
Information technology — Trusted Platform Module Library —

Part 3: Commands

*Technologies de l'information — Bibliothèque de module
de plate-forme de confiance —
Partie 3: Commandes*

**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	xxiv
Introduction	xxv
1 Scope	1
2 Normative references	2
3 Terms and Definitions	2
4 Symbols and abbreviated terms	2
5 Notation	2
5.1 Introduction	2
5.2 Table Decorations	2
5.3 Handle and Parameter Demarcation	4
5.4 AuthorizationSize and ParameterSize	4
6 Command Processing	5
6.1 Introduction	5
6.2 Command Header Validation	5
6.3 Mode Checks	5
6.4 Handle Area Validation	6
6.5 Session Area Validation	7
6.6 Authorization Checks	8
6.7 Parameter Decryption	10
6.8 Parameter Unmarshaling	10
6.8.1 Introduction	10
6.8.2 Unmarshaling Errors	10
6.9 Command Post Processing	11
7 Response Values	13
7.1 Tag	13
7.2 Response Codes	13
8 Implementation Dependent	16
9 Detailed Actions Assumptions	17
9.1 Introduction	17
9.2 Pre-processing	17
9.3 Post Processing	17
10 Start-up	18
10.1 Introduction	18
10.2 _TPM_Init	18
10.2.1 General Description	18
10.2.2 Detailed Actions	19
10.3 TPM2_Startup	20
10.3.1 General Description	20
10.3.2 Command and Response	23
10.3.3 Detailed Actions	24
10.4 TPM2_Shutdown	27
10.4.1 General Description	27

ISO/IEC 11889-3:2015(E)

10.4.2	Command and Response.....	28
10.4.3	Detailed Actions	29
11	Testing.....	31
11.1	Introduction	31
11.2	TPM2_SelfTest	32
11.2.1	General Description.....	32
11.2.2	Command and Response.....	33
11.2.3	Detailed Actions	34
11.3	TPM2_IncrementalSelfTest	35
11.3.1	General Description.....	35
11.3.2	Command and Response.....	36
11.3.3	Detailed Actions	37
11.4	TPM2_GetTestResult	38
11.4.1	General Description.....	38
11.4.2	Command and Response.....	39
11.4.3	Detailed Actions	40
12	Session Commands	41
12.1	TPM2_StartAuthSession	41
12.1.1	General Description.....	41
12.1.2	Command and Response.....	43
12.1.3	Detailed Actions	44
12.2	TPM2_PolicyRestart	46
12.2.1	General Description.....	46
12.2.2	Command and Response.....	47
12.2.3	Detailed Actions	48
13	Object Commands.....	49
13.1	TPM2_Create.....	49
13.1.1	General Description.....	49
13.1.2	Command and Response.....	52
13.1.3	Detailed Actions	53
13.2	TPM2_Load	55
13.2.1	General Description.....	55
13.2.2	Command and Response.....	56
13.2.3	Detailed Actions	57
13.3	TPM2_LoadExternal	59
13.3.1	General Description.....	59
13.3.2	Command and Response.....	61
13.3.3	Detailed Actions	62
13.4	TPM2_ReadPublic.....	64
13.4.1	General Description.....	64
13.4.2	Command and Response.....	65

13.4.3	Detailed Actions	66
13.5	TPM2_ActivateCredential	67
13.5.1	General Description.....	67
13.5.2	Command and Response.....	68
13.5.3	Detailed Actions	69
13.6	TPM2_MakeCredential	71
13.6.1	General Description.....	71
13.6.2	Command and Response.....	72
13.6.3	Detailed Actions	73
13.7	TPM2_Unseal	74
13.7.1	General Description.....	74
13.7.2	Command and Response.....	75
13.7.3	Detailed Actions	76
13.8	TPM2_ObjectChangeAuth	77
13.8.1	General Description.....	77
13.8.2	Command and Response.....	78
13.8.3	Detailed Actions	79
14	Duplication Commands	81
14.1	TPM2_Duplicate	81
14.1.1	General Description.....	81
14.1.2	Command and Response.....	82
14.1.3	Detailed Actions	83
14.2	TPM2_Rewrap	85
14.2.1	General Description.....	85
14.2.2	Command and Response.....	86
14.2.3	Detailed Actions	87
14.3	TPM2_Import	90
14.3.1	General Description.....	90
14.3.2	Command and Response.....	92
14.3.3	Detailed Actions	93
15	Asymmetric Primitives	97
15.1	Introduction	97
15.2	TPM2_RSA_Encrypt.....	97
15.2.1	General Description.....	97
15.2.2	Command and Response.....	99
15.2.3	Detailed Actions	100
15.3	TPM2_RSA_Decrypt	102
15.3.1	General Description.....	102
15.3.2	Command and Response.....	103
15.3.3	Detailed Actions	104
15.4	TPM2_ECDH_KeyGen.....	106

ISO/IEC 11889-3:2015(E)

