INTERNATIONAL STANDARD

ISO/IEC 11889-2

First edition
2009-05-15

Information technology — Trusted Platform Module —

Part 2: Design principles

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

Partie 2: Principes de conception

Reference number
ISO/IEC 11889-2:2009(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 11889-2 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

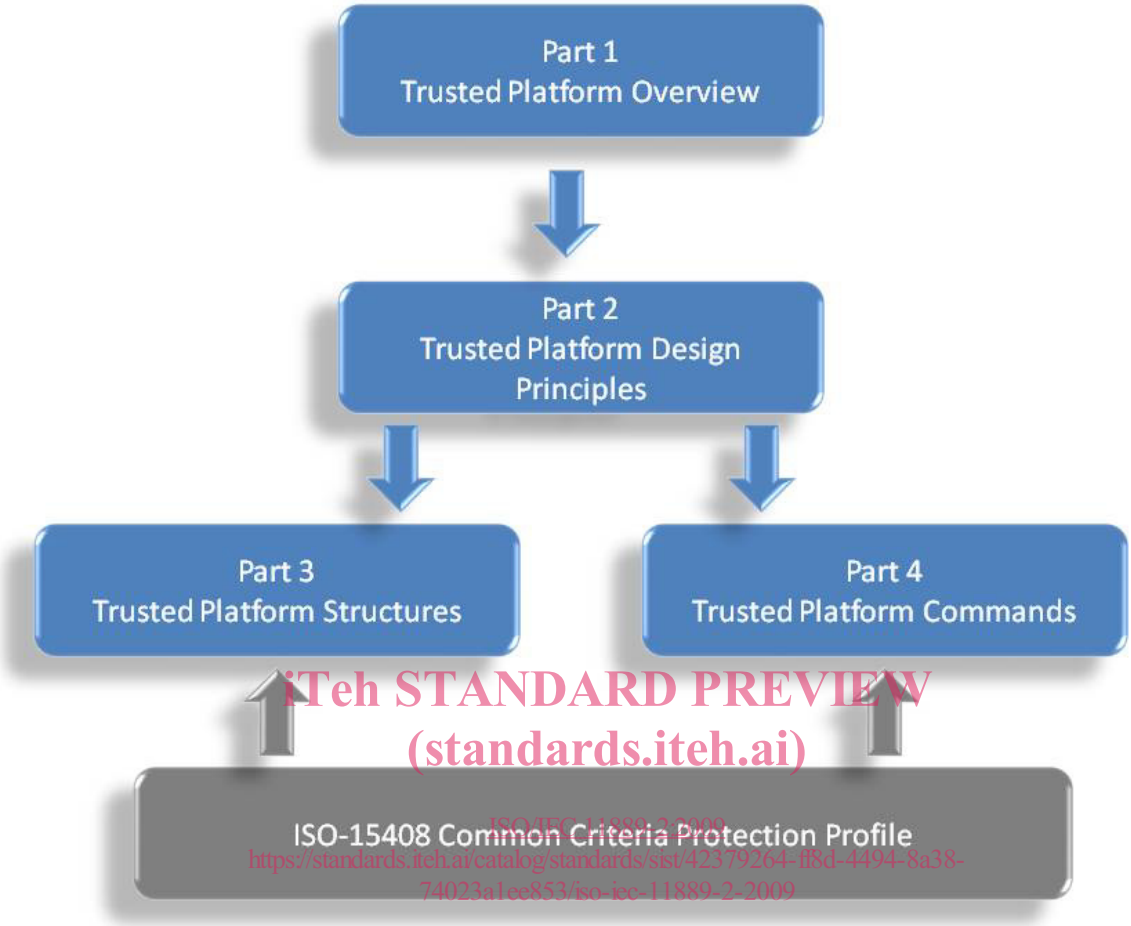

Figure 1. TPM Main Specification Roadmap

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 2: Design principles

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 to understand all of the TPM requirements.

Part 2 defines the principles of TPM operation. The base operating modes, the algorithms and key choices, along with basic interoperability requirements make up the majority of the normative statements in part 2.

1.1 Key words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document’s normative statements are to be interpreted as described in RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*.

1.2 Statement Type

Please note a very important distinction between different sections of text throughout this document. You will encounter two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, you can consider it of the kind normative statements.

For example:

Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the standard the user must read the standard. (This use of MUST does not require any action).

End of informative comment

This is the first paragraph of one or more paragraphs (and/or sections) containing the text of the kind normative statements ...

To understand the standard the user MUST read the standard. (This use of MUST indicates a keyword usage and requires an action).

2. Normative references

The following referenced documents are indispensable for the application 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 8825-1 | ITU-T X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

ISO/IEC 10118-3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions, Clause 9, SHA-1

ISO/IEC 18033-3, Information technology — Security techniques — Encryption algorithms — Part 3, Block ciphers, Clause 5.1 AES

IEEE P1363, Institute of Electrical and Electronics Engineers: Standard Specifications For Public-Key Cryptography

IETF RFC 2104, Internet Engineering Task Force Request for Comments 2104: HMAC: Keyed-Hashing for Message Authentication

IETF RFC 2119, Internet Engineering Task Force Request for Comments 2119: Key words for use in RFCs to Indicate Requirement Levels

PKCS #1 Version 2.1, RSA Cryptography Standard. This document is superseded by P1363, except for section 7.2 that defines the V1.5 RSA signature scheme in use by the TPM.

