DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27071

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

Secretariat: **DIN**

Voting begins on:
2022-07-12

Voting terminates on:
2022-10-04

Cybersecurity — Security recommendations for establishing trusted connections between devices and services

ICS: 35.030

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27071:2022(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 27071 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information Security, cybersecurity and privacy protection*.

Introduction

With the development of the Internet of Things (IoT), Mobile Services, Cloud Computing, Big Data and Artificial Intelligence (AI), more and more scenarios require trusted connections between devices and services.

Security channels (e.g. TLS/SSL) are used between devices and services to protect confidentiality and integrity of data, but it is not enough. The service needs to distinguish data collected by sensors of the authorised device from those of other devices or data forged by adversaries. So, it should be able to ensure the data comes from the authorised device.

Conversely, the device also needs to distinguish the genuine service from unintended services or malicious services. So, it should be able to reliably identify the genuine and intended service, in particular for cloud services, which may have thousands of such services running.

Identity without a reliable root of trust can be forged, so controls are required to ensure the utilisation of reliable roots of trust (requirements for establishing reliable virtualized roots of trust as described in ISO/IEC 27070:2021).

Mutual authentication between a device and a service is needed to prevent impersonation attacks. While insufficient in itself, remote attestation between a device and a service is also needed to protect the data handling processes and to establish a security channel to prevent interception by an adversary on the communication network.

Data captured from sensors integrated in the device, input by users, or generated (or processed) by algorithms in the device should have a label and be digitally signed (or by other crypto mechanisms) using the device's particular key designed for this purpose, to protect the integrity and authenticity of the data. Services could know the parameters of the sensor device which can help the service with the processing of the data. Trusted connections have a strong relationship with Hardware Security Modules (HSM), Trusted Computing (TC), Public Key Infrastructure (PKI) and Certification Authority (CA) technology and so on. Trusted connection issues can be broken down into several sub-categories such as:

— Hardware security modules to establish the reliable root of trust

— Identity of devices and services that issued by trusted parties

— Mutual authentication and key establishment between devices and services to estalish security channel

— Mutual remote attestation(or environment assurance) between devices and services

— Data Identity to keep the data integrity and authenticity for a long term

This document proposes security recommendations for establishing trusted connections between devices and services, which would help the related organisations to set up HSM in devices (including mobile devices, PCs, or IoT devices) and in the infrastructure of cloud services. This document can help to build a trusted environment. This document can also help trusted third parties (CA) to issue certificates to devices and services and help the applications to mitigate against attacks and identify forged data from the sensors, etc.

Cybersecurity — Security recommendations for establishing trusted connections between devices and services

1 Scope

This document provides a framework and recommendations for establishing trusted connections between devices and services based on hardware security modules, including recommendations for components such as: hardware security module, roots of trust, identity, authentication and key establishment, remote attestation, data integrity and authenticity.

This document is applicable to establishing trusted connections between devices and services based on hardware security modules.

This document does not address privacy concerns.

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 27070:2021, *Information technology — Security techniques — Requirements for establishing virtualized roots of trust*

3 Terms and definitions

3.1 General

For the purposes of this document, the terms and definitions given in ISO/IEC 27070:2021 and the following apply.

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

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

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

3.2 Terms relating to cloud computing

3.2.1
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: ISO/IEC 22123-1:2021, 3.2.1]

3.2.2
cloud service
one or more capabilities offered via *cloud computing* (3.2.1) invoked using a defined interface

[SOURCE: ISO/IEC 22123-1:2021, 3.2.2]

3.3 Terms relating to cloud computing roles and activities

3.3.1
party
natural person or legal person, whether or not incorporated, or a group of either that can assume one or more roles

[SOURCE: ISO/IEC 22123-1:2021, 3.4.1]

3.3.2
cloud service customer
party (3.3.1) which is in a business relationship for the purpose of using *cloud services* (3.2.2)

Note 1 to entry: A business relationship does not necessarily imply financial agreements.

[SOURCE: 22123-1:2021, 3.4.2]

3.3.3
cloud service provider
party (3.3.1) which makes *cloud services* (3.2.2) available

[SOURCE: ISO/IEC 22123-1:2021, 3.4.3]

3.3.4
cloud service user
natural person, or entity acting on their behalf, associated with a *cloud service customer* (3.3.2) that uses *cloud services* (3.2.2)

Note 1 to entry: Examples of such entities include devices and applications.

[SOURCE: ISO/IEC 22123-1:2021, 3.4.4]

3.3.5
tenant
one or more *cloud service users* (3.3.4) sharing access to a set of physical and virtual resources

[SOURCE: ISO/IEC 22123-1:2021, 3.5.2]

3.4 Terms relating to security and privacy

3.4.1
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 22123-1:2021, 3.14.7]

3.4.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 22123-1:2021, 3.11.1]

3.4.3
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 22123-1:2021, 3.11.2]

3.4.4
information security
preservation of *confidentiality* (3.4.2), *integrity* (3.4.3) and *availability* (3.4.1) of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 22123-1:2021, 3.11.3]

3.4.5
remote attestation
RA
process of evaluating integrity measurements generated using a *root of trust* (3.4.11) for measurement, storage and reporting to establish trust in a platform remotely

[SOURCE: ISO/IEC 27070:2021]

3.4.6
hardware security module
HSM
tamper-resistant hardware module which safeguards and manages keys and provides cryptographic functionsNote 1 to entry: *Trusted module* (3.4.7) is a specific kind of HSM.