15.4.1	General Description.....	106
15.4.2	Command and Response.....	107
15.4.3	Detailed Actions	108
15.5	TPM2_ECDH_ZGen	110
15.5.1	General Description.....	110
15.5.2	Command and Response.....	111
15.5.3	Detailed Actions	112
15.6	TPM2_ECC_Parameters	113
15.6.1	General Description.....	113
15.6.2	Command and Response.....	113
15.6.3	Detailed Actions	114
15.7	TPM2_ZGen_2Phase	114
15.7.1	General Description.....	114
15.7.2	Command and Response.....	116
15.7.3	Detailed Actions	117
16	Symmetric Primitives.....	119
16.1	Introduction	119
16.2	TPM2_EncryptDecrypt.....	121
16.2.1	General Description.....	121
16.2.2	Command and Response.....	122
16.2.3	Detailed Actions	123
16.3	TPM2_Hash	125
16.3.1	General Description.....	125
16.3.2	Command and Response.....	126
16.3.3	Detailed Actions	127
16.4	TPM2_HMAC.....	128
16.4.1	General Description.....	128
16.4.2	Command and Response.....	129
16.4.3	Detailed Actions	130
17	Random Number Generator.....	132
17.1	TPM2_GetRandom	132
17.1.1	General Description.....	132
17.1.2	Command and Response.....	133
17.1.3	Detailed Actions	134
17.2	TPM2_StirRandom	135
17.2.1	General Description.....	135
17.2.2	Command and Response.....	136
17.2.3	Detailed Actions	137
18	Hash/HMAC/Event Sequences	138
18.1	Introduction	138
18.2	TPM2_HMAC_Start.....	138

18.2.1	General Description.....	138
18.2.2	Command and Response.....	140
18.2.3	Detailed Actions	141
18.3	TPM2_HashSequenceStart.....	143
18.3.1	General Description.....	143
18.3.2	Command and Response.....	144
18.3.3	Detailed Actions	145
18.4	TPM2_SequenceUpdate	146
18.4.1	General Description.....	146
18.4.2	Command and Response.....	147
18.4.3	Detailed Actions	148
18.5	TPM2_SequenceComplete.....	150
18.5.1	General Description.....	150
18.5.2	Command and Response.....	151
18.5.3	Detailed Actions	152
18.6	TPM2_EventSequenceComplete	154
18.6.1	General Description.....	154
18.6.2	Command and Response.....	155
18.6.3	Detailed Actions	156
19	Attestation Commands.....	158
19.1	Introduction	158
19.2	TPM2_Certify	160
19.2.1	General Description.....	160
19.2.2	Command and Response.....	161
19.2.3	Detailed Actions	162
19.3	TPM2_CertifyCreation	164
19.3.1	General Description.....	164
19.3.2	Command and Response.....	165
19.3.3	Detailed Actions	166
19.4	TPM2_Quote.....	168
19.4.1	General Description.....	168
19.4.2	Command and Response.....	169
19.4.3	Detailed Actions	170
19.5	TPM2_GetSessionAuditDigest	172
19.5.1	General Description.....	172
19.5.2	Command and Response.....	173
19.5.3	Detailed Actions	174
19.6	TPM2_GetCommandAuditDigest	176
19.6.1	General Description.....	176
19.6.2	Command and Response.....	177
19.6.3	Detailed Actions	178
19.7	TPM2_GetTime	180

ISO/IEC 11889-3:2015(E)

19.7.1	General Description.....	180
19.7.2	Command and Response.....	181
19.7.3	Detailed Actions	182
20	Ephemeral EC Keys	184
20.1	Introduction	184
20.2	TPM2_Commit.....	185
20.2.1	General Description.....	185
20.2.2	Command and Response.....	186
20.2.3	Detailed Actions	187
20.3	TPM2_EC_Ephemeral.....	190
20.3.1	General Description.....	190
20.3.2	Command and Response.....	191
20.3.3	Detailed Actions	192
21	Signing and Signature Verification	193
21.1	TPM2_VerifySignature.....	193
21.1.1	General Description.....	193
21.1.2	Command and Response.....	194
21.1.3	Detailed Actions	195
21.2	TPM2_Sign	197
21.2.1	General Description.....	197
21.2.2	Command and Response.....	198
21.2.3	Detailed Actions	199
22	Command Audit.....	201
22.1	Introduction	201
22.2	TPM2_SetCommandCodeAuditStatus	202
22.2.1	General Description.....	202
22.2.2	Command and Response.....	203
22.2.3	Detailed Actions	204
23	Integrity Collection (PCR).....	206
23.1	Introduction	206
23.2	TPM2_PCR_Extend	207
23.2.1	General Description.....	207
23.2.2	Command and Response.....	208
23.2.3	Detailed Actions	209
23.3	TPM2_PCR_Event	210
23.3.1	General Description.....	210
23.3.2	Command and Response.....	211
23.3.3	Detailed Actions	212
23.4	TPM2_PCR_Read	214
23.4.1	General Description.....	214
23.4.2	Command and Response.....	215
23.4.3	Detailed Actions	216

