
**Information technology — Trusted
Platform Module —**

**Part 2:
Design principles**

*Technologies de l'information — Module de plate-forme de confiance —
Partie 2: Principes de conception*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Withdrawn



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

| | |
|--|----|
| 1. Scope | 1 |
| 1.1 Key words | 1 |
| 1.2 Statement Type | 1 |
| 2. Normative references | 2 |
| 3. Abbreviated Terms | 3 |
| 4. Conformance | 5 |
| 4.1 Introduction | 5 |
| 4.2 Threat | 6 |
| 4.3 Protection of functions | 6 |
| 4.4 Protection of information | 6 |
| 4.5 Side effects | 7 |
| 4.6 Exceptions and clarifications | 7 |
| 5. TPM Architecture | 8 |
| 5.1 Interoperability | 8 |
| 5.2 Components | 8 |
| 5.2.1 Input and Output | 9 |
| 5.2.2 Cryptographic Co-Processor | 9 |
| 5.2.3 Key Generation | 11 |
| 5.2.4 HMAC Engine | 12 |
| 5.2.5 Random Number Generator | 13 |
| 5.2.6 SHA-1 Engine | 15 |
| 5.2.7 Power Detection | 16 |
| 5.2.8 Opt-In | 16 |
| 5.2.9 Execution Engine | 17 |
| 5.2.10 Non-Volatile Memory | 17 |
| 5.3 Data Integrity Register (DIR) | 18 |
| 5.4 Platform Configuration Register (PCR) | 18 |
| 6. Endorsement Key Creation | 20 |
| 6.1 Controlling Access to PRIVEK | 21 |
| 6.2 Controlling Access to PUBEK | 21 |
| 7. Attestation Identity Keys | 22 |
| 8. TPM Ownership | 23 |
| 8.1 Platform Ownership and Root of Trust for Storage | 23 |
| 9. Authentication and Authorization Data | 24 |
| 9.1 Dictionary Attack Considerations | 25 |
| 10. TPM Operation | 26 |
| 10.1 TPM Initialization & Operation State Flow | 27 |
| 10.1.1 Initialization | 27 |

| | | |
|--------|---|----|
| 10.2 | Self-Test Modes | 28 |
| 10.2.1 | Operational Self-Test | 29 |
| 10.3 | Startup | 32 |
| 10.4 | Operational Mode | 33 |
| 10.4.1 | Enabling a TPM | 34 |
| 10.4.2 | Activating a TPM | 35 |
| 10.4.3 | Taking TPM Ownership | 36 |
| 10.4.4 | Transitioning Between Operational States | 38 |
| 10.5 | Clearing the TPM | 38 |
| 11. | Physical Presence | 40 |
| 12. | Root of Trust for Reporting (RTR) | 42 |
| 12.1 | Platform Identity | 42 |
| 12.2 | RTR to Platform Binding | 43 |
| 12.3 | Platform Identity and Privacy Considerations | 43 |
| 12.4 | Attestation Identity Keys | 43 |
| 12.4.1 | AIK Creation | 44 |
| 12.4.2 | AIK Storage | 45 |
| 13. | Root of Trust for Storage (RTS) | 46 |
| 13.1 | Loading and Unloading Blobs | 46 |
| 14. | Transport Sessions and Authorization Protocols | 47 |
| 14.1 | Authorization Session Setup | 48 |
| 14.2 | Parameter Declarations for OIAP and OSAP Examples | 50 |
| 14.2.1 | Object-Independent Authorization Protocol (OIAP) | 52 |
| 14.2.2 | Object-Specific Authorization Protocol (OSAP) | 56 |
| 14.3 | Authorization Session Handles | 59 |
| 14.4 | Authorization-Data Insertion Protocol (ADIP) | 60 |
| 14.5 | AuthData Change Protocol (ADCP) | 64 |
| 14.6 | Asymmetric Authorization Change Protocol (AACP) | 65 |
| 15. | ISO/IEC 19790 Evaluations | 66 |
| 15.1 | TPM Profile for successful ISO/IEC 19790 evaluation | 66 |
| 16. | Maintenance | 67 |
| 16.1 | Field Upgrade | 69 |
| 17. | Proof of Locality | 70 |
| 18. | Monotonic Counter | 71 |
| 19. | Transport Protection | 74 |
| 19.1 | Transport encryption and authorization | 75 |
| 19.1.1 | MGF1 parameters | 77 |
| 19.1.2 | HMAC calculation | 78 |
| 19.1.3 | Transport log creation | 78 |
| 19.1.4 | Additional Encryption Mechanisms | 78 |

