ETSI GS NFV-IFA 026 V3.2.1 (2019-07)

Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification

Disclaimer

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

Reference
DGS/NFV-IFA026

Keywords
architecture, management, MANO, NFV, orchestration, security

ETSI

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

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

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

Important notice

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

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

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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

Trademarks

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document defines the requirements to interface the Security Control to NFV-MANO as described in ETSI GS NFV-SEC 013 [1] and the LI Controller in ETSI GR NFV-SEC 011 [2]. The present document identifies the extensions to the NFV-MANO architecture related to security management and monitoring. Multiple trust domains are considered.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI GS NFV-SEC 013 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification".

[2] ETSI GR NFV-SEC 011 (V3.1.1): "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[3] ETSI GS NFV-SEC 012 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

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

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-IFA 033: "Network Functions Virtualization (NFV) Release 3; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification".

[i.2] ETSI GS NFV 003 (V1.3.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS NFV 003 [i.1] and the following apply.

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in ETSI GS NFV 003 [i.1].

security manager: function within an NFV network responsible for enforcing security policy for VNFs and for instructing NFV-MANO to take VNF specific or system wide security actions

NOTE: The security manager is a logical sub component of a CSP's overall network security management and monitoring systems.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.1] and the following apply.

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI GS NFV 003 [i.1].

CSP	Communication Service Provider
HMEE	Hardware Mediated Execution Environment
NS	Network Service
NSD	Network Service Descriptor
SM	Security Manager
sNSD	security enhanced Network Service Descriptor
VSF	Virtual Security Function

4 Introduction

Within a CSP's network, it is necessary to be able to monitor and manage all components making up a network (including application layer software, NFVI software and hardware components). Therefore, a CSP's overall security management platform needs to have real-time access and understanding of NFV-MANO VNF orchestration and management events. In some scenarios it is sufficient to simply observe and alert on those events from a security perspective, while in other scenarios the CSP security management platform may be required to specifically authorize some or all actions undertaken by NFV-MANO. A CSP security management platform may require one or more Security Manager (SM) depending on the security isolation required between different trust domains.

ETSI GS NFV-SEC 013 [1] describes security management and monitoring in an NFV environment. The NFV SM as described in ETSI GS NFV-SEC 013 [1] is responsible for making security decisions associated with the instantiation, modification and termination of VNFs.

In order to achieve this the SM requires real-time information from NFV-MANO on VNF instantiation, modification and termination. This information needs to be sufficiently detailed for the SM to be able to resolve the type and version of a VNF(s) being instantiated, VNFD constraints applied to those VNFs, OSS / BSS application layer VNF(s) ID(s) (i.e. VNF instance name) and information about the intended physical hardware environment (host IDs / location etc). It is not important to the SM which NFV-MANO sub-components provide which specific pieces of information but it is important that the information is provided in an intelligible format. The SM is responsible for maintaining the cumulative state of the information received from NFV-MANO. However, in the case of SM failure or for state recovery under network / NFV-MANO failure conditions, it is desirable for NFV-MANO to be able to provide the SM

with the current state of all VNFs (including hardware / resource usage and VNF and VNFCI interconnections routing table).

The SM is responsible for analysing information received from NFV-MANO and where necessary instructing NFV-MANO to take actions accordingly (e.g. applying security policy to a VNF being initiated). In addition, when the SM becomes aware of a security event (e.g. VNF compromise) the SM is responsible for instructing NFV-MANO to take appropriate mitigating actions (e.g. terminate a VNF instance or put a VNF into quarantine). NFV-MANO and wider network auto recovery mechanisms need to ensure that they are able to handle SM enforced VNF decisions and NFV-MANO does not attempt to restart or migrate VNFs that the SM has requested be terminated or quarantined.

In scenarios where there is not a single legal entity or CSP operating the entire virtual network (e.g. tenant hosted scenarios), the SM(s) implementation will need to ensure isolation of information, events or policy is maintained between different entities.

Where NFV-MANO has visibility of PNFs (e.g. by association with SDN routing to and from VNFs), that information also needs to be provided to the SM by NFV-MANO.

The present document contains set of requirements and analysis in annex A, for each of the reference points between NFV-MANO and the SM defined in clause 5. These requirements are derived from but not limited to those in ETSI GS NFV-SEC 013 [1].

5 Interface and Architectural Requirements

5.1 Functional blocks and reference points

Figure 5.1 shows the three new reference points and one new functional block which are required to be added to the underlying NFV architecture to support security monitoring and management, as defined in ETSI GS NFV-SEC 013 [1].

The new functional block is the Security Manager (SM). It may be necessary to have more than one Security Manager in order to meet all the security requirements, in which case each SM shall be handled independently within a separate trust domain using separate instances of endpoints on relevant interfaces defined over the three reference points. In the case of multiple security managers, each security manager may be authorized to perform different sub-sets of the requirements listed in annex A.

