

---

---

**Information technology — Trusted  
Platform Module Library —**

**Part 2:  
Structures**

*Technologies de l'information — Bibliothèque de module  
de plate-forme de confiance —  
Partie 2: Structures*

This document is a preview generated by ERS



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Ch. de Blandonnet 8 • CP 401  
CH-1214 Vernier, Geneva, Switzerland  
Tel. +41 22 749 01 11  
Fax +41 22 749 09 47  
copyright@iso.org  
www.iso.org

## CONTENTS

|                                                   |     |
|---------------------------------------------------|-----|
| Foreword .....                                    | xv  |
| Introduction .....                                | xvi |
| 1 Scope .....                                     | 1   |
| 2 Normative references .....                      | 1   |
| 3 Terms and definitions .....                     | 1   |
| 4 Symbols and abbreviated terms .....             | 1   |
| 5 Notation .....                                  | 1   |
| 5.1 Introduction .....                            | 1   |
| 5.2 Named Constants .....                         | 2   |
| 5.3 Data Type Aliases (typedefs) .....            | 3   |
| 5.4 Enumerations .....                            | 3   |
| 5.5 Interface Type .....                          | 4   |
| 5.6 Arrays .....                                  | 5   |
| 5.7 Structure Definitions .....                   | 6   |
| 5.8 Conditional Types .....                       | 7   |
| 5.9 Unions .....                                  | 8   |
| 5.9.1 Introduction .....                          | 8   |
| 5.9.2 Union Definition .....                      | 8   |
| 5.9.3 Union Instance .....                        | 9   |
| 5.9.4 Union Selector Definition .....             | 10  |
| 5.10 Bit Field Definitions .....                  | 11  |
| 5.11 Parameter Limits .....                       | 12  |
| 5.12 Enumeration Macro .....                      | 13  |
| 5.13 Size Checking .....                          | 13  |
| 5.14 Data Direction .....                         | 14  |
| 5.15 Structure Validations .....                  | 15  |
| 5.16 Name Prefix Convention .....                 | 15  |
| 5.17 Data Alignment .....                         | 16  |
| 5.18 Parameter Unmarshaling Errors .....          | 16  |
| 6 Base Types .....                                | 18  |
| 6.1 Primitive Types .....                         | 18  |
| 6.2 Miscellaneous Types .....                     | 18  |
| 7 Constants .....                                 | 19  |
| 7.1 TPM_SPEC (Specification Version Values) ..... | 19  |
| 7.2 TPM_GENERATED .....                           | 19  |
| 7.3 TPM_ALG_ID .....                              | 20  |
| 7.4 TPM_ECC_CURVE .....                           | 24  |
| 7.5 TPM_CC (Command Codes) .....                  | 24  |

|       |                                         |    |
|-------|-----------------------------------------|----|
| 7.5.1 | Format .....                            | 24 |
| 7.5.2 | Description.....                        | 25 |
| 7.5.3 | TPM_CC Listing .....                    | 26 |
| 7.6   | TPM_RC (Response Codes) .....           | 29 |
| 7.6.1 | Description.....                        | 29 |
| 7.6.2 | Response Code Formats.....              | 30 |
| 7.6.3 | TPM_RC Values.....                      | 33 |
| 7.7   | TPM_CLOCK_ADJUST .....                  | 38 |
| 7.8   | TPM_EO (EA Arithmetic Operands) .....   | 38 |
| 7.9   | TPM_ST (Structure Tags) .....           | 39 |
| 7.10  | TPM_SU (Startup Type).....              | 41 |
| 7.11  | TPM_SE (Session Type).....              | 41 |
| 7.12  | TPM_CAP (Capabilities) .....            | 42 |
| 7.13  | TPM_PT (Property Tag).....              | 43 |
| 7.14  | TPM_PT_PCR (PCR Property Tag).....      | 48 |
| 7.15  | TPM_PS (Platform Specific).....         | 50 |
| 8     | Handles .....                           | 51 |
| 8.1   | Introduction.....                       | 51 |
| 8.2   | TPM_HT (Handle Types) .....             | 51 |
| 8.3   | Persistent Handle Sub-ranges .....      | 52 |
| 8.4   | TPM_RH (Permanent Handles) .....        | 53 |
| 8.5   | TPM_HC (Handle Value Constants) .....   | 54 |
| 9     | Attribute Structures.....               | 56 |
| 9.1   | Description .....                       | 56 |
| 9.2   | TPMA_ALGORITHM .....                    | 56 |
| 9.3   | TPMA_OBJECT (Object Attributes) .....   | 56 |
| 9.3.1 | Introduction.....                       | 56 |
| 9.3.2 | Structure Definition .....              | 57 |
| 9.3.3 | Attribute Descriptions .....            | 58 |
| 9.4   | TPMA_SESSION (Session Attributes).....  | 63 |
| 9.5   | TPMA_LOCALITY (Locality Attribute)..... | 64 |
| 9.6   | TPMA_PERMANENT.....                     | 65 |
| 9.7   | TPMA_STARTUP_CLEAR.....                 | 66 |
| 9.8   | TPMA_MEMORY .....                       | 67 |
| 9.9   | TPMA_CC (Command Code Attributes) ..... | 68 |
| 9.9.1 | Introduction.....                       | 68 |
| 9.9.2 | Structure Definition .....              | 68 |
| 9.9.3 | Field Descriptions .....                | 68 |
| 10    | Interface Types.....                    | 71 |
| 10.1  | Introduction.....                       | 71 |
| 10.2  | TPMI_YES_NO .....                       | 71 |
| 10.3  | TPMI_DH_OBJECT .....                    | 71 |

