INTERNATIONAL STANDARD

ISO/IEC 11889-3

First edition
2009-05-15

Information technology — Trusted Platform Module —

Part 3: Structures

Technologies de l'information — Module de plate-forme de confiance — Partie 3: Structures

withdrawn

Reference number
ISO/IEC 11889-3:2009(E)

© ISO/IEC 2009

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withdrawn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

© ISO/IEC 2009 – All rights reserved

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. Structures and Formats 5
4.1 Representation of Information 5
4.1.1 Endness of Structures 5
4.1.2 Byte Packing 5
4.1.3 Lengths 5
4.1.4 Structure Definitions 5
4.2 Defines 6
4.2.1 Basic data types 6
4.2.2 Boolean types 6
4.2.3 Helper redefinitions 6
4.2.4 Vendor specific 8
5. Structure Tags 9
5.1 TPM_STRUCTURE_TAG 10
6. Types 12
6.1 TPM_RESOURCE_TYPE 12
6.2 TPM_PAYLOAD_TYPE 13
6.3 TPM_ENTITY_TYPE 14
6.4 Handles 15
6.4.1 Reserved Key Handles 16
6.5 TPM_STARTUP_TYPE 17
6.6 TPM_STARTUP_EFFECTS 18
6.7 TPM_PROTOCOL_ID 19
6.8 TPM_ALGORITHM_ID 20
6.9 TPM_PHYSICAL_PRESENCE 21
6.10 TPM_MIGRATE_SCHEME 22
6.11 TPM_EK_TYPE 23
6.12 TPM_PLATFORM_SPECIFIC 24
7. Basic Structures 25
7.1 TPM_STRUCT_VER 25
7.2 TPM_VERSION_BYTE 26
7.3 TPM_VERSION 27
7.4 TPM_DIGEST 28

Withdrawn

© ISO/IEC 2009 – All rights reserved

7.4.1 Creating a PCR composite hash 29
7.5 TPM_NONCE 30
7.5.1 TPM_PROOF 31
7.6 TPM_AUTHDATA 32
7.7 TPM_KEY_HANDLE_LIST 33
7.8 TPM_KEY_USAGE values 34
7.8.1 Mandatory Key Usage Schemes 34
7.9 TPM_AUTH_DATA_USAGE values 36
7.10 TPM_KEY_FLAGS 37
7.11 TPM_CHANGEAUTH_VALIDATE 38
7.12 TPM_MIGRATIONKEYAUTH 39
7.13 TPM_COUNTER_VALUE 40
7.14 TPM_SIGN_INFO Structure 41
7.15 TPM_MSA_COMPOSITE 42
7.16 TPM_CMK_AUTH 43
7.17 TPM_CMK_DELEGATE values 44
7.18 TPM_SELECT_SIZE 45
7.19 TPM_CMK_MIGAUTH 46
7.20 TPM_CMK_SIGTICKET 47
7.21 TPM_CMK_MA_APPROVAL 48
8. TPM_TAG (Command and Response Tags) 49
9. Internal Data Held By TPM 50
9.1 TPM_PERMANENT_FLAGS 51
9.1.1 Flag Restrictions 55
9.2 TPM_STCLEAR_FLAGS 56
9.2.1 Flag Restrictions 58
9.3 TPM_STANY_FLAGS 59
9.3.1 Flag Restrictions 60
9.4 TPM_PERMANENT_DATA 61
9.4.1 Flag Restrictions 64
9.5 TPM_STCLEAR_DATA 65
Flag Restrictions 66
Deferred Physical Presence Bit Map 66
9.6 TPM_STANY_DATA 67
9.6.1 Flag Restrictions 68
10. PCR Structures 69
10.1 TPM_PCR_SELECTION 70
10.2 TPM_PCR_COMPOSITE 72
10.3 TPM_PCR_INFO 73
10.4 TPM_PCR_INFO_LONG 74

