [30](#__RefHeading___Toc116919995)

5.25 Key Issue 24: Data synchronicity through network [30](#__RefHeading___Toc116919996)

5.25.1 Key issue detail [30](#__RefHeading___Toc116919997)

5.25.2 Security threats [31](#__RefHeading___Toc116919998)

5.25.3 Potential security requirements [31](#__RefHeading___Toc116919999)

5.26 Key Issue 25: Container Security [31](#__RefHeading___Toc116920000)

5.26.1 Key issue detail [31](#__RefHeading___Toc116920001)

5.26.2 Security threats [31](#__RefHeading___Toc116920002)

5.26.3 Potential security requirements [32](#__RefHeading___Toc116920003)

5.27 Key Issue 26: Container breakout [32](#__RefHeading___Toc116920004)

5.27.1 Key issue detail [32](#__RefHeading___Toc116920005)

5.27.2 Security threats [32](#__RefHeading___Toc116920006)

5.27.3 Potential security requirements [32](#__RefHeading___Toc116920007)

5.28 Key Issue 27: Secrets in NF container images [33](#__RefHeading___Toc116920008)

5.28.1 Key issue detail [33](#__RefHeading___Toc116920009)

5.28.2 Security threats [33](#__RefHeading___Toc116920010)

5.28.3 Potential security requirements [33](#__RefHeading___Toc116920011)

5.29 Key Issue 28: Management APIs [33](#__RefHeading___Toc116920012)

5.29.1 Key issue detail [33](#__RefHeading___Toc116920013)

5.29.2 Security threats [34](#__RefHeading___Toc116920014)

5.29.3 Potential security requirements [34](#__RefHeading___Toc116920015)

5.30 Key Issue 29: Image Snapshot and VNF Mobility [34](#__RefHeading___Toc116920016)

5.30.1 Key issue detail [34](#__RefHeading___Toc116920017)

5.30.2 Security threats [35](#__RefHeading___Toc116920018)

5.30.3 Potential security requirements [35](#__RefHeading___Toc116920019)

5.31 Key Issue 30: Sensitive Function Pinning [35](#__RefHeading___Toc116920020)

5.29.1 Key issue detail [35](#__RefHeading___Toc116920021)

5.31.2 Security threats [35](#__RefHeading___Toc116920022)

5.31.3 Potential security requirements [36](#__RefHeading___Toc116920023)

6 Mitigations and Solutions [36](#__RefHeading___Toc116920024)

6.1 Introduction [36](#__RefHeading___Toc116920025)

6.2 Solution 1: Trust domains and separation [36](#__RefHeading___Toc116920026)

6.2.1 Introduction [36](#__RefHeading___Toc116920027)

6.2.2 Solution details [36](#__RefHeading___Toc116920028)

6.2.2.1 Definition of trust domains [36](#__RefHeading___Toc116920029)

6.2.2.2 Software separation of VNFs [37](#__RefHeading___Toc116920030)

6.2.2.3 Separation of physical infrastructure [37](#__RefHeading___Toc116920031)

6.2.2.4 Virtualisation platform [37](#__RefHeading___Toc116920032)

6.2.3 Evaluation [37](#__RefHeading___Toc116920033)

6.3 Solution 2: Lock-down of infrastructure [37](#__RefHeading___Toc116920034)

6.3.1 Introduction [37](#__RefHeading___Toc116920035)

6.3.2 Solution details [37](#__RefHeading___Toc116920036)

6.3.3 Evaluation [38](#__RefHeading___Toc116920037)

6.4 Solution 3: Administration of the virtualisation fabric [38](#__RefHeading___Toc116920038)

6.4.1 Introduction [38](#__RefHeading___Toc116920039)

6.4.2 Solution Details [38](#__RefHeading___Toc116920040)

6.4.3 Evaluation [38](#__RefHeading___Toc116920041)

6.5 Solution 4: Hardware Mediated Execution Enclave (HMEE) [39](#__RefHeading___Toc116920042)

6.5.1 Introduction [39](#__RefHeading___Toc116920043)

6.5.2 Solution details [39](#__RefHeading___Toc116920044)

6.5.3 Evaluation [39](#__RefHeading___Toc116920045)

6.6 Solution 5: Solution Using Boot Time Attestation for NF Registration [40](#__RefHeading___Toc116920046)

6.6.1 General [40](#__RefHeading___Toc116920047)

6.6.2 Introduction [40](#__RefHeading___Toc116920048)

6.6.2.1 Reference Architecture for Attestation [40](#__RefHeading___Toc116920049)

6.6.2.2 Attestation in NFV Environments [41](#__RefHeading___Toc116920050)

6.6.3 Solution Details [42](#__RefHeading___Toc116920051)

6.6.3.1 General [42](#__RefHeading___Toc116920052)

6.6.3.2 Attestation of the NFVI [42](#__RefHeading___Toc116920053)

6.6.3.3 Attestation of VNFs [43](#__RefHeading___Toc116920054)

6.6.3.4 Proposed Requirements for Attestation in NFV Environments [44](#__RefHeading___Toc116920055)

6.6.3.5 Profile and Attestation Check Function (PACF) [44](#__RefHeading___Toc116920056)

6.6.3.6 NF Service Registration Procedure with Remote Attestation [45](#__RefHeading___Toc116920057)

6.6.4 Evaluation [46](#__RefHeading___Toc116920058)

6.7 Solution 6: Solution Using Attestation for Key Issue 13 [46](#__RefHeading___Toc116920059)

6.7.1 General [46](#__RefHeading___Toc116920060)

6.7.2 Introduction [47](#__RefHeading___Toc116920061)

6.7.3 Solution Details [47](#__RefHeading___Toc116920062)

6.7.4 Evaluation [49](#__RefHeading___Toc116920063)

6.8 Solution #7: Ticket-based access control for NFV [49](#__RefHeading___Toc116920064)

6.8.1 Introduction [49](#__RefHeading___Toc116920065)

6.8.2 Solution details [49](#__RefHeading___Toc116920066)

6.8.3 Evaluation [51](#__RefHeading___Toc116920067)

6.9 Solution 8: Slice isolation in both service and resource layer [51](#__RefHeading___Toc116920068)

6.9.1 General [51](#__RefHeading___Toc116920069)

6.9.3 Solution Details [51](#__RefHeading___Toc116920070)

6.9.4 Evaluation [52](#__RefHeading___Toc116920071)

7 Conclusions [52](#__RefHeading___Toc116920072)

8 Recommendations [52](#__RefHeading___Toc116920073)

Annex A: Principles for administration of virtualisation infrastructure [52](#__RefHeading___Toc116920074)

Annex B: KI Mitigations Summary [53](#__RefHeading___Toc116920075)

Annex T: Temporary Holding Annex Security Areas [55](#__RefHeading___Toc116920076)

Annex <X>: Change history [57](#__RefHeading___Toc116920077)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

Virtualisation is a fundamental building block of 5G and while not the only way of implementing a 5G network, it is nevertheless the primary implementation method being pursued to some degree (great or small) by all operators and manufacturers. Furthermore, virtualisation is being applied to earlier 3GPP architectures (e.g. LTE) and part virtualised networks containing a mixture of physical, containerised and virtualised network functions will be common place for most operators for the foreseeable future.

# 1 Scope

The present document considers the consequences of virtualisation on 3GPP architectures, in order to identify threats and subsequent security requirements. 3GPP function security relies on the underlying implementation technology and physical environment being secure. In legacy deployments, physical rack security and separation implicitly provided underlying security. Many legacy physical security requirements were not formally documented in 3GPP standards and relied on proprietary domain knowledge by 3GPP operators and manufacturers. Legacy core network security models also assume that threats primarily apply at the edge of the function or network only, where the network or physical network functions are exposed by external interfaces.

To provide equivalent security in virtualised deployments, the underlying infrastructure needs to provide minimum security capabilities in a standardised form which can be requested and or consumed at the 3GPP layer. This is necessary since virtual functions need to co-exist in shared virtualisation environments and the legacy physical security models don’t address the new threat vectors introduced by virtualisation.

While a number of the key issues identified in the present document may not necessarily fully be within the scope of 3GPP to resolve, in order to implement 3GPP functions securely it is necessary for 3GPP to set requirements that may be addressed outside 3GPP.

The present document identifies security requirements which need to be addressed outside of 3GPP in order for 3GPP to specify fully secure virtualised 3GPP functions. The present document identifies extensions to 3GPP security capabilities which are required to provide direct explicit security visibility of the underlying virtualised infrastructure platform at the 3GPP layer and extensions to 3GPP functions to make use of such capabilities.

The wider requirements captured within the present document are intended to allow outside groups such as ETSI or open-source groups to develop any necessary capabilities and fill identified standardisation gaps.

Identification of requirements for the standardisation of the overall security framework (e.g. top to bottom, 3GPP, NFVI, hardware, SDN) and minimum-security capabilities which should be used by a virtualised implementation to meet Critical National Infrastructure (CNI) or other regulatory requirements are outside the scope of the present document.

Since there is no single approach to virtualisation, the security threats and risks will vary depending on the deployment use case and virtualisation technology choices. The present document considers both virtualisation threats and risks that apply to specific implementations (e.g., Virtual Machine or Container based) and more generic threat and risks that apply in all use cases.

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

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

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

[4] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security"

[5] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement"

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[7] "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable"; Shahzad and Litchfield 2015; <https://arxiv.org/ftp/arxiv/papers/1606/1606.01356.pdf>

[8] "OpenStack"; <https://www.openstack.org/>

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

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

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

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

[13] 3GPP TS 23.502: "System architecture for the 5G System (5GS)".

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

[15] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[16] 3GPP TS 28.533 "Management and orchestration; Architecture framework".

[17] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[18] IETF RFC 4210: "The Kerberos Network Authentication Service (V5)".

[19] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[20] IETF: RATS Working Group: Remote Attestation Procedures Architecture, <https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.txt>

[21] ETSI GS NFV-IFA 013 (V2.4.1) (2018-02): "Network Function Virtualisation (NFV); Release 2; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

# 3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Clause numbering depends on applicability and should be renumbered accordingly.

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Global Administrator:** A role in the access control hierarchy which gives access to all administrative features and abilities in the NFV environment. Depending on the operating system this role might be known as root or as a superuser.

**Noisy Neighbour Problem:** When a VM accessing shared resources uses more than it should do. This causes other VMs accessing those resources to suffer from reduced or erratic performance.

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

Abbreviation format (EW)

AUC Authentication Centre

BSS Business Support System

CNI Critical National Infrastructure

CoT Chain of Trust

COTS Commercial Off The Shelf

CSP Communication Service Provider

DRM Digital Rights Management

GDPR General Data Protection Directive

HMEE Hardware Mediated Execution Environment

HSM Hardware Security Module

IAAS Infrastructure As A Service

LI Lawful Interception

MANO Management and Orchestration

MnF Management Function

NAAS Network As A Service

NF Network Function

NFV Network Functions Virtualisation

NFVI Network Functions Virtualisation Infrastructure

OS Operating System

OSS Operations Support System

PNF Physical Network function

PS Provisioning Server

RoT Root of Trust

SBA Service Based Architecture

SDN Software Defined Network

TPM Trusted Platform Module

TLS Transport Layer Security

UICC Universal Integrated Circuit Card

VM Virtual Machine

VNO Virtual Network Operator

VNF Virtual Network Function

# 4 Virtualisation Background, Concepts and Assumptions

Editor’s Note: This section will contain a basic description of virtualisation, hierarchical implementation model and deployment assumptions

## 4.1 Introduction

In computing, virtualisation encompasses a number of different techniques to create a virtual, or software, version of a computing device. Examples of devices and systems which may be virtualised include hardware platforms, memory, storage or a network. The present document primarily addresses the security of Network Function Virtualisation (NFV) as defined by ETSI. However, the security threat, risks and mitigations are applicable to any other similar virtualisation approach. In the context of a 3GPP network, NFV refers to the deployment of Network Functions (NFs) as software modules which run on off the shelf computing hardware. This contrasts with the traditional deployment of 3GPP network components as specialised hardware devices. Implementation of the 5G Service Based Architecture (SBA) relies on the use of NFV, among other technologies.

## 4.2 Architecture

ETSI GS NFV 002 [2] defines the high-level NFV Framework which consists of three working domains, as shown by Figure 4.2-1.

The NFV Infrastructure (NFVI) includes all the hardware and software which provide a platform on which VNFs can be deployed. The NFVI includes:

- Hardware resources, which are assumed to be COTS.

- Virtualisation Layer, for example a hypervisor or container engine, which separates the VNF software from underlying hardware.

NOTE: The choice to use a hypervisor or container engine as the virtualisation layer has security implications. In particular, containers do not present a security boundary, without use of additional security mechanisms.

- Virtualised Resources.

VNFs run on top of the NFVI and are software implementations of network functions. A VNF may run in one Virtual Machine (VM) or over several.

NFV Management and Orchestration consists of the systems and functions which are responsible for virtualisation specific management tasks, such as lifecycle management of VNFs and orchestration of resources required to support virtualisation.

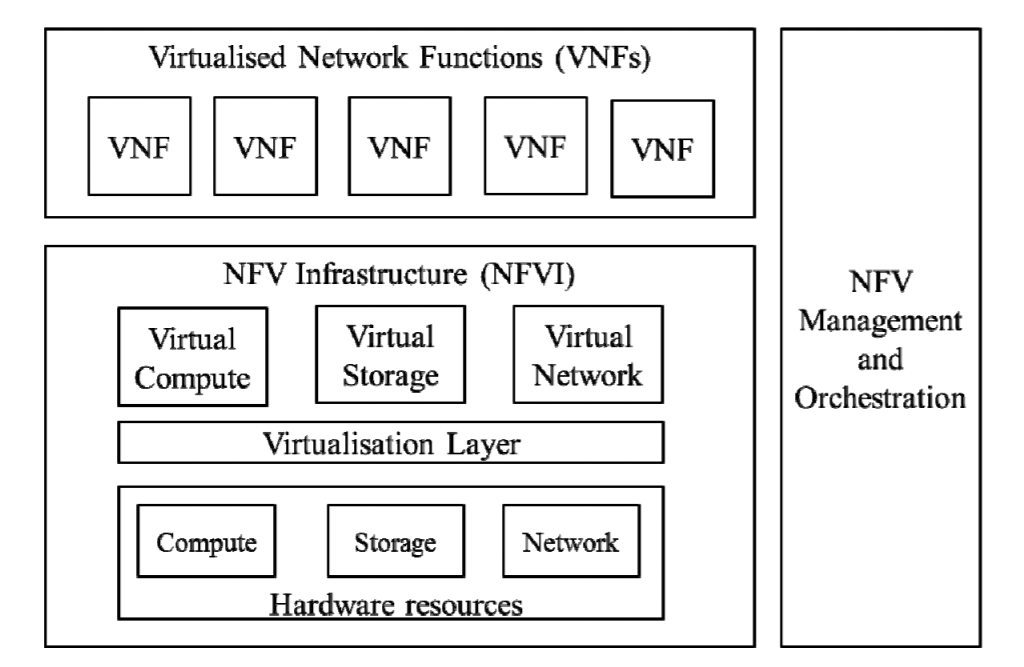


Figure 4.2-1: ETSI NFV high-level architecture (ETSI GS NFV 002)

## 4.3 Virtualisation of 3GPP Network Functions

The 5G core network is defined as service-based and consists of network functions (NFs) which can register themselves to the network and subscribe to other services using service based interfaces. 3GPP NFs are assumed to be virtualised, but do not necessarily correspond in a 1:1 manner with ETSI VNFs. CSPs may choose to group multiple NFs into a single managed VNF or to deploy each NF in an individual VNF. We assume that a NF is not split between multiple VNFs, but beyond that decisions on grouping NFs are out of scope of 3GPP.

## 4.4 General NFV security issues

Editor’s Note: This subsection contains an overview of general NFV security issues, which are not specific to 3GPP but which give background to specific 3GPP security decisions.

### 4.4.1 Access to VNFs via virtualisation layer

Most virtualisation platforms make it possible for a user with root access to the virtualisation layer to view and edit the memory of hosted VMs. This administrator may be able to change or stop processes running in the VM, give other applications access to the VM or steal security critical data. These challenges are discussed in ETSI NFV-SEC 009 [3].

