DRAFT INTERNATIONAL STANDARD

# ISO/IEC DIS 27070

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
**2020-12-14**

Voting terminates on:
**2021-03-08**

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

ICS: 35.030





This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27070:2020(E)



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

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27070 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information Security, cybersecurity and privacy protection*.

# 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 is developing fast since its establishment in the 1980s.

The emergence of cloud computing provides a new application scenario for trusted computing technology. Trusted Virtual Machines (VMs) based on a physical Root of Trust (RoT) is an effective way to ensure the secure and trusted migration of VMs in cloud. However, 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 utilized. 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 each step will diminish the robustness of virtualized RoTs, resulting in the failure of trusted functions.

This document specifies functional requirements and security requirements for establishment and operation of virtualized RoTs. The development of this standard also provides a reference for applying the trusted computing technology in the cloud computing environment. The goal of the document is to provide a unified approach to virtualize RoTs based on hardware trusted modules.

# 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

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 11889-1:2015, *Information technology — Trusted platform module library — Part 1: Architecture*

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

## 3 Terms and definitions



### 3.1 General

For the purposes of this document, the terms and definitions given in ISO/IEC 27070 apply.



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

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org.obp

### 3.2 Terms relating to security and privacy

**3.2.1**
**attestation key**
particular type of *trusted module* (3.2.8) signing key that has a restriction on its use, in order to prevent forgery

**3.2.2**
**endorsement Key**
a key that is used in a process for the issuance of *attestation key* (3.2.1) credentials and to establish a platform owner

**3.2.3**
**integrity measurement**
process of calculating the hash value of the measured object using the cryptographic hash algorithm

**3.2.4**
**protected area**
shielded locations are places (memory, register, etc.) where it is safe to operate on *sensitive information* (3.2.7)

**3.2.5**
**root of trust**
component that needs to always behave in the expected manner because its misbehavior 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 11889-1:2015]

**3.2.6**
**remote attestation**
process of evaluating integrity measurements generated using a *root of trust* (3.2.5) for measurement, storage and reporting to establish trust in a platform remotely

**3.2.7**
**sensitive information**
information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction, or loss will cause perceivable damage to someone or something

[SOURCE: ISO/IEC 2382:2015]

**3.2.8**
**trusted module**
hardware 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.



**3.2.9**
**virtual machine**
a virtualized hardware environment in which an operating system may execute, but whose functions are accomplished by sharing the resources of a real data processing system

**3.2.10**
**virtual trusted module**
component associated with a single *virtual machine* (3.2.9) that provides the functionality described in a *trusted module* (3.2.8)

**3.2.11**
**virtual platform configuration register**
one or more platform configuration registers within a *virtualized trusted module* (3.2.10)

## 4 Symbols and abbreviated terms

| | |
|---|---|
| AK | Attestation Key |
| BIOS | Basic Input/Output System |
| CPU | Central Processing Unit |
| CRTM | Core Root of Trust for Measurement |
| EK | Endorsement Key |
| 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 |
| RA | Remote Attestation |
| RoT | Root of Trust |
| ROM | Read-Only Memory |
| SRK | Storage Root Key |
| TM | Trusted Module |
| TSS | Trusted Software Stack |
| UEFI | Unified Extensible Firmware Interface |
| VM | Virtual Machine |
| VMM | Virtual Machine Monitor |
| vRTM | virtual Root of Trust for Measurement |
| vRTR | virtual Root of Trust for Reporting |
| vRTS | virtual Root of Trust for Storage |
| vSRK | virtual Storage Root Key |
| vTM | virtual Trusted Module |
| vPCR | virtual Platform Configuration Register |
| WK | Work Key |



# 5 Functional view

## 5.1 Overview

This clause provides a neutral architectural view of functional components required by trusted computing activities in the cloud computing environment, and presents the functional and security requirements for key components.

Figure 1 shows a framework of the required functional components, where specific types of functions are grouped into each layer.

