



Q

Menu

ISO/IEC 11889-1:2009

Information technology

Trusted Platform Module

Part 1: Overview

- Status : **Published** (Under review)
- ✓

This standard was last reviewed and confirmed in 2017. Therefore this version remains current.
- !

This standard has been revised by [ISO/IEC 11889-1:2015](#)

This edition of the standard exceptionally remains valid until 2025.

The electronic version of this International Standard can be [downloaded](#) from the ISO/IEC Information Technology Task Force (ITTF) web site.

Abstract

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889-1:2009 is an overview of the TPM. It describes the TPM and how it fits into the trusted platform. ISO/IEC 11889-1:2009 describes trusted platform concepts such as the trust boundary, transitive trust, integrity measurement, and integrity reporting.

General information

Status : Published

Publication date : 2009-05

Stage : International Standard confirmed [[90.93](#)]

Edition : 1

Number of pages : 12

Technical Committee : [ISO/IEC JTC 1](#)

ICS (International Classification for Standards) : [35.030](#)

 [RSS](#) updates



[Read sample](#) 

Preview this standard in our Online Browsing Platform (OBP)

Life cycle

Now

Published
ISO/IEC 11889-1:2009

A standard is reviewed every 5 years
Stage: **90.93** (Confirmed) 

Revised by

Published
[ISO/IEC 11889-1:2015](#)



This standard contributes to the following [Sustainable Development Goals](#)

11 9 8

Got a question?

Check out our [FAQs](#)

Customer care
+41 22 749 08 88
customerservice@iso.org

Opening hours:
Monday to Friday - 09:00-12:00, 14:00-17:00 (UTC+1)

[Home](#) / [Store](#) / [Standards catalogue](#) / [ICS](#) / [35](#) / [35.030](#) / [ISO/IEC 11889-1:2009](#)

[Sitemap](#) ▾

ISO/IEC 11889-1:2009(en) Information technology:

Trusted Platform Module — Part 1: Overview

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 11889-1](#) was prepared by the Trusted Computing Group (TCG) and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

ISO/IEC 11889 consists of the following parts, under the general title *Information technology — Trusted Platform Module*:

- — *Part 1: Overview*
- — *Part 2: Design principles*
- — *Part 3: Structures*
- — *Part 4: Commands*

Introduction

Designers of secure distributed systems, when considering the exchange of information between systems, must identify the endpoints of communication. The composition and makeup of the endpoint is as important to the overall ability of the system to serve as an authentication and attestation device of the system as is the communications protocol.

Endpoints are minimally comprised of asymmetric keys, key storage and processing that protects protocol data items. Classic message exchange based on asymmetric cryptography suggests that messages intended for one and only one individual can be encrypted using a public key. Furthermore, the message can be protected from tampering by signing with the private key.

Keys are communication endpoints and improperly managed keys can result in loss of attestation and authentication. Additionally, improperly configured endpoints may also result in loss of attestation and authentication ability.

This is an informative background document and contains no specifications or normative information. To find normative information and specifications about the TPM, refer to [ISO/IEC 11889-2](#) to [ISO/IEC 11889-4](#).

