



**Network Functions Virtualisation (NFV);
NFV Security;
Report on use cases and technical approaches
for multi-layer host administration**

[ETSI GR NFV-SEC 009 V1.3.1 \(2025-01\)](https://standards.iteh.ai/catalog/standards/etsi/94fb29d7-b3f2-426a-8108-89ffbd1c0c34/etsi-gr-nfv-sec-009-v1-3-1-2025-01)

<https://standards.iteh.ai/catalog/standards/etsi/94fb29d7-b3f2-426a-8108-89ffbd1c0c34/etsi-gr-nfv-sec-009-v1-3-1-2025-01>

Disclaimer

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

ReferenceRGR/NFV-SEC009ed131

Keywordsadministration, regulation, security

ETSI650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

Contents

| | |
|--|----|
| Intellectual Property Rights | 6 |
| Foreword..... | 6 |
| Modal verbs terminology..... | 6 |
| Introduction | 6 |
| 1 Scope | 8 |
| 2 References | 8 |
| 2.1 Normative references | 8 |
| 2.2 Informative references..... | 8 |
| 3 Definition of terms, symbols and abbreviations..... | 9 |
| 3.1 Terms..... | 9 |
| 3.2 Symbols..... | 9 |
| 3.3 Abbreviations | 9 |
| 4 Use cases for multi-layer administration..... | 11 |
| 4.0 Use cases - introduction | 11 |
| 4.1 Multi-tenant hosting | 11 |
| 4.2 Infrastructure as a service (IaaS) | 12 |
| 4.3 Security Sensitive Application Functions..... | 12 |
| 4.3.1 Introduction..... | 12 |
| 4.3.2 Applicability of security requirements in the context of Sensitive Application Functions..... | 13 |
| 4.3.3 Notes on the technologies and measures in the context of Sensitive Application Functions..... | 14 |
| 4.4 Security Network Monitoring & Control Functions..... | 14 |
| 4.4.1 Introduction..... | 14 |
| 4.4.2 Applicability of security requirements in the context of Network Monitoring & Control Functions..... | 15 |
| 4.4.3 Notes on the technologies and measures in the context of Network Monitoring & Control Functions..... | 16 |
| 4.5 Lawful Interception | 16 |
| 4.5.1 Introduction and baseline references..... | 16 |
| 4.5.2 Applicability of security requirements in the context of Lawful Interception | 17 |
| 4.5.3 Notes on the technologies and measures in the context of Lawful Interception | 18 |
| 4.6 Retained Data | 18 |
| 4.6.1 Introduction and baseline references..... | 18 |
| 4.6.2 Applicability of security requirements in the context of RD Storage and Query | 19 |
| 4.6.3 Notes on the technologies and measures in the context of RD Storage and Query | 20 |
| 4.7 Personally Identifiable Information protection..... | 20 |
| 4.7.1 Introduction..... | 20 |
| 4.7.2 Applicability of security requirements in the context of PII protection..... | 20 |
| 5 Security requirements..... | 21 |
| 5.0 Void..... | 21 |
| 5.0.1 Overview | 21 |
| 5.0.2 Prevention versus remediation..... | 22 |
| 5.0.3 Channels for assertions by the hosting service | 22 |
| 5.0.4 The value of assertions | 23 |
| 5.0.5 Use cases to requirements mapping..... | 23 |
| 5.1 Requirements - hosting service | 24 |
| 5.1.1 Capability assertion and attestation at boot-time | 24 |
| 5.1.2 Capability assertion and attestation at run-time | 24 |
| 5.1.3 Assert secure provision of hosted application..... | 25 |
| 5.1.4 Assert own system integrity at boot..... | 25 |
| 5.1.5 Assert continued integrity of own system at run-time | 25 |
| 5.1.6 Location assertion | 26 |
| 5.2 Requirements - hosted application | 26 |
| 5.2.1 Confidentiality of data | 26 |
| 5.2.2 Confidentiality of data-related metadata..... | 26 |
| 5.2.3 Confidentiality of processes..... | 26 |