23.5	TPM2_PCR_Allocate	217
23.5.1	General Description	217
23.5.2	Command and Response	218
23.5.3	Detailed Actions	219
23.6	TPM2_PCR_SetAuthPolicy	220
23.6.1	General Description	220
23.6.2	Command and Response	221
23.6.3	Detailed Actions	222
23.7	TPM2_PCR_SetAuthValue	223
23.7.1	General Description	223
23.7.2	Command and Response	224
23.7.3	Detailed Actions	225
23.8	TPM2_PCR_Reset	226
23.8.1	General Description	226
23.8.2	Command and Response	227
23.8.3	Detailed Actions	228
23.9	_TPM_Hash_Start	229
23.9.1	Description	229
23.9.2	Detailed Actions	230
23.10	_TPM_Hash_Data	231
23.10.1	Description	231
23.10.2	Detailed Actions	232
23.11	_TPM_Hash_End	233
23.11.1	Description	233
23.11.2	Detailed Actions	234
24	Enhanced Authorization (EA) Commands	236
24.1	Introduction	236
24.2	Signed Authorization Actions	237
24.2.1	Introduction	237
24.2.2	Policy Parameter Checks	237
24.2.3	Policy Digest Update Function (PolicyUpdate())	238
24.2.4	Policy Context Updates	239
24.2.5	Policy Ticket Creation	240
24.3	TPM2_PolicySigned	241
24.3.1	General Description	241
24.3.2	Command and Response	243
24.3.3	Detailed Actions	244
24.4	TPM2_PolicySecret	247
24.4.1	General Description	247
24.4.2	Command and Response	248
24.4.3	Detailed Actions	249

ISO/IEC 11889-3:2015(E)

24.5	TPM2_PolicyTicket	251
24.5.1	General Description.....	251
24.5.2	Command and Response.....	252
24.5.3	Detailed Actions	253
24.6	TPM2_PolicyOR	255
24.6.1	General Description.....	255
24.6.2	Command and Response.....	256
24.6.3	Detailed Actions	257
24.7	TPM2_PolicyPCR	259
24.7.1	General Description.....	259
24.7.2	Command and Response.....	261
24.7.3	Detailed Actions	262
24.8	TPM2_PolicyLocality	264
24.8.1	General Description.....	264
24.8.2	Command and Response.....	265
24.8.3	Detailed Actions	266
24.9	TPM2_PolicyNV.....	268
24.9.1	General Description.....	268
24.9.2	Command and Response.....	269
24.9.3	Detailed Actions	270
24.10	TPM2_PolicyCounterTimer.....	273
24.10.1	General Description.....	273
24.10.2	Command and Response.....	274
24.10.3	Detailed Actions	275
24.11	TPM2_PolicyCommandCode	278
24.11.1	General Description.....	278
24.11.2	Command and Response.....	279
24.11.3	Detailed Actions	280
24.12	TPM2_PolicyPhysicalPresence	281
24.12.1	General Description.....	281
24.12.2	Command and Response.....	282
24.12.3	Detailed Actions	283
24.13	TPM2_PolicyCpHash.....	284
24.13.1	General Description.....	284
24.13.2	Command and Response.....	285
24.13.3	Detailed Actions	286
24.14	TPM2_PolicyNameHash.....	288
24.14.1	General Description.....	288
24.14.2	Command and Response.....	289
24.14.3	Detailed Actions	290
24.15	TPM2_PolicyDuplicationSelect.....	292

24.15.1	General Description.....	292
24.15.2	Command and Response.....	293
24.15.3	Detailed Actions	294
24.16	TPM2_PolicyAuthorize	296
24.16.1	General Description.....	296
24.16.2	Command and Response.....	297
24.16.3	Detailed Actions	298
24.17	TPM2_PolicyAuthValue	300
24.17.1	General Description.....	300
24.17.2	Command and Response.....	301
24.17.3	Detailed Actions	302
24.18	TPM2_PolicyPassword.....	303
24.18.1	General Description.....	303
24.18.2	Command and Response.....	304
24.18.3	Detailed Actions	305
24.19	TPM2_PolicyGetDigest.....	306
24.19.1	General Description.....	306
24.19.2	Command and Response.....	307
24.19.3	Detailed Actions	308
24.20	TPM2_PolicyNvWritten.....	309
24.20.1	General Description.....	309
24.20.2	Command and Response.....	310
24.20.3	Detailed Actions	311
25	Hierarchy Commands.....	313
25.1	TPM2_CreatePrimary	313
25.1.1	General Description.....	313
25.1.2	Command and Response.....	314
25.1.3	Detailed Actions	315
25.2	TPM2_HierarchyControl	317
25.2.1	General Description.....	317
25.2.2	Command and Response.....	318
25.2.3	Detailed Actions	319
25.3	TPM2_SetPrimaryPolicy.....	321
25.3.1	General Description.....	321
25.3.2	Command and Response.....	322
25.3.3	Detailed Actions	323
25.4	TPM2_ChangePPS	325
25.4.1	General Description.....	325
25.4.2	Command and Response.....	326
25.4.3	Detailed Actions	327
25.5	TPM2_ChangeEPS	328

ISO/IEC 11889-3:2015(E)