3.4.7
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.

[SOURCE: ISO/IEC 27070:2021]

3.4.8
trust anchor module
TAM
one (or more) *hardware security modules* (3.4.6) that acts as the *roots of trust* (3.4.11)

3.4.9
trusted user interface
TUI
device component with a user interface whose integrity and authenticity is managed by the trust anchor module

3.4.10
identity key
IK
signing key used to authentication and sign characteristics of the device (or service) environment (e.g. a digest) in order to prevent forgery and protect the integrity of the device (or service) environment characteristics

3.4.11
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 27070:2021]

3.4.12
physical root of trust
in this document, *root of trust* (3.4.11) refers to a physical *root of trust* (3.4.11)

3.4.13
virtualized root of trust
vRoT
security function component established based on the *root of trust* (3.4.11), which provides similar function as the *root of trust* (3.4.11)

Note 1 to entry: In practical environments, there could be multiple virtualized roots of trust based on the single *root of trust* (3.4.11) simultaneously

3.4.14
root of trust for measurement
computation engine that resets one or more platform configuration registers, makes the initial integrity measurement, and extends it into a platform configuration register

Note 1 to entry: A *root of trust* (3.4.11) that collects device environment characteristics (e.g. firmware integrity measurements) and puts them in a format suitable for attestation (e.g. TPM Platform Configuration Registers).

3.4.15
root of trust for storage
component of the *root of trust* (3.4.11) that provides storing confidential information and measured values in shielded locations accessed using protected capabilities

3.4.16
root of trust for reporting
component of the *root of trust* (3.4.11) that reliably provides authenticity and nonrepudiation services for the purposes of attesting to the origin and integrity of platform characteristics

Note 1 to entry: a *root of trust* (3.4.11) that uses the device's (or service's) *identity key* (3.4.10) to reliably provide authenticity and nonrepudiation services for the purposes of attesting to the origin and integrity of device (or service) environment characteristics.

3.4.17
secure element
SE
tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities

3.4.18
trusted computing
TC
a technology protect computer consistently behave in expected ways

Note 1 to entry: Trusted computing is developed and promoted by the Trusted Computing Group (TCG).

3.4.19
trusted execution environment
TEE
execution environment that runs alongside but isolated from the device main operating system

3.4.20
trusted network connect
TNC
open architecture for network access control, promulgated by the Trusted Network Connect Work Group (TNC-WG) of the TCG

3.4.21
chain of trust
extension of trust from a component (e.g. a root of trust) to another component accomplished through the act of measurement and verification of the integrity and authenticity of the new component before the system begins execution of the new component

Note 1 to entry: Such an act builds a chain of trust from the old component to the new component, which is now a trusted component. The old component can be either a root of trust or a trusted component.

3.4.22
trusted environment
TE
execution mode where the process/mechanism/functionality is protected/launched by a ROT service

Note 1 to entry: TEE is a specific TE.

3.5 Miscellaneous terms

3.5.1
device
physical entity that communicates directly or indirectly with one or more *cloud services* (3.2.2)

[SOURCE: ISO/IEC 22123-1:2021, 3.14.4]

3.5.2
device holder
person possesses and using the device

Note 1 to entry: In some cases, the person possesses and using the mobile device is the device holder. But in cases of IoT, most of the sensors (devices) may not have a corresponding device holder.

4 Symbols and abbreviated terms

CA	Certification Authority (in a PKI)
CSP	Cloud Service Providers
CPU	Central Processing Unit
HSM	Hardware Security Module
IK	Identity Key
IMC	Integrity Measurement Collectors
IMV	Integrity Measurement Verifiers
OS	Operating System

PCR	Platform Configuration Register
PKI	Public Key Infrastructure
RoT	Root of Trust
REE	Rich Execution Environment
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SE	Secure Element
TAM	Trust Anchor Module
TC	Trusted Computing
TCG	Trusted Computing Group
TCM	Trusted Cryptography Module
TE	Trusted Environment
TEE	Trusted Execution Environment
TM	Trusted Module
TNC	Trusted Network Connect
TPM	Trusted Platform Module
vIK	Virtual Identity Key
vRoT	Virtualized Root of Trust

5 Framework and components for establishing a trusted connection

5.1 Overview

This clause provides an overview of the framework and components of a trusted connection between a device and a service based on hardware security modules.

Security channels are used between devices and services to protect confidentiality and integrity of data, but it is not enough. The service needs to distinguish data collected by sensors of the authorised device from those of other devices or data forged by adversaries. So, it should be able to ensure the data comes from the authorised device. Conversely, the device also needs to distinguish the genuine service from unintended services or malicious services. So, it should be able to reliably identify the genuine and intended service, in particular for cloud services, which may have thousands of such services running. Threats on a trusted connection see Annex A. A trusted connection between a device and a service provides the ability to protect confidentiality, integrity and authenticity of data; provides the ability to prevent identity spoofing by binding the identity of the device (or service) to root of trust; and provides the ability to ensure trusted processing of data by remote attestation or environment assurance.

To establish trusted connection between a device and a service faces the risks from several involved parties. Figure 1 describes the parties involved in establishing a trusted connection, including identity issuer (e.g. CA), HSM manufacturer, device manufacturer, system integrator, cloud service provider, tenant, and device holder (may not exist in some scenarios such as IoT).