An attacker may have access to the virtualisation layer via a variety of means. The access could be legitimate, such as a rogue employee at the hosting company, or illegitimate i.e. hyperjacking. From the point of view of the VNF these attack vectors are the same, as both result in a rogue actor gaining access. In general, such access would be invisible to the VNF.

### 4.4.2 Sharing of private keys between VNFs

In the 5G Core Network, NF communications are secured using TLS, according to the profiles in TS 33.210 [4]. ECDSA and RSA are used to authenticate these communications. Therefore, a VNF must contain private keys to authenticate these exchanges. These keys need to be provisioned to VMs securely on first boot, or need to be stored securely on the image in some fashion. A decision also needs to be made as to whether two NF instances may share the same key pair, for example if the second instance is deployed in the case that the first fails. These challenges are discussed in more detail in section 6.8 of ETSI NFV-SEC 001 [5].

### 4.4.3 Isolation

One of the attractions of NFV is that it allows resources to be used flexibly. Sharing hardware resources between VNFs allows networks to scale services up and down as required and to centralise the management and orchestration. However, the adoption of shared resources raises security questions which do not apply when using discrete physical infrastructure. In particular, virtualisation technology needs to ensure that VNFs can be isolated from one another, particularly in the case where they have specific security requirements. There are various approaches to isolating VNFs, ranging from using physically separate hardware to using separate containers. Where VNFs do share resources, these might be managed in different ways, as discussed in Section 6.5 of [2]. Sharing memory and specialised hardware could require special considerations.

There are a number of security threats if VNFs are not appropriately isolated and resources are not shared effectively. These include the noisy neighbour problem and potential side-channel attacks.

### 4.4.4 Vulnerabilities of physical hosts

X86 and similar server architectures have a number of physical security weaknesses from a critical national infrastructure perspective. Plug and play interfaces (e.g. USB and removal RAID discs) unless disabled or tightly controlled represent a risk to 3GPP NF security. However, more difficult to control attack vectors such as PCI Express bus Direct Memory Access (DMA) or use of OS swap/page files represent risks if physical access to the server(s) hosting a 3GPP NF becomes possible. Similarly, most server firmware would detect hardware changes (e.g. adding an extra copy physical network port which is visible to the host firmware), but if the replacement hardware uses the same IDs and declared interfaces this is much more difficult to detect.

In legacy PNF implementations, such risks are better understood with physical constraints including secured racks, physical testing of interfaces to confirm they are disabled and careful placement of more sensitive functions (e.g. AUC) within CSP data centres. However, for virtualised implements using large common hosts pools, physically securing all hosts (rather than those dedicated ones for a specific function) so that any 3GPP function can run on any host, while controlling physical access attacks is difficult to achieve. This threat potentially increases with IAAS and NAAS deployments.

Furthermore, many data centre hosts are equipped with Baseband Management Controllers and Intelligent Management Interface Protocol. If an attacker is able to access these controllers, they effectively have direct control over all hosts and all VMs running on them. Over recent years a number of vulnerabilities have occurred. For sensitive functions such as the AUC or LI functions, the risks would obviously be increased.

### 4.4.5 Secure Administration

A key aim of virtualisation is implementation of the network using flexible resources which can be scaled and sized in near real-time to fit customer demand. To achieve this effectively NFV deployments rely on a single administration domain, where a global administrator is able to manage the hosts and NFV environment.

While this administrator is not necessarily able to manage the entire deployment directly from a single account, as they are able to give themselves roles and permissions, they can use it as a starting point to gain other capabilities. Without extra security controls an attacker who gains access to one of these accounts would be able to exploit, control and manage the entire NFV environment.

The global administrator role is considered to exist in the highest trust domain for the 3GPP architecture.

## 4.5 Limited Virtualisation vs Full Virtualisation

There are a very wide number of definitions as to the meaning of "virtualisation". A number of vendors have been offering "virtualised" implementations for 15+ years using common hardware platforms running VM implementation architectures. However, these limited virtualisation implementations use dedicated hardware instances for each network function.

While these limited implementations have some of the same risks as a fully virtualised implementation (e.g. common software environment), they are essentially identical to non-virtualised legacy PNF implementations as they have physical testable and securable boundaries. On the other hand, these limited implementations do not offer many of the benefits, including security benefits, of fully virtualised deployments. Many limited virtualised implementations can be readily migrated into fully virtualised environments and will be migrated as networks become increasingly virtualised during the VNF’s operational lifetime.

Editor’s Note: Further security issues are FFS

# 5 Key Issues

## 5.1 Introduction

This clause details the key issues identified for security aspects related to the Virtualisation of 3GPP functions and architectures. Each key issue defines the background to the issue, defines the threats related to the issue and proposes requirements that resolve or mitigate the key issue.

## 5.2 Key Issue 1: Establishment of trust domains for Network Functions

### 5.2.1 Key issue detail

5G Network Functions can be grouped into different trust domains which have different security requirements. For example, trust in functions which contain long term cryptographic keys might require different levels of trust to functions which only hold session keys or those which do not contain cryptographic values at all. However, this classification is too simplistic. Nearly all 3GPP NFs will contain some privacy sensitive information for billing purposes or cryptographic material. Applying the same security policies to NFs in different trust domains could lead to reduced security and/or to reduced functionality.

Security domains based on grouping whole NFs may not be sufficient. In some scenarios (e.g. LI), sub-functions of NFs (e.g. LI POIs) may need to belong to different trust domains to the rest of the NF functionality.

Definition of appropriate segregation and security policies for NFs in different trust domains requires establishment of trust domains for 3GPP NFs. It is up to 3GPP to define what a sensitive function or sub-function is and how they must be handled to protect privacy or security sensitive data, within a virtualised environment.

While 3GPP TS 33.501 [6] provides some consideration for 5G functions, CSPs are also in the process of virtualising IMS or 3G/4G networks, for which similar consideration has not yet been given.

Editor’s Note: It may be necessary to liaise with ETSI ISG NFV or open source groups to ensure the necessary capabilities are available or developed.

### 5.2.2 Security threats

If 3GPP network functions with different security requirements are defined to be in the same trust domains, the access to a high trust domain might be too open, increasing the attack surface for security critical or high trust functions.

A relatively low privilege administrator or user might have access to 3GPP network functions which are above their intended level of privilege

A user or administrator might impact one trust domain from another.

### 5.2.3 Potential security requirements

The trust domains of 3GPP network functions should be identified. Security policies should be applied depending on those trust domains. Solutions to this requirement required inside 3GPP.

The system should manage each trust domain separately. Solutions to this requirement required inside 3GPP.

The system should manage (e.g., define, enforce) the security policies for each trust domain independently. Solutions to this requirement required inside 3GPP.

## 5.3 Key Issue 2: Confidentiality of sensitive data

### 5.3.1 Key issue detail

Certain 3GPP NFs will hold sensitive data, which should not be available to other NFs or which should only be made available in a specific set of circumstances. For example, TS 33.501 [6] includes the requirement that long-term keys shall never leave the secure environment of the UDM/ARPF.

To have the same level of confidence in the confidentiality of sensitive data when stored in a VNF as when it is stored on physically separated hardware it is necessary to consider new threat vectors. For example, the long-term keys in a virtual UDM/ARPF could be stolen by an attacker with root access to the virtualisation layer. Alternatively, cache side-channel attacks as in [7] might allow the operator of a VNF sharing resources to recover data.

### 5.3.2 Security threats

Without appropriate protection, cryptographic keys or other security critical data of a virtualised 3GPP NF could be stolen by an attacker with access to the virtualisation layer.

Without appropriate protection, sensitive material of a virtualised 3GPP NF of one operator could leak to VNFs of other operators running on the same virtualisation layer.

### 5.3.3 Potential security requirements

Solutions to key issue 2 should increase assurance that sensitive information of a virtualised 3GPP NF is not exposed through the virtualisation layer.

The system should manage (e.g., define, enforce) the permission control at the virtualization layer between NFs and/or sub-NFs. Solutions to this requirement required both inside and outside 3GPP.

## 5.4 Key Issue 3: Availability of Network Functions

### 5.4.1 Key issue detail

Many 3GPP NFs are essential for the 5G Core Network to function. For example, if a UDM/ARPF is not available then a user cannot complete primary authentication. Similarly, if an AMF is not available then a connection cannot be managed. Therefore, it is important that the VNF is guaranteed to be available in the same way as a physical network function would be.

One of the advantages of virtualisation is that a network can scale and transform to meet demand. In general, it is likely that the availability of required 3GPP network functions is less of a concern than in a physical deployment. However, virtualisation does introduce new availability risks. For example, shared resources might be monopolised by a neighbouring VM (the noisy neighbour problem).

### 5.4.2 Security threats

Without appropriate protection shared resources required for a virtualized 3GPP NF could be monopolised by neighbouring VMs, reducing availability or functionality of the virtualized 3GPP NF.

In a multi-tenant cloud environment, a neighbour attacker uses vulnerabilities in shared components to attack a service, either individually or by executing a distributed denial of service (DDoS) attack.

Editor’s Note: Further new threats to availability are FFS.

### 5.4.3 Potential security requirements

Solutions to key issue 3 should increase assurance that virtualised 3GPP NFs, particularly those which are critical to the operation and security of the network, will have access to the required resources for their availability or functionality when sharing resources with other VNFs. Solutions to this KI are expected to be mainly handled outside of 3GPP.

The system should manage the utilization, traffic distribution, and overload control of the NFs and sub-NFs to ensure availability for key network processes. Solutions to this requirement are required mainly outside of 3GPP.

## 5.5 Key Issue 4: Common Software Environment

### 5.5.1 Key issue detail

Older SS7 circuit switch networks typically had much lower security than current 3GPP NFs. Their proprietary implementations, non-IP protocols (e.g. X25) and lack of flexible deployment options provided a high degree of security by obscurity. By comparison virtualised release 15 onwards implementations will provide a much higher level of basic security but the common software platform on which functions are implemented will introduce new risks.

In legacy PNF implementations each vendor typically used a proprietary platform and software with a few common web server or OS elements. This meant that if a vulnerability or zero day exploit was found and utilised by an attacker, this generally only compromised one NF. This would give the attacker access to data on that NF and the communication links into and out of that NF but the attacker would not have an advantage in attacking the next NF in the chain. Except in really poor implementations relying on network edge security only, the risk of a cascade failure is minimal with PNFs.

In virtualised implementations all NFs are implemented using a common software platform such as OpenStack [8]. While vendors may produce tweaked variants, the code core will be largely identical. Similarly, OS, Hypervisor and VM software will be identical or from a limited set of variants. What this means is that if an attacker is able to identify a software vulnerability in one VNF, that vulnerability will likely exist in many other VNFs making the attackers job much easier and increases the risk of a cascade security failure of the network. If network security functions (e.g. SEPP) use the same software core or are in the same virtualisation layer trust domain as the functions they are protecting the risk further increases if a software vulnerability occurs.

### 5.5.2 Security threats

If a vulnerability is found in software used across multiple virtualised 3GPP NFs then an attacker might be able to exploit all of these NFs with the same attack. The vulnerability might allow the attacker multiple access points into the network, or may allow them to move laterally through the network.

Use of a common software platform might give an attacker more information about how to traverse a network, meaning that compromise of one virtualised 3GPP NF might allow them to move through connected NFs using implicit trust.

### 5.5.3 Potential security requirements

Solutions to key issue 4 should increase assurance that a software vulnerability in one virtualised 3GPP NF does not affect other virtualised 3GPP NFs using the same software platform. Solutions to this requirement required both inside and outside 3GPP.

Network interfaces should be locked down so that they only accept a restricted number of expected protocols. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

Network management should be secured and should only be allowed from authorised devices and/or networks. Multi-factor authentication should be used to log into administrator accounts. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

## 5.6 Key Issue 5: Data Location and Lifecycle

### 5.6.1 Key issue detail

With PNFs you know where subscriber or other sensitive data is located, or at least have a high degree of certainty. With virtual functions by design that data can be anywhere in the host infrastructure. Indeed, if a CSP implementation spans multiple data centres in multiple countries it may be necessary to constrain where a VNF or piece of user data physically resides. For example, LI functions and LI target lists need to remain within a single legal jurisdiction. Similar restrictions may apply to content which is subject to DRM and is only licensed for a single country, or more generally to data covered by GDPR.

Furthermore, in virtualised environments, it is necessary to consider where data has been and whether that data is privacy sensitive. If a VNF moves from one host to another or is terminated, and the previous resources are allocated to another VNF without being fully cleared, this risks compromise of privacy sensitive data or keys.

OSs are not unknown to proliferate temp files, which in a PNF is much easier to contain (ignoring PNFs with external storage). In a VNF, if storage / memory is not fully erased before reuse there is a significant risk of data loss between VNFs. By extension, software is not unknown to crash or experience abnormal behaviour, increasing the risk of data remaining in undesirable locations.

### 5.6.2 Security threats

Without appropriate restriction on function location or data location, privacy sensitive information of one virtualised 3GPP NF could be exposed to a different legal jurisdiction.

Without appropriate lifecycle protection, sensitive information of one virtualised 3GPP NF could be leaked to other VNFs reusing the storage resource.

### 5.6.3 Potential security requirements

Solutions to key issue 5 should increase assurance that privacy sensitive information of a virtualised 3GPP NF is protected from being leaked out of its legal jurisdiction. Solutions to this requirement required both inside and outside 3GPP.

Solutions to key issue 5 should increase assurance that sensitive information of a virtualised 3GPP NF is protected during its lifecycle process to avoid leakage of the information to other VNFs reusing the storage resource. Solutions to this requirement required both inside and outside 3GPP.

All privacy sensitive data should be encrypted when at rest and when in transit. Solutions to this requirement required both inside and outside 3GPP.

Security policy which restricts where certain types of data can reside should be defined and implemented by CSPs. Solutions to enable this requirement potentially required both inside and outside 3GPP.

When VNF moves from one host to another or when VNF is terminated, the system should ensure that resources, privacy sensitive data, and/or keys are fully cleared. Solutions to this requirement required both inside and outside 3GPP.

## 5.7 Key Issue 6: Function Isolation

### 5.7.1 Key issue detail

3GPP architectures (including 5G) are still based on a functional "boxes", with 3GPP security applied between the functions on a reference point basis. If 3GPP functions are implemented in a common software host environment (e.g. with a common hypervisor, compute and storage), TLS and similar protocols are reduced to protecting information travelling between memory locations in a single logical memory block. As such, if an attacker (or hypervisor administrator) is able to gain access to the memory in which a set of VNFs run, then relying on reference point-based security will offer little protection, except on physically exposed hardware links.

### 5.7.2 Security threats

If appropriate protection is not in place functions might be able to directly introspect the memory of other functions.

### 5.7.3 Potential security requirements

Solutions to this KI should increase assurance that the virtualisation platform prevents one function from inspecting the memory of other functions. Solutions to this requirement required outside 3GPP.

Delegated administrator roles shall be used, with roles which could give a user or administrator the ability to inspect the memory of functions only used in exceptional circumstances. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

The system should manage reference point-based security and service-based security between VNF functional "boxes”. Solutions to this requirement required inside 3GPP.

Confidentiality protection should be provided to protect information traveling between memory locations in a single or multiple logical memory block. Solutions to this requirement required both inside and outside 3GPP.

Editor’s note: this last requirement needs a bit more work/clarification. Definition of logical memory block, etc. Multiple requirements may be needed.

## 5.8 Key Issue 7: Memory Introspection

### 5.8.1 Key issue detail

In all operating systems or virtual environments there are a number of memory management and control functions which are able to view or access all memory locations. These functions such as the kernel in desktop OSs control access to memory and are responsible for preventing applications from accessing each other’s memory spaces. In VM based NFV environments, the hypervisor is responsible for administering each VM’s resources and isolating the VMs from each other.

In legacy hardware networks, manufacturers apply physical separation within the physical hardware to keep sensitive control plane sub-components within a 3GPP function (e.g., key material or billing data) away from lower security sub functions or other general user plane traffic handling sub functions. This may include having different administration domains (e.g., LI sub-functions are managed via different interfaces and have separated administration).