25.5.1	General Description.....	328
25.5.2	Command and Response.....	329
25.5.3	Detailed Actions	330
25.6	TPM2_Clear.....	331
25.6.1	General Description.....	331
25.6.2	Command and Response.....	332
25.6.3	Detailed Actions	333
25.7	TPM2_ClearControl	335
25.7.1	General Description.....	335
25.7.2	Command and Response.....	336
25.7.3	Detailed Actions	337
25.8	TPM2_HierarchyChangeAuth.....	338
25.8.1	General Description.....	338
25.8.2	Command and Response.....	339
25.8.3	Detailed Actions	340
26	Dictionary Attack Functions.....	341
26.1	Introduction	341
26.2	TPM2_DictionaryAttackLockReset	341
26.2.1	General Description.....	341
26.2.2	Command and Response.....	342
26.2.3	Detailed Actions	343
26.3	TPM2_DictionaryAttackParameters	344
26.3.1	General Description.....	344
26.3.2	Command and Response.....	345
26.3.3	Detailed Actions	346
27	Miscellaneous Management Functions.....	347
27.1	Introduction	347
27.2	TPM2_PP_Commands	347
27.2.1	General Description.....	347
27.2.2	Command and Response.....	348
27.2.3	Detailed Actions	349
27.3	TPM2_SetAlgorithmSet	350
27.3.1	General Description.....	350
27.3.2	Command and Response.....	351
27.3.3	Detailed Actions	352
28	Field Upgrade.....	353
28.1	Introduction	353
28.2	TPM2_FieldUpgradeStart	355
28.2.1	General Description.....	355
28.2.2	Command and Response.....	356
28.2.3	Detailed Actions	357
28.3	TPM2_FieldUpgradeData	358

28.3.1	General Description.....	358
28.3.2	Command and Response.....	359
28.3.3	Detailed Actions	360
28.4	TPM2_FirmwareRead.....	361
28.4.1	General Description.....	361
28.4.2	Command and Response.....	362
28.4.3	Detailed Actions	363
29	Context Management.....	364
29.1	Introduction	364
29.2	TPM2_ContextSave.....	364
29.2.1	General Description.....	364
29.2.2	Command and Response.....	365
29.2.3	Detailed Actions	366
29.3	TPM2_ContextLoad.....	369
29.3.1	General Description.....	369
29.3.2	Command and Response.....	370
29.3.3	Detailed Actions	371
29.4	TPM2_FlushContext.....	374
29.4.1	General Description.....	374
29.4.2	Command and Response.....	375
29.4.3	Detailed Actions	376
29.5	TPM2_EvictControl.....	377
29.5.1	General Description.....	377
29.5.2	Command and Response.....	379
29.5.3	Detailed Actions	380
30	Clocks and Timers.....	382
30.1	TPM2_ReadClock.....	382
30.1.1	General Description.....	382
30.1.2	Command and Response.....	383
30.1.3	Detailed Actions	384
30.2	TPM2_ClockSet.....	385
30.2.1	General Description.....	385
30.2.2	Command and Response.....	386
30.2.3	Detailed Actions	387
30.3	TPM2_ClockRateAdjust.....	388
30.3.1	General Description.....	388
30.3.2	Command and Response.....	389
30.3.3	Detailed Actions	390
31	Capability Commands	391
31.1	Introduction	391
31.2	TPM2_GetCapability.....	391

ISO/IEC 11889-3:2015(E)

31.2.1	General Description.....	391
31.2.2	Command and Response.....	395
31.2.3	Detailed Actions	396
31.3	TPM2_TestParms	399
31.3.1	General Description.....	399
31.3.2	Command and Response.....	400
31.3.3	Detailed Actions	401
32	Non-volatile Storage.....	402
32.1	Introduction	402
32.2	NV Counters	404
32.3	TPM2_NV_DefineSpace.....	405
32.3.1	General Description.....	405
32.3.2	Command and Response.....	407
32.3.3	Detailed Actions	408
32.4	TPM2_NV_UndefineSpace.....	411
32.4.1	General Description.....	411
32.4.2	Command and Response.....	412
32.4.3	Detailed Actions	413
32.5	TPM2_NV_UndefineSpaceSpecial.....	414
32.5.1	General Description.....	414
32.5.2	Command and Response.....	415
32.5.3	Detailed Actions	416
32.6	TPM2_NV_ReadPublic.....	417
32.6.1	General Description.....	417
32.6.2	Command and Response.....	418
32.6.3	Detailed Actions	419
32.7	TPM2_NV_Write	420
32.7.1	General Description.....	420
32.7.2	Command and Response.....	421
32.7.3	Detailed Actions	422
32.8	TPM2_NV_Increment	424
32.8.1	General Description.....	424
32.8.2	Command and Response.....	425
32.8.3	Detailed Actions	426
32.9	TPM2_NV_Extend	428
32.9.1	General Description.....	428
32.9.2	Command and Response.....	429
32.9.3	Detailed Actions	430
32.10	TPM2_NV_SetBits.....	432
32.10.1	General Description.....	432
32.10.2	Command and Response.....	433
32.10.3	Detailed Actions	434

32.11 TPM2_NV_WriteLock	436
32.11.1 General Description.....	436
32.11.2 Command and Response.....	437
32.11.3 Detailed Actions	438
32.12 TPM2_NV_GlobalWriteLock.....	440
32.12.1 General Description.....	440
32.12.2 Command and Response.....	441
32.12.3 Detailed Actions	442
32.13 TPM2_NV_Read.....	443
32.13.1 General Description.....	443
32.13.2 Command and Response.....	444
32.13.3 Detailed Actions	445
32.14 TPM2_NV_ReadLock	446
32.14.1 General Description.....	446
32.14.2 Command and Response.....	447
32.14.3 Detailed Actions	448
32.15 TPM2_NV_ChangeAuth	450
32.15.1 General Description.....	450
32.15.2 Command and Response.....	451
32.15.3 Detailed Actions	452
32.16 TPM2_NV_Certify	453
32.16.1 General Description.....	453
32.16.2 Command and Response.....	454
32.16.3 Detailed Actions	455
Bibliography	457