|                                                              |    |
|--------------------------------------------------------------|----|
| 10.4 TPMI_DH_PERSISTENT .....                                | 72 |
| 10.5 TPMI_DH_ENTITY .....                                    | 72 |
| 10.6 TPMI_DH_PCR .....                                       | 73 |
| 10.7 TPMI_SH_AUTH_SESSION .....                              | 73 |
| 10.8 TPMI_SH_HMAC .....                                      | 73 |
| 10.9 TPMI_SH_POLICY .....                                    | 73 |
| 10.10 TPMI_DH_CONTEXT .....                                  | 74 |
| 10.11 TPMI_RH_HIERARCHY .....                                | 74 |
| 10.12 TPMI_RH_ENABLES .....                                  | 74 |
| 10.13 TPMI_RH_HIERARCHY_AUTH .....                           | 75 |
| 10.14 TPMI_RH_PLATFORM .....                                 | 75 |
| 10.15 TPMI_RH_OWNER .....                                    | 75 |
| 10.16 TPMI_RH_ENDORSEMENT .....                              | 76 |
| 10.17 TPMI_RH_PROVISION .....                                | 76 |
| 10.18 TPMI_RH_CLEAR .....                                    | 76 |
| 10.19 TPMI_RH_NV_AUTH .....                                  | 77 |
| 10.20 TPMI_RH_LOCKOUT .....                                  | 77 |
| 10.21 TPMI_RH_NV_INDEX .....                                 | 77 |
| 10.22 TPMI_ALG_HASH .....                                    | 78 |
| 10.23 TPMI_ALG_ASYM (Asymmetric Algorithms) .....            | 78 |
| 10.24 TPMI_ALG_SYM (Symmetric Algorithms) .....              | 79 |
| 10.25 TPMI_ALG_SYM_OBJECT .....                              | 79 |
| 10.26 TPMI_ALG_SYM_MODE .....                                | 80 |
| 10.27 TPMI_ALG_KDF (Key and Mask Generation Functions) ..... | 80 |
| 10.28 TPMI_ALG_SIG_SCHEME .....                              | 81 |
| 10.29 TPMI_ECC_KEY_EXCHANGE .....                            | 81 |
| 10.30 TPMI_ST_COMMAND_TAG .....                              | 81 |
| 11 Structure Definitions .....                               | 83 |
| 11.1 TPMS_EMPTY .....                                        | 83 |
| 11.2 TPMS_ALGORITHM_DESCRIPTION .....                        | 83 |
| 11.3 Hash/Digest Structures .....                            | 84 |
| 11.3.1 TPMU_HA (Hash) .....                                  | 84 |
| 11.3.2 TPMT_HA .....                                         | 84 |
| 11.4 Sized Buffers .....                                     | 85 |
| 11.4.1 Introduction .....                                    | 85 |
| 11.4.2 TPM2B_DIGEST .....                                    | 85 |
| 11.4.3 TPM2B_DATA .....                                      | 86 |
| 11.4.4 TPM2B_NONCE .....                                     | 86 |
| 11.4.5 TPM2B_AUTH .....                                      | 86 |
| 11.4.6 TPM2B_OPERAND .....                                   | 86 |
| 11.4.7 TPM2B_EVENT .....                                     | 87 |
| 11.4.8 TPM2B_MAX_BUFFER .....                                | 87 |
| 11.4.9 TPM2B_MAX_NV_BUFFER .....                             | 87 |
| 11.4.10 TPM2B_TIMEOUT .....                                  | 88 |
| 11.4.11 TPM2B_IV .....                                       | 88 |
| 11.5 Names .....                                             | 88 |
| 11.5.1 Introduction .....                                    | 88 |
| 11.5.2 TPMU_NAME .....                                       | 88 |
| 11.5.3 TPM2B_NAME .....                                      | 89 |
| 11.6 PCR Structures .....                                    | 89 |
| 11.6.1 TPMS_PCR_SELECT .....                                 | 89 |

|                                              |     |
|----------------------------------------------|-----|
| 11.6.2 TPMS_PCR_SELECTION.....               | 90  |
| 11.7 Tickets .....                           | 90  |
| 11.7.1 Introduction.....                     | 90  |
| 11.7.2 A NULL Ticket.....                    | 91  |
| 11.7.3 TPMT_TK_CREATION.....                 | 92  |
| 11.7.4 TPMT_TK_VERIFIED.....                 | 93  |
| 11.7.5 TPMT_TK_AUTH .....                    | 94  |
| 11.7.6 TPMT_TK_HASHCHECK.....                | 95  |
| 11.8 Property Structures .....               | 95  |
| 11.8.1 TPMS_ALG_PROPERTY.....                | 95  |
| 11.8.2 TPMS_TAGGED_PROPERTY.....             | 95  |
| 11.8.3 TPMS_TAGGED_PCR_SELECT.....           | 96  |
| 11.9 Lists .....                             | 96  |
| 11.9.1 TPML_CC.....                          | 96  |
| 11.9.2 TPML_CCA.....                         | 97  |
| 11.9.3 TPML_ALG.....                         | 97  |
| 11.9.4 TPML_HANDLE.....                      | 97  |
| 11.9.5 TPML_DIGEST.....                      | 98  |
| 11.9.6 TPML_DIGEST_VALUES .....              | 98  |
| 11.9.7 TPM2B_DIGEST_VALUES.....              | 98  |
| 11.9.8 TPML_PCR_SELECTION.....               | 99  |
| 11.9.9 TPML_ALG_PROPERTY.....                | 99  |
| 11.9.10 TPML_TAGGED_TPM_PROPERTY.....        | 99  |
| 11.9.11 TPML_TAGGED_PCR_PROPERTY.....        | 100 |
| 11.9.12 TPML_ECC_CURVE .....                 | 100 |
| 11.10 Capabilities Structures.....           | 100 |
| 11.10.1 TPMU_CAPABILITIES.....               | 100 |
| 11.10.2 TPMS_CAPABILITY_DATA.....            | 101 |
| 11.11 Clock/Counter Structures .....         | 101 |
| 11.11.1 PMS_CLOCK_INFO .....                 | 101 |
| 11.11.2 <i>Clock</i> .....                   | 101 |
| 11.11.3 <i>ResetCount</i> .....              | 101 |
| 11.11.4 <i>RestartCount</i> .....            | 102 |
| 11.11.5 <i>Safe</i> .....                    | 102 |
| 11.11.6 TPMS_TIME_INFO .....                 | 102 |
| 11.12 TPM Attestation Structures .....       | 103 |
| 11.12.1 Introduction.....                    | 103 |
| 11.12.2 TPMS_TIME_ATTEST_INFO .....          | 103 |
| 11.12.3 TPMS_CERTIFY_INFO .....              | 103 |
| 11.12.1 TPMS_QUOTE_INFO.....                 | 103 |
| 11.12.2 TPMS_COMMAND_AUDIT_INFO.....         | 104 |
| 11.12.3 TPMS_SESSION_AUDIT_INFO.....         | 104 |
| 11.12.4 TPMS_CREATION_INFO.....              | 104 |
| 11.12.5 TPMS_NV_CERTIFY_INFO .....           | 104 |
| 11.12.6 TPMI_ST_ATTEST .....                 | 105 |
| 11.12.7 TPMU_ATTEST .....                    | 105 |
| 11.12.8 TPMS_ATTEST.....                     | 105 |
| 11.12.9 TPM2B_ATTEST.....                    | 106 |
| 11.13 Authorization Structures.....          | 106 |
| 11.13.1 Introduction.....                    | 106 |
| 11.13.2 TPMS_AUTH_COMMAND .....              | 106 |
| 11.13.3 TPMS_AUTH_RESPONSE .....             | 106 |
| 12 Algorithm Parameters and Structures ..... | 107 |

