***Disclaimer***

The present document has been produced and approved by the <long ISGname> (<short ISGname>) 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.

ETSI GS NFV-SEC 023 V0.0.1 (2019-10)

**Group Specification**

Network Functions Virtualisation (NFV);

Security;

Container Security Specification

Release 4

<

**This DRAFT is a working document of ETSI. It is provided for information only and is for future development work within ETSI. DRAFTS may be updated, deleted, replaced, or obsoleted by other documents at any time.**

**ETSI and/or its Members have no liability for any current or further use/implementation of the present DRAFT.**

**Do not use as reference material.
Do not cite this document other than as "work in progress."**

**Any draft approved and PUBLISHED shall be obtained exclusively as a deliverables via the ETSI Standards search page at:**

<http://www.etsi.org/standards-search>

Reference

DGS/NFV-SEC023

Keywords

Container, Cyber Security, 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](http://www.etsi.org/standards-search#Pre-defined Collections)

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](http://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>

***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 2019.

All rights reserved.

**DECT**TM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
**3GPP**TM and **LTE**TM 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.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

Executive summary 4

Introduction 4

1 Scope 5

2 References 5

2.1 Normative references 5

2.2 Informative references 5

3 Definition of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 6

3.3 Abbreviations 6

4 NFV deployment using containers 6

4.1 Introduction 6

4.2 Framework Overview 6

5 Threat Analysis 6

5.1 Application-to-container attacks 6

5.2 Containers-to-host attacks 6

5.3 Containers-to-containers 6

5.4 Host-to-containers attacks 6

6 Security Solutions 7

6.1 Software Solutions 7

6.1.1 Namespaces 7

6.1.2 CGroups 7

6.1.3 Capabilities 7

6.1.4 Seccomp 7

6.2 Hardware Solutions 7

6.2.1 Trusted Execution Support 7

6.2.1.1 vHMEE in host OS kernel 7

6.2.2.2 vHMEE in dedicated container 7

6.2.2 Secure Enclaves 7

Annex A (normative or informative): Title of annex 7

Annex B (normative or informative): Title of annex 8

B.1 First clause of the annex 8

B.1.1 First subdivided clause of the annex 8

Annex (informative): Authors & contributors 9

Annex (informative): Bibliography 10

Annex (informative): Change History 11

History 12

# 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](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 Network Function Virtualization (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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

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

# Executive summary

# Introduction

# 1 Scope

The present document specifies the security and hardening requirement for running NFV software (e.g. VNFs) in containerised environments. This specification covers as a minimum a threat analysis for a container based NFV deployment, a state of the art on container security, an isolation analysis with namespaces. This document proposes a set of solutions for attack surface reduction and privilege limitation and analyses existing solutions for resource limitations (cgroups); Hardware protections (HMEE); Container hardening (inc patching); Containers in VMs and containers on bare metal. The consider alignment with existing IFA specifications and reports (e.g. IFA 029).

# 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](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] <Standard Organization acronym> <document number>: "<Title>".

[2] <Standard Organization acronym> <document number>: "<Title>".

## 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] ETSI GR NFV-IFA 029: "Network Functions Virtualisation (NFV); Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"

[i.3] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

#  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:

**OS Container:** a virtualisation container utilizing a shared operating system (OS) kernel of its host.

NOTE: The host providing the shared OS kernel can be a physical compute node or another virtualisation container.

## 3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

## 3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

# 4 NFV deployment using containers

## 4.1 Introduction

## 4.2 Framework Overview

# 5 Threat Analysis

## 5.1 Application-to-container attacks

## 5.2 Containers-to-host attacks

## 5.3 Containers-to-containers

## 5.4 Host-to-containers attacks

# 6 Security Solutions

## 6.1 Software Solutions

## 6.1.1 Namespaces

## 6.1.2 CGroups

## 6.1.3 Capabilities

## 6.1.4 Seccomp

## 6.2 Hardware Solutions

## 6.2.1 Trusted Execution Support

## 6.2.1.1 vHMEE in host OS kernel

## 6.2.2.2 vHMEE in dedicated container

## 6.2.2 Secure Enclaves

Annex A (normative or informative):
Title of annex

Annex B (normative or informative):
Title of annex

# B.1 First clause of the annex

## B.1.1 First subdivided clause of the annex

Annex (informative):
Authors & contributors

The following people have contributed to the present document:

**Rapporteur**:
Title, Firstname, Lastname, company

**Other contributors**:Title, Firstname, Lastname, company

Annex (informative):
Bibliography

Annex (informative):
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| <Month year> | <#> | <Changes made are listed in this cell> |
|  |  |  |
|  |  |  |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

*Latest changes made on 2019-01-08*