The three reference points are:

- Sc-Or: the reference point between the Security Manager and the NFV Orchestrator.
- Sc-Vnfm: the reference point between the Security Manager and VNF Manager.
- Sc-Vi: the reference point between the Security Manager and Virtualised Infrastructure Manager.

NOTE: The interfaces which run over these reference points are defined in ETSI GS NFV IFA 033 [4], which also contains requirements for those interfaces.

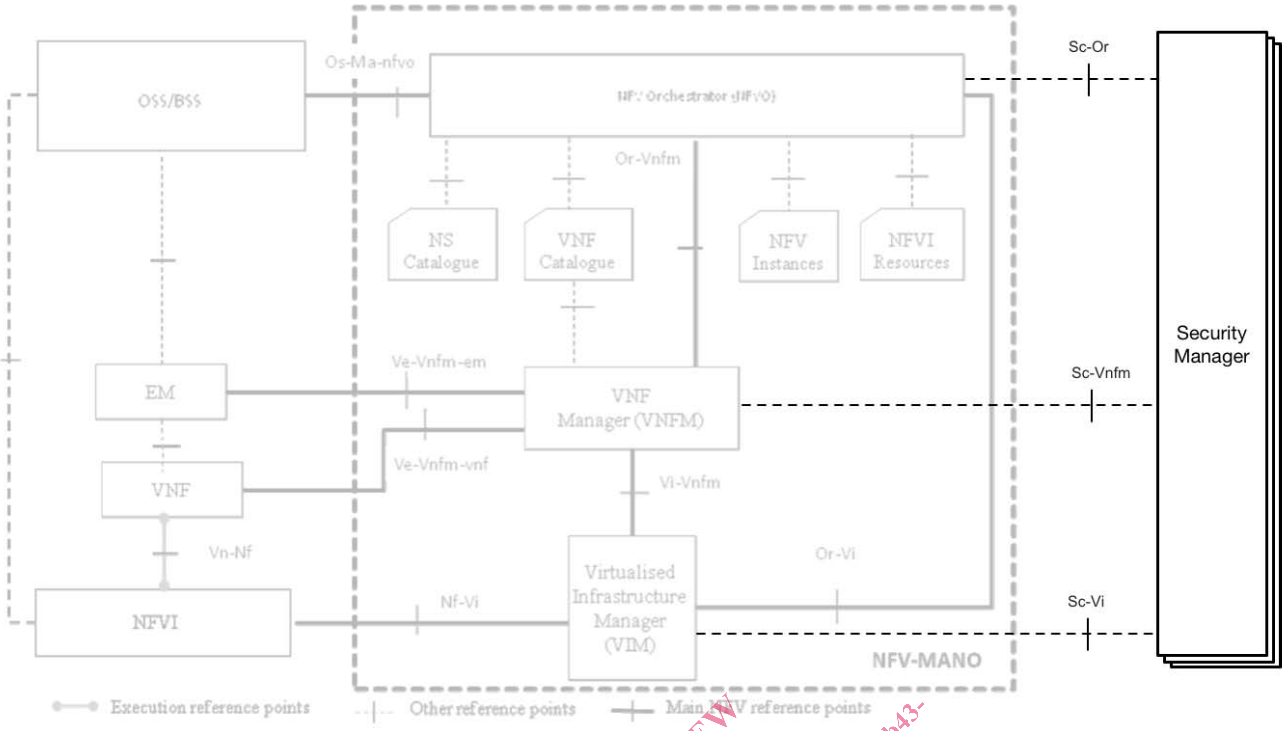

Figure 5.1: Security Manager and NFV-MANO Reference Architecture

5.2 SM Modes

The SM and NFV-MANO shall support three modes of operation:

- Passive: SM is able to subscribe to applicable lifecycle management events passed to it by NFV-MANO but the SM does not take any active part in the lifecycle management of the VNFs.
- Semi-Active: SM analyses applicable lifecycle management events passed to it by NFV-MANO. The SM may provide security policies to NFV-MANO as part of a VNF lifecycle management but the SM takes an otherwise passive part in VNF lifecycle management. The SM is able to request NFV-MANO to undertake security mitigation actions (e.g. terminate a VNF instance).
- Fully-Active: NFV-MANO passes applicable VNF lifecycle events to the SM and requests approval from the SM. The SM authorizes, modifies with security policy, or rejects NFV-MANO requests. The SM is also able to instruct NFV-MANO to take security mitigation actions (e.g. immediately terminate a VNF instance).

NOTE: The full scope of lifecycle events which are applicable to the SM in Passive, Semi-Active and Fully-Active modes are outside the scope of the present document. However, the applicability of specific VNF lifecycle management events would be determined based on the necessity to meet the requirements defined in clause 5 and annex A.

5.3 Multiple Trust Domains and Security Managers

In networks with multiple trust domains or where a CSP wishes to achieve security role separation, there may be one or more SMs. Each SM may operate in Passive, or Semi-Active or Fully Active mode as described in clause 5.2.