ISO/IEC 11889-3:2015(E)

Tables

Table 1 — Command Modifiers and Decoration.....	3
Table 2 — Separators.....	4
Table 3 — Unmarshaling Errors.....	11
Table 4 — Command-Independent Response Codes.....	14
Table 5 — TPM2_Startup Command.....	23
Table 6 — TPM2_Startup Response.....	23
Table 7 — TPM2_Startup Errors.....	24
Table 8 — TPM2_Shutdown Command.....	28
Table 9 — TPM2_Shutdown Response.....	28
Table 10 — TPM2_Shutdown Errors.....	29
Table 11 — TPM2_SelfTest Command.....	33
Table 12 — TPM2_SelfTest Response.....	33
Table 13 — TPM2_SelfTest Errors.....	34
Table 14 — TPM2_IncrementalSelfTest Command.....	36
Table 15 — TPM2_IncrementalSelfTest Response.....	36
Table 16 — TPM2_IncrementalSelfTest Errors.....	37
Table 17 — TPM2_GetTestResult Command.....	39
Table 18 — TPM2_GetTestResult Response.....	39
Table 19 — TPM2_StartAuthSession Command.....	43
Table 20 — TPM2_StartAuthSession Response.....	43
Table 21 — TPM2_StartAuthSession Errors.....	44
Table 22 — TPM2_PolicyRestart Command.....	47
Table 23 — TPM2_PolicyRestart Response.....	47
Table 24 — TPM2_Create Command.....	52
Table 25 — TPM2_Create Response.....	52
Table 26 — TPM2_Create Errors.....	53
Table 27 — TPM2_Load Command.....	56
Table 28 — TPM2_Load Response.....	56
Table 29 — TPM2_Load Errors.....	57
Table 30 — TPM2_LoadExternal Command.....	61
Table 31 — TPM2_LoadExternal Response.....	61
Table 32 — TPM2_LoadExternal Errors.....	62
Table 33 — TPM2_ReadPublic Command.....	65
Table 34 — TPM2_ReadPublic Response.....	65
Table 35 — TPM2_ReadPublic Errors.....	66
Table 36 — TPM2_ActivateCredential Command.....	68
Table 37 — TPM2_ActivateCredential Response.....	68
Table 38 — TPM2_ActivateCredential Errors.....	69

Table 39 — TPM2_MakeCredential Command	72
Table 40 — TPM2_MakeCredential Response	72
Table 41 — TPM2_MakeCredential Errors	73
Table 42 — TPM2_Unseal Command	75
Table 43 — TPM2_Unseal Response	75
Table 44 — TPM2_Unseal Errors	76
Table 45 — TPM2_ObjectChangeAuth Command	78
Table 46 — TPM2_ObjectChangeAuth Response	78
Table 47 — TPM2_ObjectChangeAuth Errors	79
Table 48 — TPM2_Duplicate Command	82
Table 49 — TPM2_Duplicate Response	82
Table 50 — TPM2_Duplicate Errors	83
Table 51 — TPM2_Rewrap Command	86
Table 52 — TPM2_Rewrap Response	86
Table 53 — TPM2_Rewrap Errors	87
Table 54 — TPM2_Import Command	92
Table 55 — TPM2_Import Response	92
Table 56 — TPM2_Import Errors	93
Table 57 — Padding Scheme Selection	97
Table 58 — Message Size Limits Based on Padding	98
Table 59 — TPM2_RSA_Encrypt Command	99
Table 60 — TPM2_RSA_Encrypt Response	99
Table 61 — TPM2_RSA_Encrypt Errors	100
Table 62 — TPM2_RSA_Decrypt Command	103
Table 63 — TPM2_RSA_Decrypt Response	103
Table 64 — TPM2_RSA_Decrypt Errors	104
Table 65 — TPM2_ECDH_KeyGen Command	107
Table 66 — TPM2_ECDH_KeyGen Response	107
Table 67 — TPM2_ECDH_KeyGen Errors	108
Table 68 — TPM2_ECDH_ZGen Command	111
Table 69 — TPM2_ECDH_ZGen Response	111
Table 70 — TPM2_ECDH_ZGen Errors	112
Table 71 — TPM2_ECC_Parameters Command	113
Table 72 — TPM2_ECC_Parameters Response	113
Table 73 — TPM2_ECC_Parameters Errors	114
Table 74 — TPM2_ZGen_2Phase Command	116
Table 75 — TPM2_ZGen_2Phase Response	116
Table 76 — TPM2_ZGen_2Phase Errors	117
Table 77 — Symmetric Chaining Process	120

ISO/IEC 11889-3:2015(E)