In a virtual environment while the hypervisor plays a role in preventing one VM from accessing the memory of another (except through declared VM shared memory locations), the hypervisor is also able to inspect any memory which is directly under hypervisor control. Such access to memory or other VM resources cannot be detected by VM or 3GPP security mechanisms. Encrypting memory provides some resistance but if the keys used to encrypt the memory are also under hypervisor control (including hypervisor resource controlled TPM / HSMs) then this does not prevent introspection.

Editor’s Note: FFS whether TPM/HSSs term in KI#7 section 5.8.1 need to be generalised.

In addition to reading memory, the hypervisor is also in many cases able to write directly to memory, bypassing normal memory access controls and security within the VNF VM. This allows an attacker with access to the hypervisor to change data within a 3GPP function at run-time or indeed change the operation of the function itself.

Container based NFV environments are subject to similar memory introspection risks, with the container (or cluster) management engine providing similar functionality to the hypervisor in VM based implementations. KI#25 (see clause 5.26) addresses the issues and additional threats introduced by containers.

### 5.8.2 Security threats

If appropriate protection is not in place functions might be able to directly introspect the memory of other functions.

### 5.8.3 Potential security requirements

An NFV environment shall use a virtualisation platform which prevents one function from inspecting the memory of other functions. Solutions to this requirement required outside 3GPP.

Delegated administrator roles shall be used to ensure that administrators do not have the ability to inspect memory of functions except under exceptional circumstances. Solutions to this requirement required outside 3GPP.

Firmware/UEFI updates shall be applied in a timely manner to protect against hardware bugs and security flaws, including those which are newly found. Solutions to this requirement required outside 3GPP.

The system should manage the hypervisor to enforce the network security policies. This includes, but is not limited to, ensuring that;

VMs are isolated from each other,

Applications are prevented from accessing each other’s memory spaces,

VMs are prevented from accessing the memory of another VM,

Keys used to encrypt the memory are also under hypervisor control,

Hypervisors are not allowed to write directly to memory,

Hypervisors are not allowed to bypass normal memory access controls and security within the VNF/VM,

Hypervisors are not allowed to change data within a 3GPP VNF at run-time.

Solutions to this requirement required outside 3GPP.

The system should apply physical and/or logical separation to keep sensitive control plane sub-components within a 3GPP function (e.g. key material or billing data) away from lower security sub-functions or other general user plane traffic handling sub-functions. Solutions to this requirement required both inside and outside 3GPP.

## 5.9 Key Issue 8: Test Isolation and Assurance

### 5.9.1 Key issue detail

In legacy hardware deployments,3GPP, GSMA or other testing schemes generally involve testing 3GPP functions as opaque boxes or pentesting them in isolation from other network functions. While it is possible to test virtual functions in this way, the level of assurance gained is different. Such stand-alone testing relies on the underlying virtualisation and hardware layers being 100% secure and that no future vulnerabilities are found in those underlying components.

Testing functions in isolation does not guarantee that when a VNF is instantiated on a different host virtualisation environment or is instantiated in a larger virtualisation environment containing multiple VNFs that a 3GPP function tested in isolation remains secure.

Isolation in testing refers to VNF to VNF isolation as well as platform to VNF isolation. In general, it means that the VNF is firstly tested on its own in a dedicated NFVI and then tested with other VNFs in a shared NFVI.

### 5.9.2 Security threats

Testing virtualized 3GPP Network Functions in isolation might miss threats and vulnerabilities which arise from the way in which the virtualized 3GPP NF interacts with other components in the operator’s environment. Without clarity around the scope and limitations of a given testing scheme CSPs might have a false sense of security around use of a product.

As different virtualization environments may provide different levels of security protection for the application layer, stand-alone testing of a virtualized 3GPP NF may not ensure that the desired level of assurance of the 3GPP NF remains the same when deployed in different virtualized scenarios. When a virtualized 3GPP NF successfully tested in isolation or a more secured virtualization environment is deployed in a less secured virtualization environment, it may not provide the required level of assurance and hence risks potential attacks.

Furthermore, virtualized 3GPP NFs used in different service types (e.g. network slices) or different services (e.g. vertical services) may face different security assurance requirements from the service layer. A virtualized 3GPP NF successfully tested in isolation may not provide the required level of assurance of a specific slice/service, for a given NFVI.

### 5.9.3 Potential security requirements

Security assurance testing of a virtualized 3GPP NF needs to be performed using a standardized NFVI environment used to test all VNFs. When testing security assurance of a virtualized 3GPP NF, the scope of testing should be clarified, including defining the pre-conditions of the virtualized test environment/platform and defining assumptions made in the process. Where possible recreate these assumptions in the product deployment e.g. close ports which do not need to be open. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

Both positive and common vulnerability testing (e.g negative testing) should be carried out against virtualized 3GPP NF and the underlying virtualization and hardware layers. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

Virtualized 3GPP NFs should be checked regularly to see if they are using out-of-date or insecure versions of a library and these libraries should be updated if and when possible. This is required to mitigate the increased attack surface which was partly addressed by physical security assurance protections in physical networks. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

## 5.10 Key Issue 9: Trust domain and Slice Isolation

### 5.10.1 Key issue detail

3GPP TS 33.501 [6], defines requirements for slice isolation. However, if one or more slices are implemented on the same common hypervisor, hosts and virtualisation layer resources / management (MANO) then requirements in TS 33.501 may only be met at the 3GPP functional application layer. Unlike slices built using PNFs, the slice isolation would only be virtual in nature and subject to the threats of other key issues described in the present document.

A similar isolation challenges and risks occur for different trust domains within a 3GPP operator network. IMS security was standardised by SA3 in release 5 to exist in a separate security / trust domain from the 3GPP or non-3GPP access networks used to connect to IMS. Using PNFs, CSCF are largely isolated from 4G or 5G core functions, except through a limited number of defined interfaces. Implementing IMS in a fully virtualised network is similar to the problem of virtualised slice isolation.

### 5.10.2 Security threats

An attacker could take advantage of the virtualised environment to move from a lower to a higher trust domain or to move between slices.

Sensitive data might be visible outside of the slice it should be confined to.

### 5.10.3 Potential security requirements

3GPP trust model needs to be defined in 33.501 to identify isolation and trust relationships between 3GPP NFs. Solutions to enable this requirement are required inside 3GPP.

An NFV environment should use a virtualisation platform which prevents one function from inspecting the memory of other functions. Solutions to this requirement required outside 3GPP.

The 5GC should be configured so that NFs can only communicate with NFs which they have a valid reason to communicate with. The default should be that functions are not able to communicate. Solutions to enable this requirement potentially required both inside and outside 3GPP.

Delegated administrator roles shall be used and should only give the user or administrator the minimum necessary privileges. Solutions to this requirement required outside 3GPP.

The system should manage slice isolation, security domains and trust domains. Solutions to this requirement required inside 3GPP.

## 5.11 Key Issue 10: Single Administrator Domain

### 5.11.1 Key issue detail

As discussed in 4.4.x, NFV deployments usually rely on a single administration domain, with a global administrator who is able to manage the hosts and NFV environment. As such, at some level, all VNFs regardless of their sensitivity are potentially reduced to the same security level of the single administration domain. Therefore, if an attacker is able to gain global administrator privileges, they will be able to control and manage all Network Functions, regardless of their sensitivity and trust domain.

### 5.11.2 Security threats

An attacker with access to a global admin account has access to all VNFs, including high security environments like the UDM/ARPF, could change the routing of a network to send traffic to a location of their choosing or could shut down a network altogether.

### 5.11.3 Potential security requirements

In general, delegated administrator roles shall be used. The global administrator role shall only be used in exceptional cases, e.g. to add permissions for other high-level administrators. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

The highest security controls shall be applied to use of the global administrator role. In particular all use of this role should be logged and audited. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

An alert should be raised in the global administrator role is used, or if any account attempts a function it is not meant to attempt. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

All administration and management should only be permitted from known, attested devices and multi-factor authentication should be enforced. Solutions to this requirement required both inside (SCAS) and outside 3GPP.

## 5.12 Key Issue 11: Where are my Keys and Confidential Data

### 5.12.1 Key issue detail

In PNFs there is a reasonable expectation that if a PNF contains dedicated key storage that any cryptographic keys which are required for PNF functionality will only be accessible to that PNF and the key storage is within the PNF.

With virtualised implementations this gets much more complicated. Firstly, a VM has no direct access to any hardware. A VM’s view of the world is limited to that presented to it by the hypervisor or underlying host environment. However, it has no idea whether physical key storage hardware is in the same host as the VM, or indeed whether any such key storage is actually a physical tamper proof hardware environment as opposed to a virtual key storage instance using software-based approaches. While in some special scenarios a VNF may have special dedicated hardware key storage as part of a dedicated specially allocated (and separately administered host), VM and a VNFs will in general need to use arbitrary hosts within the cloud environment.

It should also be noted that in general a VM cannot actually tell the difference between different types of memory, hard disc or storage unless specific mechanisms are used to provide visibility or confirmation (e.g. a RAM disc looks identical to physical storage to a VM).

### 5.12.2 Security threats

If a VNF cannot securely attest what host it is running on then high security functions could be deployed on vulnerable hosts. This could increase the risk of compromise of the data held by the NF.

### 5.12.3 Potential security requirements

It should be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts. Solutions to enable this requirement potentially required both inside and outside 3GPP.

Note: 3GPP need to identify specific security resources which need to be supported and requestable from MANO.

Binding should be verified by secure hardware backed attestation of the health and security of the host. Controls should be verified and enforced at boot time and each time a function is migrated. Solutions to enable this requirement potentially required both inside and outside 3GPP.

Note: This requirement relies on the VNF trusting the virtualisation layer to implement the rules applied.

The system should manage (e.g., assign/log bindings) key storage and confidential data in a manner that provides protection against data compromise. Solutions to enable this requirement potentially required inside 3GPP.

## 5.13 Key Issue 12: Where the is my function

### 5.13.1 Key issue detail

Similar to the key issue 11 Where are my Keys and Confidential Data and key issue 5 Data Location and Lifecycle, for some VNFs (or sub components) it is necessary to know exactly where a VNF is (or at least in which data centre it resides). The same also applies in the case of physical attack in post event forensic scenarios.

By default, cloud hosting environments do not by nature provide an attestable guarantee of physical location of a host or VM. It is possible to indirectly attest location through host IDs but as with SA3 studies on physical locking down femto cells to specific locations have shown, it is possible to move a host from one location to another. 3GPP functions such as AUC, UDM or LI functions need to be attestable within to specific physical location boundaries and those boundaries need to be attestable within 3GPP scope. ETSI TR NFV-SEC 016 [9] discusses some of these issues, but the additional 3GPP specific constraints required, are within the scope of 3GPP and not ETSI ISG NFV.

Furthermore, if functions such as SEPP are supposed to be the physical boundary of the network then it may be necessary to be able to constrain them and the SDN routing to them, to specific physical locations.

### 5.13.2 Security threats

VNFs might be instantiated in or migrated to locations which are not appropriate for the services provided or which violate legal requirements or regulations.

### 5.13.3 Potential security requirements

It should be possible to deploy a VNF to a host that provides specific security resources (e.g. HMEE, secure compute, secure memory) in order to bind a VNF to a specific host or group of hosts. Solutions to enable this requirement potentially required both inside and outside 3GPP.

Note: 3GPP need to identify specific security resources which need to be supported and requestable from MANO.

These controls should be verified by secure hardware backed attestation of the health and security of the host. Controls should be verified and enforced at boot time and each time a function is migrated. Solutions to this requirement potentially required both inside and outside 3GPP.

Note: This requirement relies on the VNF trusting the virtualisation layer to implement the rules applied.

The system should manage the physical location of the VNFs and sub-components and SDN routing to provide the attestation that the VNF/sub-components provided a commensurate level of security to match the requirements of the service or to meet legal/regulatory requirements. Solutions to this requirement required both inside and outside 3GPP.

## 5.14 Key Issue 13: Attestation at 3GPP Function level

### 5.14.1 Key issue detail

ETSI ISG NFV specifications such as ETSI GS NFV-SEC 012 [10] provide various requirements and recommendations for attestation of host hardware, VMs and VNFs during boot-time / instantiation time. Attestation can be of multiple types (e.g. Boot-time and run-time). However, since security cannot exist in isolation at hardware layer, NFV layer and 3GPP NF layer (VNF functionality layer), it is necessary for the 3GPP to set explicit requirements on attestation. Similarly, ETSI ISG NFV or open source group working on NFV software platform cannot specify the functionality of 3GPP NF or requirement with respect to their attestation.

3GPP NFs especially in multiple vendor and IAAS scenarios, need assurance that hardware or other critical security functions have not been modified and can be trusted. For example, the NRF in SBA needs to attest that a discovered NF is what it claims to be and has the capabilities it claims to have. While the OSS / BSS allow an NRF to become aware of a new VNF instance (e.g. AMF) it is the underlying attestation chain from a security perspective that verifies the NF is secure.

Possession of a 3GPP level identity / certificate is not in itself a means to prove authenticity of a VNF, unless there is a full attestation chain back to hardware. To support multi-vendor scenarios that chain needs to be standardised either in 3GPP or standards bodies with a wider remit such as ETSI TC CYBER.

### 5.14.2 Security threats

Without full attestation chain from 3GPP function level to hardware level, a 3GPP Network at the application layer is not able to verify the trustworthiness of VNFs or the NFVI. This means that a 3GPP NF can only make a limited judgement as to whether or not to trust another virtualized NF. For example, the NRF may authorize a maliciously altered virtualized NF to access a service it intends to abuse.

### 5.14.3 Potential security requirements

It shall be possible to attest a virtualized 3GPP NF through the full attestation chain from the hardware layer through the virtualization layer to the VNF layer. Solutions to enable this requirement potentially required both inside and outside 3GPP.

Attestation of a platforms integrity should be linked to the application layer and possible for other functions to query. If platform attestation fails the virtualized 3GPP NF should not be allowed to run. Solutions to this requirement potentially required both inside and outside 3GPP.

Attestation of the VNF should be performed prior to deployment/network integration and during operations. Solutions to this requirement required both inside and outside 3GPP.

Attestation of the VNF should be done at the hardware, virtualization, and NF layers. The solution is inside and outside 3GPP.The system should manage VNF attestation. Solutions to this requirement required both inside and outside 3GPP.

## 5.15 Key Issue 14: VNF Host Spanning

### 5.15.1 Key issue detail

3GPP specifies 3GPP NFs in terms of large complex lumps of functionality which span multiple physical hardware hosts in both legacy and virtualised implementations. While there is a risk of an attacker gaining physical access to the interconnections between servers making up a single PNF, this generally requires physical access to the hardware. However, in a virtualised environment access can be gained much more easily as the servers making up a function are more likely to be physically distributed and the SDN v-switch would allow an attacker to much more easily fork IP packets flowing between hosts remotely. Such forking is very difficult to detect or prevent from within a 3GPP NF or VM, unless specific design mitigation is taken to minimise the risk.

While TLS automatically applied by the NFV / SDN layer between VMs reduces external attacker threat, it is much less effective against attackers who have (or gained) access to NFV MANO etc.

### 5.15.2 Security threats

An attacker could read data in transit.

### 5.15.3 Potential security requirements

All control plane data in transit between hosts should be sent over an encrypted and authenticated channel using non-proprietary protocols. User plane traffic between hosts may be protected. Solutions to this requirement required outside 3GPP.

Note: It is assumed that the 3GPP layer does not need explicit real-time confirmation of the status of the host to host layer encryption (intra VNF). 3GPP layer security in 3GPP TS 33.501 [6] already covers VNF to VNF security (e.g. AMF to SMF).

The system should prevent and detect unauthorized VNF host spanning. Solutions to this requirement required both inside and outside 3GPP.

## 5.16 Key Issue 15: Encrypted Data Processing

### 5.16.1 Key issue detail

As an extension to key issue 7 Memory Introspection and key issue 19 Time Manipulation, in a virtualised environment it is necessary to explicitly consider the risk to cryptographic processing of data within a VNF where a fully hardened HSM or HMEE is not used to perform the cryptographic function.