|                                        |     |
|----------------------------------------|-----|
| 12.1 Symmetric .....                   | 107 |
| 12.1.1 Introduction .....              | 107 |
| 12.1.2 TPMI_AES_KEY_BITS .....         | 107 |
| 12.1.3 TPMI_SM4_KEY_BITS .....         | 107 |
| 12.1.4 TPMI_CAMELLIA_KEY_BITS .....    | 108 |
| 12.1.5 TPMU_SYM_KEY_BITS .....         | 108 |
| 12.1.6 TPMU_SYM_MODE .....             | 108 |
| 12.1.7 TPMU_SYM_DETAILS .....          | 109 |
| 12.1.8 TPMT_SYM_DEF .....              | 109 |
| 12.1.9 TPMT_SYM_DEF_OBJECT .....       | 110 |
| 12.1.10 TPM2B_SYM_KEY .....            | 110 |
| 12.1.11 TPMS_SYMCIPHER_PARMS .....     | 110 |
| 12.1.12 TPM2B_SENSITIVE_DATA .....     | 110 |
| 12.1.13 TPMS_SENSITIVE_CREATE .....    | 111 |
| 12.1.14 TPM2B_SENSITIVE_CREATE .....   | 111 |
| 12.1.15 TPMS_SCHEME_SIGHASH .....      | 112 |
| 12.1.16 TPMI_ALG_HASH_SCHEME .....     | 112 |
| 12.1.17 HMAC_SIG_SCHEME .....          | 112 |
| 12.1.18 TPMS_SCHEME_XOR .....          | 113 |
| 12.1.19 TPMU_SCHEME_HMAC .....         | 113 |
| 12.1.20 TPMT_KEYEDHASH_SCHEME .....    | 113 |
| 12.2 Asymmetric .....                  | 114 |
| 12.2.1 Signing Schemes .....           | 114 |
| 12.2.2 Encryption Schemes .....        | 116 |
| 12.2.3 Key Derivation Schemes .....    | 116 |
| 12.2.4 RSA .....                       | 119 |
| 12.2.5 ECC .....                       | 122 |
| 12.3 Signatures .....                  | 124 |
| 12.3.1 TPMS_SIGNATURE_RSASSA .....     | 124 |
| 12.3.2 TPMS_SIGNATURE_RSAPSS .....     | 124 |
| 12.3.3 TPMS_SIGNATURE_ECDSA .....      | 125 |
| 12.3.4 TPMU_SIGNATURE .....            | 125 |
| 12.3.5 TPMT_SIGNATURE .....            | 126 |
| 12.4 Key/Secret Exchange .....         | 126 |
| 12.4.1 Introduction .....              | 126 |
| 12.4.2 TPMU_ENCRYPTED_SECRET .....     | 126 |
| 12.4.3 TPM2B_ENCRYPTED_SECRET .....    | 127 |
| 13 Key/Object Complex .....            | 128 |
| 13.1 Introduction .....                | 128 |
| 13.2 Public Area Structures .....      | 128 |
| 13.2.1 Description .....               | 128 |
| 13.2.2 TPMI_ALG_PUBLIC .....           | 128 |
| 13.2.3 Type-Specific Parameters .....  | 128 |
| 13.2.4 TPMT_PUBLIC .....               | 132 |
| 13.2.5 TPM2B_PUBLIC .....              | 132 |
| 13.3 Private Area Structures .....     | 133 |
| 13.3.1 Introduction .....              | 133 |
| 13.3.2 Sensitive Data Structures ..... | 133 |
| 13.3.3 TPM2B_SENSITIVE .....           | 134 |
| 13.3.4 Encryption .....                | 135 |
| 13.3.5 Integrity .....                 | 135 |
| 13.3.6 _PRIVATE .....                  | 135 |
| 13.3.7 TPM2B_PRIVATE .....             | 135 |

