ETSI GS NFV-SEC 014 V3.1.1 (2018-04)

Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points

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-SEC014

Keywords
interface, MANO, NFV, security

ETSI

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

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

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

Important notice

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

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

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

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

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 provides the results of a simplified threat analysis for NFV-MANO functional blocks (NFVO, VNFM, VIM) and reference points Or-Vnfm, Vi-Vnfm, Or-Vi based on the guidance given in ETSI GS NFV-SEC 006 [5].

The present document is structured such that clause 4 identifies the scope of the analysis, in the form of a target of evaluation, whilst the results of the threat analysis in the form of identified requirements that when implemented will counter or mitigate the threats are given in clause 5 of the present document. A summary is provided in clause 6 of the impact when the requirements are implemented. Threat analysis is a continual process and should be reviewed regularly.

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-IFA 005: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[2] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV); Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[3] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV); Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[4] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV); Management and Orchestration; Functional requirements specification".

[5] ETSI GS NFV-SEC 006: "Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns".

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 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ISO/IEC 15408-1/2/3 2005: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.3] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

4 NFV-MANO Functional Blocks and Reference points

4.0 Overview

This clause provides an overview of NFV-MANO functional blocks and its associated reference points as identified in ETSI GS NFV-IFA 010 [4]. There are three main functional blocks associated with NFV-MANO:

i) NFV Orchestrator (NFVO);

ii) VNF Manager (VNFM); and

iii) Virtualised Infrastructure Manager (VIM).

There are six reference points associated with MANO:

i) Or-Vnfm reference point;

ii) Or-Vi reference point;

iii) Vi-Vnfm reference point;

iv) Os-Ma-nfvo reference point;

v) Ve-Vnfm-em reference point; and

vi) Ve-Vnfm-Vnf reference point.

The Or-Vnfm, Or-Vi and Vi-Vnfm reference points are grouped as NFV-MANO internal reference points whereas the Os-Ma-nfvo, Ve-Vnfm-em and Ve-Vnfm-vnf reference point are grouped as NFV-MANO external reference points:

i) The Or-Vnfm reference point is between NFVO and VNFM.

ii) The Or-Vi reference point is between NFVO and VNFM.

iii) The Vi-Vnfm reference point is between the VIM and VNFM.

iv) The Os-Ma-nfvo reference point is between OSS/BSS and NFVO.

v) The Ve-Vnfm-em reference point is between EM and VNFM.

vi) The Ve-Vnfm-vnf reference point is between VNF and VNFM.

The present document provides a threat analysis for NFV-MANO functional blocks and internal NFV-MANO reference points, i.e. the Or-Vnfm, Vi-Vnfm, Or-Vi reference points. Threat analysis for the external NFV-MANO reference points, i.e. the Os-Ma-nfvo, Ve-Vnfm-em and Ve-Vnfm-Vnf reference points are for further study.

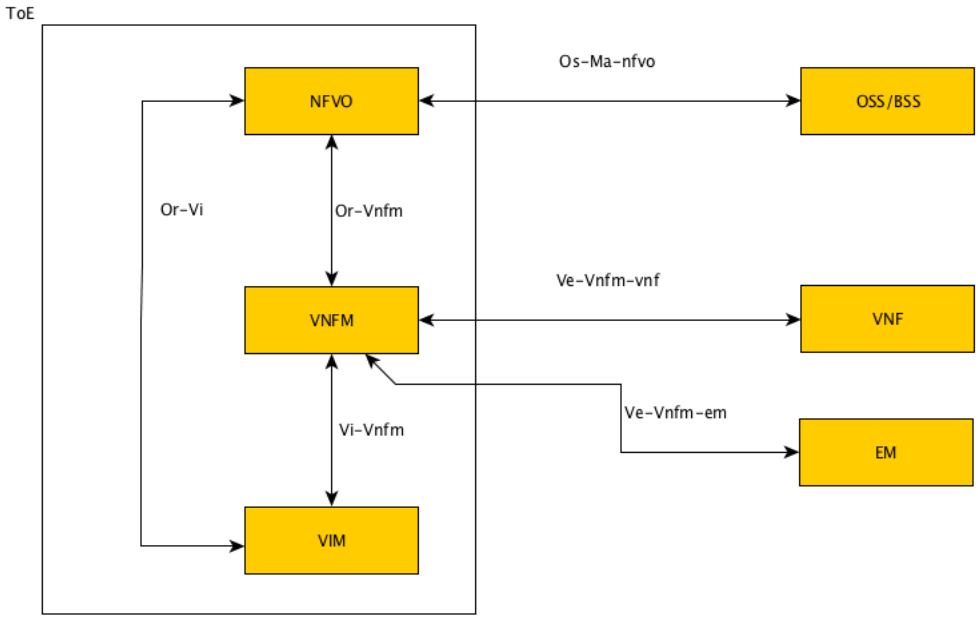

Figure 1: Visual interpretation of Target of Evaluation

The external elements (EM, VNF, OSS/BSS) and their associated reference points are not considered in the present analysis.