Most software manipulating data with cryptographic operations will perform modification actions on encrypted data by first unencrypting the data either in general memory (less than ideal) or CPU cache (better but vulnerabilities exist). Following the necessary processing, the data will be encrypted again.

Within existing SA3 specifications, while some specialist operations are performed in tamper resistant hardware (e.g. UICC), the bulk of cryptographic processing (e.g. user plane protection) will be performed using general X86 (or similar) servers within the core network.

In a virtualised environment there are various ways in which unencrypted data can be captured; through the hypervisor; server management hardware; modification of VNF images; instantiating a parallel VM on the same physical CPU; or any number of other options. The risks of being able to capture encrypted data in an unencrypted form due to processing of that data, increases significantly. If that processing is highly sensitive (e.g. AUC or LI functions) then the risk may not be acceptable. Placing entire VMs in fully hardened HMEEs may reduce the risk in the longer term but not all cryptographic functions can be placed in a HMEE (this will not scale) and currently no suitable X86 (or similar architecture) HMEEs exist in commercial data centre servers capable of the scale required to support 5G deployments.

### 5.16.2 Security threats

If data is decrypted and/or processed in an unencrypted format in an insecure environment it could be intercepted or copied.

### 5.16.3 Potential security requirements

Sensitive data should only be decrypted or handled in an unencrypted format in VNFs on trusted and well-known hosts. Solutions to enable this requirement potentially required both inside and outside 3GPP.

It shall be possible to control whether untrusted or lower trusted VNFs are allowed to run on the same host as VNFs in a higher trust domain. Solutions to enable this requirement potentially required both inside and outside 3GPP.

It shall be possible to further restrict VNFs on a single host depending on whether they handle decrypted sensitive data. Solutions to enable this requirement potentially required both inside and outside 3GPP.

These controls should be verified by secure hardware backed attestation of the health and security of the host. Controls should be verified and enforced at boot time and each time a function is migrated. Solutions to enable this requirement potentially required both inside and outside 3GPP.

The system should prevent and detect unauthorized or unintended data manipulation and leakage (e.g., modification of VNF images, instantiating parallel VM(s) on same physical CPU). Solutions to enable this requirement required outside 3GPP.

## 5.17 Key Issue 16: Mixed Virtual and Legacy PNF Deployments

### 5.17.1 Key issue detail

One of basic tenants of a VM or a VNF is that it does not know that it is virtual (a PNF doesn’t know it is physical either). Similarly, 3GPP specifies application layer functionality of core NFs but does not (with the exception of RAN groups) specify physical implementation aspects.

With the exception of green field 5G only operators, most virtualised deployments will commence with adding VNFs to an insisting PNF based networks. Overtime the number of VNFs will increase but mixed network deployments will be the default for the next 10+ years. Similarly, mixed SDN and non- SDN linked NFs will also co-exist. By default, PNFs and VNFs have to be able to implicitly trust each other in mixed deployments, given that 3GPP SA3 currently does not specify different handling or trust relationships based on PNF or VNF implementation.

As discussed in other key issues, PNFs and VNFs are susceptible to different types of attack and in turn different have different security capabilities. Furthermore, it is likely that PNFs will be less easily patched for security vulnerabilities compared with VNFs over time.

In mixed deployments, especially where older 3G CS NFs share common NFs (e.g. virtualised HSS, UDM) with 4G or 5G higher security level VNFs, additional 3GPP security mechanisms may be required to prevent attackers using insecure interfaces as the injection points against the otherwise secure VNFs (i.e. VNF implicitly accepts messages from legacy PNF with lower security). However, the reverse attack also exists were an attacker uses the much larger attack surface offered by VNFs to attack PNFs. VNFs would ignore the messages but may well forward them to the less secure PNFs. Attacks are also possible depending on the chain of VNF and PNFs, were an attacker injects messages towards a VNF, which is forwarded to a PNF and finally to another VNF. While the first VNF and PNF are unharmed by the attack, the second VNF falls foul of the implicit trust of PNF and VNF communications. It is possible to conceive other similar chained attack scenarios where PNFs and VNFs exist together without knowledge of each other’s implementation or trust domain segregation.

### 5.17.2 Security threats

Vulnerabilities of 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.

Vulnerabilities of 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.

### 5.17.3 Potential security requirements

The 5GC should be configured so that NFs can only communicate with NFs which they are specifically authorised to communicate with. These rules should be applied 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. Solutions to this requirement required inside 3GPP.

The security policies enforced by the system should complement each other in order to protect mixed PNF-VNF deployments. Solutions to this requirement required inside 3GPP.

## 5.18 Key Issue 17: Software Catalogue Image Exposure.

### 5.18.1 Key issue detail

In legacy PNF implementations there is a high degree of security by obscurity in terms of the software images that form vendor implementations of 3GPP NFs. While 3GPP specifications describe the high-level functionality of NFs and CT stage 3 specs describe the protocol of the interfaces between them, without "stealing/borrowing" numerous large racks of servers, it is difficult for an attacker to directly analyse the source code or executable software in a PNF.

Virtualised networks define convenient software onboarding APIs and use central software catalogues to hold the VNF images prior to instantiation. There has been significant resistance in ETSI ISG NFV and open source communities to mandate full mandatory integrity checking of software images at both the overall package and sub-component (artefact) level. Current implementations offer minimal if any mandatory signing and where they do, this is based purely on vendor signatures. Therefore, in theory at least, any image from the same vendor would past verification checks if loaded into the wrong CSP software catalogue.

Furthermore, the software catalogues with or without integrity protection provide a standardised description of the VNFs, their resource requirements, their configuration and ultimately the compiled executables that makeup the VNF. If an attacker is able to access the catalogue then they will be able directly gain a lot of information which can then be used to attack the running instances of the VNF. Where those VNFs contain cryptographic functions or sensitive information, this increases the risk further.

Based on current virtualisation standards in ETSI and Open Source, confidentiality protection of whole image or artefacts during; run-time, on-boarding, storage and instantiation is not supported, although for LI purposes this was recommended in ETSI TS NFV-SEC 011 [11].

### 5.18.2 Security threats

If a software catalogue holding the images of virtualized 3GPP NFs is not integrity protected, the information within the catalogue could be exploited by attackers to launch attacks on the 3GPP NFs.

If the software package of a virtualized 3GPP NF is not integrity protected, an attacker could tamper the information inside the package before it is onboarded into the MANO software catalogue of an operator.

If the artefacts within the software package of a virtualized 3GPP NF are not integrity protected after the onboarding of the software package, the individual artifacts could be tampered by an attacker with access to MANO before the 3GPP NF is instantiated.

If the software package or the artefacts within the package of a virtualized 3GPP NF containing sensitive information is not confidentiality protected during its onboarding, storage and instantiation, the sensitive information of the 3GPP NF could be compromised to an attacker with access to MANO.

### 5.18.3 Potential security requirements

The software package and the artefacts within the package of a virtualized 3GPP NF shall be integrity protected by the vendor’s signature. Solutions to this requirement required outside 3GPP.

The software package and the artefacts within the package of a virtualized 3GPP NF and the software catalogue holding its image should be integrity protected after its onboarding. Solutions to this requirement required outside 3GPP.

The software package and the artefacts within the package of a virtualized 3GPP NF containing sensitive information shall support confidentiality protection. Solutions to this requirement required outside 3GPP.

Software package and artefacts within the package of a virtualized 3GPP NF shall be bound to a specific network after onboarding, such that unauthorized software cannot be instantiated even if it has valid vendor certificate. Solutions to this requirement required outside 3GPP.

## 5.19 Key Issue 18: The Startup Paradox

### 5.19.1 Key issue detail

Following on from key issue 17, it is unclear how to start a security sensitive function in a virtualised environment unless that security level of the whole virtualisation environment is the same as the VNF (or VNF sub-component) being instantiated.

For example, in a PNF legacy network, the AUC is typically only accessible by a handful of specifically authorised individuals. In a virtualised environment, if the AUC is to be virtualised and form part of the fully virtualised network then its image needs to be stored in the MANO software catalogues and instantiated as per any other VNF. Therefore, any certificates or information held in a sensitive function may be visible to anyone with access to MANO unless additional security measures are applied.

Ignoring the risks in key issue 17 associated with image protection at rest, once a VNF containing sensitive functions is instantiated it is unclear how to establish initial communication with those sensitive functions and to install certificates etc, without reducing the security level to that of general MANO.

### 5.19.2 Security threats

If a certificate is provisioned from MANO to an instantiated 3GPP NF, it could be compromised to anyone who has access to MANO but is not authorized to access the NF.

### 5.19.3 Potential security requirements

Access to the MANO shall be restricted to a limited number of administrators. Solutions to this requirement are expected to be handled inside 3GPP SCAS and outside 3GPP.

VNF should include a secured boot process. Solutions to this requirement are expected to be handled inside 3GPP SCAS and outside 3GPP.

## 5.20 Key Issue 19: Time Manipulation

### 5.20.1 Key issue detail

A fundamental problem with all virtualised implementations is that VMs and VNFs have trouble accurately telling the time and generating entropy. Unlike a PNF which can easily be designed to have direct access to a physical clock, a VM’s view of time is only virtual.

If an attacker, hypervisor administrator, or in some scenarios a malicious VM on the same host is able to manipulate the virtual CPU clock then is it possible to affect management or service functions such as manipulating cryptographic algorithms, key generation or other processes which are highly time dependent or may also impact the synchornization between UEs and the network. Such manipulation may involve stretching the shape of clock cycles rather than simply increasing or decreasing their frequency.

ETSI TR NFV-SEC 016 [9] provides more detailed discussion on timing issues with virtualised environments

Editor’s Note: Need to add reference to background research, NFV SEC timing papers and attack papers.

### 5.20.2 Security threats

It is possible to move clock back and forth in order to confuse the VM’s OS and VNFs. This could introduce several threats 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.

### 5.20.3 Potential security requirements

The system should provide a protected and trusted network time source. Solutions to this requirement required outside 3GPP.

The VNFs shall synchronize with trustedtime servers. Solutions to this requirement required outside 3GPP.

## 5.21 Key Issue 20: 3rd Party Hosting Environments

### 5.21.1 Key issue detail

Large tier 1 CSPs typically own their own data centres and will operate their own virtualisation host infrastructure, even if the management of that infrastructure may be outsourced to 3rd parties. However, smaller VNOs will likely want to consider an IAAS or NAAS model. In these scenarios sensitive personal data belong to subscriber and cryptographic (e.g. keys and algorithms) are now being stored in a 3rd party shared environment which is not within their control. Whereas, a tier 1 CSP has tight control over where their data centres are located and therefore where their sensitive data is located (and in turn who has access to that data), in a tenant IAAS or NAAS this is more difficult to control. 3GPP functions need to be securable both where CSPs have tight control over NF host environment (including location) and where they don’t.

### 5.21.2 Security threats

When deployed by an operator who uses a 3rd party host environment not in the operator’s control, without appropriate protection, the sensitive information of a virtualized 3GPP NF could be compromised by the 3rd party.

### 5.21.3 Potential security requirements

Sensitive information of virtualized 3GPP NFs shall be confidentiality protected by operators when using a 3rd party environment (e.g. NFVI). The types of sensitive information to be confidentiality protected should be defined inside 3GPP.

Third party hosting environments that support virtualized 3GPP NFs should meet 3GPP virtualisation security requirements and to enable operators to meet legal/regulatory requirements. Solutions to this requirement required inside 3GPP.

The system should be able to monitor the attestation of 3rd party hosting environments. Solutions to this requirement required both inside and outside 3GPP.

## 5.22 Key Issue 21: VM and Hypervisor Breakout

### 5.22.1 Key issue detail

As a specific extension to Key Issue 4 Common Software Environment, the VM software and hypervisor present a uniquely high risk to network security in the event that they have vulnerabilities. While hypervisor vulnerabilities are rare (especially zero-day vulnerabilities), the impact of one occurring could be devastating to network security.

In a legacy PNF scenario, while common management interfaces link PNFs together, if an attacker breaches a PNF they must breach each subsequent PNF. So, for example to attack the AUC, an external attacker would typically have to breach 2 or 3 3GPP PNFs and a set of hardware firewalls.

By comparison in a fully virtualised network with a common hypervisor, hosts and resources, if an attacker is able to execute a hypervisor breakout from the first VNF they attack, additional security needs to be applied to prevent them from tunnelling through the virtualisation layer from the attacked VNF to any other VNF.

Similarly, a VM breakout although less catastrophic would compromise all other VMs within a host or limited set of hosts. A VM breakout is considered more likely than a hypervisor breakout.

### 5.22.2 Security threats

In a fully virtualised network with a common virtualization platform, without appropriate protection, a virtualized 3GPP NF could be attacked, via tunnelling through the virtualisation layer, by an attacker executing a hypervisor breakout or VM breakout from another compromised 3GPP NF.

An attacker may break out of a VNF and gain code execution at the virtualisation layer or elsewhere in the NFVI, as described in Section 4.4.1.

### 5.22.3 Potential security requirements

The NFVI shall provide security isolation to minimize the impact of and detect hypervisor/VM breakout on a virtualized 3GPP NF. Solutions to this requirement are expected to be handled outside of 3GPP.

The NFVI and VNFs should be patched regularly. Solutions to this requirement are expected to be handled inside 3GPP SCAS and outside 3GPP.

The system should prevent and detect attacks that breakout from an attacked VNF through the virtualisation layer to any other VNF or any other location. Solutions to this requirement required outside of 3GPP.

## 5.23 Key Issue 22: MANO Single Point of Failures

### 5.23.1 Key issue detail

The NFV Management Network Orchestration functions (MANO) are responsible for on-boarding, instantiation and life cycle management of all VNF within a virtualised network. Combined with 3GPP layer OSS/BSS functions they control all VNFs and indirectly (via the hypervisor or hosts) can access all data within those VNFs, unless specially protected. Compromising MANO would effectively compromise all VNFs (to a much less extent the same applies to the OSS/BSS). Therefore, for 3GPP NFs to be secure, 3GPP NFs need to have minimum security guarantees from MANO and be designed to be resistant to compromise of the underlying MANO system.

### 5.23.2 Security threats

Without appropriate protection, virtualized 3GPP NFs could be compromised (forged/tampered/terminated) by an attacker with access to MANO system.

Without appropriate protection, the data within virtualized 3GPP NFs could be eavesdropped or tampered by an attacker with access to MANO system.

Without appropriate protection, virtualized 3GPP NFs may receive wrong or no management information from OSS/BSS or EM which is misled by a compromised MANO system.

### 5.23.3 Potential security requirements

Solutions to key issue 22 should increase assurance that virtualized 3GPP NFs are protected from being attacked via MANO system compromised by attackers. Solutions to this requirement required both inside and outside 3GPP.

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. Solutions to this requirement required both inside and outside 3GPP.

## 5.24 Key Issue 23: IP layer vs Application layer Security

### 5.24.1 Key issue detail

In a PNF implementation there are significant differences (pros and cons) between using security protocols such as IPSec designed to protect IP traffic over 3GPP reference points and over the top end to end application layer security (typically using TLS). Both are good at providing protection again a physical attacker trying to attack a physical cable or optical fibre but their characteristics vary in terms of where the encryption terminates vs where the data is processed or stored. TLS is considered to terminate closer to the point where a function processes or manages data, whereas IPSec may terminate at a PNF closer to the edge of the network.

In flat virtualised deployments with common hypervisor and resources, there is very little difference between IPSec and TLS, with neither by default offering protection from virtualization layer (e.g. hypervisor) attacks. In this scenario, both an IPSec and TLS tunnels terminate in arbitrary memory locations which will be in the same accessible range as the plain text data they are intended to protect. Unless the IPSec or TLS tunnels transverse a physical network link external to the data centres, the threats they mitigate can largely become irrelevant. Using HMEEs massively improves security (see ETSI TS NFVSEC 012 [10]. However, it is clearly impractical for all TLS or IPSec endpoints for all control plane or user plane traffic, to be terminated in HMEEs.

### 5.24.2 Security threats

In a virtualized environment, end-to-end or hop-by-hop security mechanisms in upper layers (e.g. IP layer or application layer) higher than virtualization layer (e.g. hypervisor) may not provide virtualized 3GPP NFs the same level of protection as in physical NFs. (e.g., if both ends/hops are terminated in a common virtualization platform).

