

ISO/IEC ~~JTC1/SC 27 WG 4~~
~~Date: 2023-05-12~~
~~ISO/IEC DIS FDIS 27033--7:2023(E)~~
ISO/IEC-JTC 1/SC-27/WG-4
Secretariat: DIN
~~Date: 2023-07-14~~
Information technology — Network security — Part 7: Guidelines for
network virtualization security

iTeh STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-8c23-1d1a4951/iso-iec-fdis-27033-7>

Style Definition: Heading 1: Indent: Left: 0 pt, First line: 0 pt, Tab stops: Not at 21.6 pt
Style Definition: Heading 2: Font: Bold, Tab stops: Not at 18 pt
Style Definition: Heading 3: Font: Bold
Style Definition: Heading 4: Font: Bold
Style Definition: Heading 5: Font: Bold
Style Definition: Heading 6: Font: Bold
Style Definition: zzCopyright
Style Definition: ANNEX
Style Definition: AMEND Terms Heading: Font: Bold
Style Definition: AMEND Heading 1 Unnumbered: Font: Bold
Style Definition: List Bullet: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab
Style Definition: List Bullet 2: Indent: Left: 14.15 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 32.15 pt, List tab
Style Definition: List Bullet 3: Indent: Left: 28.3 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 46.3 pt, List tab
Style Definition: List Bullet 4: Indent: Left: 42.45 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 60.45 pt, List tab
Style Definition: List Bullet 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab
Style Definition: List Number: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab
Style Definition: List Number 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO ~~copyright office~~ Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Tel. +41 22 749 01 11

Fax +41 22 749 09 47

E-mail ~~copyright@iso.org~~

Web ~~www.iso.org~~

Email: ~~copyright@iso.org~~

Website: ~~www.iso.org~~

Published in Switzerland.

Formatted: Section start: New page

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 27033-7

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-fdis-27033-7>

Formatted: Space After: 30 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: Bold

Formatted: None, Tab stops: Not at 20 pt + 28 pt

Contents

Foreword	i
Introduction	ii
1— Scope	1
2— Normative references	1
3— Terms and definitions	1
4— Symbols and abbreviated terms	2
5— Overview	3
5.1— General.....	3
5.2— Description of network virtualization.....	3
5.3— Security model.....	4
5.3.1— Model of network virtualization security.....	4
5.3.2— Network virtualization components.....	5
6— Security threats	6
7— Security recommendations	7
7.1— General.....	7
7.2— Confidentiality.....	7
7.3— Integrity.....	8
7.4— Availability.....	8
7.5— Authentication.....	8
7.6— Access control.....	8
7.7— Non repudiation.....	8
8— Security controls	10
8.1— General.....	10
8.2— Virtual network infrastructure security.....	10
8.3— Virtual network function security.....	11

Edited DIS -
MUST BE USED
FOR FINAL
DRAFT

8.4	Virtual network management security	12
8.4.1	SDN controller security	12
8.4.2	NFV orchestrator security	12
9	Design techniques and considerations	12
9.1	Overview	12
9.2	Integrity protection of platform	13
9.3	Hardening for network virtualization	14
9.4	API authentication and authorization	14
9.5	Software defined security for virtual network	14
Annex A (Informative)	Use cases of network virtualization	16
A.1	Software defined wide area network	16
A.2	Network slicing	16
A.3	Virtual WAF	17
A.4	Cloud CDN with centralized control	18
Annex B (Informative)	Detailed security threat description of network virtualization	19
B.1	Security threats to virtual network infrastructure	19
B.2	Security threats to virtual network functions	19
B.2.1	Security threats to virtual network function	19
B.2.2	Security threats to software defined networks	20
B.3	Security threats to virtual network management	21
B.3.1	General	21
B.3.2	Software defined networks controller security	21
B.3.3	Management and orchestration security	21
B.3.4	Interface security	22
B.4	Virtualization specific threats	22
B.4.1	Threats to security segmentation	22
B.4.2	Threats to resource exhaustion	22

ITeH STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 27033-7
<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c251d1a4951/iso-iec-fdis-27033-7>

Formatted: Space After: 30 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: Bold

B.4.3 Threats to central mangement 22

Bibliography 23

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 2

5 Overview 4

 5.1 General 4

 5.2 Description of network virtualization 5

 5.3 Security model 5

 5.3.1 Model of network virtualization security 5

 5.3.2 Network virtualization components 8

6 Security threats 9

7 Security recommendations 10

 7.1 General 10

 7.2 Confidentiality 10

 7.3 Integrity 10

 7.4 Availability 11

 7.5 Authentication 11

 7.6 Access control 11

 7.7 Non-repudiation 11

8 Security controls 12

 8.1 General 12

 8.2 Virtual network infrastructure security 13

 8.3 Virtual network function security 13

Edited DIS -
MUST BE USED
FOR FINAL
DRAFT

8.4	Virtual network management security	14
8.4.1	SDN controller security	14
8.4.2	NFV orchestrator security	15
9	Design techniques and considerations	15
9.1	Overview	15
9.2	Integrity protection of platform	16
9.3	Hardening for network virtualization	16
9.4	API authentication and authorization	16
9.5	Software defined security for virtual network	17
Annex A (informative)	Use cases of network virtualization	19
A.1	Software-defined wide-area network	19
A.2	Network slicing	20
A.2 —	Network slicing based on SDN and NFV	21
A.3	Virtual WAF	21
A.4	Cloud CDN with centralized control	22
Annex B (informative)	Detailed security threat description of network virtualization	23
B.1	Security threats to virtual network infrastructure	23
B.2	Security threats to virtual network functions	23
B.2.1	Security threats to virtual network function	23
B.2.2	Security threats to software-defined networks	24
B.3	Security threats to virtual network management	25
B.3.1	General	25
B.3.2	Software-defined networks controller security	25
B.3.3	Management and orchestration security	25
B.3.4	Interface security	25
B.4	Virtualization-specific threats	26
B.4.1	Threats to network segmentation	26