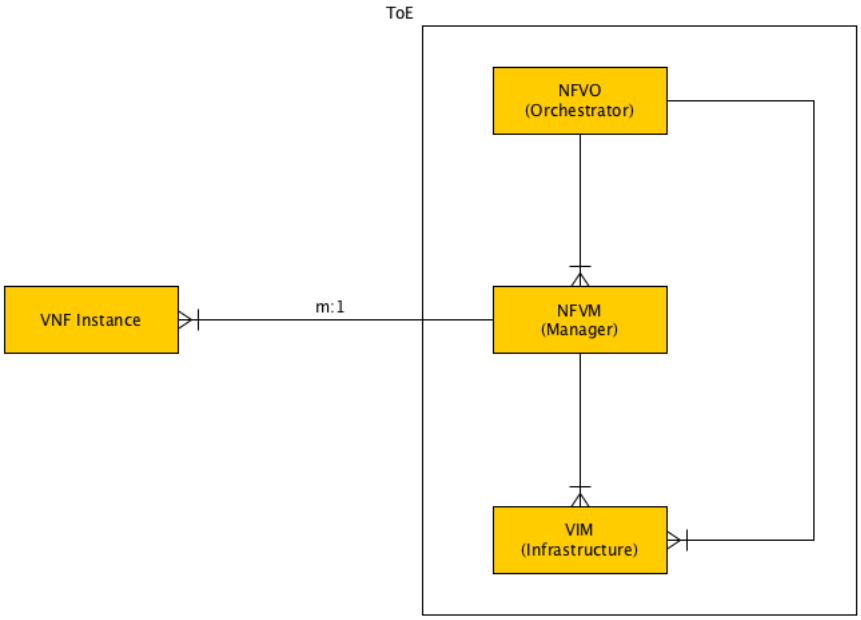

Figure 2: Examination of cardinality of relationships between MANO and VNFIs

The cardinality of relations within MANO has an important impact on the security that may be offered. In simple terms a one-to-one relationship is more straightforward to make secure than a one-to-many or a many-to-many relationship. It is assumed for the purposes of the present document that there is a one-to-many relationship between the NFVO defined in ETSI GS NFV-IFA 010 [4] and the VNFM, and similarly a one-to-many relationship between the VNMF and the VIM. The external relationship from MANO to instances of VNFs is also considered as one-to-many.

4.1 NFV Orchestrator

The NFV Orchestrator (NFVO) is responsible for life cycle management of network services and VNF packages, validation and authorization of requests, policy management, and managing resources of NFV-PoPs via multiple VIMs and VNFMs. It also tracks the network services and the use of resources by using different data repositories. For a detailed description of the NFV orchestrator and its functionalities, refer to clause 5.4.1 in ETSI GS NFV-IFA 010 [4].

4.2 VNF Manager(s)

VNF Manager (VNFM) is responsible for the lifecycle management of VNF instances. Each VNF instance has an associated VNF manager. VNF manager functions are generic in nature and applicable to any type of VNF. The detail description of VNF managers and its functionalities are discussed in ETSI GS NFV-IFA 010 [4].

4.3 Virtualised Infrastructure Manager(s)

Virtualised Infrastructure Manager (VIM) is responsible for controlling and managing the NFVI resources such as compute, storage and network resource of one or more NFVI-Point of Presence (PoPs). VIM exposes virtualised resource management interfaces/APIs to the VNFM and NFVO. The detail description of VIM and its functionalities are discussed in ETSI GS NFV-IFA 010 [4].

4.4 NFV Or-Vi reference point

The reference point Or-Vi is used to exchange information elements between NFV Orchestrator (NFVO) and Virtual Infrastructure Manager (VIM). The Or-Vi reference point supports the resource management operations. The detailed description of Or-Vi reference point between NFVO and VIM are discussed in ETSI GS NFV-IFA 005 [1].