| | | |
|---------|--|----|
| 5.2.4 | Confidentiality of process-related metadata..... | 26 |
| 5.2.5 | Concealment of resource usage | 26 |
| 5.2.6 | Secure communications | 27 |
| 5.2.7 | Secure storage | 27 |
| 5.2.8 | Secure clean-up..... | 28 |
| 5.2.9 | Secure routing/switching | 28 |
| 5.2.10 | Assurance of compliance by hosting service | 28 |
| 5.2.11 | Availability of entropy source | 28 |
| 5.3 | Requirements - other components | 29 |
| 5.3.0 | Introduction..... | 29 |
| 5.3.1 | Secure routing/switching | 29 |
| 5.3.2 | Workload placement policy and operation security..... | 29 |
| 5.3.3 | Availability of an attestation authority..... | 30 |
| 6 | Available technologies and measures..... | 30 |
| 6.0 | Introduction | 30 |
| 6.1 | Memory inspection..... | 30 |
| 6.1.0 | Introduction..... | 30 |
| 6.1.1 | Memory inspection as an attack vector..... | 31 |
| 6.1.2 | Memory inspection as a security enabler | 31 |
| 6.2 | Secure logging | 31 |
| 6.3 | OS-level access control | 32 |
| 6.4 | Post-incident analysis | 32 |
| 6.5 | Physical controls and alarms | 32 |
| 6.6 | Personnel controls and checks..... | 33 |
| 6.7 | Logical authentication controls | 33 |
| 6.8 | Read-only partitions | 34 |
| 6.9 | Write-only partitions | 34 |
| 6.10 | Policies for workload placement | 34 |
| 6.11 | Communications Security | 35 |
| 6.12 | Measured boot | 35 |
| 6.13 | Secured boot..... | 35 |
| 6.14 | Concealed resource usage | 36 |
| 6.15 | Attestation | 36 |
| 6.16 | Hardware-mediated execution enclaves | 36 |
| 6.17 | Trusted Platform Module (TPM)..... | 37 |
| 6.17.0 | Introduction..... | 37 |
| 6.17.1 | Shared TPM..... | 37 |
| 6.17.2 | Virtual TPM..... | 38 |
| 6.18 | Self-encrypting drives/storage..... | 38 |
| 6.19 | Direct Memory Access to hardware resources | 39 |
| 6.20 | Hardware Security Modules | 39 |
| 6.20.1 | Introduction..... | 39 |
| 6.20.2 | Physical Hardware Security Modules | 39 |
| 6.20.3 | Virtual Hardware Security Modules | 40 |
| 6.21 | Software integrity protection and verification..... | 40 |
| 7 | Technical approaches to multi-layer administration | 40 |
| 7.0 | Introduction | 40 |
| 7.1 | Approaches to address specific requirements..... | 41 |
| 7.2 | Generic approaches | 41 |
| 7.2.0 | Basic comparison..... | 41 |
| 7.2.1 | Single, restricted hosts | 43 |
| 7.2.2 | Pooled, restricted hosts | 45 |
| 7.2.2.0 | General case | 45 |
| 7.2.2.1 | Type 1 - no resource concealment..... | 46 |
| 7.2.2.2 | Type 2 - resource concealment..... | 47 |
| 7.2.3 | Pooled, unrestricted hosts | 50 |
| 8 | Roadmap to secure-execution hosts | 52 |
| 8.0 | Applicability of secure-execution hosts | 52 |
| 8.1 | Moving to single, restricted hosts..... | 52 |
| 8.2 | Moving to pooled, restricted hosts | 53 |

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

Introduction

The Security Problem Statement, ETSI GS NFV-SEC 001 [i.1] identifies an issue with multi-layer administration for NFV. Multi-layer administration seeks to provide methods, capabilities, procedures and assurances that safeguard Virtual Machines or Containers running on a virtualisation host from interference. The specific problem is that any user or process with root access to the hosting service can normally view and change the memory and processes of any hosted application. This is due to the fact that in the default administrative configuration for the majority of host-based virtualisation systems - whether using hypervisors or Containers - any process or administrator operating at the "base" level has access to the memory of all applications - including VMs and Containers - running on that host. The term *inspection* is often used to refer to the ability for processes to directly interact with system memory. Further detail is provided in clause 6.1.1.

Although this configuration is generally acceptable when the hosted applications and the hosting service operate in the same trust domain, or when the hosted applications are in the same trust context and a subordinate trust domain to the hosting service, there are a number of use cases where the trust relationship from the hosted application to the hosting service does not conform to this model. In these cases, the hosted application may wish to protect a set of its resources from the hosting service.

