INTERNATIONAL STANDARD

ISO/IEC 27071

First edition
2023-07

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

Cybersécurité — Recommandations de sécurité pour l'établissement de connexions de confiance entre dispositifs et services

Reference number
ISO/IEC 27071:2023(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.

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use 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 https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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.

Introduction

With the development of the internet of things (IoT), mobile services, cloud computing, big data and artificial intelligence (AI), it is essential to establish trusted connections between devices and services in a growing number of scenarios.

Security channels [e.g. secure sockets layer (SSL) or transport layer security (TLS) protocols] are used between devices and services to protect confidentiality and integrity of data, but it is not enough. It is essential for the service to distinguish data collected by sensors of the authorized device from those of other devices or data forged by adversaries. Thus, the service should be able to ensure that the data comes from the authorized device.

In addition, it is crucial for the device to distinguish the genuine service from unintended services or malicious services. In this way, 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 critical to ensure the utilization of reliable roots of trust. The requirements for establishing reliable virtualized roots of trust are described in ISO/IEC 27070.

Mutual authentication between a device and a service is essential for preventing impersonation attacks. While insufficient in itself, remote attestation between a device and a service is also critical for protecting the data handling processes and establishing 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. It is possible that services know the parameters of the sensor device which can help it to process 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. 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 issued by trusted parties;

— mutual authentication and key establishment between devices and services to establish a security channel;

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

— data identity to keep the data integrity and authenticity 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 (i.e. CA) to issue certificates to devices and services, and help applications to mitigate against attacks and identify forged data from the sensors.

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. It includes 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 scenarios that establish trusted connections between devices and services based on hardware security modules.

This document does not address privacy concerns.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, *Information technology — Security techniques — Requirements for establishing virtualized roots of trust*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27070 and the following 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 Terms relating to cloud computing

3.1.1
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 22123-1:2023, 3.1.1, modified — note 2 to entry has been deleted.]

3.1.2
cloud service
capabilities offered via *cloud computing* (3.1.1) invoked using a defined interface

[SOURCE: ISO/IEC 22123-1:2023, 3.1.2]

3.2 Terms relating to cloud computing roles and activities

3.2.1
party
natural person or legal person or a group of either, whether or not incorporated, that can assume one or more roles

[SOURCE: ISO/IEC 22123-1:2023, 3.3.1]

3.2.2
cloud service provider
party (3.2.1) that is acting in a *cloud service* (3.1.2) provider role

[SOURCE: ISO/IEC 22123-1:2023, 3.3.3]

3.2.3
cloud service user
natural person, or entity acting on their behalf, associated with a *cloud service customer* (3.2.2) that uses *cloud services* (3.1.2)

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

[SOURCE: ISO/IEC 22123-1:2023, 3.3.4]

3.2.4
tenant
cloud service user (3.2.4) sharing access to a set of physical and virtual resources

[SOURCE: ISO/IEC 22123-1:2023, 3.4.2, modified — "one or more" has been deleted from original definition.]

3.3 Terms relating to security and privacy

3.3.1
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.3.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.3.3
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.3.4
hardware security module
HSM
tamper-resistant hardware module which safeguards and manages keys and provides cryptographic functions

Note 1 to entry: Trusted module is a specific kind of HSM.

3.3.5
trust anchor module
TAM
hardware security module (3.3.4) that acts as the *roots of trust* (3.3.8)

Note 1 to entry: Trust anchor module is an abstract module that contains one or more hardware security modules.

3.3.6
trusted user interface
TUI
device component with a user interface whose *integrity* (3.3.3) and authenticity is managed by the *trust anchor module* (3.3.5)

3.3.7
identity key
IK
signing key used for authentication and to sign characteristics of the device (or service) environment (e.g. a digest) in order to prevent forgery and protect the *integrity* (3.3.3) of the device (or service) environment characteristics

3.3.8
root of trust
RoT
physical root of trust
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, modified — "physical root of trust" has been added as an admitted term.]

3.3.9
virtualized root of trust
vRoT
security function component established based on the *root of trust* (3.3.8), which provides similar function as the root of trust

Note 1 to entry: In practical environments, there can be multiple virtualized roots of trust based on the single root of trust simultaneously.

3.3.10
root of trust for measurement
computation engine that resets one or more platform configuration registers, makes the initial *integrity* (3.3.3) measurement, and extends it into a platform configuration register

Note 1 to entry: A *root of trust* (3.3.8) that collects device environment characteristics (e.g. firmware integrity measurements) and puts them in a format suitable for attestation (e.g. trusted platform module platform configuration registers).

3.3.11
root of trust for storage
component of the *root of trust* (3.3.8) that provides storing confidential information and measured values in shielded locations accessed using protected capabilities

3.3.12
root of trust for reporting
component of the *root of trust* (3.3.8) that reliably provides authenticity and nonrepudiation services for the purposes of attesting to the origin and *integrity* (3.3.3) of platform characteristics

Note 1 to entry: A root of trust that uses the device's (or service's) *identity key* (3.3.7) to reliably provide authenticity and nonrepudiation services for the purposes of attesting to the origin and integrity of device (or service) environment characteristics.