Withdrawn

© ISO/IEC 2009 – All rights reserved

10.5 TPM_PCR_INFO_SHORT 75
10.6 TPM_LOCALITY_SELECTION 76
10.7 PCR Attributes 77
10.8 TPM_PCR_ATTRIBUTES 78
10.8.1 Comparing command locality to PCR flags 79
10.9 Debug PCR register 80
10.10 Mapping PCR Structures 81
11. Storage Structures 83
11.1 TPM_STORED_DATA 83
11.2 TPM_STORED_DATA12 84
11.3 TPM_SEALED_DATA 85
11.4 TPM_SYMMETRIC_KEY 86
11.5 TPM_BOUND_DATA 87
12. TPM_KEY complex 88
12.1 TPM_KEY_PARMS 89
12.1.1 TPM_RSA_KEY_PARMS 90
12.1.2 TPM_SYMMETRIC_KEY_PARMS 90
12.2 TPM_KEY 91
12.3 TPM_KEY12 92
12.4 TPM_STORE_PUBKEY 93
12.5 TPM_PUBKEY 94
12.6 TPM_STORE_ASYMKEY 95
12.7 TPM_STORE_PRIVKEY 96
12.8 TPM_MIGRATE_ASYMKEY 97
12.9 TPM_KEY_CONTROL 98
13. Signed Structures 99
13.1 TPM_CERTIFY_INFO Structure 99
13.2 TPM_CERTIFY_INFO2 Structure 100
13.3 TPM_QUOTE_INFO Structure 101
13.4 TPM_QUOTE_INFO2 Structure 102
14. Identity Structures 103
14.1 TPM_EK_BLOB 103
14.2 TPM_EK_BLOB_ACTIVATE 104
14.3 TPM_EK_BLOB_AUTH 105
14.4 TPM_CHOSENID_HASH 106
14.5 TPM_IDENTITY_CONTENTS 107
14.6 TPM_IDENTITY_REQ 108
14.7 TPM_IDENTITY_PROOF 109
14.8 TPM_ASYM_CA_CONTENTS 110
14.9 TPM_SYM_CA_ATTESTATION 111

Withdrawn

© ISO/IEC 2009 – All rights reserved

15. Transport structures 112
15.1 TPM _TRANSPORT_PUBLIC 112
15.1.1 TPM_TRANSPORT_ATTRIBUTES Definitions 112
15.2 TPM_TRANSPORT_INTERNAL 113
15.3 TPM_TRANSPORT_LOG_IN structure 114
15.4 TPM_TRANSPORT_LOG_OUT structure 115
15.5 TPM_TRANSPORT_AUTH structure 116
16. Audit Structures 117
16.1 TPM_AUDIT_EVENT_IN structure 117
16.2 TPM_AUDIT_EVENT_OUT structure 118
17. Tick Structures 119
17.1 TPM_CURRENT_TICKS 119
18. Return codes 120
19. Ordinals 125
19.1 TSC Ordinals 133
20. Context structures 134
20.1 TPM_CONTEXT_BLOB 134
20.2 TPM_CONTEXT_SENSITIVE 136
21. NV storage structures 137
21.1 TPM_NV_INDEX 137
21.1.1 Required TPM_NV_INDEX values 138
21.1.2 Reserved Index values 139
21.2 TPM_NV_ATTRIBUTES 140
21.3 TPM_NV_DATA_PUBLIC 142
21.4 TPM_NV_DATA_SENSITIVE 143
21.5 Max NV Size 144
21.6 TPM_NV_DATA_AREA 145
22. Delegate Structures 146
22.1 Structures and encryption 146
22.2 Delegate Definitions 147
22.2.1 Owner Permission Settings 148
22.2.2 Owner commands not delegated 149
22.2.3 Key Permission settings 150
22.2.4 Key commands not delegated 151
22.3 TPM_FAMILY_FLAGS 152
22.4 TPM_FAMILY_LABEL 153
22.5 TPM_FAMILY_TABLE_ENTRY 154
22.6 TPM_FAMILY_TABLE 155
22.7 TPM_DELEGATE_LABEL 156
22.8 TPM_DELEGATE_PUBLIC 157