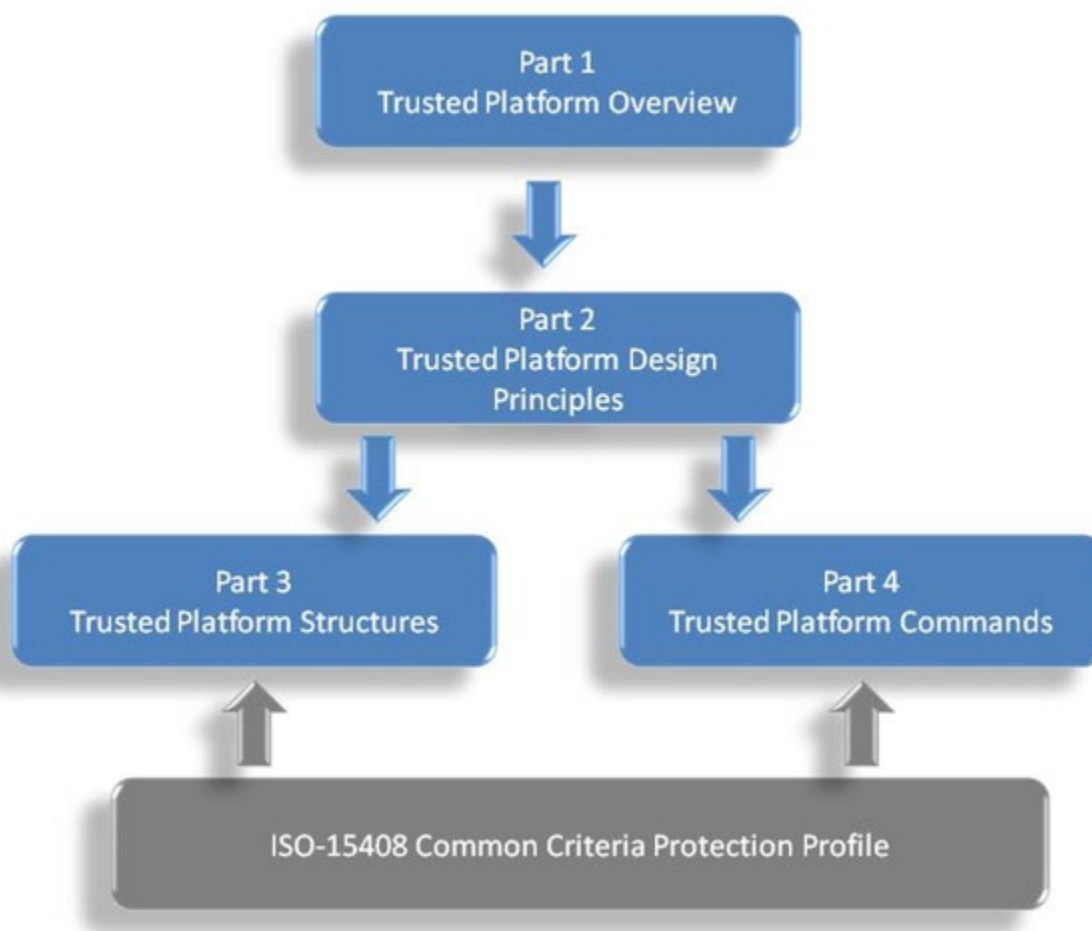
A Trusted Platform Module (TPM) is an implementation of a defined set of capabilities that is intended to provide authentication and attestation functionality for a computing device, and protect information by controlling access to plain-text data.

A TPM is self-sufficient as a source of authentication and as a means of enhancing the protection of information from certain physical attacks. A TPM requires the cooperation of a TCG “Trusted Building Block” (outside the TPM, that is also part of the computing device) in order to provide attestation and protect information from software attacks on the computing device.

Typical TPM implementations are affixed to the motherboard of a computing device.

A computing device that contains both a TPM and a Trusted Building Block is called a Trusted Platform. Trusted Platforms offer improved, hardware-based security in numerous applications, such as file and folder encryption, local password management, S-MIME e-mail, VPN and PKI authentication and wireless authentication for 802.1x and LEAP.

Figure 1 — TPM Documentation Roadmap



Start of informative comment

ISO/IEC 11889 is from the Trusted Computing Group (TCG) Trusted Platform Module (TPM) specification 1.2 version 103. The part numbers for ISO/IEC 11889 and the TCG specification do not match. The reason is the inclusion of the Overview document that is not a member of the TCG part numbering. The mapping between the two is as follows:

ISO Reference

TCG Reference

Part 1 Overview
Part 2 Design Principles
Part 3 Structures
Part 4 Commands

Not published
Part 1 Design Principles
Part 2 Structures
Part 3 Commands

End of informative comment

1 Scope

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889 is broken into parts to make the role of each document clear. Any version of the standard requires all parts to be a complete standard.

A TPM designer **MUST** be aware that for a complete definition of all requirements necessary to build a TPM, the designer **MUST** use the appropriate platform specific specification for all TPM requirements.

Part 1 provides an overview of the concepts behind the TPM and trusted platforms.

Only informative sections of standards are publicly available. To view the full content, you will need to purchase the standard by clicking on the "Buy" button.

© 2009 ISO/IEC — All rights reserved