ETSI GS NFV-SEC 028 V4.5.1 (2023-11)

Network Functions Virtualisation (NFV) Release 4; Security; Security Assurance Specification (SCAS) for Generic NFV-MANO

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-SEC028

Keywords
MANO, NFV, SCAS, security, test

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 defines the security assurance of generic NFV-MANO products. The outcome of the present document expects the security assets, security threats, security requirements and test cases for evaluating the generic security of NFV-MANO products. In the present document, the security assurance methodology introduced in 3GPP specifications will be leveraged. Security test cases including testing goals, testing steps, and evidence of testing results will be produced for evaluating whether the security requirements are implemented by NFV-MANO products.

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 TS 133 117: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Catalogue of general security assurance requirements (3GPP TS 33.117)".

[2] ETSI GS NFV-SOL 013: "Network Functions Virtualisation (NFV) Release 3; Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs".

[3] ETSI GS NFV-SEC 022: "Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access".

[4] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[5] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[6] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

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

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 TR 133 926: "LTE; 5G; Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (3GPP TR 33.926)".

[i.2] ETSI GR NFV 003: "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 GR NFV 003 [i.2] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.2] apply.

4 Catalogue of security requirements and related test cases for generic part of NFV-MANO products

4.1 Introduction

The present clause describes security functional requirements and the corresponding test cases for generic part of NFV-MANO products.

4.2 Security functional requirements and related test cases

4.2.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases, independent of a specific NFV-MANO product class. In particular the proposed security requirements are classified in two groups:

- Security functional requirements deriving from ETSI specifications and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in the ETSI specifications but whose support is also important to ensure a NFV-MANO product conforms to a common security baseline detailed in clause 4.2.3.

By default all test cases in clause 4.2 of ETSI TS 133 117 [1] can be applied to generic NFV-MANO products. Any additions, deletions or modification are listed separately in the following clauses.

4.2.2 Security functional requirements on the NFV-MANO deriving from ETSI specifications and related test cases

4.2.2.1 Security functional requirements deriving from ETSI NFV specifications - general approach

The present clause describes the general approach taken towards security functional requirements deriving from ETSI specifications and the corresponding test cases, independent of a specific network product class.

It is assumed for the purpose of the present SCAS that a network product conforms to all mandatory security-related provisions in ETSI specifications pertaining to it, in particular:

- all ETSI NFV SEC specifications (security specifications) that are pertinent to the network product class;
- other ETSI specifications that make reference to security specifications or are referred to from one of them.

Security procedures pertaining to a network product are typically embedded in non-security procedures and are hence assumed to be tested together with them.

It is the purpose of the present SCAS to identify security requirements from the NFV security architecture that require special attention in testing as they may:

a) lead to vulnerabilities when not satisfied;

b) not be captured through ordinary testing activity for non-security procedures;

c) address security-relevant failure cases and exceptions or 'negative' requirements of the kind: "The network product shall not…".

It is not an intention of the present document to provide an exhaustive set of test cases that would be sufficient to demonstrate conformance of all security procedures with the above-mentioned specifications.

4.2.2.2 Security functional requirements derived from ETSI specifications - general Interface aspects

4.2.2.2.1 Introduction

The purpose of clauses 4.2.2.2.1 and 4.2.2.2.2 is to identify and describe the general baseline requirements from NFV security architecture and the corresponding test cases. The general baseline requirements are applicable to all NFV Management and Orchestration (MANO) functions.

4.2.2.2.2 Protection at the transport layer

Requirement Name: Protection at the transport layer

Requirement Reference: ETSI GS NFV-SOL 013 [2], clause 4.1, clause 8.1, clause 8.2.2, clause 8.2.5, clause 8.3.2, ETSI GS NFV-SEC 022 [3], clause 5.3

Requirement Description:

"*APIs shall use TLS version 1.2 as defined by IETF RFC 5246 [4] or later. Versions of TLS earlier than 1.2 shall neither be supported nor used*". As specified in ETSI GS NFV-SOL 013 [2], clause 4.1.

"*As part of setting up the TLS tunnel for the access token request, the client and authorization server perform mutual authentication based on X.509 certificates. As part of the access token request, the client presents its client identifier*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.1.

"*In order to ensure that no third party can eavesdrop on sensitive information such as client credentials or access tokens, TLS is used to protect the transport of HTTP messages. If mutual authentication using TLS protocol is used, then the producer/server is authenticated to the consumer/client, but also the consumer/client is authenticated by the producer/server at the same time. To facilitate this mutual authentication, the server shall request a client certificate*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.1.

"*As a precondition for step 1 to succeed, a TLS channel has been set up between API consumer and authorization server. Unless the API consumer is allowed to use client password, the API consumer and the authorization server have mutually authenticated based on TLS certificates during TLS tunnel set-up*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.2.2.

"*Unless the API consumer is allowed to use client password, the API producer and the notification authorization server have mutually authenticated based on TLS certificates during TLS tunnel set-up*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.2.5.

"*As a precondition for the access token request to succeed, client and authorization server shall have mutually authenticated based on TLS certificates during TLS tunnel set-up, unless the use of client password is allowed for the client*". As specified in ETSI GS NFV-SOL 013 [2], clause 8.3.2.

"*The TLS connection between the client and the authorization server token endpoint shall be established with mutual TLS X.509 certificate authentication, i.e. using certificate and certificate verify messages sent during the TLS Handshake*". As specified in ETSI GS NFV-SEC 022 [3], clause 5.3.

Threat References: ETSI GS NFV-SEC 012 [7], clause 6.5, Weak cryptographic algorithms.

Test case:

Test Name: TC_PROTECT_TRANSPORT_LAYER

Purpose:

Verify that TLS protocol for NFV-MANO API mutual authentication and NFV-MANO API transport layer protection is implemented in the network products based on the profile required.

Procedure and execution steps:

Pre-Conditions:

Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the requirements specified in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] (3GPP Release 16 or later).

Execution Steps

1) The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.

2) The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test. Additionally, verify that the certificate used by the product under test is signed by a trusted certificate authority.

3) The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile or the certificate presented is not signed by a trusted certificate authority.

Expected Results:

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the requirements in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] and the server certificate is signed by a trusted certificate authority.

- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in clause 6.2.3 (if TLS version 1.2 as defined by IETF RFC 5246 [4] is used) or clause 6.2.2 (if TLS version 1.3 as defined by IETF RFC 8446 [5] is used) of ETSI TS 133 210 [6] or the certificate is not signed by a trusted certificate authority.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.