3. 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	Cerifiable/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
DSA	Digital Signature Algorithm
DSAP	Delegate-Specific Authorization Protocol
ECB	Electronic Codebook Mode
EK	Endorsement Key
ET	ExecuteTransport or Entity Type
FIPS	Federal Information Processing Standard
GPIO	General Purpose I/O
HMAC	Hash Message Authentication Code
HW	Hardware Interface
IB	Internal Base
I/O	Input/Output
IV	Initialization Vector
KH	Key Handle
LEAP	Lightweight Extensible Authentication Protocol for wireless computer networks
LK	Loaded Key
LOM	Limited Operation Mode
LPC	Low Pin Count
LSB	Least Significant Byte
MA	Migration Authority/Authorization
MIDL	Microsoft Interface Definition Language
MSA	Migration Selection Authority
MSB	Most Significant Byte
NV	Non-volatile

Abbreviation	Description
NVRAM	Non-Volatile Random Access Memory
OAEP	Optimal Asymmetric Encryption Padding
OEM	Original Equipment Manufacturer
OIAP	Object-Independent Authorization Protocol
OID	Object Identifier
OSAP	Object-Specific Authorization Protocol
PCR	Platform Configuration Register
PI	Personal Information
PII	Personally Identifiable Information
POST	Power On Self Test
PRIVEK	Private Endorsement Key
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
PUBEK	Public Endorsement Key
RNG	Random Number Generator
RSA	Algorithm for public-key cryptography. The letters R, S, and A represent the initials of the first public describers of the algorithm.
RTM	Release to Manufacturing/Ready to Market
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SHA	Secure Hash Algorithm
SRK	Storage Root Key
STF	Self Test Failed
TA	Time Authority
TBB	Threading Building Blocks
TCG	Trusted Computing Group
TCV	Tick Count Value
TIR	Tick Increment Rate
TIS	TPM Interface Specification
TNC	Trusted Network Connect
TOE	Target of Evaluation
TOS	Trusted Operating System
TPCA	Trusted Platform Computing Alliance
TPM	Trusted Platform Module
TPME	Trusted Platform Module Entity
TSC	Tick Stamp Counter
TSC_	TPM Software Connection, when used as a command prefix
TSN	Tick Session Name
TSR	Tick Stamp Reset
TSRB	TickStampReset for blob
TSS	TCG Software Stack
TTP	Trusted Third Party/Time-Triggered Protocol
TS	Tick Stamp
UTC	Universal Time Clock
VPN	Virtual Private Network

4. Conformance

4.1 Introduction

Start of informative comment

The Protection Profile in the Conformance part of the specification defines the threats that are resisted by a platform. This section, “Protection,” describes the properties of selected capabilities and selected data locations within a TPM that has a Protection Profile and has not been modified by physical means.

This section introduces the concept of protected capabilities and the concept of shielded locations for data. The ordinal set defined in part II and III is the set of protected capabilities. The data structures in part II define the shielded locations.

- A protected capability is one whose correct operation is necessary in order for the operation of the TPM Subsystem to be trusted.
- A shielded location is an area where data is protected against interference and prying, independent of its form.

ISO/IEC 11889 uses the concept of protected capabilities so as to distinguish platform capabilities that must be trustworthy. Trust in the TPM depends critically on the protected capabilities. Platform capabilities that are not protected capabilities must (of course) work properly if the TPM Subsystem is to function properly.

ISO/IEC 11889 uses the concept of shielded locations, rather than the concept of “shielded data.” While the concept of shielded data is intuitive, it is extraordinarily difficult to define because of the imprecise meaning of the word “data.” For example, consider data that is produced in a safe location and then moved into ordinary storage. It is the same data in both locations, but in one it is shielded data and in the other it is not. Also, data may not always exist in the same form. For example, it may exist as vulnerable plaintext, but also may sometimes be transformed into a logically protected form. This data continues to exist, but doesn't always need to be shielded data - the vulnerable form needs to be shielded data, but the logically protected form does not. If a specific form of data requires protection against interference or prying, it is therefore necessary to say “if the data-D exists, it must exist only in a shielded location.” A more concise expression is “the data-D must be extant only in a shielded location.”

Hence, if trust in the TPM Subsystem depends critically on access to certain data, that data should be extant only in a shielded location and accessible only to protected capabilities. When not in use, such data could be erased after conversion (using a protected capability) into another data structure. Unless the other data structure was defined as one that must be held in a shielded location, it need not be held in a shielded location.