### 5.24.3 Potential security requirements

Solutions to key issue 23 should increase assurance that security mechanisms in upper layers higher than the common virtualization platform layer (e.g. hypervisor) can provide virtualized 3GPP NFs the same protection as in physical NFs. Solutions to this requirement required both inside and outside 3GPP.

The system should be able to communicate security policies to the hypervisor(s) to protect NF resource selection. Solutions to this requirement required both inside and outside 3GPP.

## 5.25 Key Issue 24: Data synchronicity through network

### 5.25.1 Key issue detail

In 3GPP networks there are many defined message flows between Network Functions. For example, during the authentication procedure, a known series of messages will pass between the SEAF and AUSF and the AUSF and the UDM. In a virtualised environment, flexible and low cost (both in money and resource terms) security monitoring agents (see ETSI TS NFVSEC 013 [12]) can be easily inserted around multiple VNFs across the network, which could allow an attacker to identify the different messages making up a single procedure. Therefore, it may be possible to identify the same data in different signalling messages and to take action based on this information, potentially elsewhere in the network. This is in contrast to legacy PNF networks where it is very difficult to monitor many points in the network in parallel or to take a snap shot of the memory state of a large number of PNFs.

### 5.25.2 Security threats

Without appropriate protection, an attacker may be able to access multiple logical locations within NFVI gaining internal information of the virtualized 3GPP NFs, and see the same data of a user on multiple interfaces as it moves through the network, correlate signalling and take action based on this, in order to launch attacks. The data leaked to the attacker could even expose the privacy of users.

### 5.25.3 Potential security requirements

Solutions to key issue 24 should increase assurance that virtualized 3GPP NFs are protected from distributed monitoring attacks. Solutions to this requirement required outside 3GPP.

The system should dynamically assign VNF resources (e.g. memory address) to prevent long-term data leakage and exposure and protect network resources. Solutions to this requirement required outside 3GPP.

## 5.26 Key Issue 25: Container Security

### 5.26.1 Key issue detail

First generation NFV implementations were based on Virtual Machine (VM) architectures. While VM architectures contain a number of points of weakness including Hypervisor breakout (see key issue#21), VMs provide relatively strong memory isolation and containment of virtual NF components running in those VMs.

Current generation NFV implementations are migrating to use a Container based implementation architecture as either full replacement to VMs, or through groups of containers running with VMs.

In comparison to VM only deployments, containers have much faster instantiation times but also much shorter life times. For example, containers may be created in real time on the fly for a specific service event and then released leaving the resources free for re-use for other purposes.

From a security and isolation perspective, the VM Hypervisor is replaced by a Container Engine which manages the life-cycle of a container within a given group of containers (e.g. pod or cluster). However, the Container Engine does not provide equivalent VM security memory isolation or breakout protection. The container application usually runs on “bare metal” with no OS equivalent to the OS used in VM based implementations.

Container acceleration capabilities such as container caching also present security challenges as otherwise encrypted VM equivalent image artefacts may be available in unencrypted form in the cache to allow for fast container re-instantiation. This is similar to risks associated with key issue 5, although the impact is more localised.

The fast cycle times of containers also make traditional security monitoring and policy enforcement more challenging as network security enforcement decision engines cannot so easily make real-time access permission decisions as is possible for longer lifetime VMs.

Techniques using both containers and VMs provide some mitigation (e.g. running all containers for a specific VNF with a large VM, or using VMs for VNF security sensitive components such as TLS end points). However, using this approach restricts the flexibility of containers and introduces additional complexity / cost.

### 5.26.2 Security threats

Without appropriate restrictions on container placement, bare metal containers introduce security risks which cannot be mitigated using the same inherent security mechanism provided by VMs. Appropriate restrictions may include;

* User handling containers relative to network management containers within a VNF.
* Separation of containers belonging to different NFs on different physical servers.
* Special handling of containers implementing interfaces between different trust domains (intra-VNF and inter-VNF).

Without appropriate restrictions on the use of container caching, sensitive data or sensitive VNF components may be exposed through the common container caches.

### 5.26.3 Potential security requirements

Solutions to key issue 25 should aim to reduce or mitigate the security risk of containers to an equivalent level to that of VMs.

Security policy which restricts the placement and co-existence of containers belonging to different trust domains should be defined and implemented by CSPs. Solutions to enable this requirement potentially required both inside (e.g. trust domain policy and separation requirements) and outside 3GPP (e.g. mechanism within NFV layer used to enforce 3GPP policy requirements).

Security policy which restricts which sub-functions within an NF if implemented using containers may be cached within the general unencrypted container cache, or define security protection mechanisms for sensitive containers at rest within the cache, should be defined and implemented by CSPs. Solutions to enable this requirement potentially required both inside and outside 3GPP.

## 5.27 Key Issue 26: Container breakout

### 5.27.1 Key issue detail

The newer generation of NFV implementations choose to deploy NF as group of containers especially due to the benefits associated to containers and its deployment aspects over traditional VM deployment. Such deployments can be highly flexible by allowing the operators to deploy multiple NFs as a collection of small microservices on same physical machines and/or even deploy NF containers within VMs. Containers co-hosted on the same physical machine as tenants share the same kernel and OS resources. This allows for a potential risk of a rogue container escaping the container confinement and impacting other co-hosted containers. The KI is about container breakouts and its impact on other containers.

There are multiple ways for attackers to escape container isolation. There have been reported a number of CVEs that document known vulnerabilities that have been identified in the past. One way to escape containers is to exploit vulnerabilities in the Linux kernel. The Linux kernel enforces container isolation by employing namespaces and cgroups. However, if attackers gain kernel level privileges through privilege escalation, they can circumvent isolation as reported in CVEs (e.g. CVE20144699 and CVE20163134). There are CVEs that have reported vulnerabilities in container runtimes that allow container breakouts.

### 5.27.2 Security threats

When a malicious container escapes isolation, it can gain full control over the underlying host and cause any of the below serious threats:

- attacker would gain the ability to mount attacks on host OS or compromise host OS functionalities

- compromise the confidentiality & integrity of co-hosted containers and tenants

- introduce new vulnerabilities

Such threats can have a devastating effect in multi-tenant deployments. A malicious container breakout of one tenant can potentially comprise all co-hosted containers of other tenants

### 5.27.3 Potential security requirements

The virtualization platform shall provide capabilities to limit impact on co-hosted containers caused by a rogue container escaping its isolation. One of the commonly practiced security control is to enforce strict resource limits on container usage, which helps in preventing resource starvation due to an attack by a rogue container.

The virtualization platform shall enforce principle of least privilege (PLOP) that ensure that no containers run with a privilege higher than what is actually required.

## 5.28 Key Issue 27: Secrets in NF container images

### 5.28.1 Key issue detail

There are scenarios which benefit from including configuration and secrets, such as passwords or credentials in NF container images. For e.g. containers require to be able to connect to other containers within the deployment as well as with external entities. All these connections need to be authenticated and secured. One way of achieving this is to provide the requisite secrets or keys to the containers which allow them to authenticate and be authenticated and secure the communication channel. A common but in-secure means of providing secrets to the containers is by packaging the secrets or the keys with the image itself. There is the risk that the same can be extracted, read or manipulated before the container is deployed and the secret used.

### 5.28.2 Security threats

With a long supply chain, container images are vulnerable to outside scrutiny. With container images containing secrets or keys, this becomes a serious threat vector. Adversaries can extract them by obtaining a copy of the image and they can be potentially shared with third parties for illicit gain.

- Secrets embedded within a container image can be stolen.

- Secrets embedded within a container image can be modified

### 5.28.3 Potential security requirements

The embedded secrets such as passwords or credentials, or any other critical configuration data in VNF images shall be properly protected.

## 5.29 Key Issue 28: Management APIs

### 5.29.1 Key issue detail

Both legacy and virtualised networks make extensive use of management APIs to manage NFs. These management APIs allow access to privacy and security sensitive information. APIs exist at all layers of network including the 3GPP application layer (e.g those with SBA), MANO systems and underlying NFV infrastructure (e.g. server management APIs supported by the server hardware). Management APIs provide a range of security critical NF management capabilities including basic configuration of NFs, policy management, audit and license management.

Specific to this KI, MANO systems provide a set of APIs (e.g. those standardised by ETSI ISG NFV SOL) which allow standardised subscription to a range of information, metrics and points of control for NFs or MANO itself. Many of these APIs and access credentials can be shared across multiple NFs, and as MANO is not specifically aware of VNF purpose at the 3GPP layer, can span slice or other 3GPP security domain boundaries.

Furthermore, many APIs currently allow different security access control mechanisms to those specified by 3GPP. Therefore, any difference in API security strength between those specified by 3GPP and those supported by the underlying MANO / NFV infrastructure risk impacting 3GPP security minima. Until late 2020, common MANO API standards in industry use still mandated support for TLS 1.0 or allowed use of weaker username and password authentication mechanisms. Such mechanisms have been prohibited by 3GPP for a number of years. Approaches using self-signed certificates are also common.

Management APIs can have subscribers that are both internal and external to the 3GPP network. In the case of external APIs these provide standardised access to all NFs or MANO functions shared by all NFs, which do not pass through the 3GPP defined security interfaces (e.g. via SEPP) and do not fall into the scope of 3GPP Security Assurance Standards.

### 5.29.2 Security threats

Without appropriate security level minima (e.g TLS version, algorithm, token types), underlying management and licensing APIs introduce standardised mechanisms to access 3GPP NFs with lower levels of security than those accepted by 3GPP. This risk existed in legacy networks but there was no common published API available for an attacker to subscribe to.

Without appropriate linkage between security requirements for APIs all, at all system layers (3GPP, MANO, NFVI), a 3GPP system cannot achieve 3GPP specified security strength and attack resistance.

Some NFs or NF components are more sensitive than others (e.g. LI components, Cryptographic functions). Therefore, without appropriate API access restriction rules (both access to APIs and specific information or commands available for a given user), NFV level APIs may bridge or bypass 3GPP level NF security isolation requirements.

### 5.29.3 Potential security requirements

Solutions to this Key Issue should ensure minimum levels of API security and support for isolation requirements across all layers in a 3GPP virtualised network. Based on current 3GPP requirements in TS 33.501 such a minimum level should cover authentication, authorization, integrity protection, replay deterrence, confidentiality protection, TLS profile and certificate profiles.

The system should be able to support a single 3GPP defined security level, for all APIs (including 3GPP layer, NFV layer and NFVI layer) within a 3GPP network. Solutions to this requirement required both inside and outside 3GPP.

The system should be able to support 3GPP defined API access restrictions for specific NFs, NF components and network slices. Solutions to this requirement required both inside and outside 3GPP.

## 5.30 Key Issue 29: Image Snapshot and VNF Mobility

### 5.30.1 Key issue detail

Starting, checkpointing, restarting or migration of virtual workloads are fundamental operational tasks in a cloud environment.

Potential security risks are related to a migration of a virtual workload from a secure environment to a less secure environment or to attacking data while on rest (e.g., as part of a snapshot file) or while in transit (e.g., during live migration).

In general, these threats can be handled using appropriate mechanism, i.e., ensuring that source and target environment are secure, that snapshot files are protected, that the mechanism used during migration is secure, or that the underlying operational processes are secure.

This approach, however, assumes that the cloud environment is trustworthy, i.e., the operator, who deploys VNFs in a cloud environment trusts that the cloud operator has secure mechanisms and processes in place with respect to lifecycle management of virtual workloads.

If, however, a cloud environment is regarded as potentially malicious, things are different. In such a case typically remote attestation techniques can be used to verify that a VNF is running in a trustworthy execution environment. Such a setup makes migration of VNFs more complicated, since the attestation is valid only for the source environment and not for the target environment, i.e., some form of re-attestation needs to be executed for the target environment. Furthermore, data (including security credentials) used by the VNF in the source environment are protected ("sealed") so that they are readable and usable only in the source environment. Thus, the migration needs to include a mechanism, which allows unsealing (on the source environment) and sealing (on the target environment) of the data to be transferred (i.e., the persistent state) in a secure way without opening the possibility of running several copies of a VNF with different persistent state (so called forking or roll-back attacks).

### 5.30.2 Security threats

An attacker might initiate migration of a VNF from a trustworthy execution environment into a non-trustworthy environment. The non-trustworthy environment might be under the control of the attacker and might be used for direct attacks against a VNF.

An attacker might attack VNF data, while they are at rest as part of a VNF snapshot or in transition during live migration.

An attacker, who has control over the deployment of VNFs (i.e., the attacker can start, pause, restart, or migrate a VNF), could run several instances of the same VNF with different persistent state. While not trivial, this kind of fork or roll-back attacks can be used to initiate complex attacks against the overall integrity of the 5G system.

### 5.30.3 Potential security requirements

Migration of a VNF from a trustworthy environment to an untrustworthy environment shall not be possible, e.g., the access to virtualization management operations, like starting, stopping, pausing, restarting, live migration of a VNF, shall be subject to authentication and authorization. Solutions to this requirement required both inside and outside 3GPP.

VNF data shall be confidentiality protected when stored as part of a VNF snapshot or during migration of the VNF to another execution environment. Solutions to this requirement required both inside and outside 3GPP.

Where VNF sub-components are in different trust domains, the snapshot shall maintain security and isolation requirements for each trust domain within the snapshot of the VNF. Solutions to this requirement required outside 3GPP.

The ability of a VNF to verify the trustworthiness of another VNF (as described in KI#13) shall not be impeded by pausing, stopping, restarting, or migrating a VNF. Solutions to this requirement required both inside and outside 3GPP.

All VNF Snapshot and VNF mobility operations shall preserve the persistent state of the VNF in order to prevent forking or roll-back attacks. Solutions to this requirement required outside 3GPP.

It shall be possible to protect and prevent sensitive VNF or VNF-components from being subject to snapshot or migration without explicit authorization. Solutions to this requirement required both inside and outside 3GPP.

All system snapshots events shall be subject to secure logging. Solutions to this requirement required outside 3GPP.

Snapshots shall be securely deleted, once they are no longer required or after a specified maximum snapshot age has been reached. Solutions to this requirement required outside 3GPP.

## 5.31 Key Issue 30: Sensitive Function Pinning

### 5.29.1 Key issue detail

Editor’s Note: How does 3GPP describe and pin sensitive sub-functions to specific security hardware in VNFD and NSD. What types and language are required for this to be done in a multi-vendor interoperable environment?

Editor’s Note: How is this attested and linked to KI#13.

### 5.31.2 Security threats

### 5.31.3 Potential security requirements

# 6 Mitigations and Solutions

## 6.1 Introduction

Editor’s Note: This section will contain any potential Mitigations or Solutions that may be used to address or reduce the risk associated with Key Issues identified in section 5.

## 6.2 Solution 1: Trust domains and separation

### 6.2.1 Introduction

Virtualisation is a widely employed technique to provide separation between workloads, allowing the resources available to be used in the most efficient and secure manner. This separation requires the definition of trust domains but can be implemented and enforced in a variety of different ways. This can include software defined rules, separate physical infrastructure and appropriate choices of virtualisation infrastructure. Risk appetite and use case will determine which combination of these controls are appropriate.

### 6.2.2 Solution details

#### 6.2.2.1 Definition of trust domains

All workloads, functions and VNFs are allocated a trust domain, based upon their sensitivity. Functions identified as security critical do not share trust domains with workloads that are not security critical functions.

All physical hosts are categorised into security pools based upon risk. The risk is based upon the host type, the security features of the host, and the environment within which that host resides. Hosts can be pooled for resilience purposes to ensure that parallel workloads are in physically separate locations. Host pools are tagged with trust domains they can execute. This will be based on risk and ensure that sensitive functions are not executed alongside vulnerable functions, or in high-risk locations.

When determining whether a virtual workload is permitted to run on a host, the following aspects are considered:

* the trust domain of the workload being deployed,
* the host’s security pool,
* the existing workloads running on the host, and their trust domains.

Using these criteria, the system enforces rules, as appropriate, to ensure that critical and sensitive workloads and highly exposed workloads do not run on the same host pool. Further segregation is available, for example if the workload vendor is viewed as high risk.