Withdrawn

© ISO/IEC 2009 – All rights reserved

22.9 TPM_DELEGATE_TABLE_ROW 158
22.10 TPM_DELEGATE_TABLE 159
22.11 TPM_DELEGATE_SENSITIVE 160
22.12 TPM_DELEGATE_OWNER_BLOB 161
22.13 TPM_DELEGATE_KEY_BLOB 162
22.14 TPM_FAMILY_OPERATION Values 163
23. Capability areas 164
23.1 TPM_CAPABILITY_AREA for TPM_GetCapability 164
23.2 CAP_PROPERTY SubCap values for TPM_GetCapability 167
23.3 Bit ordering for structures 169
23.3.1 Deprecated GetCapability Responses 169
23.4 TPM_CAPABILITY_AREA Values for TPM_SetCapability 170
23.5 SubCap Values for TPM_SetCapability 171
23.6 TPM_CAP_VERSION_INFO 172
23.7 TPM_DA_INFO 173
23.8 TPM_DA_INFO_LIMITED 174
23.9 TPM_DA_STATE 175
23.10 TPM_DA_ACTION_TYPE 176
24. DAA Structures 177
24.1 Size definitions 177
24.2 Constant definitions 177
24.3 TPM_DAA_ISSUER 178
24.4 TPM_DAA_TPM 179
24.5 TPM_DAA_CONTEXT 180
24.6 TPM_DAA_JOINDATA 181
24.7 TPM_STANY_DATA Additions 182
24.8 TPM_DAA_BLOB 183
24.9 TPM_DAA_SENSITIVE 184
25. Redirection 185
25.1 TPM_REDIR_COMMAND 185
26. Deprecated Structures 186
26.1 Persistent Flags 186
26.2 Volatile Flags 186
26.3 TPM persistent data 186
26.4 TPM volatile data 186
26.5 TPM SV data 187
26.6 TPM_SYM_MODE 187
27. Bibliography 188

Withdrawn

© ISO/IEC 2009 – All rights reserved

List of Tables

Table 1: Basic data type parameters 6
Table 2: Boolean types 6
Table 3: Helper redefinition parameters 6
Table 4: Vendor specific parameters 8
Table 5: TPM_StructureTag 10
Table 6: TPM_ResourceTypes 12
Table 7: TPM_PAYLOAD_TYPE values 13
Table 8: TPM_ENTITY_TYPE LSB Values 14
Table 9: TPM_ENTITY_TYPE MSB Values 14
Table 10: Key Handle Values 16
Table 11: TPM_STARTUP_TYPE Values 17
Table 12: Types of Startup 18
Table 13: TPM_PROTOCOL_ID Values 19
Table 14: TPM_ALGORITHM_ID values 20
Table 15: TPM_PHYSICAL_PRESENCE parameters 21
Table 16: TPM_MIGRATE_SCHEME values 22
Table 17: TPM_EK_TYPE parameters 23
Table 18: TPM_PLATFORM_SPECIFIC parameters 24
Table 19: TPM_STRUCT_VER parameters 25
Table 20: TPM_VERSION_BYTE rule 26
Table 21: TPM_VERSION parameters 27
Table 22: TPM_DIGEST parameters 28
Table 23: TPM_DIGEST redefinitions 28
Table 24: TPM_NONCE parameters 30
Table 25: TPM_NONCE redefinitons 30
Table 24: TPM_PROOF parameters 31
Table 26: TPM_AUTHDATA redefinitions 32
Table 27: TPM_KEY_HANDLE_LIST parameters 33
Table 28: TPM_KEY_USAGE values 34
Table 29: Mandatory Key Usage Schemes 35
Table 30: Valid encryption schemes 35
Table 31: Valid signature schemes 35
Table 32: Combinations of TPM_AUTH_DATA_USAGE values 36
Table 33: TPM_AUTH_DATA_USAGE values 36
Table 34: TPM_KEY_FLAGS Values 37
Table 35: TPM_CHANGEAUTH_VALIDATE parameters 38
Table 36: TPM_MIGRATIONKEYAUTH parameters 39
Table 37: TPM_COUNTER_VALUE parameters 40