4.5 NFV Vi-Vnfm reference point

The reference point Vi-Vnfm is used to exchange information elements between Virtualised Infrastructure Manager (VIM) and VNF Manager (VNFM). Vi-Vnfm reference point also supports the resource management operations. The detailed discussion of Vi-Vnfm reference point between VIM and VNFM is in ETSI GS NFV-IFA 006 [2].

4.6 NFV Or-Vnfm reference point

The reference point Or-Vnfm is used to exchange information elements between NFV Orchestrator (NFVO) and VNF Manager (VNFM). Or-Vnfm reference point supports the VNF lifecycle management operations. The detailed description of Or-Vnfm reference point between NFV Orchestrator and VNFM is in ETSI GS NFV-IFA 007 [3].

5 Security Threats and Requirements

5.1 Analysis of components and reference points

5.1.1 Fixed asset risks

As outlined in clause 4 the MANO entity consists of 3 discrete internal components (NFVO, VNFM, and VIM) each of which has to manage a set of fixed data assets. The MANO system is defined as an enclosed system thus all attackers are by definition insider attackers, having legitimate access to elements of the system. Mitigation against insider attacks is not trivial and may require a number of non-technical provisions consistent with the human resource aspects of the ISO/IEC 27000 [i.3] series of guidelines or equivalent.

The MANO functionality is realized in software only that is targeted to general purpose hardware.

NOTE: There is scope for the realization of MANO to implement each of the internal components and their reference points by externalised interfaces and protocols which requires that the analysis of MANO is treated as if it were an open rather than an enclosed system.

5.1.2 Data transfer risks

As outlined in clause 4 there are a number of internal reference points that may be instantiated in interfaces. The interfaces may be instantiated as APIs within a single processing environment, as communications interfaces within a networked environment, or as hybrid modes of API and network communications that may be used for support of Remote Procedure Calls or similar in a networked or other distributed processing environment. Similarly to clause 5.1 the only attacker considered is an inside attacker.

5.2 Risk analysis and requirements

Security threats and requirements are presented in this clause with respect to NFV-MANO functional blocks (NFVO, VNFM and VIM), the associated NFV-MANO reference points (Or-Vi, Vi-Vnfm and Or-Vnfm) and any known means of implementing or mapping reference points to corresponding interfaces. Security threats (T) and their associated security requirements (R) are identified. For all threat scenarios, the assumption is that the attackers are attached to the network and have access to the NFV- MANO functional blocks and reference points.

NOTE 1: Implementation of the Identity Management is necessary for enforcing the requirements of the present document.

NOTE 2: It is assumed that identity management is sufficient to assert some of the semantic knowledge of the NFV devices and services that include role, e.g. to distinguish VNFM from VIM, as well as unique identification of any instance of a role.

Table 1: Risk analysis summary
(from the template defined in annex A of ETSI GS NFV-SEC 006 [5])

A Security Environment		
a.1 Assumptions		
Label	Assumptions	Citation
a.1.1	Internal attackers have access to the network	See clause 4.0
a.1.2	NFV- MANO functional blocks and reference points support NFV management entities	See clause 4.0
a.1.3	Internal attackers have access to the NFVO	See clause 4.1
a.1.4	NFVO supports NFV package operations	See clause 4.1
a.1.5	Internal attackers have access to VIM	See clause 4.3
a.1.6	VNFM supports VNF's management operations	See clause 4.2
a.1.7	Internal attackers are attached to the network	See clause 4.0
a.1.8	NFVO supports Network service instances and VNF instances operations	See clause 4.1
a.1.9	MANO manages many VNFI	See clause 4.0 [Figure 2]
a.1.10	An NFVI is managed by only one MANO	See clause 4.0 [Figure 2]
a.1.11	The VIM and VNFM may be virtualised entities created by NFVO on demand	See clause 4.2 and 4.3
a.2 Assets		
a.2.1	NFV- MANO functional blocks and reference points	
a.2.2	The credentials of Authorized administrators with legitimate access to the NFV- MANO functional blocks and reference points	
a.2.3	The credentials of Authorized administrators with legitimate access to the NFVO	
a.2.4	The credentials of Authorized administrators with legitimate access to the VIM	
a.3 Threat agents		
a.3.1	Active probe on interface	
a.3.2	Users or administrators with escalated privilege able to access the NFV- MANO functional blocks and reference points	
a.4 Threats		
a.4.1	Masquerade of NFVO to VIM	
a.4.2	Masquerade of NFVO to VNMF	
NOTE 1: Threats from transport level attacks, e.g. Denial of Service attacks, are not considered as they are not viewed as specific to MANO but rather address any service on any network. NOTE 2: Attacks arising from poor implementation of MANO functionality are similarly not considered as they are not viewed as specific to MANO.		