| | | |
|--------|---|-----|
| 19.2 | Transport Error Handling | 79 |
| 19.3 | Exclusive Transport Sessions | 79 |
| 19.4 | Transport Audit Handling | 80 |
| 19.4.1 | Auditing of wrapped commands | 80 |
| 20. | Audit Commands | 81 |
| 20.1 | Audit Monotonic Counter | 83 |
| 21. | Design Section on Time Stamping | 84 |
| 21.1 | Tick Components | 84 |
| 21.2 | Basic Tick Stamp | 85 |
| 21.3 | Associating a TCV with UTC | 85 |
| 21.4 | Additional Comments and Questions | 87 |
| 22. | Context Management | 89 |
| 23. | Eviction | 91 |
| 24. | Session pool | 92 |
| 25. | Initialization Operations | 93 |
| 26. | HMAC digest rules | 94 |
| 27. | Generic authorization session termination rules | 95 |
| 28. | PCR Grand Unification Theory | 96 |
| 28.1 | Validate Key for use | 98 |
| 29. | Non Volatile Storage | 100 |
| 29.1 | NV storage design principles | 101 |
| 29.1.1 | NV Storage use models | 101 |
| 29.2 | Use of NV storage during manufacturing | 103 |
| 30. | Delegation Model | 104 |
| 30.1 | Table Requirements | 104 |
| 30.2 | How this works | 105 |
| 30.3 | Family Table | 106 |
| 30.4 | Delegate Table | 107 |
| 30.5 | Delegation Administration Control | 108 |
| 30.5.1 | Control in Phase 1 | 109 |
| 30.5.2 | Control in Phase 2 | 110 |
| 30.5.3 | Control in Phase 3 | 110 |
| 30.6 | Family Verification | 110 |
| 30.7 | Use of commands for different states of TPM | 112 |
| 30.8 | Delegation Authorization Values | 112 |
| 30.8.1 | Using the authorization value | 112 |
| 30.9 | DSAP description | 113 |
| 31. | Physical Presence | 116 |
| 31.1 | Use of Physical Presence | 116 |
| 32. | TPM Internal Asymmetric Encryption | 117 |

| | | |
|--------|--|-----|
| 32.1.1 | TPM_ES_RSAESOAEP_SHA1_MGF1 | 117 |
| 32.1.2 | TPM_ES_RSAESPKCSV15 | 118 |
| 32.1.3 | TPM_ES_SYM_CTR | 118 |
| 32.1.4 | TPM_ES_SYM_OFB | 118 |
| 32.2 | TPM Internal Digital Signatures | 118 |
| 32.2.1 | TPM_SS_RSASSAPKCS1v15_SHA1 | 119 |
| 32.2.2 | TPM_SS_RSASSAPKCS1v15_DER | 119 |
| 32.2.3 | TPM_SS_RSASSAPKCS1v15_INFO | 120 |
| 32.2.4 | Use of Signature Schemes | 120 |
| 33. | Key Usage Table | 121 |
| 34. | Direct Anonymous Attestation | 123 |
| 34.1 | TPM_DAA_JOIN | 123 |
| 34.2 | TPM_DAA_Sign | 124 |
| 34.3 | DAA Command summary | 125 |
| 34.3.1 | TPM setup | 125 |
| 34.3.2 | JOIN | 126 |
| 34.3.3 | SIGN | 129 |
| 35. | General Purpose IO | 132 |
| 36. | Redirection | 133 |
| 37. | Structure Versioning | 134 |
| 38. | Certified Migration Key Type | 135 |
| 38.1 | Certified Migration Requirements | 135 |
| 38.2 | Key Creation | 136 |
| 38.3 | Migrate CMK to a MA | 136 |
| 38.4 | Migrate CMK to a MSA | 136 |
| 39. | Revoke Trust | 138 |
| 40. | Mandatory and Optional Functional Blocks | 139 |
| 41. | 1.1a and 1.2 Differences | 142 |
| 42. | Bibliography | 143 |