Withdrawn

© ISO/IEC 2009 – All rights reserved

Table 38: TPM_SIGN_INFO Structure parameters 41
Table 39: TPM_MSA_COMPOSITE parameters 42
Table 40: TPM_CMK_AUTH parameters 43
Table 41: TPM_CMK_DELEGATE values 44
Table 42: TPM_SELECT_SIZE parameters 45
Table 43: TPM_CMK_MIGAUTH parameters 46
Table 44: TPM_CMK_SIGTICKET parameters 47
Table 45: TPM_CMK_MA_APPROVALparameters 48
Table 46: TPM_TAG (Command and Response Tags) 49
Table 47: TPM_PERMANENT_FLAGS parameters 51
Table 48: TPM_PERMANENT_FLAGS restrictions 55
Table 49: TPM_STCLEAR_FLAGS parameters 56
Table 50: TPM_STCLEAR_FLAGS restrictions 58
Table 51: TPM_STANY_FLAGS parameters 59
Table 52: TPM_STANY_FLAGS restrictions 60
Table 53: TPM_PERMANENT_DATA parameters 62
Table 54: Flag Restrictions 64
Table 55: TPM_STCLEAR_DATA parameters 65
Table 56: Flag Restrictions 66
Table 57: Deferred Physical Presence Bit Map 66
Table 58: TPM_STANY_DATA parameters 67
Table 59: Flag Restrictions 68
Table 60: TPM_PCR_SELECTION parameters 71
Table 61: TPM_PCR_COMPOSITE parameters 72
Table 62: TPM_PCR_INFO parameters 73
Table 63: TPM_PCR_INFO_LONG parameters 74
Table 64: TPM_PCR_INFO_SHORT parameters 75
Table 65: TPM_LOCALITY_SELECTION definitions 76
Table 66: TPM_PCR_ATTRIBUTES - types of persistent data 78
Table 67: TPM_STORED_DATA parameters 83
Table 68: TPM_STORED_DATA12 parameters 84
Table 69: TPM_SEALED_DATA parameters 85
Table 70: TPM_SYMMETRIC_KEY parameters 86
Table 71: TPM_BOUND_DATA parameters 87
Table 72: TPM_KEY_PARMS parameters 89
Table 73: TPM_KEY_PARMS descriptions 89
Table 74: TPM_RSA_KEY_PARMS parameters 90
Table 75: TPM_SYMMETRIC_KEY_PARMS parameters 90
Table 76: TPM_KEY parameters 91
Table 77: TPM_KEY12 parameters 92

Withdrawn

© ISO/IEC 2009 – All rights reserved

Table 78: TPM_STORE_PUBKEY parameters 93
Table 79: TPM_STORE_PUBKEY algorithm 93
Table 80: TPM_PUBKEY parameters 94
Table 81: TPM_STORE_ASYMKEY parameters 95
Table 82: TPM_STORE_PRIVKEY parameters 96
Table 83: TPM_STORE_PRIVKEY algorithm 96
Table 84: TPM_MIGRATE_ASYMKEY parameters 97
Table 85: TPM_KEY_CONTROL parameters 98
Table 86: TPM_CERTIFY_INFO Structure parameters 99
Table 87: TPM_CERTIFY_INFO2 Structure parameters 100
Table 88: TPM_QUOTE_INFO Structure parameters 101
Table 89: TPM_QUOTE_INFO2 Structure parameters 102
Table 90: TPM_EK_BLOB parameters 103
Table 91: TPM_EK_BLOB_ACTIVATE parameters 104
Table 92: TPM_EK_BLOB_AUTH parameters 105
Table 93: TPM_CHOSENID_HASH parameters 106
Table 94: TPM_IDENTITY_CONTENTS parameters 107
Table 95: TPM_IDENTITY_REQ parameters 108
Table 96: TPM_IDENTITY_PROOF parameters 109
Table 97: TPM_ASYM_CA_CONTENTS parameters 110
Table 98: TPM_SYM_CA_ATTESTATION parameters 111
Table 99: TPM _TRANSPORT_PUBLIC parameters 112
Table 100: TPM_TRANSPORT_ATTRIBUTES Definitions 112
Table 101: TPM_TRANSPORT_INTERNAL parameters 113
Table 102: TPM_TRANSPORT_LOG_IN structure parameters 114
Table 103: TPM_TRANSPORT_LOG_OUT structure parameters 115
Table 104: TPM_TRANSPORT_AUTH structure parameters 116
Table 105: TPM_AUDIT_EVENT_IN structure parameters 117
Table 106: TPM_AUDIT_EVENT_OUT structure parameters 118
Table 107: TPM_CURRENT_TICKS parameters 119
Table 108: Mask Parameters 121
Table 109: TPM-defined fatal error codes 122
Table 110: TPM-defined non-fatal errors 124
Table 111: Ordinal masks 125
Table 112: Ordinal purviews 126
Table 113: Ordinal combinations 126
Table 114: Column descriptions 126
Table 115: Ordinal table 127
Table 116: TSC Ordinals 133
Table 117: TPM_CONTEXT_BLOB parameters 135