B Security Objectives		
b.1 Security objectives for the asset		
b.1.1	See clause 6	
b.2 Security objectives for the environment		
b.2.1	See clause 6	
C IT Security Requirements		
c.1 asset security requirements		
c.1.1 asset security functional requirements		
Label	Requirement	Dependencies [i.2]
c.1.1.1	The receiving party shall not allow any actions from received data before successfully identifying and verifying the identity of the transmitting party	FIA_UID FIA_UAU
c.1.1.2	The transmitter of a message shall provide means that will allow for the determination of any of modification, deletion, insertion, or replay has occurred	FDP_UIT
c.1.1.3	The receiver of a message shall be able to determine if any of modification, deletion, insertion, or replay has occurred	FPD_UIT
c.1.1.4	The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred	FDP_SDI
c.1.1.5	Data transferred over any internal interface of MANO shall be protected to prevent disclosure of data to unauthorized entities	FDP_UCT
c.1.1.6	Security events or alarms shall be recorded in an Audit log sufficient to identify the impacted element, the time and location of the event, and the outcome of the event. The severity of the event shall be noted and for severe events the impacted element shall be isolated and where practical excluded from any further activity	FAU_GEN FAU_ARP
c.1.1.7	The MANO system shall allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations	FDP_ACF
c.1.1.8	Relying parties shall not allow any actions from received data before successfully identifying and verifying the location of the relied upon party	FIA-UID FIA_UAU
c.1.2 asset security assurance requirements		
c.1.2.1	See clause 6 of the present document and ISO/IEC 15408 class [i.2]	
c.2 Environment security requirements (OPTIONAL)		
c.2.1	None	
D Application notes (OPTIONAL)		
None		
E Rationale		
To strengthen the security of MANO		

6 Summary of Security Requirements

The present document addresses the security requirement specifications and threat analysis for MANO components (NFVO, VNFM and VIM) and MANO reference point's Or-Vnfm, Or-Vi, Vi-Vnfm. The security analysis addressed in the present document shows that there are various threats that pose significant risks for the MANO components and reference points. As pointed out in table 1 threats and malicious activities like malware and DDoS attacks may cause the risk level to increase but such threats are not considered as specific to MANO but apply equally to any networked software based system.

- The receiving party shall not allow any actions from received data before successfully identifying and verifying the identity and location of the transmitting party:
  - When translated to countermeasures this requirement should eliminate most elements of masquerade and when placed alongside access control schemes should also eliminate most forms of privilege escalation.
- The transmitter of a message shall provide means that will allow for the determination of any of modification, deletion, insertion, or replay has occurred:
  - When translated to countermeasures this requirement will allow the transmitting party to enable a complete message and session integrity service.

- The receiver of a message shall be able to determine if any of modification, deletion, insertion, or replay has occurred:
  - When translated to countermeasures this requirement will provide for a closed loop message and session integrity service.
- The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred:
  - When translated to countermeasures this requirement provides for proof of integrity of the data stores used for VM images and when combined with the data transfer integrity services.
- Data transferred over any internal interface of MANO shall be protected to prevent disclosure of data to unauthorized entities:
  - When translated to countermeasures this requirement will provide confidentiality of internal transfers probably using an encryption mode of well-known network protocols.
- The MANO system shall allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations:
  - When translated to countermeasures this requirement is expected to enforce some form of attribute based access control and attribute based or multi-factor authentication (where location is one of the behavioural factors). In implementing countermeasures and mechanisms to allow geo-restrictions the ability of the implementation to meet legal and policy obligations with respect to the location where data can be processed is likely to be improved.
- Relying parties shall not allow any actions from received data before successfully identifying and verifying the location of the relied upon party:
  - As above this requirement leads to multi-attribute authentication and authorization schemes being deployed.

NOTE: The location restriction requirements may apply to pairs (peers) of components with both source and sink being deployed in the same geographic area (e.g. for performance), or in the same geographic jurisdiction (e.g. for legal and policy compliance).