|                                                        |     |
|--------------------------------------------------------|-----|
| 13.4 Identity Object .....                             | 136 |
| 13.4.1 Description.....                                | 136 |
| 13.4.2 _ID_OBJECT .....                                | 136 |
| 13.4.3 TPM2B_ID_OBJECT .....                           | 136 |
| 14 NV Storage Structures .....                         | 137 |
| 14.1 TPM_NV_INDEX.....                                 | 137 |
| 14.2 TPMA_NV (NV Index Attributes).....                | 138 |
| 14.3 TPMS_NV_PUBLIC .....                              | 141 |
| 14.4 TPM2B_NV_PUBLIC .....                             | 141 |
| 15 Context Data .....                                  | 142 |
| 15.1 Introduction.....                                 | 142 |
| 15.2 TPM2B_CONTEXT_SENSITIVE .....                     | 142 |
| 15.3 TPMS_CONTEXT_DATA.....                            | 142 |
| 15.4 TPM2B_CONTEXT_DATA.....                           | 142 |
| 15.5 TPMS_CONTEXT .....                                | 143 |
| 15.6 Parameters of TPMS_CONTEXT .....                  | 143 |
| 15.6.1 <i>sequence</i> .....                           | 143 |
| 15.6.2 <i>savedHandle</i> .....                        | 144 |
| 15.6.3 <i>hierarchy</i> .....                          | 145 |
| 15.7 Context Protection.....                           | 145 |
| 15.7.1 Context Integrity .....                         | 145 |
| 15.7.2 Context Confidentiality.....                    | 145 |
| 16 Creation Data .....                                 | 146 |
| 16.1 TPMS_CREATION_DATA .....                          | 146 |
| 16.2 TPM2B_CREATION_DATA .....                         | 146 |
| Annex A (informative) Algorithm Constants .....        | 147 |
| A.1 Introduction.....                                  | 147 |
| A.2 Allowed Hash Algorithms .....                      | 147 |
| A.2.1 SHA1 .....                                       | 147 |
| A.2.2 SHA256 .....                                     | 147 |
| A.2.3 SHA384 .....                                     | 147 |
| A.2.4 SHA512 .....                                     | 148 |
| A.2.5 SM3_256 .....                                    | 148 |
| A.3 Architectural Limits .....                         | 148 |
| Annex B (informative) Implementation Definitions ..... | 149 |
| B.1 Introduction.....                                  | 149 |
| B.2 Logic Values.....                                  | 149 |
| B.3 Processor Values .....                             | 149 |
| B.4 Implemented Algorithms.....                        | 150 |
| B.5 Implemented Commands .....                         | 151 |
| B.6 Algorithm Constants .....                          | 154 |
| B.6.1 RSA .....                                        | 154 |
| B.6.2 ECC .....                                        | 154 |

|       |                                      |     |
|-------|--------------------------------------|-----|
| B.6.3 | AES.....                             | 154 |
| B.6.4 | SM4 .....                            | 154 |
| B.6.5 | CAMELLIA.....                        | 155 |
| B.6.6 | Symmetric.....                       | 155 |
| B.7   | Implementation Specific Values ..... | 156 |
|       | Bibliography .....                   | 159 |

## Tables

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Table 1 — Name Prefix Convention .....                                               | 15 |
| Table 2 — Unmarshaling Errors .....                                                  | 17 |
| Table 3 — Definition of Base Types .....                                             | 18 |
| Table 4 — Definition of Types for Documentation Clarity .....                        | 18 |
| Table 5 — Definition of (UINT32) TPM_SPEC Constants <> .....                         | 19 |
| Table 6 — Definition of (UINT32) TPM_GENERATED Constants <O> .....                   | 19 |
| Table 7 — Legend for TPM_ALG_ID Table .....                                          | 20 |
| Table 8 — Definition of (UINT16) TPM_ALG_ID Constants <IN/OUT, S> .....              | 21 |
| Table 9 — Definition of (UINT16) {ECC} TPM_ECC_CURVE Constants <IN/OUT, S> .....     | 24 |
| Table 10 — TPM Command Format Fields Description .....                               | 24 |
| Table 11 — Legend for Command Code Tables .....                                      | 25 |
| Table 12 — Definition of (UINT32) TPM_CC Constants (Numeric Order) <IN/OUT, S> ..... | 26 |
| Table 13 — Format-Zero Response Codes .....                                          | 31 |
| Table 14 — Format-One Response Codes .....                                           | 32 |
| Table 15 — Response Code Groupings .....                                             | 32 |
| Table 16 — Definition of (UINT32) TPM_RC Constants (Actions) <OUT> .....             | 33 |
| Table 17 — Definition of (INT8) TPM_CLOCK_ADJUST Constants <IN> .....                | 38 |
| Table 18 — Definition of (UINT16) TPM_EO Constants <IN/OUT> .....                    | 38 |
| Table 19 — Definition of (UINT16) TPM_ST Constants <IN/OUT, S> .....                 | 39 |
| Table 20 — Definition of (UINT16) TPM_SU Constants <IN> .....                        | 41 |
| Table 21 — Definition of (UINT8) TPM_SE Constants <IN> .....                         | 41 |
| Table 22 — Definition of (UINT32) TPM_CAP Constants .....                            | 42 |
| Table 23 — Definition of (UINT32) TPM_PT Constants <IN/OUT, S> .....                 | 43 |
| Table 24 — Definition of (UINT32) TPM_PT_PCR Constants <IN/OUT, S> .....             | 48 |
| Table 25 — Definition of (UINT32) TPM_PS Constants <OUT> .....                       | 50 |
| Table 26 — Definition of Types for Handles .....                                     | 51 |
| Table 27 — Definition of (UINT8) TPM_HT Constants <S> .....                          | 51 |
| Table 28 — Definition of (TPM_HANDLE) TPM_RH Constants <S> .....                     | 53 |
| Table 29 — Definition of (TPM_HANDLE) TPM_HC Constants <S> .....                     | 55 |
| Table 30 — Definition of (UINT32) TPMA_ALGORITHM Bits .....                          | 56 |
| Table 31 — Definition of (UINT32) TPMA_OBJECT Bits .....                             | 57 |
| Table 32 — Definition of (UINT8) TPMA_SESSION Bits <IN/OUT> .....                    | 63 |
| Table 33 — Definition of (UINT8) TPMA_LOCALITY Bits <IN/OUT> .....                   | 65 |
| Table 34 — Definition of (UINT32) TPMA_PERMANENT Bits <OUT> .....                    | 65 |
| Table 35 — Definition of (UINT32) TPMA_STARTUP_CLEAR Bits <OUT> .....                | 66 |
| Table 36 — Definition of (UINT32) TPMA_MEMORY Bits <Out> .....                       | 67 |
| Table 37 — Definition of (TPM_CC) TPMA_CC Bits <OUT> .....                           | 68 |