Withdrawn

© ISO/IEC 2009 – All rights reserved

Table 118: TPM_CONTEXT_SENSITIVE parameters 136
Table 119: Required TPM_NV_INDEX values 138
Table 120: Reserved Index values 139
Table 121: TPM_NV_ATTRIBUTES parameters 140
Table 122: TPM_NV_ATTRIBUTES attribute values 141
Table 123: TPM_NV_DATA_PUBLIC parameters 142
Table 124: TPM_NV_DATA_SENSITIVE parameters 143
Table 125: Delegate Definitions parameters 147
Table 126: Owner Permission Settings - Per1 bits 148
Table 127: Owner Permission Settings - Per2 bits 149
Table 128: Owner commands not delegated 149
Table 129: Key Permission settings - Per1 bits 150
Table 130: Key Permission settings - Per2 bits 151
Table 131: Key commands not delegated 151
Table 132: TPM_FAMILY_FLAGS bit settings 152
Table 133: TPM_FAMILY_LABEL parameters 153
Table 134: TPM_FAMILY_TABLE_ENTRY parameters 154
Table 135: TPM_FAMILY_TABLE parameters 155
Table 136: TPM_DELEGATE_LABEL parameters 156
Table 137: TPM_DELEGATE_PUBLIC parameters 157
Table 138: TPM_DELEGATE_TABLE_ROW 158
Table 139: TPM_DELEGATE_TABLE parameters 159
Table 140: TPM_DELEGATE_SENSITIVE parameters 160
Table 141: TPM_DELEGATE_OWNER_BLOB parameters 161
Table 142: TPM_DELEGATE_KEY_BLOB parameters 162
Table 143: TPM_FAMILY_OPERATION Values 163
Table 144: TPM_CAPABILITY_AREA Values for TPM_GetCapability 165
Table 145: TPM_CAP_PROPERTY SubCap Values for TPM_GetCapability 167
Table 146: Deprecated GetCapability Responses 169
Table 147: TPM_CAPABILITY_AREA Values for TPM_SetCapability 170
Table 148: TPM_CAP_VERSION_INFO parameters 172
Table 149: TPM_CAP_VERSION_INFO example output 172
Table 150: TPM_DA_INFO parameters 173
Table 151: TPM_DA_INFO_LIMITED parameters 174
Table 152: TPM_DA_STATE Values 175
Table 153: TPM_DA_ACTION_TYPE parameters 176
Table 154: TPM_DA_ACTION_TYPE action values 176
Table 155: TPM_DAA_ISSUER parameters 178
Table 156: TPM_DAA_TPM parameters 179
Table 157: TPM_DAA_CONTEXT parameters 180

Withdrawn

© ISO/IEC 2009 – All rights reserved

Table 158: TPM_DAA_JOINDATA parameters 181
Table 159: TPM_STANY_DATA Additions: types of volatile data 182
Table 160: TPM_DAA_BLOB parameters 183
Table 161: TPM_DAA_SENSITIVE parameters 184
Table 162: TPM_REDIR_COMMAND 185
Table 163. TPM_SYM_MODE values 187

Withdrawn

© ISO/IEC 2009 – All rights reserved

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 11889-3 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*