Note that there are also attacks in the opposite direction: from the hosted application against the hosting service. While serious, these are well understood issues and most hosting services already track vulnerabilities in this context and provide defensive measures against these types of attacks. Another type of attack is from one hosted application against another hosted application on the same hosting service. Neither of these "top-down" attacks are considered explicitly in the present document, however, some of the methods and techniques presented here will reduce the incidence of such attacks (e.g. hardware mediated secure enclaves). The focus of the present document, then, is on securing hosted applications against attacks by the hosting service, as well as limiting undesired visibility.

Note that multi-layer administration in the context of NFV should not be confused with the similar term "Multi-Layer Security" (MLS), though certain concepts relevant to MLS may be relevant or referenced in the present document.

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ETSI GR NFV-SEC 009 V1.3.1 \(2025-01\)](https://standards.iteh.ai/catalog/standards/etsi/94fb29d7-b3f2-426a-8108-89ffbd1c0c34/etsi-gr-nfv-sec-009-v1-3-1-2025-01)

<https://standards.iteh.ai/catalog/standards/etsi/94fb29d7-b3f2-426a-8108-89ffbd1c0c34/etsi-gr-nfv-sec-009-v1-3-1-2025-01>

1 Scope

The present document addresses multi-layer administration use cases and technical approaches, an issue identified in the Security Problem Statement, ETSI GS NFV-SEC 001 [i.1]. Multi-layer administration seeks to provide methods, capabilities, procedures and assurances - of various strengths based on requirements and available technologies and techniques - that safeguard Virtual Machines or Containers running on a virtualisation host ("hosted applications") - from interference (of various types) by the host system or platform ("hosting service").

The scope of the present document is generally the system comprising the hosting service, associated hardware (including TPM, GPU, etc.), software and configuration, and the hosted application. Some requirements and measures outside this context are also considered, but not necessarily in equal depth.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

- [i.1] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".
- [i.2] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".
- [i.3] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".
- [i.4] ETSI TS 102 232: "Lawful Interception (LI); Handover Interface for IP delivery".
- [i.5] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".
- [i.6] ETSI TS 102 656: "Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data".
- [i.7] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".
- [i.8] ETSI GR NFV-SEC 007: "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".
- [i.9] [NIST Special Publication 800-122](#): "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".
- [i.10] [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data](#).
- [i.11] TCG PC: "Client Specific Implementation Specification for Conventional BIOS - Specification Version 1.21 Errata".

- [i.12] ETSI GS NFV-SEC 004: "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications".
- [i.13] [Forensics Whitepapers](#).
- [i.14] [TCG TPM 2.0 Library](#): "Trusted Platform Module Library Specification, Family 2.0".
- [i.15] [TCG TSS 2.0 TAB and Resource Manager](#): "TSS TAB and Resource Manager Specification".
- [i.16] [NIST FIPS 140-2](#): "Security Requirements for Cryptographic Modules".
- [i.17] [TCG](#): "Virtualized Trusted Platform Architecture Specification".
- [i.18] ETSI GS NFV-SEC 010: "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".
- [i.19] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

| | |
|-------|---|
| AAA | Authentication, Authorisation & Auditing |
| ADMF | Administrative Function (for Lawful Interception) |
| API | Application Programming Interface |
| AUC | AUthentication Centre |
| BIOS | Basic Input/Output System |
| BMSC | Broadcast-Multicast Service Centre |
| BRAS | Broadband Remote Access Server |
| CA | Certificate Authority |
| CIA | Confidentiality, Integrity and Availability |
| CoT | Chain of Trust |
| CPU | Central Processing Unit |
| CRTM | Core Root of Trust for Measurement |
| CS | Circuit Switched |
| CSCF | Call Session Control Function |
| DMA | Direct Memory Access |
| DSLAM | Digital Subscriber Line Access Multiplexer |
| EMS | Element Management System |
| ESXi | Elastic Sky X integrated |
| FIPS | Federal Information Processing Standards |
| GGSN | Gateway GPRS support node |
| GMSC | Gateway Mobile Switching Centre |
| GPU | Graphics Processing Unit |
| HBRT | Hardware-Based Root of Trust |
| HLR | Home Location Register |
| HSM | Hardware Security Module |
| HSS | Home Subscriber Server |
| HW | Hardware |