It is acknowledged that when an NFV system is provisioned it will provide the ability for communications service providers to significantly transform their networks over the next few years and beyond, so as security requirements and threat analysis for each MANO component and reference points will play a vitally important role for securing the NFV-MANO and all the applications trusting on them. These inputs are limited, but it shall provide guidance on which entity and what kind of threat to focus on in order to reduce the overall risks of MANO components and interfaces most efficiently. This analysis is a continual process that should be reviewed regularly to ensure that security requirement and specification shall meet the required objective. Compliance with the present document significantly reduces the security risks for NFV MANO system components, in terms of authenticity, integrity, confidentiality and privacy. The security and threat analysis should be an integral part of an overall lifecycle of NFV system.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Dr. Pradheepkumar Singaravelu, NEC Corporation

Other contributors:
Mr. Prabhu T, NEC Europe Ltd

Dr. Sivabalan Arumugam, NEC Europe Ltd

Dr. Anand R. Prasad, NEC Corporation

Dr. Zarrar Yousaf, NEC Europe Ltd

Mr. Kapil Sood, Intel Corporation

Dr. Ashutosh Dutta, AT&T

Mr. Ihab Guirguis, Sprint

Mr. Esa Salahuddin, Cisco

Mr. Diego Lopez, Telefonica

Mr. Scott Cadzow, C3L UK

Mr. Michael Bilca, OTD

Mr.Olivier Legrand, Orange

Annex B (informative): Bibliography

- ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".
- ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

Annex C (informative): Change History

Date	Version	Information about changes
February 2016	0.0.1	Updating the scope and TOC for the SEC014 draft. Both scope and TOC was approved during NFVSEC#65 meeting
March 2016	0.0.2	Below mentioned contribution document accepted in NFVSEC#68 meeting: NFVSEC(16)000017r3_General_Security_Threats_and_requirements in clause 5 NFVSEC(16)000018r3_Threat_Analysis_for_NFV_Or-Vi_reference point in clause 7.1 NFVSEC(16)000019r3_Threat Analysis_for_NFV_Vi-Vnfm_reference point in clause 7.2 NFVSEC(16)000020r3_Threat_Analysis_for_NFV_Or-Vnfm_reference_point in clause 7.3 Annex A updates A.1 Risk analysis and assessment for general threats and requirements A.2 Risk analysis and assessment for Or-Vi reference point A.3 Risk analysis and assessment for Vi-Vnfm reference point A.4 Risk analysis and assessment for Or-Vnfm reference point
April 2016	0.0.3	Below mentioned contribution document accepted in NFVSEC#74 meeting: NFVSEC(16)000091 Threat Analysis for NFV Orchestrator in clause 6.1 NFVSEC(16)000092 Threat Analysis for VNF Manager(s) in clause 6.2 Annex A updates A.5 Risk analysis and assessment for NFV orchestrator A.6 Risk analysis and assessment for VNF Manger(s)
May 2016	0.0.4	Below mentioned contribution document accepted in NFVSEC#75 meeting: NFVSEC(16)000093r1CoverPage_Threat Analysis for Virtualised Infrastructure Manager(s)_r1 in clause 6.3 NFVSEC(16)000119CoverPage_Additional text to clause 6.3.2-Threat Analysis for Virtualised Infrastructure Manager(s) Annex A updates A.7 Risk analysis and assessment for Virtualised Infrastructure Manager
June 2016	0.0.5	Below mentioned contribution document accepted in NFVSEC#78 meeting: NFVSEC(16)077003r1 Additional Text to clause 6.1 Threat Analysis for NFV Orchestrator NFVSEC(16)077004r1 Additional text to clause 6.2 Threat Analysis for VNF Manager(s)
July 2016	0.0.6	Below mentioned contribution document accepted in NFVSEC#81 meeting: NFVSEC(16)000141 [SEC 014] clause 8 Summary of Security Requirements NFVSEC(16)000142 [SEC 014] clause 1 MANO and Interfaces
August 2016	0.0.7	Updated the ETSI Comments
May 2017	0.0.8	Changing Internal Interface to reference point (recommended by IFA WG). Some Editorial changes recommended by SECWG and Incorporating Orange comments OTD comments
August 2017	0.0.9	Incorporated the teleconference meeting update
September 2017	0.0.10	Incorporated the teleconference meeting update by OTD
December 2017	0.0.11	Incorporated the NFV#19 meeting review comments
January 2018	0.0.12	Alignment with style and format of SEC006
February 2018	0.0.13	Incorporated review comments NFVSEC#117, 118 and 119. This version includes ETSI edit comments also
February 2018	0.0.14	Incorporated review comments from TSC and NFVSEC#120 meeting
March 2018	0.0.15	Incorporated review comments during NFV#20 Closing plenary meeting

History

Document history		
V3.1.1	April 2018	Publication