It shall be possible for the SMs to act independently of each other or for SMs to operate in a hierarchical arrangement where one SM may be able to issue VNF termination instructions across all trust domains of one or more sub SMs.

NOTE: In hierarchy terms, a sub SM is an SM which is overseen or controlled by another higher security level SM. For example, a sub SM in Semi-Active Mode may be subservient to a network wide Fully Active SM. The sub SM is able to fulfil its role autonomously but the higher-level SM would be able to overrule it at any time. NFV-MANO needs to be able to support such hierarchical models and provide interface instance isolation for such sub SM to SM relationships.

Each SM shall interface to NFV-MANO using a logically separate, dedicated instance of interfaces as defined in clause 5.1. Each set of SM to NFV-MANO interfaces shall use independent integrity and confidentially protection from all other SM to NFV-MANO interface sets.

NFV-MANO is responsible for ensuring that VNF lifecycle management events are sent to the correct one or more SMs subject to the trust domain separation model being implemented by a network.

NFV-MANO shall not accept instructions from an SM in one trust domain for VNFs managed by another SM in another trust domain (hierarchical layering requirement above notwithstanding).

SM to NFV-MANO trust domain separation shall include support for management of sensitive components as defined in ETSI GS NFV-SEC 012 [3].

NFV-MANO shall support an authorization framework where each SM is authorized in Passive or Semi-Active or Fully-Active mode to undertake interactions with NFV-MANO.

Each SM to NFV-MANO authorization shall be independent of any other SM binding. NFV-MANO shall ensure that each SM is invisible to any other SM (hierarchical layering requirement notwithstanding).

Where one SM spans multiple trust domains, it shall be possible for the SM to operate in different modes (Passive, Semi-Active, Fully-Active) for each trust domain.

NFV-MANO shall be able to manage and authorize these different modes for different trust domain for a single SM independently.

The present document assumes that where more than one SM exist in an NFV implementation, one SM will act as a master SM such that is able to instruct NFV-MANO to immediately terminate any VNF belonging to any sub SM trust domain or over-rule the actions of a sub SM.

Where NFV-MANO is required to maintain audit logs of lifecycle management events, NFV-MANO shall be able to separate these based on the SM and trust domain separation requirements above.

Detailed requirements for multiple trust domains and multiple SMs are defined in annex A.

Annex A (normative): Reference point functional requirements

A.0 General

This annex provides requirements to be supported by NFV-MANO over the three functional reference points identified in clause 5.1 and the consequential functional requirements on the NFV-MANO functional blocks terminating those reference points. Clause A.1 provides requirements derived directly from ETSI GS NFV-SEC 013 [1], while clause A.2 provides additional requirements to address areas which are not covered in ETSI GS NFV-SEC 013 [1] in sufficient detail.

A specific NFV-MANO and SM pairing will support a subset of these requirements depending on the operational deployment model and the role of the SM.

The requirements includes functionality required to support the LI Controller as specified in ETSI GR NFV-SEC 011 [2].

The assignment of specific requirements in this annex to one or more of the 3 functional reference points (Sc-Or, Sc-Vnfm, Sc-Vi) as described in clause 5, is provided in ETSI GS NFV-IFA 033 [i.1].

A.1 Requirements on security management and monitoring from ETSI GS NFV-SEC 013

The following requirements are derived from ETSI GS NFV-SEC 013 [1].

In ETSI GS NFV-SEC 013 [1], clause 6.5.1 "Requirements for Multi-Trust-Domain Security Management":

R1.1.10. Entities (e.g. VNFs) building up telco networks (e.g. IMS network) shall be assignable to different trust domains.

R1.1.20. One or more dedicated NFV-MANO trust domains shall exist.

R1.1.30. Each NFV-MANO functional block shall be assignable to one or more dedicated NFV-MANO trust domain(s).

R1.1.40. Trust relationships shall be defined between trust domains.

R1.1.50. For two or more domains without existing trust relationships, the effect of an attack on one domain shall not impact the other domains either directly or indirectly (e.g. through Management channels).

R1.1.60. MANO shall support one or more NFV SMs, per trust domain.

R1.1.70. There shall be controls enforcing separation of duties and privileges, least privilege use and least common mechanism between security management and NFV-MANO. These controls shall apply in conjunction with the corresponding separation of trust domains.

R1.1.80. A NFV SM shall manage security policies and implement the security requirements of a trust domain to be implemented by dedicated security functions or security functions embedded within VNFs.

R1.1.90. A SM shall manage security policies and requirements between trust domains according to the defined trust relationship, including establishing security association between VNFs in different trust domains and between VNFs and NFV-MANO entities when it has visibility and permissions available to perform such duties:

- Security policies reflecting trust relationships between trust domains could include access control (authentication and authorization), traffic/resource separation and segmentation, VPN SeGW, etc.