| | |
|-------------|--|
| I/O | Input/Output |
| IaaS | Infrastructure as a Service |
| IBCF | Interconnection Border Control Function |
| ID | IDentifier |
| IMS | IP Multimedia Subsystem |
| IMS-ALG | IMS Application Level Gateway |
| KVM | KVM hypervisor software |
| LBA | Logical Block Array(s) |
| LEA | Law Enforcement Agency |
| LI | Lawful Interception |
| LTE | Long Term Evolution |
| MAC | Modify, Access, Create |
| MFRP | Multimedia Resource Function Processor |
| MME | Mobility Management Entity |
| MRFC | Media Resource Function Controller |
| MSC | Mobile Switching Centre |
| NFV | Network Function Virtualisation |
| NFVI | Network Function Virtualisation Infrastructure |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| OSS | Operations Support Systems |
| PC | Personal Computer |
| PCI | Payment Card Industry |
| PCR | Platform Configuration Register |
| P-CSCF | Proxy - Call Session Control Function |
| PDN-Gateway | Packet Data Network Gateway |
| PII | Personal Identifiable Information |
| PKI | Public Key Infrastructure |
| POI | Point Of Interception |
| pTPM | physical Trusted Platform Module |
| RAID | Redundant Array of Inexpensive Disks OR Redundant Array of Independent Disks |
| RAM | Random Access Memory |
| RD | Retained Data |
| RoT | Root of Trust |
| RSA | RSA encryption algorithm |
| RTM | Root-of Trust for Measurement |
| SBC | Session Border Controller |
| S-CSCF | Serving – Call Session Control Function |
| SDN | Software-Defined Networking |
| SED | Self-Encrypting Drive |
| SGSN | Serving GPRS support node |
| S-GW | Serving - GateWay |
| SLA | Service Level Agreement |
| SMSC | Short Message Service Centre |
| SW | Software |
| TAB | TPM Access Broker |
| TBB | Trusted Building Block |
| TCG | Trusted Computing Group |

NOTE: See www.trustedcomputinggroup.org.

| | |
|------|-------------------------------------|
| ToR | Top of Rack |
| TPM | Trusted Platform Module |
| UICC | Universal Integrated Circuit Card |
| vCPE | virtual Customer Premises Equipment |
| vHSM | virtual HSM |
| VIM | Virtual Infrastructure Manager |
| VLR | Visitor Location Register |
| VM | Virtual Machine |
| VMM | Virtual Machine Manager |
| VNF | Virtual Network Function |

| | |
|-------|---|
| VNFCI | Virtual Network Function Component Instance |
| VNFI | Virtual Network Function Instance |
| VNFM | Virtual Network Function Manager |
| VoLTE | Voice over LTE |
| vTPM | virtual TPM. |

4 Use cases for multi-layer administration

4.0 Use cases - introduction

These use case descriptions provide various levels of detail, some referencing items in clause 5.0.5 to note which specific requirements are relevant to the use case. This is particularly the case where regulatory requirements allow for detailed definition of requirements (in the case, for instance, of Lawful Interception clause 4.5 and Retained Data clause 4.6. In other cases, the specific requirements will depend more on the business requirements of the operator, the current business environment and local norms: here, a general description of the use case is provided, and some suggestions made.

4.1 Multi-tenant hosting

This is the case where one operator hosts VNFs (or VNFCIs) from one or more operators on NFVI owned and/or operated by the first operator. This is identified in ETSI GS NFV 001 [i.19] as Use Case #1 "Infrastructure as a Service", but is differentiated in the present document from the use case in clause 4.2.

The relevance to the present document is that the first operator (the hosting operator) may need to be able to provide assurances that sensitive processes, algorithms and data (e.g. subscriber details) owned by the other operators cannot be viewed or changed by the NFVI operator, whether intentionally or unintentionally. The exact requirements for such an agreement will be subject to contractual arrangements between different operators, and are not therefore considered in detail in the present document. They may include, however, the requirements described in the following clauses of the present document:

- 5.1.1 Capability assertion and attestation at boot-time.
- 5.1.3 Assert secure provision of hosted application.
- 5.1.6 Location assertion.
- 5.2.1 Confidentiality of data.
- 5.2.3 Confidentiality of processes.
- 5.2.6 Secure communications.
- 5.2.7 Secure storage.
- 5.2.8 Secure clean-up.
- 5.2.10 Assurance of compliance by hosting service.
- 5.2.11 Availability of entropy source.
- 5.3.2 Workload placement policy and operation security.
- 5.3.3 Availability of an attestation authority.