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Table 38 — Definition of (BYTE) TPMI_YES_NO Type .....                         | 71 |
| Table 39 — Definition of (TPM_HANDLE) TPMI_DH_OBJECT Type.....                 | 71 |
| Table 40 — Definition of (TPM_HANDLE) TPMI_DH_PERSISTENT Type .....            | 72 |
| Table 41 — Definition of (TPM_HANDLE) TPMI_DH_ENTITY Type <IN> .....           | 72 |
| Table 42 — Definition of (TPM_HANDLE) TPMI_DH_PCR Type <IN> .....              | 73 |
| Table 43 — Definition of (TPM_HANDLE) TPMI_SH_AUTH_SESSION Type <IN/OUT> ..... | 73 |
| Table 44 — Definition of (TPM_HANDLE) TPMI_SH_HMAC Type <IN/OUT> .....         | 73 |
| Table 45 — Definition of (TPM_HANDLE) TPMI_SH_POLICY Type <IN/OUT> .....       | 73 |
| Table 46 — Definition of (TPM_HANDLE) TPMI_DH_CONTEXT Type .....               | 74 |
| Table 47 — Definition of (TPM_HANDLE) TPMI_RH_HIERARCHY Type .....             | 74 |
| Table 48 — Definition of (TPM_HANDLE) TPMI_RH_ENABLES Type .....               | 74 |
| Table 49 — Definition of (TPM_HANDLE) TPMI_RH_HIERARCHY_AUTH Type <IN> .....   | 75 |
| Table 50 — Definition of (TPM_HANDLE) TPMI_RH_PLATFORM Type <IN> .....         | 75 |
| Table 51 — Definition of (TPM_HANDLE) TPMI_RH_OWNER Type <IN> .....            | 75 |
| Table 52 — Definition of (TPM_HANDLE) TPMI_RH_ENDORSEMENT Type <IN> .....      | 76 |
| Table 53 — Definition of (TPM_HANDLE) TPMI_RH_PROVISION Type <IN> .....        | 76 |
| Table 54 — Definition of (TPM_HANDLE) TPMI_RH_CLEAR Type <IN> .....            | 76 |
| Table 55 — Definition of (TPM_HANDLE) TPMI_RH_NV_AUTH Type <IN> .....          | 77 |
| Table 56 — Definition of (TPM_HANDLE) TPMI_RH_LOCKOUT Type <IN> .....          | 77 |
| Table 57 — Definition of (TPM_HANDLE) TPMI_RH_NV_INDEX Type <IN/OUT> .....     | 77 |
| Table 58 — Definition of (TPM_ALG_ID) TPMI_ALG_HASH Type.....                  | 78 |
| Table 59 — Definition of (TPM_ALG_ID) TPMI_ALG_ASYM Type .....                 | 78 |
| Table 60 — Definition of (TPM_ALG_ID) TPMI_ALG_SYM Type.....                   | 79 |
| Table 61 — Definition of (TPM_ALG_ID) TPMI_ALG_SYM_OBJECT Type .....           | 79 |
| Table 62 — Definition of (TPM_ALG_ID) TPMI_ALG_SYM_MODE Type.....              | 80 |
| Table 63 — Definition of (TPM_ALG_ID) TPMI_ALG_KDF Type .....                  | 80 |
| Table 64 — Definition of (TPM_ALG_ID) TPMI_ALG_SIG_SCHEME Type.....            | 81 |
| Table 65 — Definition of (TPM_ALG_ID) TPMI_ECC_KEY_EXCHANGE Type.....          | 81 |
| Table 66 — Definition of (TPM_ST) TPMI_ST_COMMAND_TAG Type.....                | 81 |
| Table 67 — Definition of TPMS_EMPTY Structure <IN/OUT> .....                   | 83 |
| Table 68 — Definition of TPMS_ALGORITHM_DESCRIPTION Structure <OUT> .....      | 83 |
| Table 69 — Definition of TPMU_HA Union <IN/OUT, S> .....                       | 84 |
| Table 70 — Definition of TPMT_HA Structure <IN/OUT> .....                      | 84 |
| Table 71 — Definition of TPM2B_DIGEST Structure .....                          | 85 |
| Table 72 — Definition of TPM2B_DATA Structure .....                            | 86 |
| Table 73 — Definition of Types for TPM2B_NONCE .....                           | 86 |
| Table 74 — Definition of Types for TPM2B_AUTH .....                            | 86 |
| Table 75 — Definition of Types for TPM2B_OPERAND .....                         | 86 |
| Table 76 — Definition of TPM2B_EVENT Structure.....                            | 87 |