Formatted: Space After: 30 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: Bold

B.4.2 Threats to resource exhaustion.....	26
B.4.3 Threats to centralized management.....	26
Bibliography.....	27

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC FDIS 27033-7

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-fdis-27033-7>

~~Edited DIS~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

Formatted: Font: 11.5 pt

Formatted: Justified

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

Formatted: English (United Kingdom)

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of documents, document, should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Attention is drawn to the possibility that some of the elements implementation of this document may be involve the subject of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <http://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding_standards.

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

This document was prepared by Joint Technical Committee ISO/IEC JTC-1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

A list of all parts in the ISO/IEC 27033 series can be found on the ISO and IEC websites.

Formatted: Pattern: Clear

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Space After: 30 pt, Line spacing: Exactly 12 pt

Formatted: Font: 11.5 pt

Formatted: Font: Bold

Introduction

The purpose of this document is to address the key challenges and risks of network virtualization security. Network virtualization includes virtual network infrastructure, virtual network function, virtual control and resource management. This document aims to:

- 1) identify security risks of network virtualization;
- 2) propose a network virtualization security model;
- 3) propose security guidelines for virtual network infrastructure, virtual network function, virtual control and resource management.

Formatted: List Continue 1, No bullets or numbering, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left

This document intends to help stakeholders in understanding the main characteristics of network virtualization security. For example, this document can help software and hardware suppliers to securely design and develop products that implement network virtualization, and help operators to evaluate the security of these products and deploy them securely for network services. By proposing security guidelines, this document aims to help the industry to improve system security that is built on network virtualization technology.

The target audience can include the network equipment vendors, network operators, internet service providers and software service providers.

With the rapid development of IT technologies such as cloud computing, IT systems and communication systems are increasingly evolving with the adoption of virtualization technology. Virtualization enables systems to have high agility, flexibility and scalability with low cost, but at the same time, introduces ~~lots~~ ~~of~~ many security challenges.

ISO/IEC FDIS 27033-7

<https://standards.iteh.ai/catalog/standards/sist/75435c1a-2159-4810-b1bf-8c231d1a4951/iso-iec-fdis-27033-7>

~~Edited DIS~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Information technology — Network security—Part 7: Guidelines for network virtualization security

Formatted: Left

1 Scope

This document aims to identify security risks of network virtualization and proposes guidelines for the implementation of network virtualization security.

Overall, this document intends to considerably aid the comprehensive definition and implementation of security for any organization’s virtualization environments. It is aimed at users and implementers who are responsible for the implementation and maintenance of the technical controls required to provide secure virtualization environments.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org>

3.1 network virtualization

technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple heterogeneous virtual networks can simultaneously coexist over the shared infrastructures

Note 1 to entry: Network virtualization allows the aggregation of multiple resources and makes the aggregated resources appear as a single resource.

[SOURCE: ISO/IEC TR 29181-1:2012, 3.3]

3.2 network functions virtualization NFV

technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks

Note 1 to entry: This includes the aggregation of multiple resources in a provider and appearing as a single resource.

[SOURCE: ISO/IEC TR 22417:2017, 3.8]

3.3

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: std_year

Formatted: std_section

Formatted: Line spacing: At least 11.5 pt

Formatted: Line spacing: At least 11 pt

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Font: Not Bold

Formatted: Font: Not Bold

ISO/IEC FDIS 27033-7:2023(E)

Formatted: Justified

Formatted: Font: 11.5 pt

software-defined networking

set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner

Formatted: Line spacing: At least 11.5 pt

[SOURCE: ITU-T Y.3300:2014, 3.2.1]

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

3.4

virtual machine

virtual data processing system that appears to be at the disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.4564]

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

3.5

container

isolated execution environment for running software that uses a virtualized operating system kernel

[SOURCE: ISO/IEC 22123-1:2021/2023, 3.1312.4]

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Font: Italic

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Formatted: Pattern: Clear

3.6

orchestrator

tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into *containers*, (3.5), and manage the running containers

[SOURCE: NIST SP 800-190]

3.7

service function chain

ordered set of abstract functions and ordering constraints that are applied to packets and/or frames and/or flows selected as a result of classification

[SOURCE: IETF RFC 7665, modified — removed “a service function chain defines an” at the beginning of the definition and replaced “must” with “are” in the definition.]

Formatted: Pattern: Clear

Formatted: Pattern: Clear

4 Abbreviated terms

The following abbreviated terms apply to this document.

5G	the 5th ^{5th} generation mobile network
AMF	access and mobility management function
API	application programming interface
AUSEF	authentication server function
CDN	content delivery network
API	application programming interface
AUSEF	authentication server function
CDN	content delivery network
CIS	centre for internet security
DoS	denial of service

Formatted Table

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Edited DIS -
MUST BE USED
FOR FINAL
DRAFT