Another requirement that may arise is that of resource allocation: particularly the availability of sufficient CPU cycles and network bandwidth for hosted VNFs/VNFCIs. This is outside the scope of the present document, and it is expected that guarantees would be made by contractual agreements such as Service Level Agreements (SLAs). Monitoring for such SLAs is also considered outside the scope of the present document.

4.2 Infrastructure as a service (IaaS)

Infrastructure as a service ("IaaS") is the case where a service provider may wish to provide infrastructure services to third party with the extra guarantee that the service provider cannot view or change data or algorithms in the hosted applications. This is not considered a "pure" NFV use case, as it is more akin to data centre hosting than service provision, but is briefly considered here as it shares similar requirements with multi-tenant and the measures available are also applicable. Infrastructure as a service is also a service offered by other business units of operators, and it is expected that best practice should be shared in both directions. A key point here is that customers may have requirements to keep encryption keys safe (see [example 1](#) or [example 2](#)), and it will therefore fall to the hosting service provider to ensure that measures are in place to service this requirement.

The exact requirements for such a service will depend on the services offered by the hosting service provider, and are not therefore considered in detail in the present document. They may include, however, the requirements described in the following clauses of the present document:

- 5.1.1 Capability assertion and attestation at boot-time
- 5.1.3 Assert secure provision of hosted application
- 5.1.6 Location assertion
- 5.2.1 Confidentiality of data
- 5.2.3 Confidentiality of processes
- 5.2.6 Secure communications
- 5.2.7 Secure storage
- 5.2.8 Secure clean-up
- 5.2.10 Assurance of compliance by hosting service
- 5.2.11 Availability of entropy source
- 5.3.2 Workload placement policy and operation security
- 5.3.3 Availability of an attestation authority

As with Multi-tenant hosting clause 4.1, another requirement that may arise is that of fair resource allocation: particularly the availability of sufficient CPU cycles and network bandwidth for hosted VNFs/VNFs. This is outside the scope of the present document, and it is expected that guarantees would be made by contractual agreements such as Service Level Agreements (SLAs). Monitoring for such SLAs is also considered outside the scope of the present document.

4.3 Security Sensitive Application Functions

4.3.1 Introduction

This use case concerns the segregation of sensitive application functions from other network functions, where restricted access and additional security domain separation requirements may be applied by operators.

Examples of such functions are the 3GPP AUC (master cryptographic key database responsible for holding UICC keys and generating authentication vectors) and the HSS which contains the 3GPP user subscription information. Typically operators allow a very restricted set of administrators access to such sensitive functions compared with other network elements.

These functions are considered to be largely standalone islands within an operator's network although they will interconnect with other VNFs in other administrative domains via specific restricted interfaces at the virtualised application layer.

4.3.2 Applicability of security requirements in the context of Sensitive Application Functions

This clause gives specific interpretation of clause 5 in the context of Sensitive Application Functions.