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| Table 77 — Definition of TPM2B_MAX_BUFFER Structure .....                | 87  |
| Table 78 — Definition of TPM2B_MAX_NV_BUFFER Structure .....             | 87  |
| Table 79 — Definition of TPM2B_TIMEOUT Structure <IN/OUT> .....          | 88  |
| Table 80 — Definition of TPM2B_IV Structure <IN/OUT> .....               | 88  |
| Table 81 — Definition of TPMU_NAME Union <> .....                        | 88  |
| Table 82 — Definition of TPM2B_NAME Structure .....                      | 89  |
| Table 83 — Definition of TPMS_PCR_SELECT Structure .....                 | 90  |
| Table 84 — Definition of TPMS_PCR_SELECTION Structure .....              | 90  |
| Table 85 — Values for <i>proof</i> Used in Tickets .....                 | 91  |
| Table 86 — General Format of a Ticket .....                              | 91  |
| Table 87 — Definition of TPMT_TK_CREATION Structure .....                | 92  |
| Table 88 — Definition of TPMT_TK_VERIFIED Structure .....                | 93  |
| Table 89 — Definition of TPMT_TK_AUTH Structure .....                    | 94  |
| Table 90 — Definition of TPMT_TK_HASHCHECK Structure .....               | 95  |
| Table 91 — Definition of TPMS_ALG_PROPERTY Structure <OUT> .....         | 95  |
| Table 92 — Definition of TPMS_TAGGED_PROPERTY Structure <OUT> .....      | 95  |
| Table 93 — Definition of TPMS_TAGGED_PCR_SELECT Structure <OUT> .....    | 96  |
| Table 94 — Definition of TPML_CC Structure .....                         | 96  |
| Table 95 — Definition of TPML_CCA Structure <OUT> .....                  | 97  |
| Table 96 — Definition of TPML_ALG Structure .....                        | 97  |
| Table 97 — Definition of TPML_HANDLE Structure <OUT> .....               | 97  |
| Table 98 — Definition of TPML_DIGEST Structure .....                     | 98  |
| Table 99 — Definition of TPML_DIGEST_VALUES Structure .....              | 98  |
| Table 100 — Definition of TPM2B_DIGEST_VALUES Structure .....            | 98  |
| Table 101 — Definition of TPML_PCR_SELECTION Structure .....             | 99  |
| Table 102 — Definition of TPML_ALG_PROPERTY Structure <OUT> .....        | 99  |
| Table 103 — Definition of TPML_TAGGED_TPM_PROPERTY Structure <OUT> ..... | 99  |
| Table 104 — Definition of TPML_TAGGED_PCR_PROPERTY Structure <OUT> ..... | 100 |
| Table 105 — Definition of {ECC} TPML_ECC_CURVE Structure <OUT> .....     | 100 |
| Table 106 — Definition of TPMU_CAPABILITIES Union <OUT> .....            | 100 |
| Table 107 — Definition of TPMS_CAPABILITY_DATA Structure <OUT> .....     | 101 |
| Table 108 — Definition of TPMS_CLOCK_INFO Structure .....                | 101 |
| Table 109 — Definition of TPMS_TIME_INFO Structure .....                 | 102 |
| Table 110 — Definition of TPMS_TIME_ATTEST_INFO Structure <OUT> .....    | 103 |
| Table 111 — Definition of TPMS_CERTIFY_INFO Structure <OUT> .....        | 103 |
| Table 112 — Definition of TPMS_QUOTE_INFO Structure <OUT> .....          | 103 |
| Table 113 — Definition of TPMS_COMMAND_AUDIT_INFO Structure <OUT> .....  | 104 |
| Table 114 — Definition of TPMS_SESSION_AUDIT_INFO Structure <OUT> .....  | 104 |
| Table 115 — Definition of TPMS_CREATION_INFO Structure <OUT> .....       | 104 |

|                                                                                       |     |
|---------------------------------------------------------------------------------------|-----|
| Table 116 — Definition of TPMS_NV_CERTIFY_INFO Structure <OUT> .....                  | 104 |
| Table 117 — Definition of (TPM_ST) TPMI_ST_ATTEST Type <OUT> .....                    | 105 |
| Table 118 — Definition of TPMU_ATTEST Union <OUT> .....                               | 105 |
| Table 119 — Definition of TPMS_ATTEST Structure <OUT> .....                           | 105 |
| Table 120 — Definition of TPM2B_ATTEST Structure <OUT> .....                          | 106 |
| Table 121 — Definition of TPMS_AUTH_COMMAND Structure <IN> .....                      | 106 |
| Table 122 — Definition of TPMS_AUTH_RESPONSE Structure <OUT> .....                    | 106 |
| Table 123 — Definition of {AES} (TPM_KEY_BITS) TPMI_AES_KEY_BITS Type .....           | 107 |
| Table 124 — Definition of {SM4} (TPM_KEY_BITS) TPMI_SM4_KEY_BITS Type .....           | 107 |
| Table 125 — Definition of {CAMELLIA} (TPM_KEY_BITS) TPMI_CAMELLIA_KEY_BITS Type ..... | 108 |
| Table 126 — Definition of TPMU_SYM_KEY_BITS Union .....                               | 108 |
| Table 127 — Definition of TPMU_SYM_MODE Union .....                                   | 108 |
| Table 128 — Definition of TPMU_SYM_DETAILS Union .....                                | 109 |
| Table 129 — Definition of TPMT_SYM_DEF Structure .....                                | 109 |
| Table 130 — Definition of TPMT_SYM_DEF_OBJECT Structure .....                         | 110 |
| Table 131 — Definition of TPM2B_SYM_KEY Structure .....                               | 110 |
| Table 132 — Definition of TPMS_SYMCIPHER_PARMS Structure .....                        | 110 |
| Table 133 — Definition of TPM2B_SENSITIVE_DATA Structure .....                        | 111 |
| Table 134 — Definition of TPMS_SENSITIVE_CREATE Structure <IN> .....                  | 111 |
| Table 135 — Definition of TPM2B_SENSITIVE_CREATE Structure <IN, S> .....              | 111 |
| Table 136 — Definition of TPMS_SCHEME_SIGHASH Structure .....                         | 112 |
| Table 137 — Definition of (TPM_ALG_ID) TPMI_ALG_KEYEDHASH_SCHEME Type .....           | 112 |
| Table 138 — Definition of Types for HMAC_SIG_SCHEME .....                             | 112 |
| Table 139 — Definition of TPMS_SCHEME_XOR Structure .....                             | 113 |
| Table 140 — Definition of TPMU_SCHEME_KEYEDHASH Union <IN/OUT, S> .....               | 113 |
| Table 141 — Definition of TPMT_KEYEDHASH_SCHEME Structure .....                       | 113 |
| Table 142 — Definition of {RSA} Types for RSA_SIG_SCHEMES .....                       | 114 |
| Table 143 — Definition of {ECC} Types for ECC_SIG_SCHEMES .....                       | 114 |
| Table 144 — Definition of {ECC} TPMS_SCHEME_ECDSA Structure .....                     | 114 |
| Table 145 — Definition of TPMU_SIG_SCHEME Union <IN/OUT, S> .....                     | 115 |
| Table 146 — Definition of TPMT_SIG_SCHEME Structure .....                             | 115 |
| Table 147 — Definition of {RSA} TPMS_SCHEME_OAEP Structure .....                      | 116 |
| Table 148 — Definition of {ECC} TPMS_SCHEME_ECDH Structure .....                      | 116 |
| Table 149 — Definition of TPMS_SCHEME_MGF1 Structure .....                            | 116 |
| Table 150 — Definition of {ECC} TPMS_SCHEME_KDF1_SP800_56a Structure .....            | 116 |
| Table 151 — Definition of TPMS_SCHEME_KDF2 Structure .....                            | 117 |
| Table 152 — Definition of TPMS_SCHEME_KDF1_SP800_108 Structure .....                  | 117 |
| Table 153 — Definition of TPMU_KDF_SCHEME Union <IN/OUT, S> .....                     | 117 |
| Table 154 — Definition of TPMT_KDF_SCHEME Structure .....                             | 117 |

