ETSI GS NFV-SEC 024 V1.1.1 (2026-04)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV); Security; Security Management

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-SEC024

Keywords
cyber security, network monitoring, NFV,
policy management, security,
security management, threat analysis,
threat intelligence

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

Contents

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 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 describes the whole-system security framework required to manage NFV-based virtualised networks securely. The present document provides an architecture and capabilities for security management, which includes MANO, NFVI (including the underlying compute hardware infrastructure), the virtualised function application layer (e.g. 5G) and PNFs. The security management architecture addresses all network and VNF lifecycle stages from VNF onboarding, instantiation, VNF instance runtime and post-VNF instance teardown cleanup.

The present document considers both baseline security requirements and policies which need to be applied across all network functions and additional requirements that are applicable to sensitive network functions.

The present document is intended to include, update and replace NFV Security Management and Monitoring concepts that were defined in ETSI GS NFV-SEC 013 [i.2].

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 in the ETSI docbox.

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 026 (V3.2.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification".

[2] ETSI GS NFV-SEC 025: "Network Functions Virtualisation (NFV)Release 4; Security; Secure End-to-End VNF and NS management specification".

[3] ETSI GS NFV-SEC 021: "Network Functions Virtualisation (NFV) Release 5; Security; VNF Package Security Specification".

[4] ETSI GS NFV-SEC 026: "Network Functions Virtualisation (NFV) Release 5; Security; Isolation and trust domain specification".

[5] ETSI TS 104 000: "Lawful Interception (LI); Internal Network Interface X0".

[6] ETSI TS 104 007: "Lawful Interception (LI); Lawful Interception Architecture".

[7] NIST SP 800-88 Rev.2: "Guidelines for Media Sanitization".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Security Agent: distributed security function performing security monitoring/management with a local actionable behaviour

Security Management: functionality that applies security policy to a virtualised network based on both predefined default policy and active analysis of information provided through security monitoring

NOTE: Security management actions will consist of both passive default security policy automatically applied by NFV-MANO (including through VNFDs or of vendor / CSP configuration) and active real-time security management actions where the Security Management system actively updates or overrides default passive policy.

Security Monitoring: functionality that collects and performs analysis of relevant events from across the virtualised network, which allow the Security Management and Monitoring system to make informed security management decisions

NOTE: Security monitoring is not restricted to real-time (or near real-time) collection and analysis of network events. Virtual network-wide monitoring will include security analysis of longer-term logging, AI data set analysis and human intelligence to predict and update monitoring criteria.

3.2 Symbols

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

3.3 Abbreviations

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

ABAC	Attribute Based Access Control
AI/ML	Artificial Intelligence / Machine Learning
A-SA	Adjunct Security Agent
CA	Certificate Authority
CSP	Communication Service Provider
DLP	Data Loss Prevention
EOL	End-Of-Life
E-SM	Embedded Security Agent
FQDN	Fully Qualified Domain Name
GUID	Globally Unique Identifier
HA	High Availability
HMEE	Hardware-Mediated Execution Enclave
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I-SA	Infrastructure Security Agent
M-SA	MANO Security Agent
OSSM	OSS/BSS Security Manager