Table 78 — TPM2_EncryptDecrypt Command.....	122
Table 79 — TPM2_EncryptDecrypt Response.....	122
Table 80 — TPM2_EncryptDecrypt Errors	123
Table 81 — TPM2_Hash Command.....	126
Table 82 — TPM2_Hash Response	126
Table 83 — TPM2_HMAC Command.....	129
Table 84 — TPM2_HMAC Response	129
Table 85 — TPM2_HMAC Errors	130
Table 86 — TPM2_GetRandom Command.....	133
Table 87 — TPM2_GetRandom Response	133
Table 88 — TPM2_StirRandom Command	136
Table 89 — TPM2_StirRandom Response.....	136
Table 90 — Hash Selection Matrix	138
Table 91 — TPM2_HMAC_Start Command	140
Table 92 — TPM2_HMAC_Start Response	140
Table 93 — TPM2_HMAC_Start Errors.....	141
Table 94 — TPM2_HashSequenceStart Command.....	144
Table 95 — TPM2_HashSequenceStart Response	144
Table 96 — TPM2_HashSequenceStart Errors.....	145
Table 97 — TPM2_SequenceUpdate Command	147
Table 98 — TPM2_SequenceUpdate Response.....	147
Table 99 — TPM2_SequenceUpdate Errors	148
Table 100 — TPM2_SequenceComplete Command	151
Table 101 — TPM2_SequenceComplete Response.....	151
Table 102 — TPM2_SequenceComplete Errors	152
Table 103 — TPM2_EventSequenceComplete Command	155
Table 104 — TPM2_EventSequenceComplete Response.....	155
Table 105 — TPM2_EventSequenceComplete Errors	156
Table 106 — TPM2_Certify Command.....	161
Table 107 — TPM2_Certify Response	161
Table 108 — TPM2_Certify Errors.....	162
Table 109 — TPM2_CertifyCreation Command	165
Table 110 — TPM2_CertifyCreation Response	165
Table 111 — TPM2_CertifyCreation Errors	166
Table 112 — TPM2_Quote Command	169
Table 113 — TPM2_Quote Response.....	169
Table 114 — TPM2_Quote Errors	170
Table 115 — TPM2_GetSessionAuditDigest Command	173
Table 116 — TPM2_GetSessionAuditDigest Response	173

Table 117 — TPM2_GetSessionAuditDigest Errors	174
Table 118 — TPM2_GetCommandAuditDigest Command	177
Table 119 — TPM2_GetCommandAuditDigest Response	177
Table 120 — TPM2_GetCommandAuditDigest Errors	178
Table 121 — TPM2_GetTime Command	181
Table 122 — TPM2_GetTime Response	181
Table 123 — TPM2_GetTime Errors	182
Table 124 — TPM2_Commit Command	186
Table 125 — TPM2_Commit Response	186
Table 126 — TPM2_Commit Response Errors	187
Table 127 — TPM2_EC_Ephemeral Command	191
Table 128 — TPM2_EC_Ephemeral Response	191
Table 129 — TPM2_VerifySignature Command	194
Table 130 — TPM2_VerifySignature Response	194
Table 131 — TPM2_VerifySignature Errors	195
Table 132 — TPM2_Sign Command	198
Table 133 — TPM2_Sign Response	198
Table 134 — TPM2_Sign Response Errors	199
Table 135 — TPM2_SetCommandCodeAuditStatus Command	203
Table 136 — TPM2_SetCommandCodeAuditStatus Response	203
Table 137 — TPM2_PCR_Extend Command	208
Table 138 — TPM2_PCR_Extend Response	208
Table 139 — TPM2_PCR_Extend Errors	209
Table 140 — TPM2_PCR_Event Command	211
Table 141 — TPM2_PCR_Event Response	211
Table 142 — TPM2_PCR_Event Errors	212
Table 143 — TPM2_PCR_Read Command	215
Table 144 — TPM2_PCR_Read Response	215
Table 145 — TPM2_PCR_Allocate Command	218
Table 146 — TPM2_PCR_Allocate Response	218
Table 147 — TPM2_PCR_Allocate Errors	219
Table 148 — TPM2_PCR_SetAuthPolicy Command	221
Table 149 — TPM2_PCR_SetAuthPolicy Response	221
Table 150 — TPM2_PCR_SetAuthPolicy Errors	222
Table 151 — TPM2_PCR_SetAuthValue Command	224
Table 152 — TPM2_PCR_SetAuthValue Response	224
Table 153 — TPM2_PCR_SetAuthValue Errors	225
Table 154 — TPM2_PCR_Reset Command	227
Table 155 — TPM2_PCR_Reset Response	227

ISO/IEC 11889-3:2015(E)