Table 1

| Clause of the present document | Notes for Security Sensitive Application Functions |
|--|--|
| 5.0.1 Overview | Depending on the Sensitive Function availability is likely to be important (e.g. HSS & AUC), as network and/or user services will not be available without these functions. |
| 5.0.2 Prevention versus remediation | Prevention is likely more important than remediation as the network may not function without these functions. However if a negative security event cannot be prevented, remediation is very important. |
| 5.1.1 Capability assertion and attestation at boot-time | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.1.2 Capability assertion and attestation at run-time | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.1.3 Assert secure provision of hosted application | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.1.4 Assert own system integrity at boot | Important for Sensitive Application Functions. VNFI may be to verify integrity of databases, static configuration data and application root key chain (e.g. AUC). |
| 5.1.5 Assert continued integrity of own system at run-time | Important for Sensitive Application Functions. Loss of integrity of Sensitive Functions may lead to loss of integrity of whole virtualised network and services. |
| 5.1.6 Location assertion | Depends on specific Sensitive Function. |
| 5.2.1 Confidentiality of data | Depends on specific Sensitive Function. Would be critical for functions containing application cryptographic functions (e.g. AUC) but may not be critical in all functions. |
| 5.2.2 Confidentiality of data-related metadata | Depends on specific Sensitive Function. Would be critical for functions containing application cryptographic functions (e.g. AUC) or subscriber databases (e.g. HSS) but may not be critical in all functions. |
| 5.2.3 Confidentiality of processes | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.2.4 Confidentiality of process-related metadata | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.2.5 Concealment of resource usage | May be desirable for some functions to prevent attacks on cryptographic functions but absolute concealment unlikely to be required. |
| 5.2.6 Secure communications | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.2.7 Secure storage | Important for Sensitive Application Functions. Storage of cryptographic keys, algorithms and other sensitive information will require secure storage. |
| 5.2.8 Secure clean-up | Important for Sensitive Application Functions. Cryptographic keys, algorithms and customer data subject to Data Protection requirements will require secure clean-up. |
| 5.2.9 Secure routing/switching | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.2.10 Assurance of compliance by hosting service | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.2.11 Availability of entropy source | May be important for some functions (e.g. AUC) but not for other. |
| 5.3.1 Secure routing/switching | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.3.2 Workload placement policy and operation security | Important for Sensitive Application Functions but no specific provisions are noted. |
| 5.3.3 Availability of an attestation authority | May be important for some functions. |

4.3.3 Notes on the technologies and measures in the context of Sensitive Application Functions

The following notes give specific interpretation of clause 6 in the context of Sensitive Application Functions.

Table 2

| Clause of the present document | Notes for Sensitive Application Functions |
|--|--|
| 6.1 Memory inspection | Memory inspection by a hosting service would cause issues for some Sensitive Functions (e.g. AUC). In general hosting services may not be trusted to introspect Sensitive Function details on hosted services. |
| 6.2 Secure logging | There is a requirement for capability of logging for Sensitive Application Functions. However depending on the function, these logs may be need to be treat separately from other functions. |
| 6.3 OS-level access control and 6.4 Post-incident analysis | This is important, but no specific provisions are noted. |
| 6.5 Physical controls and alarms and 6.6 Personnel controls and checks | This is important and will depend on the specific function (e.g. AUC), but no specific provisions are noted. |
| 6.8 Read-only partitions and 6.9 Write-only partitions | Read or write-only partitions will be required by some Sensitive Application Functions. |
| 6.11 Communications Security | Confidentiality and integrity of network traffic are critical for most Sensitive Functions. |
| 6.12 Measured boot, 6.13 Secured boot | This is important, but no specific provisions are noted. |
| 6.14 Constant resource usage | Unlikely to be necessary in most sensitive functions. However may be required for specific components of cryptographic and similar functions (e.g. AUC). |
| 6.15 Attestation, 6.16 Hardware-mediated execution enclaves, 6.17 Trusted Platform Module (TPM) | TPMs or equivalent implementations that include the protection capabilities, as provided by TPMs, may be mandated to be hardware based. Virtual modules may not be sufficiently robust. |
| 6.18 Self-encrypting drives/storage | Confidentiality and integrity of data at rest is critical for most Sensitive Functions. |
| 6.19 Direct Memory Access to hardware resources | Unlikely to be necessary in most sensitive functions but some VNFs are likely to require access to hardware accelerator functional (e.g. specialist cryptographic functions - see, for example, clause 6.20). |
| 6.20 Hardware Security Modules | Some VNFs may require access to the security capabilities offered by HSMs. |
| 6.21 Software integrity protection and verification | Software integrity protection and verification is expected to be required for almost all use cases. |

4.4 Security Network Monitoring & Control Functions

4.4.1 Introduction

This use case concerns the segregation of monitoring functions from other network functions, where restricted access and additional security domain separation requirements may be applied by operators.

Examples of such functions are the routers, firewalls, packet monitoring filters or other network defensive functions (e.g. proxy servers). These functions are used logically to protect virtualised functions running in other VMs.

These functions may be grouped in a single administrative domain or multiple parallel domains each containing one or more functions (e.g. one or more firewalls).