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

**Part 3:
Commands**

Technologies de l'information — Bibliothèque de module

de plate-forme de confiance

Partie 3: Commandes

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

ISO/IEC 11889-3:2015

<https://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 11889-3:2015](https://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015)

<https://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015>



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

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

iTech STANDARD PREVIEW
(standards.itech.ai)

ISO/IEC 11889-3:2015
<https://standards.itech.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd0cc5e53/iso-iec-11889-3-2015>

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

ITh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 11889-3:2015

<https://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca9bd6ce5e53/iso-iec-11889-3-2015>

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

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

iTeH STANDARD PREVIEW
 (standards.iteh.ai)
 ISO/IEC 11889-3:2015
<https://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015>

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

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

iTech STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 11889-3:2015
<http://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015>

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

iTech STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 11889-3:2015

<http://standards.iteh.ai/catalog/standards/sist/eb48015c-c089-46ae-930b-ca0bd6ce5e53/iso-iec-11889-3-2015>