DRAFT International Standard

ISO/IEC DIS 25093-1

Cybersecurity — Confidential computing —

Part 1: Overview and concepts

ICS: 35.030

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

Secretariat: **DIN**

Voting begins on:
2026-06-11

Voting terminates on:
2026-09-03

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 25093-1:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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 Abbreviations ... **2**
5 Overview ... **2**
5.1 General ... 2
5.2 Roles ... 3
5.3 Threat Model ... 4
5.3.1 TCB ... 4
5.3.2 Attacks that confidential computing can cope with ... 4
6 Basic concept ... **5**
6.1 Goals ... 5
6.2 Prerequisites ... 5
6.2.1 Hardware Isolation ... 5
6.2.2 Trusted execution environment (TEE) ... 5
6.2.3 Boot security ... 5
6.2.4 Attestation ... 5
6.3 Mechanism ... 6
6.4 Properties ... 6
6.4.1 Properties overview ... 6
6.4.2 Main properties ... 6
6.4.3 Extended properties ... 7
Annex A (informative) **Deployment model** ... **8**
Annex B (informative) **Isolation Methodologies** ... **10**
Bibliography ... **11**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

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

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.

This document was prepared by Technical Committee ISO/IEC JTC1, *Information Technology*, Subcommittee SC 27, *IT Security techniques*.

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.

© ISO/IEC 2026 – All rights reserved

Introduction

Data exists in three states: in motion, at rest, and in use. Technologies for protecting data in motion and at rest are mature and are as such not covered by this document. Solutions for protecting data while being processed have not been standardized. Confidential Computing (CC) requires a secure environment which ensures the confidentiality and integrity of important data and code in use where the system has passed a verification process including both secure boot and attestation.

A growing number of application scenarios take advantage of CC. For example, in the financial field, CC can be used to protect the security and privacy of transaction data and ensure the credibility and integrity of transactions; in the telecommunications field, CC can be used to protect users' communication privacy and data security and prevent information leakage; in the medical field, CC can be used to protect patients' medical records and personal privacy, promoting secure sharing of medical data and cross-institutional collaboration; in artificial intelligence and big data analytics field, CC enables secure processing and protection of sensitive data, enabling data cooperation and sharing, and promoting cross organizational data analysis.

CC introduces an architectural capability to decouple physical infrastructure perimeters from logical trust boundaries—a separation not feasible in conventional computing architectures. This capability allows an organization to extend its security domain to encompass resources within an external infrastructure. Consequently, it enables the establishment of an isolated execution environment that effectively resides within the extended trust boundaries of multiple collaborating entities simultaneously.

This document outlines an overview and concepts behind confidential computing based on the work of the Confidential Compute Consortium (CCC), Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE), etc. to provide a common understanding for industry stakeholders.

© ISO/IEC 2026 – All rights reserved

Cybersecurity — Confidential computing —

Part 1:
Overview and concepts

1 Scope

This document provides the overview and concepts of confidential computing. It is applicable to organizations and stakeholders involved in the development, implementation, or use of confidential computing.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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
confidential computing
protection of data in use by performing computation in a hardware-based, attested trusted execution environment

3.2
trusted execution environment (TEE)
environment that provides a level of assurance for data confidentiality, data integrity and code integrity

3.3
confidential application
application running inside the *TEE* (3.2) that is protected from other confidential processes and system operators

Note 1 to entry: System operators include administrators, privileged users, and other entities with elevated access to the hosting infrastructure.

Note 2 to entry: The CPU executing TEE instructions is part of the trusted computing base and is not considered part of the system operator domain.

3.4
attestation
verify the integrity and authenticity of the software and hardware components within a TEE through a cryptographically signed proof (attestation report)

3.5
attestation report
report signed by a hardware protected key, containing evidence of TCB measurements

© ISO/IEC 2026 – All rights reserved

3.6
trusted computing base (TCB)
totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy

3.7
data at rest
data recorded on stable, non-volatile storage

[SOURCE: ISO/IEC 27040:2024(en), 3.2.3]

3.8
data in use
data loaded into memory for processing, accessing or manipulation by one or more applications subsystems or users

3.9
data in motion
data being transferred from one location to another

Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e. never exposed outside of an interface, chip, or device).

[SOURCE: ISO/IEC 27040:2024(en), 3.2.4]

4 Abbreviations

TEE	trusted execution environment
TCB	trusted computing base
CC	confidential computing
CA	confidential application
GA	general application
OS	operating system
SDK	software development kit
VM	virtual machine
VMM	virtual machine monitor
CPU	central processing unit
DoS	denial of service
DDos	distributed denial of service

5 Overview

5.1 General

CC is a computing model used to protect the confidentiality and integrity of data in use. This mode is based on trusted hardware, hardware isolation, and remote attestation to ensure that code cannot be modified and data cannot be accessed by unauthorized entities. In the context of CC, unauthorized entities include other applications on the host, the host OS and hypervisor, system administrators, service providers, and

© ISO/IEC 2026 – All rights reserved