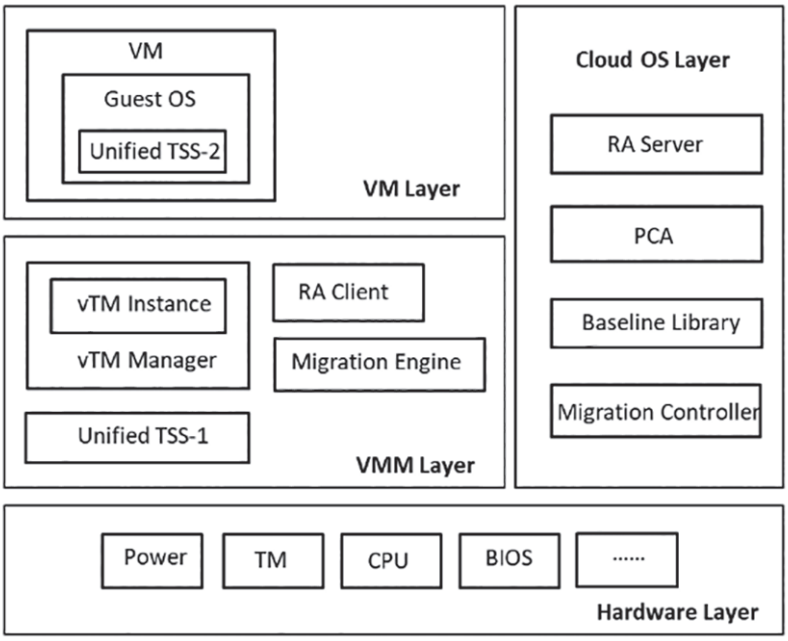


**Figure 1 — Framework of functional components**



## 5.2 Hardware layer components

At the bottom of the architecture, the hardware layer that includes hardware resources and devices is the base for building a trusted computing platform. This layer provides a Root of Trust (RoT) for the physical machine that typically offers trusted platform services for the Virtual Machine Monitor (VMM) layer.



NOTE The VMM layer is also known as the hypervisor layer.

This layer also includes the Core Root of Trust for Measurement (CRTM), the initial set of instructions executed for establishing a new chain of trust for integrity measurement. Typically, the CRTM is embedded in a CPU.

The hardware layer components include but are not limited to:

— **Power:** Powering the computer system for booting and running. TM does not monitor the power supply level, in some circumstances, TM will control the power, such as power off when trusted boot fail.

— **TM:** A trusted module on a special co-processor or chip with capabilities that include but not limited to integrity measurement, integrity reporting, generation of signatures for measured integrity values, key management, secure storage, identity verification, etc.

— **BIOS/UEFI:** A firmware with capabilities of initializing the platform, starting an Operating System (OS) loader and providing runtime services to the OS.

— **CPU:** The operating centre of the computing system.

The Power, BIOS/UEFI and Central Processing Unit (CPU) have no special functional or security features to support virtualized RoTs. Hence this document only lists the functional and security requirements for the Trusted Module (TM) in following sections.

### 5.2.1 Functional requirements of key components

#### 5.2.1.1 TM

A TM shall provide the following functions:

— Support the integrity measurement, storing, generation of signatures for measured integrity values and reporting measured values for platform.

— Support key generation for use as signature keys.

— Support cryptographic algorithms, such as hash algorithm, encryption/decryption algorithm, but are not limit to any specific sets of algorithms.

— Protect integrity measurements in the Platform Configuration Register (PCR) during system start-up.

### 5.2.2 Security requirements of key components

#### 5.2.2.1 TM

A TM shall meet the following security requirements:

— Process the instructions using the internal firmware and logic circuits, which does not depend on the OS and is not affected by external vulnerabilities.

NOTE This document does not preclude integrated TPM designs prevalent in the industry today.

— Ensure the security of confidential information, such as PCR values, keys, etc.

— Provide the secure storage area to store a Storage Root Key (SRK) to ensure the security of the key information.



## 5.3 VMM layer components

The VMM layer provides virtualization services to VMs and ensures that VMs can operate independently.

This layer also provides virtualized RoTs for VMs, which includes virtual Root of Trust for Measurement (vRTM), virtual Root of Trust for Reporting (vRTR) and virtual Root of Trust for Storage (vRTS).

The VMM layer components include but are not limited to:

— **VMM:** It virtualizes the underlying hardware platform to enable multiple VMs to run in isolated environments and share the hardware resources.

— **Unified TSS-1:** It provides a unified interface for upper layer applications to utilize TM functions without considering heterogeneous Trusted Software Stack (TSS) implementations specifically.

— **vTM Manager:** It establishes and maintains the binding list between each vTM instance and VM. It is responsible for creation, instantiation, deletion, start, stop and migration of the vTM instance associated with each VM.

— **vTM Instance:** It emulates a hardware TM. Each vTM instance imitates interfaces and functions of the TM.

— **RA Client:** It retrieves and transmits the integrity evidence of host and VMM layer. It does not leak the sensitive information during communication with Remote Attestation (RA) server.

— **Migration Engine:** It provides capabilities of package, serialization and protection for vTM state data during transmission. It guarantees that only one vTM instance is active during transmission and the vTM instance is removed once it has been successfully migrated.