End of informative comment

1. The data structures described in ISO/IEC 11889-3 MUST NOT be instantiated in a TPM, except as data in TPM_Shielded-Locations.
2. The ordinal set defined in ISO/IEC 11889-3 and ISO/IEC 11889-4 MUST NOT be instantiated in a TPM, except as TPM_Protected-Capabilities.
3. Functions MUST NOT be instantiated in a TPM as TPM_Protected-Capabilities if they do not appear in the ordinal set defined in ISO/IEC 11889-3 or ISO/IEC 11889-4

4.2 Threat

Start of informative comment

This section, “Threat,” defines the scope of the threats that must be considered when considering whether a platform facilitates subversion of capabilities and data in a platform.

The design and implementation of a platform determines the extent to which the platform facilitates subversion of capabilities and data within that platform. It is necessary to define the attacks that must be resisted by TPM_Shielded-Locations and TPM_Protected-Capabilities in that platform.

The ISO/IEC 11889 standard defines the attacks that are resisted by the TPM. These attacks must be considered when determining whether the integrity of TPM_Protected-Capabilities and data in TPM_Shielded-Locations can be damaged. These attacks must be considered when determining whether there is a backdoor method of obtaining access to TPM_Protected-Capabilities and data in TPM_Shielded-Locations. These attacks must be considered when determining whether TPM_Protected-Capabilities have undesirable side effects.

End of informative comment

1. For the purposes of the “Protection” section of the standard, the threats that MUST be considered when determining whether the TPM facilitates subversion of TPM_Protected-Capabilities or data in TPM_Shielded-Locations SHALL include
   a. The methods inherent in physical attacks that fail if the TPM complies with the “physical protection” requirements specified by ISO/IEC 11889
   b. All methods that require execution of instructions in a computing engine in the platform

4.3 Protection of functions

Start of informative comment

A TPM_Protected-Capability must be used to modify TPM_Protected-Capabilities. Other methods must not be allowed to modify TPM_Protected-Capabilities. Otherwise, the integrity of TPM_Protected-Capabilities is unknown.

End of informative comment

1. A TPM SHALL NOT facilitate the alteration of TPM_Protected-Capabilities, except by TPM_Protected-Capabilities.

4.4 Protection of information

Start of informative comment

TPM_Protected-Capabilities must provide the only means from outside the TPM to access information represented by data in TPM_Shielded-Locations. Otherwise, a rogue can reveal data in TPM_Shielded-Locations, or create a derivative of data from TPM_Shielded-Locations (in a way that maintains some or all of the information content of the data) and reveal the derivative.

End of informative comment

1. A TPM SHALL NOT export data that is dependent upon data structures described in part 3 of ISO/IEC 11889, other than via a TPM_Protected-Capability.

4.5 Side effects

Start of informative comment

An implementation of a TPM_Protected-Capability must not disclose the contents of TPM_Shielded-Locations. The only exceptions are when such disclosure is inherent in the definition of the capability or in the methods used by the capability. For example, a capability might be designed specifically to reveal hidden data or might use cryptography and hence always be vulnerable to cryptanalysis. In such cases, some disclosure or risk of disclosure is inherent and cannot be avoided. Other forms of disclosure (by side effects, for example) must always be avoided.

End of informative comment

1. The implementation of a TPM_Protected-Capability in a TPM SHALL NOT facilitate the disclosure or the exposure of information represented by data in TPM-shielded–locations, except by means unavoidably inherent in the TPM definition.

4.6 Exceptions and clarifications

Start of informative comment

These exceptions to the blanket statements in the generic “protection” requirements (above) are fully compatible with the intended effect of those statements. These exceptions affect ISO/IEC 11889-data that is available as plain-text outside the TPM and ISO/IEC 11889-data that can be used without violating security or privacy. These exceptions are valuable because they approve use of TPM resources by vendor-specific commands in particular circumstances.

These clarifications to the blanket statements of the generic “protection” requirements (above) do not materially change the effect of those statements, but serve to approve specific legitimate interpretations of the requirements.

End of informative comment

1. A Shielded Location is a place (memory, register, etc.) where data is protected against interference and exposure, independent of its form
2. A TPM_Protected-Capability is an operation defined in and restricted to those identified in part 3 and 4 of ISO/IEC 11889
3. A vendor specific command or capability MAY use the standard ISO/IEC 11889 owner/operator authorization mechanism
4. A vendor specific command or capability MAY utilize a TPM_PUBKEY structure stored on the TPM so long as the usage of that TPM_PUBKEY structure is authorized using the standard ISO/IEC 11889 authorization mechanism.
5. A vendor specific command or capability MAY use a sequence of standard ISO/IEC 11889 commands. The command MUST propagate the locality used for the call to the used ISO/IEC 11889 commands or capabilities, or set locality to 0.
6. A vendor specific command or capability that takes advantage of exceptions and clarifications to the “protection” requirements MUST be defined as part of the security target of the TPM. Such a vendor specific command or capability MUST be evaluated to meet the Platform Specific TPM and System Security Targets.
7. If a TPM employs vendor-specific cipher-text that is protected against subversion to the same or greater extent as internal TPM-resources stored outside the TPM with ISO/IEC 11889-defined methods, that vendor-specific cipher-text does not necessarily require protection from physical attack. If a TPM location stores only vendor-specific cipher-text that does not require protection from physical attack, that location can be ignored when determining whether the TPM complies with the "physical protection" requirements specified by ISO/IEC 11889.