Withdrawn

© ISO/IEC 2009 – All rights reserved

Introduction

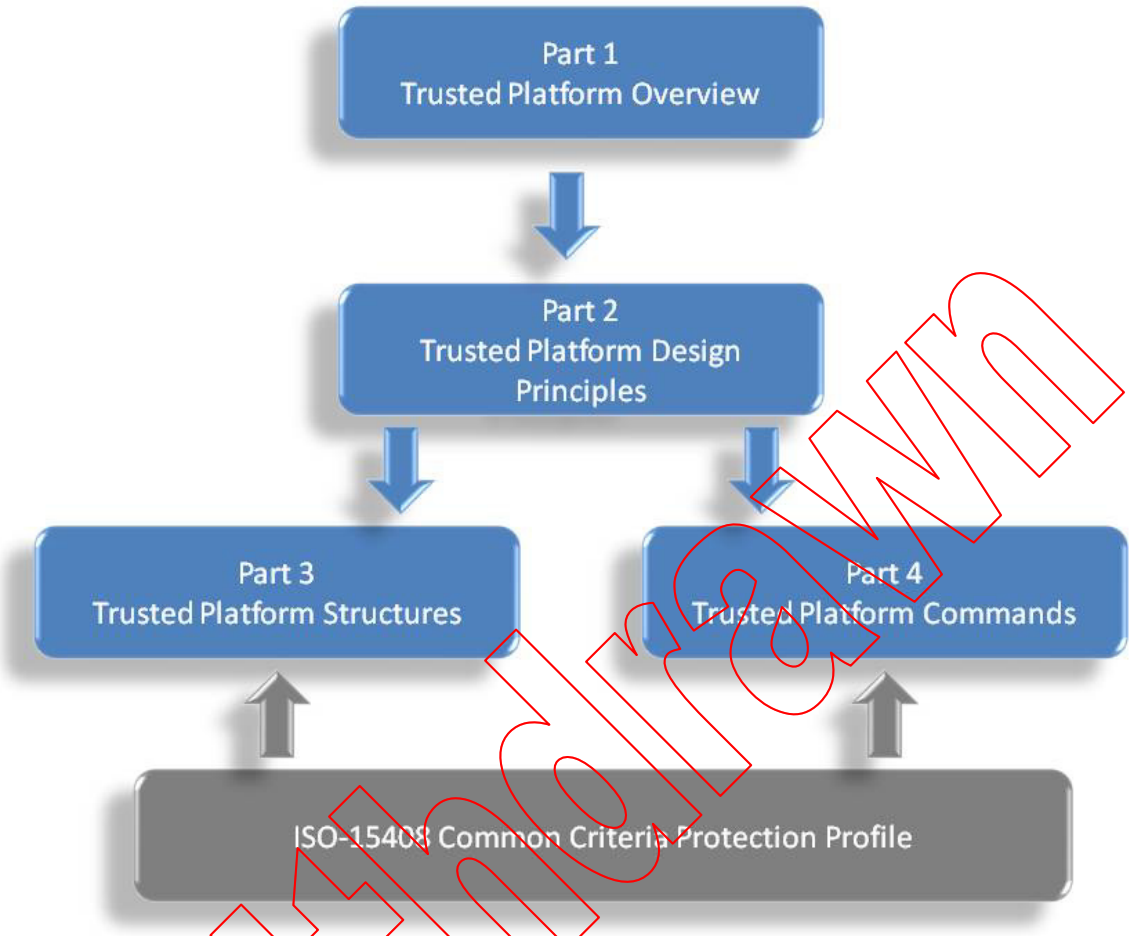

Figure 1. TPM Main Specification Roadmap

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

Withdrawn

© ISO/IEC 2009 – All rights reserved

Information technology — Trusted Platform Module —

Part 3:
Structures

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 3 defines the structures and constants in use by the TPM. As the TPM must interoperate between various implementations, these structures enable the required interoperability. The other rationale for defining the structures is that some of the structures require security properties, either confidentiality or integrity calculations. If the structures are built incorrectly the security properties may not be present, hence the need to define the structures.

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).

Withdrawn

© ISO/IEC 2009 – All rights reserved

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.

Withdrawn

© ISO/IEC 2009 – All rights reserved