

ISO/IEC 11889-2:2015-12 (E)

Information technology - Trusted Platform Module Library - Part 2: Structures

Contents	Page
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