Table 156 — TPM2_PCR_Reset Errors	228
Table 157 — TPM2_PolicySigned Command	243
Table 158 — TPM2_PolicySigned Response.....	243
Table 159 — TPM2_PolicySigned Errors	244
Table 160 — TPM2_PolicySecret Command	248
Table 161 — TPM2_PolicySecret Response.....	248
Table 162 — TPM2_PolicySecret Errors	249
Table 163 — TPM2_PolicyTicket Command.....	252
Table 164 — TPM2_PolicyTicket Response	252
Table 165 — TPM2_PolicyTicket Errors.....	253
Table 166 — TPM2_PolicyOR Command	256
Table 167 — TPM2_PolicyOR Response.....	256
Table 168 — TPM2_PolicyOR Errors	257
Table 169 — TPM2_PolicyPCR Command	261
Table 170 — TPM2_PolicyPCR Response	261
Table 171 — TPM2_PolicyPCR Errors.....	262
Table 172 — TPM2_PolicyLocality Command	265
Table 173 — TPM2_PolicyLocality Response.....	265
Table 174 — TPM2_PolicyLocality Errors	266
Table 175 — TPM2_PolicyNV Command.....	269
Table 176 — TPM2_PolicyNV Response	269
Table 177 — TPM2_PolicyNV Errors	270
Table 178 — TPM2_PolicyCounterTimer Command	274
Table 179 — TPM2_PolicyCounterTimer Response.....	274
Table 180 — TPM2_PolicyCounterTimer Errors	275
Table 181 — TPM2_PolicyCommandCode Command	279
Table 182 — TPM2_PolicyCommandCode Response.....	279
Table 183 — TPM2_PolicyCommandCode Errors	280
Table 184 — TPM2_PolicyPhysicalPresence Command.....	282
Table 185 — TPM2_PolicyPhysicalPresence Response	282
Table 186 — TPM2_PolicyCpHash Command.....	285
Table 187 — TPM2_PolicyCpHash Response.....	285
Table 188 — TPM2_PolicyCpHash Errors	286
Table 189 — TPM2_PolicyNameHash Command	289
Table 190 — TPM2_PolicyNameHash Response.....	289
Table 191 — TPM2_PolicyNameHash Errors	290
Table 192 — TPM2_PolicyDuplicationSelect Command.....	293
Table 193 — TPM2_PolicyDuplicationSelect Response	293
Table 194 — TPM2_PolicyDuplicationSelect Errors	294

Table 195 — TPM2_PolicyAuthorize Command	297
Table 196 — TPM2_PolicyAuthorize Response.....	297
Table 197 — TPM2_PolicyAuthorize Errors	298
Table 198 — TPM2_PolicyAuthValue Command	301
Table 199 — TPM2_PolicyAuthValue Response	301
Table 200 — TPM2_PolicyPassword Command.....	304
Table 201 — TPM2_PolicyPassword Response	304
Table 202 — TPM2_PolicyGetDigest Command	307
Table 203 — TPM2_PolicyGetDigest Response	307
Table 204 — TPM2_PolicyNvWritten Command.....	310
Table 205 — TPM2_PolicyNvWritten Response	310
Table 206 — TPM2_PolicyNvWritten Errors.....	311
Table 207 — TPM2_CreatePrimary Command.....	314
Table 208 — TPM2_CreatePrimary Response	314
Table 209 — TPM2_CreatePrimary Errors.....	315
Table 210 — TPM2_HierarchyControl Command	318
Table 211 — TPM2_HierarchyControl Response	318
Table 212 — TPM2_HierarchyControl Errors	319
Table 213 — TPM2_SetPrimaryPolicy Command.....	322
Table 214 — TPM2_SetPrimaryPolicy Response	322
Table 215 — TPM2_SetPrimaryPolicy Errors.....	323
Table 216 — TPM2_ChangePPS Command	326
Table 217 — TPM2_ChangePPS Response.....	326
Table 218 — TPM2_ChangeEPS Command	329
Table 219 — TPM2_ChangeEPS Response.....	329
Table 220 — TPM2_Clear Command.....	332
Table 221 — TPM2_Clear Response	332
Table 222 — TPM2_Clear Errors	333
Table 223 — TPM2_ClearControl Command.....	336
Table 224 — TPM2_ClearControl Response	336
Table 225 — TPM2_ClearControl Errors.....	337
Table 226 — TPM2_HierarchyChangeAuth Command.....	339
Table 227 — TPM2_HierarchyChangeAuth Response	339
Table 228 — TPM2_HierarchyChangeAuth Errors	340
Table 229 — TPM2_DictionaryAttackLockReset Command	342
Table 230 — TPM2_DictionaryAttackLockReset Response	342
Table 231 — TPM2_DictionaryAttackParameters Command	345
Table 232 — TPM2_DictionaryAttackParameters Response.....	345
Table 233 — TPM2_PP_Commands Command.....	348

ISO/IEC 11889-3:2015(E)