Given that the orchestration tooling requires high levels of access and privilege it is be counted as a security critical network function and protected as such. If it were compromised, the entire NFVI would be at risk.

#### 6.2.2.2 Software separation of VNFs

Virtualisation provides a well understood, software defined, mechanism to separate network functions. Software defined traffic rules applied directly to each virtual function are used to limit both incoming and outgoing traffic in an efficient and scalable way.

#### 6.2.2.3 Separation of physical infrastructure

To reduce the risk due to compromise of a single host, virtualisation infrastructure is segregated, and workloads are deployed appropriately. Hosts are physically separated such that compromise of one physical host does not allow an attacker to impact an unmanageable amount of the virtualised network, and a physical host’s risk profile is used to determine which workloads can be deployed to it.

A physical host is not able to impact hosts in other host pools. For example, among other controls, spoofing VLAN/VXLANs of virtual networks is not allowed.

#### 6.2.2.4 Virtualisation platform

Where the virtualisation platform is used to enforce separation between trust domains (i.e. where discrete physical hardware is not used), type-1 hypervisors are used. Virtual workloads do not have direct access to the physical hardware.

Containers are not used to enforce separation between trust domains. Correspondingly, containerised hosts only support a single trust domain. This is because containers only provide process-level separation between workloads, meaning a single kernel-level vulnerability allows an attacker to impact the underlying host and all the containers running on it.

Editor’s Note: 3GPP details need to be further described.

### 6.2.3 Evaluation

This solution addresses Key Issues 1, 9, 11, 12 and 13.

## 6.3 Solution 2: Lock-down of infrastructure

### 6.3.1 Introduction

To prevent enabling unnecessary attack vectors and to make it easier to monitor whether a network is behaving appropriately, the virtualisation layer is locked down so that only the necessary communications are possible. In addition, service providers need to be able to maintain and patch the virtualisation layer and underlying hardware without impacting their core services to customers.

### 6.3.2 Solution details

Virtual workloads cannot directly access the physical hardware they are running on, and it is not possible to directly communicate between physical hosts other than data flows between virtual workloads. All interfaces on physical hosts are locked down to restrict access to trusted hosts, and there is no hard-coded configuration (e.g. virtual span ports or hard-coded MAC addresses) in the NFVI as these make it significantly harder to update and patch. Virtualisation hosts only open the minimum number of ports required and all ports and services are locked down and managed.

Only hosts that have cryptographically attested to be in a good known running state can be provisioned into the network. Hosts already in the network need to continue to be cryptographically attested to be in a good known running state.

The NFVI can be updated without impacting the network functionality. This will give confidence that patches against security issues will be done in a timely manner. The NFVI is kept up to date (including firmware), to minimise security issues. It is possible to automatically update the NFVI, to minimise the time that the fabric is at risk if an issue is found

NFVI security enforcing functions always encrypt data at rest, and in transit.

Editor’s Note: 3GPP details need to be further described.

### 6.3.3 Evaluation

This solution addresses Key Issues 2, 3, 4, 5, and 14.

## 6.4 Solution 3: Administration of the virtualisation fabric

### 6.4.1 Introduction

This solution addresses Key Issue #10, Single Administrator Domain.

Administration of a network takes place in the management plane. A compromise in this part of the network infrastructure could impact the whole network, making it the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and confidentiality of the operator’s services, including critical services.

Historic management of telecoms networks has relied heavily upon standard corporate devices doubling up as administrative workstations. Consequently, machines that perform standard ‘office’ type functionality such as email, and web access are also defining the operation of the network. This is often referred to as a browse up architecture, and brings significant risk. Where it is used, several commodity classes of attack can be performed with relative ease upon administrative users, and these can achieve a significant impact. Several attack vectors exist, the most notable being the possibilities afforded to an attacker via phishing of administrative users, targeted or otherwise, which can result in credential loss, remote code execution, and further exploitation of networks or users.

Attacks of this type tend not to be noisy, meaning that there is no overt impact on the network, and they may be maintained for years, growing in scale and complexity over time. These attacks are likely to have a significant impact on the operator and hence securing the management plane should be treated as a priority. Given the risks, it is not appropriate for operators to be using a browse up architecture. Instead, operators should architect, and operate, their management plane infrastructure to inhibit network compromise through administrative access. Operators should treat virtualisation administration as a management plane.

NOTE: A host compromise will compromise all workloads running on that host, and as such the administration of the underlying hardware is as critical as the administration of the virtualisation fabric.

### 6.4.2 Solution Details

Access to the management plane needs to be temporary and time-bounded. The operator needs to constrain the number of administrator accounts able to modify the Virtualisation Fabric, and the number of administrators, to a minimal manageable number to meet their needs. Administrators need to be prevented from being able to grant themselves privileged access to the network, and should not have access to the host’s hardware or the virtualised workloads running within the environment.

All administrative access needs to be logged, and the activity of the session recorded. Manual administration of the Virtualisation Fabric (e.g. access to a command line on host infrastructure) should raise a security incident. The devices and locations from which the fabric can be modified should be limited.

All new deployments of equipment need to be administered via authenticated and encrypted channels. Insecure or proprietary security protocols need to be disabled. Administrative access needs to be via secure, encrypted, and authenticated protocols whenever technically practical. Functions that support the administration and security of the Virtualisation Fabric should not be run on the fabric itself, and should be considered as Security Critical functions running on separate dedicated hardware.

### 6.4.3 Evaluation

Editor's Note: To be added.

## 6.5 Solution 4: Hardware Mediated Execution Enclave (HMEE)

### 6.5.1 Introduction

This solution aims to address KI 6, 7, 15, and 25 by proposing to standardize the use of Hardware Mediated Execution Enclave (HMEE) when deploying a Network Function Virtualisation Infrastructure (NFVI). From ETSI GS NFV-SEC 009 [3] *A hardware-mediated execution enclave is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. This enclave is protected from eavesdropping, replay and alteration attacks as the programs within the enclave are executed.*

Utilizing an HMEE within the NFVI may solve the issue of Virtual Network Function (VNF) isolation, memory introspection, and confidentiality of data-in-use in both virtualized and containerized environments. HMEE solutions offer protection from co-located VNFs running on the same physical host as well as protection from the host itself. General purpose HMEE can be equipped with Commercial Off The Shelf (COTS) hardware that may be used to host the NFVI.

Use of an HMEE in the NFVI provides the means to support at least the following security controls:

* Security of data-in-use. When code is executed on a shared physical host it is at risk of being modified or inspected by co-located VNFs or the host itself. With HMEE, code is executed in a secure environment, protecting the code and data from co-located VNFs and the host.
* Data integrity. HMEE is resistant to unauthorized modifications of information inside HMEE.

To scale across 5G NFV this solution proposes to utilize the trust domains from solutions to key issue #1. For example, trust domains that have security critical functions are only be deployed on hosts that have HMEEs enabled. Meanwhile, less sensitive functions belong to a lower trust domain and do not need to be deployed on HMEE enabled hosts.

### 6.5.2 Solution details

This solution proposes to equip the NFVI with one or more HMEEs, where an HMEE can be deployed for a single VNF or a group of VNFs. If the HMEE is shared, it needs to provide isolation from collocated VNFs.

The HMEE is to be used for executing sensitive functions within the VNF, such as information elements marked as private (e.g., the SIDF de-concealing the SUPI from the SUCI). Other operations should use the existing security measures for NFV deployment.

When deploying an HMEE on a NFV environment, the following are required:

* The NFVI needs to be deployed using hardware resources that have an HMEE enabled.
* The NFVI is designated an appropriate trust domain for VNF deployment based on its HMEE capability. HMEE enabled hosts provide security guarantees that reduce security risks and therefore belongs to higher trust domains.

NOTE 1: Establishment of trust domains is based on solutions for key issue #1

* Data-in-use are inaccessible by either other VNFs or the virtualisation layer (container engine or hypervisor) with HMEE. VNF sensitive data and functions need to be executed using the HMEE.

### 6.5.3 Evaluation

HMEEs provide enhanced security assurance in the NFVI and can serve as a root of trust. HMEE capability should be supported within NFVI which is out of 3GPP scope.

This solution addresses key issues 6, 7, 15, and 25.

## 6.6 Solution 5: Solution Using Boot Time Attestation for NF Registration

### 6.6.1 General

This solution addresses Key Issue 13: Attestation at 3GPP Function Level. ETSI NFV reports, such as ETSI GR NFV-SEC 007 [14] and ETSI GR NFV-SEC 018 [15], provide guidance on attestation technologies, practices, and architectures. However, no standardized attestation framework is specified for virtualized 3GPP NFs. To attest a virtualized 3GPP NF through a full chain of trust from the VNF layer down to the hardware layer, attestation infrastructure and procedures are needed both within the 3GPP functional domain and outside its domain. This solution seeks to 1) identify dependencies on underlying elements outside the 3GPP functional domain and 2) introduce new functionality to coordinate access to attestation services at the 3GPP functional level.

### 6.6.2 Introduction

#### 6.6.2.1 Reference Architecture for Attestation

Attestation is a process to determine the trustworthiness of a platform. Attestation provides cryptographic evidence of the integrity of hardware, firmware, software, and other critical security functions to show that a system has not been breached and is in a valid state.

Implementation of an attestation architecture and protocols are not in scope of this solution. A conceptual attestation architecture is depicted in Figure 6.6.2.1-1 to make clear the attestation terminology used in this solution.

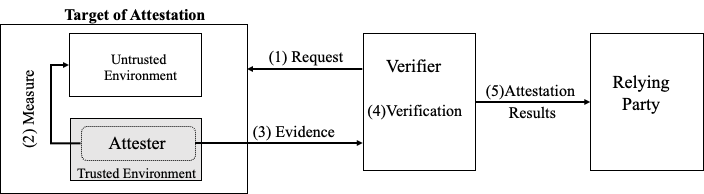


Figure 6.6.2.1-1: Reference Architecture for Attestation

An attestation architecture typically involves three roles:

* Attester: performs integrity measurements on the target system which is to be attested and generates a set of claims called Evidence.
* Verifier: verifies the Evidence on the basis of reference values or other complex logic and generates an Attestation Result that declares the target system as trustworthy or not.
* Relying Party: depends on the Attestation Results to apply specific actions.

A typical attestation cycle consists of the following steps illustrated in Figure 6.6.2.1-1:

1. Verifier sends an attestation request to the target system.
2. Upon receiving the attestation request, the Attester measures the target’s untrusted environment and collects the integrity measurements into evidence.
3. Attester sends the evidence to the Verifier.
4. Upon receiving the evidence, the Verifier validates the received measurements against reference values or applies implementation-specific logic. The validation results assert whether the system under evaluation is in trustworthy state or not.
5. Verifier sends validation results to a Relying Party. The Relying Party uses the attestation results to decide the extent to which it will interact with the attested system.

Local attestation occurs when the Attester and Verifier run on the same physical machine. When the Verifier is remote, this is referred to as remote attestation.

Attestation procedures should adhere to the following in order to trust the process:

* An Attester should run in a trusted environment with complete access to the system so that it can take accurate and comprehensive measurements even when measuring a corrupted component.
* An Attester should run on component boot up.
* Measurements should be sent from the Attester to the Verifier in a manner that ensures freshness, confidentiality, integrity, and authenticity.
* Measurements on a component should be stored in a secure manner to prevent unauthorized modification prior to being sent to the Verifier.
* A Verifier should run in a trusted environment.
* Attestation results should be sent from the Verifier to the Relying Party in a manner that ensures freshness, confidentiality, integrity, and authenticity.

#### 6.6.2.2 Attestation in NFV Environments

In a NFV environment, a virtualised 3GPP NF executes inside a virtual instance (e.g., virtual machine or OS container) created by virtualisation software (e.g., hypervisor or container engine). The virtualisation software mediates access to virtual resources that it abstracts from the physical resources in the hardware platform. The hardware platform includes other building blocks (e.g., BIOS, operating systems, etc.) for operation. Therefore, the scope of attestation of a VNF comprises all the aforementioned systems and components involved.

Attestation in an NFV environment is established with a chain of trust (CoT). That is, the trustworthiness of the VNF is guaranteed by the trustworthiness of the virtual instance, the trustworthiness of the virtual instance is guaranteed by the trustworthiness of the virtualisation software, and so on back to the trustworthiness of the hardware. A component participating in a CoT cannot influence its own measurement procedure, as its execution begins only after it has been measured and verified [14]. The CoT starts with an implicitly trusted attester, called a Root of Trust (RoT), and extends up to the last software component.

In the NFV architecture, components participating in the CoT are under the control of different domains. The VNF and virtual instance it runs within are in the 3GPP functional domain. Whereas the virtualisation software and the hardware platform are in the NFVI domain.

To illustrate the interdependency of attestation across domains, Figure 6.6.2.2-1 shows a conceptual flow of measurements needed to form a CoT from the hardware layer to the VNF. The steps include:

1. RoT measures hardware (including supporting components: firmware/BIOS, OS, etc.)
2. Hardware measures virtualisation layer (e.g., hypervisor or container engine)
3. Virtualisation layer (e.g., hypervisor or container engine) measures the virtual instance (e.g., VM or container)
4. Virtualized RoT (vRoT) measures the VNF. The vRoT is a virtual instance associated to the hardware protected RoT. The virtualisation layer software provides this virtual resource to the virtual instance.



Figure 6.6.2.2-1: Conceptual flow of measurements that form a CoT from the hardware layer to the VNF

A VNF’s trusted state relies on the state of trust of the underlying elements. More precisely, measurement of the VNF relies on a mechanism in the NFVI domain (in this example the vRoT). The cross-over in domain affects the scope of attestation for VNFs. The target of attestation, i.e., the VNF, is in the 3GPP functional domain and the mechanism for generating evidence on the target, e.g., the vRoT, is in the NFVI domain. Furthermore, trust in any measurements logged by the virtual resource (e.g., vRoT) is predicated on trust in the virtualisation layer software (e.g., hypervisor or container engine) that instantiates the resources to be used by the virtual instance (e.g., VM or OS container).

Additionally, relying parties in the 3GPP functional domain that make decisions based on attestation results may need to influence what is measured during the attestation process according to the level of assurance required by the relying party. Different 3GPP VNFs (i.e., relying parties) may have different criteria for trustworthiness. These aspects on configuration are within scope of 3GPP.

### 6.6.3 Solution Details

#### 6.6.3.1 General

This solution focuses on boot-time attestation, where a chain of trust is established during the boot process of the NFVI. The chain is extended to include attestation of the VNF when it is first instantiated on top of the NFVI. Run-time attestation methods for NFVI and VNFs are not considered in this solution.

Defining attestation for NFV environments is out of scope of 3GPP. However, attestation of NFVI and attestation of VNFs are discussed in this solution to layout the foundational building blocks and propose a set of requirements from the perspective of 3GPP functional domain. It is also necessary to examine NFVI and VNF attestation to understand how attestation results can be used within 3GPP functional domain and how the 3GPP functional domain can influence configuration of attestation in the NFV domain.

A new function called the Profile and Attestation Check Function (PACF) is proposed to enable access to the attestation results from the 3GPP functional level and distribute attestation policy to control how attestation is applied. The PACF may be standalone or co-located with OSS/BSS, NRF, or other network security functions.

This solution proposes using proof of attestation results to decide whether to register a VNF. A modified NF Registration procedure is proposed that uses the PACF to obtain access to the attestation results.

This solution is complementary to attestation services performed by the management layer.

#### 6.6.3.2 Attestation of the NFVI

Figure 4.2-1 shows the ETSI NFV high-level architecture. The NFVI is a collection of NFVI-Nodes. Each NFVI-Node is a physical device deployed and managed as a single entity, providing the NFVI functions required to support the execution environment for VNFs. Each node goes through the attestation process to produce a chain of trust starting from the server/hardware layer. Only after successful attestation of each layer, the NFVI-node joins the NFV infrastructure.

