INTERNATIONAL STANDARD

ISO/IEC 11889-1

First edition
2009-05-15

Information technology — Trusted Platform Module —

Part 1: Overview

Technologies de l'information — Module de plate-forme de confiance —

Partie 1: Aperçu général

Reference number
ISO/IEC 11889-1:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Table of Contents

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.

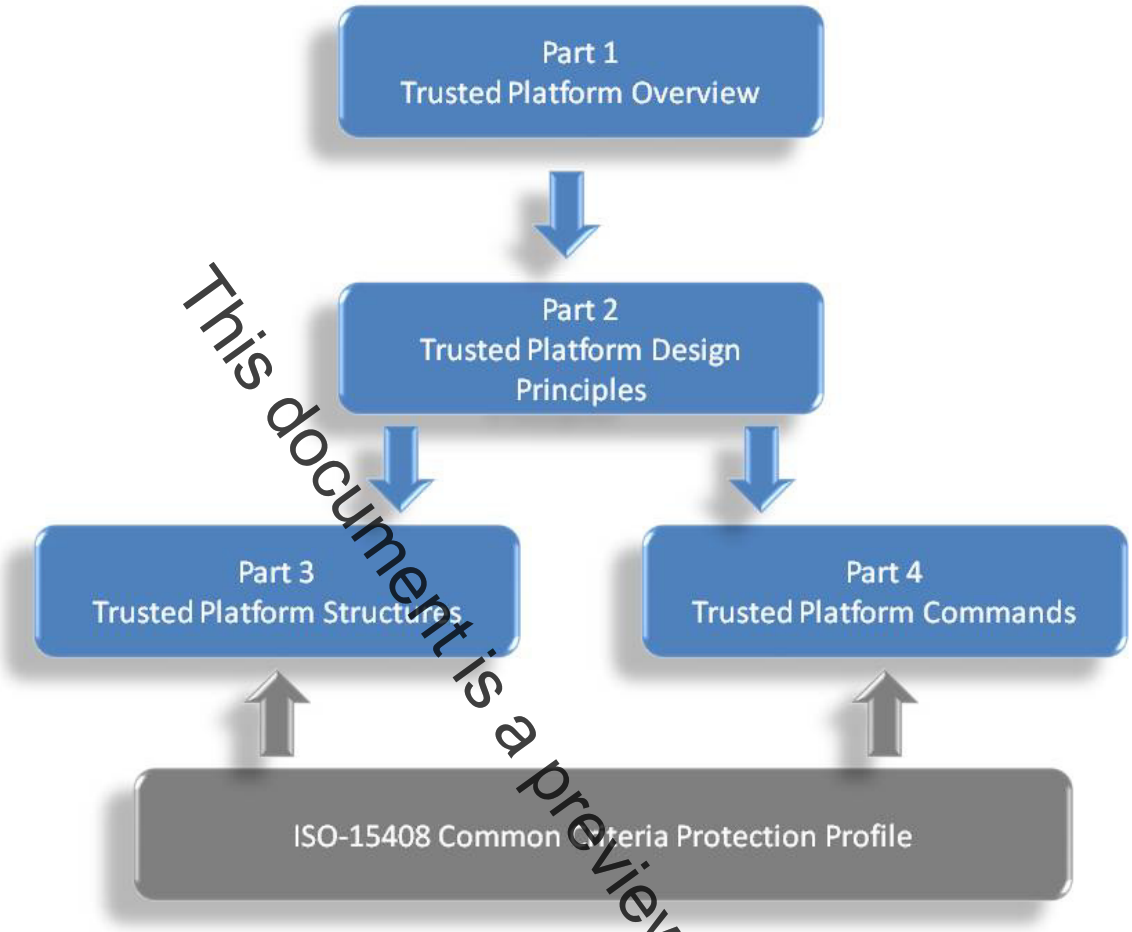

Figure 1. TPM Documentation Roadmap

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	Not published
Part 2 Design Principles	Part 1 Design Principles
Part 3 Structures	Part 2 Structures
Part 4 Commands	Part 3 Commands

End of informative comment

Information technology — Trusted Platform Module —

Part 1:
Overview

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.

2. Abbreviated Terms

Abbreviation	Description
AACP	Asymmetric Authorization Change Protocol
ADCP	Authorization Data Change Protocol
ADIP	Authorization Data Insertion Protocol
AIK	Attestation Identity Key
AMC	Audit Monotonic Counter
APIP	Time-Phased Implementation Plan
AuthData	Authentication Data or Authorization Data, depending on the context
BCD	Binary Coded Decimal
BIOS	Basic Input/Output System
CA	Certification of Authority
CDI	Controlled Data Item
CMK	Certifiable/Certified Migratable Keys
CRT	Chinese Remainder Theorem
CRTM	Core Root of Trust Measurement
CTR	Counter-mode encryption
DAA	Direct Autonomous Attestation
DIR	Data Integrity Register
DOS	Disk Operating System