Table 234 — TPM2_PP_Commands Response	348
Table 235 — TPM2_SetAlgorithmSet Command	351
Table 236 — TPM2_SetAlgorithmSet Response	351
Table 237 — TPM2_FieldUpgradeStart Command	356
Table 238 — TPM2_FieldUpgradeStart Response	356
Table 239 — TPM2_FieldUpgradeData Command	359
Table 240 — TPM2_FieldUpgradeData Response	359
Table 241 — TPM2_FirmwareRead Command	362
Table 242 — TPM2_FirmwareRead Response	362
Table 243 — TPM2_ContextSave Command	365
Table 244 — TPM2_ContextSave Response	365
Table 245 — TPM2_ContextSave Errors	366
Table 246 — TPM2_ContextLoad Command	370
Table 247 — TPM2_ContextLoad Response	370
Table 248 — TPM2_ContextLoad Errors	371
Table 249 — TPM2_FlushContext Command	375
Table 250 — TPM2_FlushContext Response	375
Table 251 — TPM2_FlushContext Errors	376
Table 252 — TPM2_EvictControl Command	379
Table 253 — TPM2_EvictControl Response	379
Table 254 — TPM2_EvictControl Errors	380
Table 255 — TPM2_ReadClock Command	383
Table 256 — TPM2_ReadClock Response	383
Table 257 — TPM2_ClockSet Command	386
Table 258 — TPM2_ClockSet Response	386
Table 259 — TPM2_ClockSet Errors	387
Table 260 — TPM2_ClockRateAdjust Command	389
Table 261 — TPM2_ClockRateAdjust Response	389
Table 262 — TPM2_GetCapability Command	395
Table 263 — TPM2_GetCapability Response	395
Table 264 — TPM2_GetCapability Errors	396
Table 265 — TPM2_TestParms Command	400
Table 266 — TPM2_TestParms Response	400
Table 267 — TPM2_NV_DefineSpace Command	407
Table 268 — TPM2_NV_DefineSpace Response	407
Table 269 — TPM2_NV_DefineSpace Errors	408
Table 270 — TPM2_NV_UndefineSpace Command	412
Table 271 — TPM2_NV_UndefineSpace Response	412
Table 272 — TPM2_NV_UndefineSpace Errors	413

Table 273 — TPM2_NV_UndefineSpaceSpecial Command.....	415
Table 274 — TPM2_NV_UndefineSpaceSpecial Response.....	415
Table 275 — TPM2_NV_UndefineSpaceSpecial Errors.....	416
Table 276 — TPM2_NV_ReadPublic Command.....	418
Table 277 — TPM2_NV_ReadPublic Response.....	418
Table 278 — TPM2_NV_Write Command.....	421
Table 279 — TPM2_NV_Write Response.....	421
Table 280 — TPM2_NV_Write Errors.....	422
Table 281 — TPM2_NV_Increment Command.....	425
Table 282 — TPM2_NV_Increment Response.....	425
Table 283 — TPM2_NV_Increment Errors.....	426
Table 284 — TPM2_NV_Extend Command.....	429
Table 285 — TPM2_NV_Extend Response.....	429
Table 286 — TPM2_NV_Extend Errors.....	430
Table 287 — TPM2_NV_SetBits Command.....	433
Table 288 — TPM2_NV_SetBits Response.....	433
Table 289 — TPM2_NV_SetBits Errors.....	434
Table 290 — TPM2_NV_WriteLock Command.....	437
Table 291 — TPM2_NV_WriteLock Response.....	437
Table 292 — TPM2_NV_WriteLock Errors.....	438
Table 293 — TPM2_NV_GlobalWriteLock Command.....	441
Table 294 — TPM2_NV_GlobalWriteLock Response.....	441
Table 295 — TPM2_NV_Read Command.....	444
Table 296 — TPM2_NV_Read Response.....	444
Table 297 — TPM2_NV_Read Errors.....	445
Table 298 — TPM2_NV_ReadLock Command.....	447
Table 299 — TPM2_NV_ReadLock Response.....	447
Table 300 — TPM2_NV_ReadLock Errors.....	448
Table 301 — TPM2_NV_ChangeAuth Command.....	451
Table 302 — TPM2_NV_ChangeAuth Response.....	451
Table 303 — TPM2_NV_ChangeAuth Errors.....	452
Table 304 — TPM2_NV_Certify Command.....	454
Table 305 — TPM2_NV_Certify Response.....	454
Table 306 — TPM2_NV_Certify Errors.....	455

ISO/IEC 11889-3:2015(E)

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).

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).

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 11889-3 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.

This second edition cancels and replaces the first edition (ISO/IEC 11889-3:2009), 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:

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

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) 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 3: Commands

1 Scope

This part of ISO/IEC 11889 contains the definitions of the Trusted Platform Module (TPM) commands. These commands make use of the constants, flags, structures, and union definitions defined in ISO/IEC 11889-2.

The detailed description of the operation of the commands is written in the C language with extensive comments. The behavior of the C code in this part of ISO/IEC 11889 is normative but does not fully describe the behavior of a TPM. The combination of this part of ISO/IEC 11889 and ISO/IEC 11889-4 is sufficient to fully describe the required behavior of a TPM.

The code in this part of ISO/IEC 11889 and ISO/IEC 11889-4 is written to define the behavior of a compliant TPM. In some cases it is not possible to provide a compliant implementation. In those cases, any implementation provided by the vendor that meets the general description of the function provided in this part of ISO/IEC 11889 would be compliant.

EXAMPLE Firmware update is a case where it is not possible to provide a compliant implementation.

The code in this part of ISO/IEC 11889 and ISO/IEC 11889-4 is not written to meet any particular level of conformance nor does this specification require that a TPM meet any particular level of conformance.

ISO/IEC 11889-3:2015(E)

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 11889-1, *Information technology — Trusted Platform Module Library — Part 1: Architecture*
- ISO/IEC 11889-2, *Information technology — Trusted Platform Module Library — Part 2: Structures*
- ISO/IEC 11889-4, *Information technology — Trusted Platform Module Library — Part 4: Supporting routines*
- TCG Vendor ID Registry, available at
<http://www.trustedcomputinggroup.org/resources/vendor_id_registry>