Each NFVI-node includes at minimum the following components:

1. Server / Hardware Resource – bare metal equipment that the entire NFV stack runs upon. It provides physical storage, compute, and network I/O to the OS and virtualization software. Virtual resources are instantiated on these physical resources for VNFs.
2. Operating System (OS) – full featured or customized OS that runs the software necessary for a NFV.
3. Virtualization Layer– software (e.g., hypervisor or container engine) that creates a virtual instance (e.g., Virtual Machine or OS container) to run VNFs

Any attestation solutions for NFVI should provide the following chain of attestation:

1. Attestation of the Server / Hardware Resource: a RoT measures and verifies the server platform consisting of firmware and hardware. After successful attestation of the server, it will act as the attester for the layer above. The attestation results and corresponding measurements are maintained by a verifier for subsequent access.
2. Attestation of the OS: the server measures and verifies the OS. After successful attestation of the OS, it will act as attester for the layer above. The attestation results and corresponding measurements are maintained by a verifier for subsequent access.
3. Attestation of the Virtualisation Layer software: the OS measures and verifies the virtualisation software. The virtualisation software may be a hypervisor or a container engine. If the virtualisation software is pre-loaded into the OS, then its attestation is included with the attestation of the OS. The attestation results and corresponding measurements are maintained by a verifier for subsequent access.

If any step in the attestation process fails, the CoT cannot be expanded further and a recovery procedure should be activated to handle the failure.

#### 6.6.3.3 Attestation of VNFs

As a precondition to attestation of VNFs, it is assumed the NFVI-node has been successfully attested and can be trusted to attest VNFs running on its platform. More precisely, the virtualization layer software has been successfully attested and can act as the attester for VNFs.

Also note that a VNF runs inside a virtual instance, either VM-based or based on an OS-container. Thus, any attestation solutions for VNFs should consider both use cases.

Any attestation solution for VNFs should provide a process that includes the following steps.

The process is initiated by the NFV MANO requesting to instantiate a new VNF.

1. The NFVI retrieves the virtual instance from network storage that is within the NFVI.
2. If the VNF software is not preloaded on the virtual instance, the VNF software specific to the type of VNF being instantiated is retrieved from network storage.
3. The NFVI attests the virtual instance and VNF:
   1. The virtualisation layer software (e.g., hypervisor or container engine) measures the virtual instance and VNF software and reports the evidence to a Verifier.
   2. The Verifier validates the measurements. The attestation results and corresponding measurements are maintained by the verifier for subsequent access.
4. NFV MANO provides the VNF with a signed NF profile [13], clause 4.17.1. (TS 23.502, clause 4.17.1, NOTE 2 states the NF profile is configured by OAM system).

Editor’s Note: References to the NFV management and orchestration as “NFV MANO” vs. “OAM” should be aligned with the terminology in TS 23.502 clause 4.17.1.

1. The NFVI begins to run the VNF.

If any step in the attestation process fails, the CoT cannot be expanded further and a recovery procedure should be activated to handle the failure.

#### 6.6.3.4 Proposed Requirements for Attestation in NFV Environments

Currently, no specification exists that defines support for attestation in NFV environments. The following requirements are proposed for consideration for future development of NFV specifications to assist the 3GPP functional domain in VNF attestation:

1. The NFV architecture shall provide support for attestation.
2. Support for attestation shall include NFVI subsystems and components described in 6.6.3.2.
3. Support for attestation of VNFs shall include VM-based and container-based use cases as described in 6.6.3.3.
4. The NFV architecture shall provide external access to the attestation measurements and attestation results.
5. Verification of attestation evidence from NFVI shall be performed by a verifier external to NFVI to support remote attestation
6. The external verifier should be within the NFV MANO domain
7. Support for a mechanism to establish trust between the 3GPP functional domain and the external verifier shall be provided.
8. The NFV architecture shall provide an interface and protocol to allow the 3GPP functional domain to send attestation policies to the NFV architecture to support configuration of attestation parameters.

#### 6.6.3.5 Profile and Attestation Check Function (PACF)

Since the attestation procedures to verify the trustworthiness of VNFs and NFVI exist outside the domain of the 3GPP functional level, access to the attestation results is needed from within the 3GPP functional level. This access allows attestation to be integrated with select procedures in the control plane, such as NF registration and slicing operations. For instance, enterprise slices for some verticals may require the ability to query for proof of successful attestation to support their use cases. Applicability to NF registration is discussed in 6.6.3.6.

Additionally, default application of the same level of attestation to every virtualized NF in a 3GPP network may not be necessary. In which case, the 3GPP functional level can provide an attestation policy to the infrastructure responsible for attestation. The attestation policy describes the conditions for applying attestation and the type of measurements required to meet a specified level of assurance per VNF.

This solution proposes the PACF to coordinate access to attestation results from the 3GPP functional level and administer policy to help control how and when attestation is applied. Figure 6.6.3.5-1 presents a reference architecture integrating PACF into the NFV architecture. This architecture assumes the NFVI has been successfully attested and the virtualization layer software can act as the attester for VNFs.

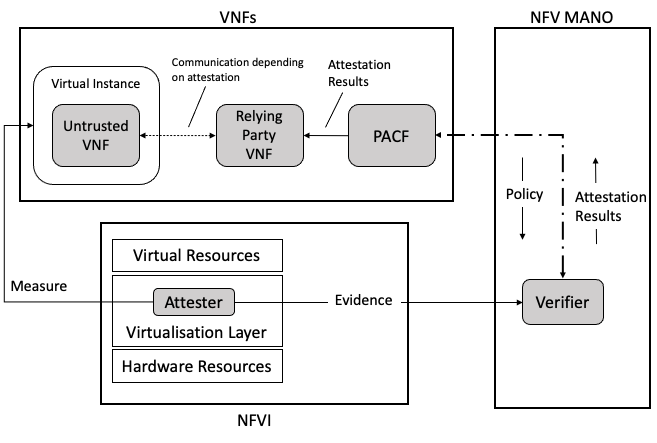


Figure 6.6.3.5-1 Reference architecture with PACF integrated with NFV architecture

The PACF serves as a bridge between the 3GPP functional level and the attestation infrastructure outside its domain. The PACF requires a secure communication path to the Verifier. Policy information is sent from PACF to the Verifier. Attestation results are sent from the Verifier to the PACF. A trust relationship must be pre-established between the PACF and the Verifier. Other network functions acting as Relying Parties must also trust the Verifier. This solution assumes the Verifier is located within the NFV MANO domain.

Editor’s Note: Communication between the PACF and NFV MANO is FFS.

#### 6.6.3.6 NF Service Registration Procedure with Remote Attestation

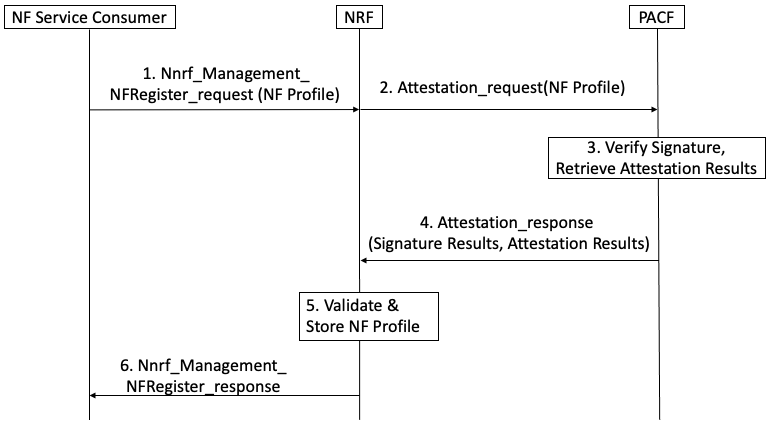
This solution proposes to provide proof to the 3GPP functional domain that a new VNF has been successfully attested before registration occurs in the 5G Core.

Editor’s Note: The process for verifying attestation results of the NRF and PACF is FFS.

Once successfully instantiated, a new VNF will register with the NRF. The original NF Service Registration procedure is detailed in [13], clause 4.17.1. The modified NF Service Registration procedure shown in Figure 6.6.3.6-1 includes attestation by adding steps 2, 3, and 4. Steps 1, 5, and 6 are steps from the original procedure.

The modified NF Service Registration procedure retrieves attestation results based on the NF Instance ID in the NF profile. This solution proposes the use of digital signatures to enable integrity protection and verification of the NF profile sent in the registration request by the VNF. The NF profile should be signed by the OAM, NFV MANO, or an authorized delegate when the VNF instance is provisioned and instantiated on the NFVI. The NF profile should only be signed after the integrity of the VNF instance has been verified. Signing the NF profile prevents the registering VNF from altering the NF profile by forging the NF Instance ID of a successfully attested VNF.

NOTE: A signed NF profile is within alignment of TS 23.502 [13] clause 4.17.1. TS 23.502 clause 4.17.1, NOTE 2 states: the NF profile is configured by OAM system and NOTE 3 states: that whether the NF profile sent by NF service consumer to NRF needs to be integrity protected by the NF service consumer and verified by the NRF is to be decided by SA3.



**Figure 6.6.3.6-1: NF Service Registration Procedure with PACF**

When an NF requires attestation results to register, the following steps are proposed for the registration procedure:

Step 1: NF service consumer, i.e. an NF instance, sends Nnrf\_NFManagement\_NFRegister Request message to NRF to inform the NRF of its NF profile when the NF service consumer becomes operative for the first time.

Step 2: The NRF initiates a request for attestation results and sends the signed NF profile to the PACF.

Step 3: The PACF verifies the signature on the NF profile and retrieves attestation results from the Verifier using the NF Instance ID from the NF profile.

If signature verification fails, the NF service consumer cannot be trusted and an exception handling procedure should be activated to handle an untrusted NF.

Step 4: The PACF responds to the NRF with attestation results it received from the Verifier.

Step 5: If the attestation results affirm successful attestation, the NF service consumer can be trusted. The NRF stores the NF profile of NF service consumer and marks the NF service consumer available.

Otherwise, if the attestation results affirm an unsuccessful attestation, the NF consumer cannot be trusted and a recovery procedure should be activated to handle an untrusted NF.

Step 6: The NRF acknowledge NF Registration is accepted via Nnrf\_NFManagement\_NFRegister response.

There can also be interactions between NFs with MnF (as defined in TS 28.533) for NF management service.

Besides the above procedures defined in 3GPP, the NFs can also interact with domains defined in other SDOs, e.g., MANO defined in ETSI.

The main idea is requiring the Verifier to expose the attestation results of different layers to the network entities (NRF, NFp, PS, MnF, MANO, OAM, etc.) which will interact with the attested NF, then, on receiving the interaction from the NF, these network entities can invoke the attestation /results and take further actions.

NOTE: The Verifier itself can also be distributed in different layers. The network entities can communicate with the Verifier directly or via a unified proxy

### 6.6.4 Evaluation

Editor’s Note: In cases where the NF does not need to register to NRF, the NRF cannot perform verification of the attestation results as proposed in the solution. Evaluation of this case is FFS.

The solution has the following 3GPP impact:

PACF: Introduction of a new 3GPP network function to enable interworking between 3GPP NF and NFV MANO domains, and also to perform the integrity check of the NF profiles.

NRF: Addition of the necessary functionalities to enable the NRF to relay the necessary information and to enforce the policies related to the attestation results.

The solution depends on attestation infrastructure outside the scope of 3GPP. The solution proposes a set of requirements for attestation in the NFV environment to assist the 3GPP functional domain in VNF attestation.

## 6.7 Solution 6: Solution Using Attestation for Key Issue 13

### 6.7.1 General

This solution addresses Key Issue 13: Attestation at 3GPP Function Level.

The solution proposes to bind the provisioning of 3GPP identities and corresponding cryptographic material to 3GPP NFs to the process of remote attestation.

### 6.7.2 Introduction

3GPP has defined an own security framework on NF level, which is based on the Service Based Architecture.

A central element of the security is transport layer security based on X.509 certificates.

If a NF acting as a service consumer requests a service from another NF acting as a service producer, the consumer and producer shall mutually authenticate by means of verifying the consumer’s client certificate and producer's server certificate. Vice versa, the producer authorizes the consumer by means of verifying an OAuth 2.0 token included in the service request.

The consumer requests and receives the OAuth 2.0 token from the NRF. During the token request the NRF authenticates the NF requesting the token. The authentication is based on a X.509 certificates and a corresponding private key, which together are acting as the consumer's OAuth Client Id and Client Secret.

There can also be interactions between NFs with MnF (as defined in TS 28.533[16]) for NF management service.

Besides the above procedures defined in 3GPP, the NFs can also interact with domains defined in other SDOs, e.g., MANO defined in ETSI.

Therefore, there can be multiple approaches, how the concept of remote attestation could be linked to the existing security concept, for instance:

1. Remote Attestation is executed during each interaction between consumer and NRF and between consumer and producer.

2. Remote Attestation is executed during enrolment of client and server certificates to the NFs. Afterwards trust is based on these certificates and their corresponding private keys.

The main idea is requiring the Remote Attestation server to exposure the RA report/result of different layers to the network entities (NRF, NFp, PS, MnF, MANO, OAM, etc.) which will interact with the attested NF, then, on receiving the interaction from the NF, these network entities can invoke the RA report/result and take further actions.

NOTE: The RA server itself can also be distributed in different layers. The network entities can communicate with the RA server directly or via a unified proxy.

The proposed solution takes the PS as an example.

This approach assumes that the NF can protect the private key linked to the certificate from any attack. That is the cryptographic material needs to reside within a trusted execution environment and must not be visible outside of the trusted execution environment at any time, not even during provisioning.

It is up to implementation and specific security requirements, if the NF is using a trusted execution environment based on enclave technologies for handing of the private key and certificate, or if the entire NF is executed in a trusted execution environment.

### 6.7.3 Solution Details

The following description provides a high-level overview about a possible solution focussing on the concept and requirements. The individual steps are only indicative. A detailed specification is FFS or up to normative work.



**Figure 6.7.3-1: Combining provision of 3GPP identities and certificates to the process of remote attestation. In terms of an attestation architecture [20] the Network Function NF is acting as Attester, the Provisioning Server PS as the Relying Party, and the Attestation Server AS as the Verifier.**

1. NF is requesting secure channel from the provisioning server.

Depending on the exact specification of the protocol in this step the NF might also verify the identity of the provisioning server. For instance, if TLS is used as a secure channel, the NF could verify the server certificate of the provisioning server using a preconfigured root certificate.

2. The provisioning server is replying with a request for evidence. The request includes a nonce, which will be used to ensure the freshness of the evidence provided in the subsequent steps.

3- The NF collects claims and prepares the signed evidence, which includes the Nonce

The claims included in the evidence are for further study and might be out of scope of 3GPP. Claims in the evidence might include claims related to the NF Software and to the NF configuration, but also claims related to the Hardware and the Cloud Software stack. If NF is deployed in the form of several components, the evidence might also include claims from the individual components.

Furthermore, the evidence needs to include a claim, which binds the secure channel to the attestation process. For instance, an ephemeral public key, whose corresponding private key is only known to the NF and protected by the NF by means of a trusted execution environment, could be included in the evidence.

4. The NF sends the evidence to the provisioning server

5. The provisioning server requests verification of the evidence from the attestation server.

6. The attestation server appraises the provided evidence using endorsements and refence values. The way, how this appraisal is executed and how the attestation server receives endorsements and reference values might be out of scope of 3GPP.

Note: In case of a negative outcome of the appraisal the attestation server might inform the management system about this incident. The management might take immediate action on this incident including identifying, isolating, and shutting down of the potentially malicious NF. Furthermore, the incident might cause a root cause analysis with the target of closing the security gap, which was causing the incident.

7. The attestation server returns the result of the appraisal to the provisioning server

8. Based on the attestation results and other policies the provisioning server decides whether the NF is eligible for provisioning or not.

9. The establishment of the secure channel is completed.

Note: The establishment of the secure channel includes usage of the claim related to the channel, which was included in the evidence provided in step 3 from the NF to the provisioning server.

10. NF and provisioning server use the secure channel to enrol necessary identities and certificates to the NF.

NOTE: The PS may need not forward messages between NF and AS but only invoke the final result directly to AS. The above procedure is just an example which may needs to be tweaked in the normative work.

### 6.7.4 Evaluation

TBD

## 6.8 Solution #7: Ticket-based access control for NFV

### 6.8.1 Introduction

This solution aims to provide one approach to address KI 10: Single Administrator Domain, and KI 22: MANO Single Point of Failures.

