INTERNATIONAL STANDARD

ISO/IEC 27070

First edition
2021-12

Information technology — Security techniques — Requirements for establishing virtualized roots of trust

Technologies de l'information — Techniques de sécurité — Exigences relatives à l'établissement de racines de confiance virtualisées



Reference number
ISO/IEC 27070:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Functional view ... **3**
5.1 Overview ... 3
5.2 Hardware layer components ... 4
5.2.1 General ... 4
5.2.2 Functional requirements of key components ... 4
5.2.3 Security requirements of key components ... 4
5.3 VMM layer components ... 5
5.3.1 Functional requirements of key components ... 5
5.3.2 Security requirements of key components ... 6
5.4 VM layer components ... 7
5.5 Cloud OS layer components ... 8
5.5.1 General ... 8
5.5.2 Functional requirements of key components ... 8
5.5.3 Security requirements of key components ... 8
6 Activity view ... **9**
6.1 General ... 9
6.2 Transitive trust ... 9
6.2.1 General ... 9
6.2.2 Transitive trust in host ... 10
6.2.3 Transitive trust in VMM ... 10
6.2.4 Transitive trust in VM ... 10
6.3 Integrity measurement ... 10
6.4 Remote attestation ... 11
6.5 Data protection ... 12
6.5.1 General ... 12
6.5.2 Data binding ... 12
6.5.3 Data sealing ... 13
6.6 vTM migration ... 14
Annex A (informative) **Relationship between activity and functional views** ... **16**
Bibliography ... **18**

© ISO/IEC 2021 – All rights reserved

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.

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 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. 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 patents.iec.ch).

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.

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

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.

© ISO/IEC 2021 – All rights reserved

Introduction

Trusted computing is a kind of security technology based on hardware trusted modules, which aims to ensure that a computer behaves as expected. The trusted computing technology has been developing fast since its establishment in the 1980s.

The emergence of cloud computing provides a new application scenario for trusted computing technology. Trust can be established in VMs using a RoT on the physical machine and a virtualized RoT in the VM and mechanism to bind them together to provide assurance they are on the same machine. The trusted migration of a VM could use trusted computing to establish trust in the state of the source and destination physical machines (including their VMM software) and components involved in the migration process. In the cloud computing environment, a single physical RoT only provides limited resources and computing efficacy, which is not enough for the large number of VMs on one server. To address this issue, virtualized RoTs are used. Using virtualization technology to create multiple virtualized RoTs on a single physical platform, providing a virtualized RoT for each VM, combined with cryptographic technology to support secure and trusted migration of VMs, thereby building a trusted cloud computing environment. The establishment procedure of virtualized RoTs consists of multiple steps, and any security problem in any step diminishes the trustworthiness of virtualized RoTs, resulting in an inability to establish trust using the virtualized RoTs.

The goal of the document is to provide a unified approach to virtualize RoTs based on hardware trusted modules.

© ISO/IEC 2021 – All rights reserved

Information technology — Security techniques — Requirements for establishing virtualized roots of trust

1 Scope

This document specifies requirements for establishing virtualized roots of trust.

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
attestation key
AK
particular type of *trusted module* (3.7) signing key that has a restriction on its use, in order to prevent forgery

3.2
endorsement key
EK
key that is used in a process for the issuance of *attestation key* (3.1) credentials and to establish a platform owner

3.3
integrity measurement
process of calculating the hash value of the measured object using the cryptographic hash algorithm

3.4
root of trust
RoT
component that needs to always behave in the expected manner because its misbehaviour cannot be detected

Note 1 to entry: The complete set of roots of trust has at least the minimum set of functions to enable a description of the platform characteristics that affect the trust of the platform.

[SOURCE: ISO/IEC 11889-1, 3.59, modified — The abbreviated term has been added.]

3.5
remote attestation
RA
process of evaluating integrity measurements generated using a *root of trust* (3.4) for measurement, storage and reporting to establish trust in a platform remotely

© ISO/IEC 2021 – All rights reserved

3.6
sensitive information
information is sensitive that the *trusted module* (3.7) does not allow access to the information without proper authority

Note 1 to entry: An example of sensitive information in a trusted module is the private of an asymmetric key.

3.7
trusted module
TM
module for trusted computing providing integrity measurement, integrity report, cryptographic service, random number generation, secure storage functions and a set of platform configuration registers

Note 1 to entry: There are several implementations of trusted module, such as TPM, TCM, etc.

3.8
virtual machine
VM
virtualized hardware environment in which an operating system can execute, but whose functions are accomplished by sharing the resources of a real data processing system

3.9
virtual trusted module
vTM
component associated with a single *virtual machine* (3.8) that provides the functionality described in a *trusted module* (3.7)

3.10
virtual platform configuration register
vPCR
one or more platform configuration registers within a *virtual trusted module* (3.9)

4 Symbols and abbreviated terms

BIOS	basic input/output system
CPU	central processing unit
CRTM	core root of trust for measurement
GPT	globally unique identifier partition table
KEK	key encryption key
MBR	master boot record
OS	operating system
PCR	platform configuration register
PCA	privacy certificate authority
PI	platform initialization
ROM	read-only memory
SRK	storage root key
TPM	trusted platform module

© ISO/IEC 2021 – All rights reserved