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Table 155 — Definition of (TPM_ALG_ID) TPMI_ALG_ASYM_SCHEME Type <>.....         | 118 |
| Table 156 — Definition of TPMU_ASYM_SCHEME Union .....                           | 118 |
| Table 157 — Definition of TPMT_ASYM_SCHEME Structure <> .....                    | 119 |
| Table 158 — Definition of (TPM_ALG_ID) {RSA} TPMI_ALG_RSA_SCHEME Type.....       | 119 |
| Table 159 — Definition of {RSA} TPMT_RSA_SCHEME Structure .....                  | 119 |
| Table 160 — Definition of (TPM_ALG_ID) {RSA} TPMI_ALG_RSA_DECRYPT Type.....      | 120 |
| Table 161 — Definition of {RSA} TPMT_RSA_DECRYPT Structure .....                 | 120 |
| Table 162 — Definition of {RSA} TPM2B_PUBLIC_KEY_RSA Structure .....             | 120 |
| Table 163 — Definition of {RSA} (TPM_KEY_BITS) TPMI_RSA_KEY_BITS Type.....       | 121 |
| Table 164 — Definition of {RSA} TPM2B_PRIVATE_KEY_RSA Structure.....             | 121 |
| Table 165 — Definition of {ECC} TPM2B_ECC_PARAMETER Structure .....              | 122 |
| Table 166 — Definition of {ECC} TPMS_ECC_POINT Structure .....                   | 122 |
| Table 167 — Definition of {ECC} TPM2B_ECC_POINT Structure .....                  | 122 |
| Table 168 — Definition of (TPM_ALG_ID) {ECC} TPMI_ALG_ECC_SCHEME Type .....      | 123 |
| Table 169 — Definition of {ECC} (TPM_ECC_CURVE) TPMI_ECC_CURVE Type.....         | 123 |
| Table 170 — Definition of (TPMT_SIG_SCHEME) {ECC} TPMT_ECC_SCHEME Structure..... | 123 |
| Table 171 — Definition of {ECC} TPMS_ALGORITHM_DETAIL_ECC Structure <OUT> .....  | 124 |
| Table 172 — Definition of {RSA} TPMS_SIGNATURE_RSASSA Structure .....            | 124 |
| Table 173 — Definition of {RSA} TPMS_SIGNATURE_RSAPSS Structure .....            | 125 |
| Table 174 — Definition of {ECC} TPMS_SIGNATURE_ECDSA Structure .....             | 125 |
| Table 175 — Definition of TPMU_SIGNATURE Union <IN/OUT, S>.....                  | 125 |
| Table 176 — Definition of TPMT_SIGNATURE Structure.....                          | 126 |
| Table 177 — Definition of TPMU_ENCRYPTED_SECRET Union <S> .....                  | 126 |
| Table 178 — Definition of TPM2B_ENCRYPTED_SECRET Structure.....                  | 127 |
| Table 179 — Definition of (TPM_ALG_ID) TPMI_ALG_PUBLIC Type .....                | 128 |
| Table 180 — Definition of TPMU_PUBLIC_ID Union <IN/OUT, S> .....                 | 129 |
| Table 181 — Definition of TPMS_KEYEDHASH_PARMS Structure.....                    | 129 |
| Table 182 — Definition of TPMS_ASYM_PARMS Structure <> .....                     | 130 |
| Table 183 — Definition of {RSA} TPMS_RSA_PARMS Structure.....                    | 130 |
| Table 184 — Definition of {ECC} TPMS_ECC_PARMS Structure .....                   | 131 |
| Table 185 — Definition of TPMU_PUBLIC_PARMS Union <IN/OUT, S>.....               | 131 |
| Table 186 — Definition of TPMT_PUBLIC_PARMS Structure .....                      | 132 |
| Table 187 — Definition of TPMT_PUBLIC Structure.....                             | 132 |
| Table 188 — Definition of TPM2B_PUBLIC Structure.....                            | 132 |
| Table 189 — Definition of TPM2B_PRIVATE_VENDOR_SPECIFIC Structure<> .....        | 133 |
| Table 190 — Definition of TPMU_SENSITIVE_COMPOSITE Union <IN/OUT, S> .....       | 133 |
| Table 191 — Definition of TPMT_SENSITIVE Structure .....                         | 134 |
| Table 192 — Definition of TPM2B_SENSITIVE Structure <IN/OUT> .....               | 134 |
| Table 193 — Definition of _PRIVATE Structure <> .....                            | 135 |