Administrators (“admins”) have many responsibilities in the NFV such as starting/stopping VNF instances, ensuring resources are provided to the VNF, and orchestrating the NFV infrastructure. These responsibilities should only be given to privileged admins. If the admin account is compromised or the admin is malicious then the account can be used to conduct attacks on the NFV (e.g., data exfiltration/espionage, selling user data, unauthorized configuration or package modification, service disruption). To reduce the risk of a malicious admin or MANO single point of failure the principles highlighted in Annex A. and Solution #3 must be followed.

To that end, this solution proposes using a ticket-based authentication system and Attribute Based Access Control (ABAC) on the NFV management plane. Within ETSI GS NFV-SEC 003 [17] it suggests *a token-based authentication mechanism such as Kerberos may be used between the Tenant Domain and Infrastructure Domain*. Similarly, this solution uses an Authentication Server (AS) to authenticate the admin. Next, a Ticket Granting Server (TGS) issues a ticket to authenticated admins which is used to connect securely to an NFV component. Tickets issued should be restricted by both time and number of usages. All other connection requests to the NFV environment shall be denied.

Another token-based authorization framework that can be used is OAuth 2.0, specified in IETF RFC 6749 [19]. Herein we only give details for the Kerberos option.

Once, the admin is authenticated and has established a secure connection with the NFV environment, they must also be authorized to perform tasks. ABAC may be used to provide fine grain access control to resources within the NFVI or the VNFs. ABAC uses policies that are based on subject attributes (e.g., user, admin, senior admin), object attributes (e.g., VNF, NFVI), and environmental conditions (e.g., time, location, authentication strength). Such attribute based policies help protect the NFV environment from unusual/ suspicious behaviour, even when the source is authenticated. Together, ticket-based authentication and ABAC provide secure access to the NFV resources, and fine grain access control.

### 6.8.2 Solution details

To implement necessary access controls, this solution proposes using a ticket-based authentication mechanism and ABAC. Kerberos, described in IETF RFC 4120 [18], is a network authentication protocol that uses tickets to authenticate a client’s connection to a server. It uses shared secret key cryptography to provide a secure connection between the client, Key Distribution Center (KDC), and server.

In this solution, a ticket-based authentication protocol, like Kerberos, is used to authenticate admins attempting to gain access to the NFV resources (VNF or the NFVI). In this case the client is an admin requesting access to the NFV environment. Additionally, ABAC is used on the resource side to authorize the admin. The ABAC server is per domain (VNF or NFVI) and implemented in such a way as to not be a single point of failure (e.g., distributed or redundant). The procedure for admin authentication and authorization to perform Management and Orchestration (MANO) functions is depicted in figure 6.8.2.1.

We note that the VNFs themselves and the infrastructure they run on (NFVI) can and should be two different administrative domains. The KDC can be per domain or can serve several domains. A policy server can be a part of the KDC and handles access control for each domain.

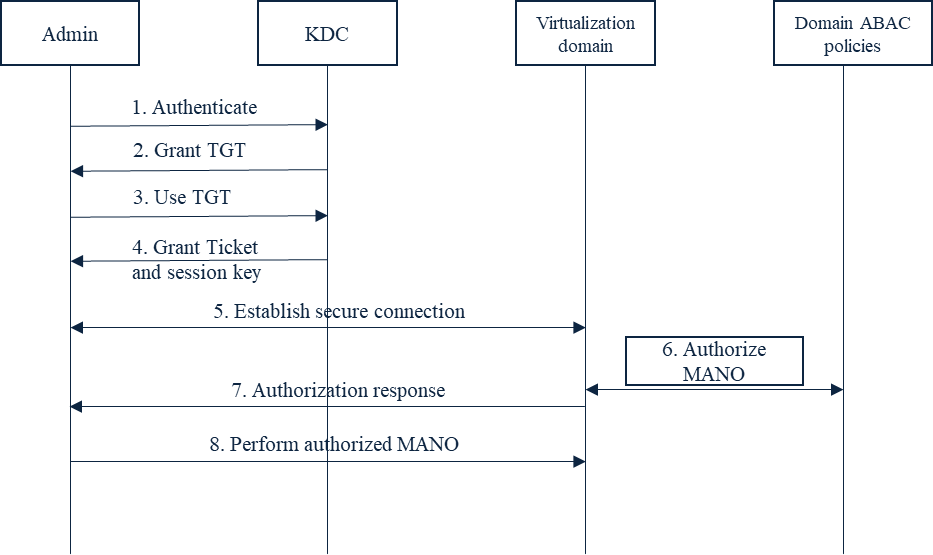


Figure 6.8.2.1: Procedure for admin authentication and authorization to perform Management and Orchestration (MANO) functions, applicable for each of the domains: NFVI and VNF.

Step 1: The admin (i.e., client) sends an authentication request to the Authentication Server (AS) that is part of the Key Distribution Center (KDC). The Kerberos configuration (e.g., KDC deployment, principals, realms) is implementation specific and out of 3GPP scope. The KDC does not need to be collocated with the resource, in this case the resource is the VNF or the NFVI depending on the administrative task and role. The interface between the admin and the KDC is out of 3GPP scope.

NOTE: The Kerberos protocol has built-in security measures for protection of messages on the interface between a client and the KDC such as timestamps, cache, and symmetric key cryptography.

Step 2: Upon successful authentication the KDC issues a Ticket Granting Ticket (TGT) to the admin.

Step 3: The admin sends the TGT to the Ticket Granting Service (TGS) that is part of the KDC to request access to the resource (NFVI/VNF).

Step 4: If access is approved, the KDC sends the admin a session key and ticket to access the resource (NFVI/VNF). If the KDC limits the number of access attempts, then the remaining access attempts should be decreased by one every time a ticket is issued.

Step 5: Once authenticated and authorized by the KDC, the admin can send the ticket with the session key to the resource (NFVI/VNF). Admin can use the session key to communicate securely with the resource (NFVI/VNF) for the duration of time on the ticket. The reference point between the admin and the NFVI or the VNF, Nf-Vi and Ve-Vnfm reference points respectively, are defined in ETSI NFV 002 [2]. Security for the Nf-Vi and Ve-Vnfm reference points is in ETSI GS NFV-SEC 003 [17].

Step 6: The resource (NFVI/VNF) sends an authorization request to the ABAC server on behalf of the admin. The ABAC server may be co-located with the resource (NFVI/VNF), but access must only be granted to authorized admins with the highest privileges. The ABAC server grants authorization using attribute based rules (e.g., admin A is allowed access to resource B from IP address: 1.2.3.4 from 9:00-10:00 UTC).

Step 7: The resource (NFVI/VNF) sends an authorization response. If the admin is unauthorized to perform the requested MANO functions, then the resource drops the connection.

Step 8: The admin performs the authorized MANO functions.

Step 9: Once the allotted time on the Ticket is reached, the resource (NFVI/VNF) drops the connection with the admin.

### 6.8.3 Evaluation

This solution is used as a reference model for secure NFV administration and addresses the key issues relating to protection from MANO single point of failures (KI #22) and malicious global admins (KI #10).

Aspects of this solution defined outside of 3GPP include implementation of ticket based access control (e.g., Kerberos, OAuth 2.0), ABAC setup, and the Nf-Vi and Ve-Vnfm reference points.

## 6.9 Solution 8: Slice isolation in both service and resource layer

### 6.9.1 General

This solution addresses Key Issue 9: Trust domain and Slice Isolation.

Generally, there are several levels of isolation in network slice. The lowest level is isolating different VNFCIs in one VNFI. For example, a particular service in one NF may be more critical than others and hence needs to be protected in a dedicated host. Another level of isolation is about VNFs within a specific network slice. For example, a NF in a network slice needs to be isolated from other NFs in the same slice. The above two level of isolation are supported by the corresponding affinity and anti-affinity attributes contained in VNFD and NSD as defined in [21]. In addition, it is proposed that 3GPP define the isolation principles and guidelines so that network managers can define the corresponding VNFD and NSD [21].

Besides the above two levels, the isolation between network slices should also be considered, e.g., two network slices should be deployed in separate host groups or DCs. The solution proposes to define umbrella isolation groups to cover such case while reusing the current affinity and anti-affinity attributes.

### 6.9.3 Solution Details

It’s proposed to first define a set of isolation principles for network design. The general 3 levels of isolation principles are listed as follows:

1. Isolation between slices: Network slices for critical sectors (e.g., energy sector, emergency services sector, critical manufacturing sector, etc.) should be isolated from general commercial network slices. This implies that all NFs in critical should be isolated from NFs in other ordinary slice or a particular set of NFs in critical slice should be isolated from other NFs.

As explained above, this type of isolation needs enhancement work in ETSI NFV ISG. The related slices need to be considered as a whole service, and then several umbrella isolation groups will be defined. Afterwards, the affinity and anti-affinity attributes should be allocated to each group. For instance, if NF\_A in slice\_A is to be isolated from NF\_B in slice\_B, then, NF\_A and NF\_B can be allocated with the same group ID. Such a group is to be assigned with a specific anti-affinity attribute. The MANO can by this means allocate isolated resources for these two NFs in two slices.

2. Isolation between network functions in the same slice: In a particular network slice, several NFs are more sensitive than others, e.g., UDM/AUSF/ARPF, etc. It may be needed to isolate these NFs from others even in the same network slice.

3. Isolation between network services in the same NF: It’s general recommended to isolate sensitive services (e.g., LI service) in a NF from other services.

Both scenarios mentioned in 2 and 3 are already supported by the existing affinity and anti-affinity attributes contained in VNFD and NSD.

NOTE: The above general principles are just examples to show some guidance that network operators can adjust in reality.

Based on the above schemes, MANO can allocate isolated resources based on the isolated attributes in NSD.

### 6.9.4 Evaluation

This solution addresses Key Issues 9. However, ETSI NFV ISG is expected to involved and enhance the MANO functionality in order to support the new parameters in NSD, i.e. the umbrella group identifier and group isolation attributes.

# 7 Conclusions

# 8 Recommendations

Annex A:  
Principles for administration of virtualisation infrastructure

Secure administration of the NFVI is critical for the security of a virtualised core network. The following principles describe a selection of basic principles for such secure management.

a) Best practice for network administration is applied to administration of the NFVI.

b) Administration of the NFVI is only available over mutually authenticated, encrypted and integrity protected channels.

c) The number of privileged accounts for the NFVI is constrained to a minimal manageable number to meet the CSP’s needs.

d) Virtualisation administrators do not have any privileged rights to other services within the CSP.

e) Virtualisation administrators are only provided with the privileges and accesses required to carry out their role.

f) Virtualisation administrators do not have access to workloads running within the virtualised environment.

g) Virtualisation administration access is limited to best practice configuration methods (e.g. authorised API calls).

h) Virtualisation administration is automated wherever possible.

i) Manual administration of the NFVI is by exception and raises a security alert.

j) Functions that manage the administration and security of the NFVI (e.g. MANO) are physically separate and do not run on the same NFVI as the NFs they manage.

k) Functions that support the administration and security of the NFVI are treated as security critical functions.

Annex B: KI Mitigations Summary

Editor’s Note: Table of summary of KIs and Mitigations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key Issue | 3GPP Mitigation or Solution Identified  Yes (Clause number) / No | In Scope of 3GPP  Yes/ No / Part | Out of Scope of 3GPP  Yes/ No / Part | New solution required outside of 3GPP?  Yes/ No / Unknown / Not Applicable |
| KI#1 |  |  |  |  |
| KI#2 |  |  |  |  |
| KI#3 |  |  |  |  |
| KI#4 |  |  |  |  |
| KI#5 |  |  |  |  |
| KI#6 |  |  |  |  |
| KI#7 |  |  |  |  |
| KI#8 |  |  |  |  |
| KI#9 |  |  |  |  |
| KI#10 |  |  |  |  |
| KI#11 |  |  |  |  |
| KI#12 |  |  |  |  |
| KI#13 |  |  |  |  |
| KI#14 |  |  |  |  |
| KI#15 |  |  |  |  |
| KI#16 |  |  |  |  |
| KI#17 |  |  |  |  |
| KI#18 |  |  |  |  |
| KI#19 |  |  |  |  |
| KI#20 |  |  |  |  |
| KI#21 |  |  |  |  |
| KI#22 |  |  |  |  |
| KI#23 |  |  |  |  |
| KI#24 |  |  |  |  |
| KI#25 |  |  |  |  |
| KI#26 |  |  |  |  |
| KI#27 |  |  |  |  |
| KI#28 |  |  |  |  |
| KI#29 |  |  |  |  |
| KI#30 |  |  |  |  |

Annex T: Temporary Holding Annex Security Areas

Editor's Note: The figure and table in this annex were provided during the 17/09/2019 conference call and are intended to help review of the KIs to ensure requirements cover all areas identified in the table.

Editor's Note: Annex to be deleted or replaced once study conclusions are completed as per 17/09/2019 conference call discussions.



Figure T-1: Simplified virtualisation security area

|  |  |
| --- | --- |
| **Security area** | **Requirements Scope** |
| (1) External interfaces | Yes |
| (2) 3GPP Data | Yes |
| (3) Border Security | Yes |
| (4) Exchange of 3GPP data with Virtualization entities | Maybe |
| (5) Exchange of 3GPP data between NVFs | Maybe |
| (6) Control and instantiation of NVFs | Maybe |
| (7) Storage and Memory | Maybe |
| (8) Access to storage | Maybe |
| (9) Access and control of Virtualization domain | Yes |
| (10) Access and control of Border Security Function | Yes |
| (11) Security of the server itself | Yes |

Table T-1: 3GPP scope per Security Area

Annex <X>:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 01-2019 | SA3#94 |  |  |  |  |  | 0.0.0 |
| 05-2019 | SA3#95 | S3-191722 |  |  |  | S3-191716,715,717,718,719,720,714,721,778,565,566 | 0.1.0 |
| 05-2019 | SA3#95 | S3-191777 | - | - | - | Fixing the history table | 0.1.1 |
| 06-2019 | SA3#95-BIS | S3-192445 | - | - | - | S3-191849,1850,1851,1855,2368,2395,2396,2446 | 0.2.0 |
| 08-2019 | SA3#96 | S3-193185 | - | - | - | S3-193091 | 0.3.0 |
| 09-2019 | Conf Call 10/09/19 |  |  |  |  | S3-192973, S3-192975, S3-193088 plus conf call comments | 0.3.0a |
| 09-2019 | Conf Call  17/09/19 |  |  |  |  | Docs and revisions as discussed on call. | 0.3.0b |
| 10-2019 | Conf Call  01/10/19 |  |  |  |  | Revisions of S3-192549/550/551/552/553/554/555/556/557 | 0.3.0c |
| 10-2019 | SA3#96 ADHOC |  |  |  |  | S3-193749 | 0.3.0cADHOC |
| 10-2019 | SA3#96 ADHOC | S3-193750 |  |  |  | S3-193751/739/740/828/742/743/774/775/422/777/776 | 0.4.0 |
| 11-2019 | SA3#97 | S3-194624 |  |  |  | S3-194568/569/570/572/573/574/575/576/578/579/580/581/582/583 /584/585/587/588/589/590/591/592/593 | 0.5.0 |
| 01-2021 | SA3#102e |  |  |  |  | S3-210087 | 0.6.0 |
| 03-2021 | SA3#102e-bis |  |  |  |  | S3-211340/341 | 0.7.0 |
| 05-2021 | SA3#103-e |  |  |  |  | S3-212388/89 | 0.8.0 |
| 08-2021 | SA3#104-e |  |  |  |  | S3-213182/190/217 | 0.9.0 |
| 11-2021 | SA3#105-e |  |  |  |  | S3-214391/393/390 | 0.10.0 |
| 02-2022 | SA3#106-e |  |  |  |  | S3-220077/78(r2) | 0.11.0 |
| 05-2022 | SA3#107-e |  |  |  |  | S3-221190,1250 | 0.12.0 |
| 07-2022 | SA3#107-adhoc-e |  |  |  |  | S3-221486, 1648, 1670, 1689, 1701, 1702 | 0.13.0 |
| 10-2022 | SA3#108-ahhoc-e |  |  |  |  | S3-222995,997 | 0.14.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |