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

**Part 4:
Supporting Routines**

*Technologies de l'information — Bibliothèque de module
de plate-forme de confiance —
Partie 4: Routines de support*



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.....	xvii
Introduction.....	xviii
1 Scope.....	1
2 Normative references	2
3 Terms and definitions	2
4 Symbols and abbreviated terms	2
5 Automation	2
5.1 Introduction	2
5.2 Configuration Parser.....	2
5.3 Structure Parser	3
5.3.1 Introduction	3
5.3.2 Unmarshaling Code Prototype.....	3
5.3.3 Marshaling Code Function Prototypes	5
5.4 Command Parser.....	6
5.5 Portability.....	6
6 Header Files.....	7
6.1 Introduction	7
6.2 BaseType.h	7
6.3 bits.h.....	8
6.4 bool.h.....	9
6.5 Capabilities.h	9
6.6 TPMB.h.....	9
6.7 TpmError.h.....	10
6.8 Global.h	10
6.8.1 Description	10
6.8.2 Includes.....	11
6.8.3 Defines and Types.....	11
6.8.4 Loaded Object Structures.....	12
6.8.5 AUTH_DUP Types	14
6.8.6 Active Session Context	14
6.8.7 PCR	16
6.8.8 Startup	17
6.8.9 NV.....	18
6.8.10 COMMIT_INDEX_MASK	19
6.8.11 RAM Global Values.....	19
6.8.12 Persistent Global Values.....	21
6.8.13 Global Macro Definitions	26
6.9 Private data.....	26
6.10 Tpm.h	31
6.11 swap.h	31
6.12 InternalRoutines.h	32
6.13 TpmBuildSwitches.h	33
6.14 VendorString.h	34
7 Main.....	36
7.1 CommandDispatcher().....	36
7.2 ExecCommand.c	36
7.2.1 Introduction	36
7.2.2 Includes.....	36
7.2.3 ExecuteCommand()	36

ISO/IEC 11889-4:2015(E)

7.3	ParseHandleBuffer()	42
7.4	SessionProcess.c	43
7.4.1	Introduction	43
7.4.2	Includes and Data Definitions	43
7.4.3	Authorization Support Functions	43
7.4.4	Session Parsing Functions	50
7.4.5	Response Session Processing	68
8	Command Support Functions	78
8.1	Introduction	78
8.2	Attestation Command Support (Attest_spt.c)	78
8.2.1	Includes	78
8.2.2	Functions	78
8.3	Context Management Command Support (Context_spt.c)	81
8.3.1	Includes	81
8.3.2	Functions	81
8.4	Policy Command Support (Policy_spt.c)	83
8.4.1	Includes	83
8.4.2	Functions	83
8.5	NV Command Support (NV_spt.c)	85
8.5.1	Includes	85
8.5.2	Functions	86
8.6	Object Command Support (Object_spt.c)	88
8.6.1	Includes	88
8.6.2	Local Functions	88
8.6.3	Public Functions	93
9	Subsystem	113
9.1	CommandAudit.c	113
9.1.1	Introduction	113
9.1.2	Includes	113
9.1.3	Functions	113
9.2	DA.c	117
9.2.1	Introduction	117
9.2.2	Includes and Data Definitions	117
9.2.3	Functions	117
9.3	Hierarchy.c	120
9.3.1	Introduction	120
9.3.2	Includes	120
9.3.3	Functions	120
9.4	NV.c	124
9.4.1	Introduction	124
9.4.2	Includes, Defines and Data Definitions	124
9.4.3	NV Utility Functions	124
9.4.4	NV Index and Persistent Object Access Functions	126
9.4.5	RAM-based NV Index Data Access Functions	130
9.4.6	Utility Functions	132
9.4.7	NV Access Functions	140
9.5	Object.c	158

9.5.1	Introduction	158
9.5.2	Includes and Data Definitions	158
9.5.3	Functions	158
9.6	PCR.c	174
9.6.1	Introduction	174
9.6.2	Includes, Defines, and Data Definitions	174
9.6.3	Functions	174
9.7	PP.c	196
9.7.1	Introduction	196
9.7.2	Includes	196
9.7.3	Functions	196
9.8	Session.c	199
9.8.1	Introduction	199
9.8.2	Includes, Defines, and Local Variables	200
9.8.3	File Scope Function -- ContextIdSetOldest()	200
9.8.4	Startup Function -- SessionStartup()	201
9.8.5	Access Functions	202
9.8.6	Utility Functions	204
9.9	Time.c	216
9.9.1	Introduction	216
9.9.2	Includes	216
9.9.3	Functions	216
10	Support	221
10.1	AlgorithmCap.c	221
10.1.1	Description	221
10.1.2	Includes and Defines	221
10.1.3	AlgorithmCapGetImplemented()	222
10.2	Bits.c	224
10.2.1	Introduction	224
10.2.2	Includes	224
10.2.3	Functions	224
10.3	CommandAttributeData.c	225
10.4	CommandCodeAttributes.c	231
10.4.1	Introduction	231
10.4.2	Includes and Defines	231
10.4.3	Command Attribute Functions	231
10.5	DRTM.c	236
10.5.1	Description	236
10.5.2	Includes	236
10.5.3	Functions	236
10.6	Entity.c	237
10.6.1	Description	237
10.6.2	Includes	237
10.6.3	Functions	237
10.7	Global.c	243
10.7.1	Description	243
10.7.2	Includes and Defines	244
10.7.3	Global Data Values	244