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| Table 194 — Definition of TPM2B_PRIVATE Structure <IN/OUT, S> .....        | 135 |
| Table 195 — Definition of _ID_OBJECT Structure <>.....                     | 136 |
| Table 196 — Definition of TPM2B_ID_OBJECT Structure <IN/OUT> .....         | 136 |
| Table 197 — Definition of (UINT32) TPM_NV_INDEX Bits <>.....               | 137 |
| Table 198 — Definition of (UINT32) TPMA_NV Bits .....                      | 139 |
| Table 199 — Definition of TPMS_NV_PUBLIC Structure.....                    | 141 |
| Table 200 — Definition of TPM2B_NV_PUBLIC Structure.....                   | 141 |
| Table 201 — Definition of TPM2B_CONTEXT_SENSITIVE Structure <IN/OUT> ..... | 142 |
| Table 202 — Definition of TPMS_CONTEXT_DATA Structure <IN/OUT, S> .....    | 142 |
| Table 203 — Definition of TPM2B_CONTEXT_DATA Structure <IN/OUT> .....      | 142 |
| Table 204 — Definition of TPMS_CONTEXT Structure .....                     | 143 |
| Table 205 — Context Handle Values.....                                     | 144 |
| Table 206 — Definition of TPMS_CREATION_DATA Structure <OUT> .....         | 146 |
| Table 207 — Definition of TPM2B_CREATION_DATA Structure <OUT> .....        | 146 |
| Table A.1 — Defines for SHA1 Hash Values.....                              | 147 |
| Table A.2 — Defines for SHA256 Hash Values.....                            | 147 |
| Table A.3 — Defines for SHA384 Hash Values.....                            | 147 |
| Table A.4 — Defines for SHA512 Hash Values.....                            | 148 |
| Table A.5 — Defines for SM3_256 Hash Values.....                           | 148 |
| Table A.6 — Defines for Architectural Limits Values .....                  | 148 |
| Table B.1 — Defines for Logic Values .....                                 | 149 |
| Table B.2 — Defines for Processor Values .....                             | 149 |
| Table B.3 — Defines for Implemented Algorithms.....                        | 150 |
| Table B.4 — Defines for Implemented Commands .....                         | 151 |
| Table B.5 — Defines for RSA Algorithm Constants.....                       | 154 |
| Table B.6 — Defines for ECC Algorithm Constants .....                      | 154 |
| Table B.7 — Defines for AES Algorithm Constants.....                       | 154 |
| Table B.8 — Defines for SM4 Algorithm Constants.....                       | 154 |
| Table B.9 — Defines for CAMELLIA Algorithm Constants .....                 | 155 |
| Table B.10 — Defines for Symmetric Algorithm Constants.....                | 155 |
| Table B.11 — Defines for Implementation Values .....                       | 156 |

**Figures**

|                                                             |     |
|-------------------------------------------------------------|-----|
| Figure 1 — Command Format .....                             | 24  |
| Figure 2 — Format-Zero Response Codes.....                  | 30  |
| Figure 3 — Format-One Response Codes .....                  | 31  |
| Figure 4 — ISO/IEC 11889 (first edition) TPM_NV_INDEX ..... | 137 |
| Figure 5 — ISO/IEC 11889 TPM_NV_INDEX .....                 | 137 |

## 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: [Foreword — Supplementary information](#).

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.

This second edition cancels and replaces the first edition (ISO/IEC 11889-2:2009), which has been technically revised.

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

- Part 1: Architecture
- Part 2: Structures
- Part 3: Commands
- Part 4: Supporting routines

## Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

|                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------|
| <b>Fujitsu Limited</b><br><b>1-1, Kamikodanaka 4-chrome, Nakahara-ku, Kawasaki-shi, Kanagawa, 211-8588 Japan</b>   |
| <b>Microsoft Corporation</b><br><b>One Microsoft Way, Redmond, WA 98052</b>                                        |
| <b>Enterasys Networks, Inc</b><br><b>50 Minuteman Road, US-Andover, MA 01810</b>                                   |
| <b>Lenovo</b><br><b>1009 Think Place, US-Morrisville, NC 27560-8496</b>                                            |
| <b>Advanced Micro devices, Inc. - AMD</b><br><b>7171 Southwest Parkway, Mailstop B100.3 US-Austin, Texas 78735</b> |
| <b>Hewlett-Packard Company</b><br><b>P.O. Box 10490, US-Palo Alto, CA 94303-0969</b>                               |
| <b>Infineon Technologies AG - Neubiberg</b><br><b>Am Campeon 1-12, DE-85579 Neubiberg</b>                          |
| <b>Sun Microsystems Inc. - Menlo Park, CA</b><br><b>10 Network Circle, UMPK10-146, US-Menlo Park, CA 94025</b>     |
| <b>IBM Corporation</b><br><b>North Castle Drive, US-Armonk, N.Y. 10504</b>                                         |
| <b>Intel Corporation</b><br><b>5200 Elam Young Parkway, US-Hillsboro, OR 97123</b>                                 |

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO ([www.iso.org/patents](http://www.iso.org/patents)) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

# Information technology — Trusted Platform Module Library —

## Part 2: Structures

### 1 Scope

This part of ISO/IEC 11889 contains the definitions of the constants, flags, structure, and union definitions used to communicate with the TPM. Values defined in this part of ISO/IEC 11889 are used by the TPM commands defined in ISO/IEC 11899-3 and by the functions in ISO/IEC 11889-4.

NOTE The structures in this document are the canonical form of the structures on the interface. All structures are "packed" with no octets of padding between structure elements. The TPM-internal form of the structures is dependent on the processor and compiler for the TPM implementation.

### 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 9797-2, *Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function*
- ISO/IEC 10116:2006, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*
- ISO/IEC 11889-1, *Information technology — Trusted Platform Module Library — Part 1: Architecture*
- ISO/IEC 11889-3, *Information technology — Trusted Platform Module Library — Part 3: Commands*
- ISO/IEC 11889-4, *Information technology — Trusted Platform Module Library — Part 4: Supporting routines*
- TCG Algorithm Registry, available at  
<[http://www.trustedcomputinggroup.org/resources/tcg\\_algorithm\\_registry](http://www.trustedcomputinggroup.org/resources/tcg_algorithm_registry)>

### 3 Terms and definitions

For the purposes of this part of ISO/IEC 11889, the terms and definitions given in ISO/IEC 11889-1 apply.

### 4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 11889, the symbols and abbreviated terms given in ISO/IEC 11889-1 apply.

### 5 Notation

#### 5.1 Introduction

The information in this part of ISO/IEC 11889 is formatted so that it may be converted to standard computer-language formats by an automated process. The purpose of this automated process is to minimize the transcription errors that often occur during the conversion process.

For the purposes of this part of ISO/IEC 11889, the conventions given in ISO/IEC 11889-1 apply.

In addition, the conventions and notations in clause 5 describe the representation of various data so that it is both human readable and amenable to automated processing.