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

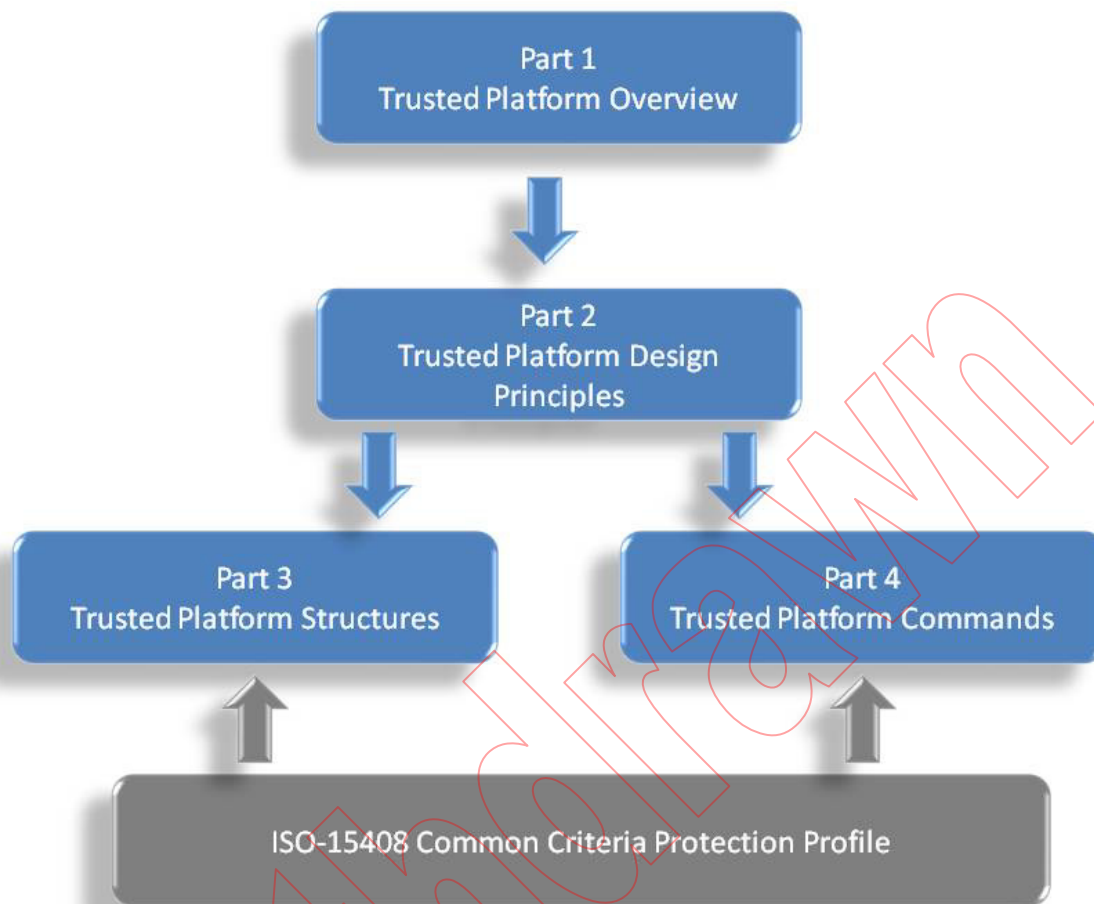


Figure 1. TPM Main Specification Roadmap

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.