3.3.13
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

3.3.14
trusted computing
TC
technology protected computer which consistently behaves in expected ways

3.3.15
trusted execution environment
TEE
execution environment that runs alongside but is isolated from the device main operating system

3.3.16
chain of trust
extension of trust from a component [e.g. a *root of trust* (3.3.8)] to another component accomplished through the act of measurement and verification of the *integrity* (3.3.3) 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.

3.3.17
trusted environment
TE
execution mode where the functionality is protected by a *root of trust* (3.3.8) service

Note 1 to entry: A *trusted execution environment* (3.3.15) is a specific TE.

3.4 Miscellaneous terms

3.4.1
device
physical entity that communicates directly or indirectly with one or more *cloud services* (3.1.2)

[SOURCE: ISO/IEC 22123-1:2023, 3.13.4, modified — note 1 to entry has been deleted.]

3.4.2
device holder
person possessing and using the device

Note 1 to entry: In some cases, the person who possesses and uses the mobile device is the device holder. But in cases of Internet of Things, it is probably that sensors (devices) do not have a corresponding device holder.

4 Abbreviated terms

API	application programming interface
CA	certification authority (in a PKI)
CPU	central processing unit
HSM	hardware security module
IK	identity key
IMC	integrity measurement collectors
IMV	integrity measurement verifiers
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
TPM	trusted platform module
vRoT	virtualized root of trust

5 Framework and components for establishing a trusted connection

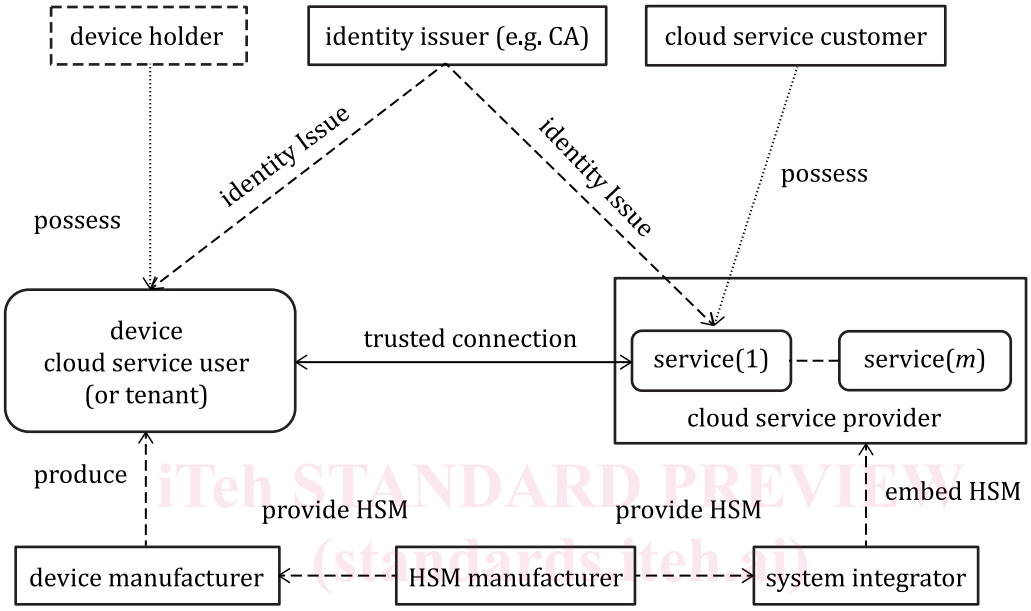
5.1 Overview

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.

A trusted connection between a device and a service provides the ability to protect confidentiality, integrity and authenticity of data; prevent identity spoofing by binding the identity of the device (or service) to a root of trust; and ensure trusted processing of data by remote attestation or environment assurance. For information on threats on a trusted connection, see Annex A.

Figure 1 describes the parties involved in establishing a trusted connection, including the identity issuer (e.g. CA), HSM manufacturer, device manufacturer, system integrator, cloud service provider, tenant, and device holder (it is possible that the party does in some scenarios such as IoT).

The HSM manufacturer produces HSMs. Device manufacturers produce a device. The cloud service provider runs the cloud service. The cloud service customer possesses the service which has a trusted connection with the device. In some scenarios, the cloud service customer and cloud service provider may be the same party. Devices act as the cloud service users (or tenants). Device holder (e.g. the holder of mobile phone) possesses and uses the device to establish trusted connection with a cloud service.



Key

----->	offline or pre-set procedure	party (the party does not exist in some scenarios)	
·····>	ownership	party	
<---->	trusted connection	*m*	number of services

Figure 1 — Parties related in trusted connection

There are several scenarios to establish a trusted connection between a device and a service.

Figure 2 shows the framework of a trusted connection for device with both TEE/SE and REE (such as a mobile device). Applications which are run in a TEE/SE environment and have a root of trust based on the TAM, can build a trusted connection to service. A trusted user interface (TUI) component is provided for interaction between the user and the device.

Figure 3 illustrates the framework of a trusted connection for a device with the TE only (such as an IoT device). To establish a trusted connection between a device (with TE only) and a service, a remote attestation component may not be required, and the user interface (or trusted user interface, TUI) may not exist.