10.7.4	Private Values	244
10.8	Handle.c	246
10.8.1	Description	246
10.8.2	Includes	246
10.8.3	Functions	246
10.9	Locality.c	248
10.9.1	Includes	248
10.9.2	LocalityGetAttributes()	248
10.10	Manufacture.c	248
10.10.1	Description	248
10.10.2	Includes and Data Definitions	248
10.10.3	Functions	249
10.11	Marshal.c	251
10.11.1	Introduction	251
10.11.2	Unmarshal and Marshal a Value	251
10.11.3	Unmarshal and Marshal a Union	252
10.11.4	Unmarshal and Marshal a Structure	254
10.11.5	Unmarshal and Marshal an Array	256
10.11.6	TPM2B Handling	258
10.12	MemoryLib.c	259
10.12.1	Description	259
10.12.2	Includes and Data Definitions	259
10.12.3	Functions on BYTE Arrays	259
10.13	Power.c	264
10.13.1	Description	264
10.13.2	Includes and Data Definitions	264
10.13.3	Functions	264
10.14	PropertyCap.c	265
10.14.1	Description	265
10.14.2	Includes	265
10.14.3	Functions	265
10.15	TpmFail.c	273
10.15.1	Includes, Defines, and Types	273
10.15.2	Typedefs	273
10.15.3	Local Functions	274
10.15.4	Public Functions	275
10.15.5	TpmFailureMode	275
11	Cryptographic Functions	279
11.1	Introduction	279
11.2	CryptUtil.c	279
11.2.1	Introduction	279
11.2.2	Includes	279
11.2.3	TranslateCryptErrors()	279
11.2.4	Random Number Generation Functions	280
11.2.5	Hash/HMAC Functions	281
11.2.6	RSA Functions	294
11.2.7	ECC Functions	302
11.2.8	Symmetric Functions	312
11.2.9	Initialization and shut down	316

11.2.10 Algorithm-Independent Functions	317
11.2.11 Math functions	339
11.2.12 Capability Support	341
11.3 Ticket.c	343
11.3.1 Introduction	343
11.3.2 Includes.....	343
11.3.3 Functions	343
11.4 CryptSelfTest.c.....	346
11.4.1 Introduction	346
11.4.2 Functions	347
Annex A (informative) Implementation Dependent	351
A.1 Introduction	351
A.2 Implementation.h	351
Annex B (informative) Cryptographic Library Interface	365
B.1 Introduction	365
B.2 Integer Format.....	365
B.3 CryptoEngine.h.....	365
B.3.1. Introduction	365
B.3.2. General Purpose Macros.....	366
B.3.3. Self-test.....	366
B.3.4. Hash-related Structures	366
B.3.5. Asymmetric Structures and Values	368
B.3.6. ECC-related Structures	368
B.3.7. RSA-related Structures	368
B.4 OsslCryptoEngine.h.....	370
B.4.1. Introduction	370
B.4.2. Defines.....	370
B.5 MathFunctions.c	371
B.5.1. Introduction	371
B.5.2. Externally Accessible Functions	371
B.6 CpriCryptPri.c.....	381
B.6.1. Introduction	381
B.6.2. Includes and Locals	381
B.6.3. Functions	381
B.7 CpriRNG.c.....	383
B.7.1. Introduction	383
B.7.2. Defines.....	383
B.7.3. Includes and Values.....	383
B.7.4. Functions	383
B.8 CpriHash.c	386
B.8.1. Description	386
B.8.2. Includes, Defines, and Types	386
B.8.3. Static Functions	386
B.8.4. Hash Functions.....	388
B.8.5. HMAC Functions.....	395
B.8.6. Mask and Key Generation Functions	397
B.9 CpriHashData.c	402
B.10 CpriMisc.c	403

B.10.1. Includes.....	403
B.10.2. Functions	403
B.11 CpriSym.c	405
B.11.1. Introduction	405
B.11.2. Includes, Defines, and Typedefs	405
B.11.3. Utility Functions	406
B.11.4. Symmetric Encryption	407
B.12 RSA Files	412
B.12.1. CpriRSA.c	412
B.12.2. Alternative RSA Key Generation.....	436
B.13 Elliptic Curve Files.....	467
B.13.1. CpriDataEcc.h	467
B.13.2. CpriDataEcc.c	468
B.13.3. CpriECC.c	471
Annex C (informative) Simulation Environment.....	509
C.1 Introduction	509
C.2 Cancel.c.....	509
C.2.1. Introduction	509
C.2.2. Includes, Typedefs, Structures, and Defines.....	509
C.2.3. Functions	509
C.3 Clock.c.....	511
C.3.1. Introduction	511
C.3.2. Includes and Data Definitions.....	511
C.3.3. Functions	511
C.4 Entropy.c.....	513
C.4.1. Includes and Defines	513
C.4.2. Local values	513
C.4.3. _plat__GetEntropy().....	513
C.5 LocalityPlat.c.....	515
C.5.1. Includes.....	515
C.5.2. Functions	515
C.6 NVMem.c	516
C.6.1. Introduction	516
C.6.2. Includes.....	516
C.6.3. Functions	516
C.7 PowerPlat.c.....	521
C.7.1. Includes.....	521
C.7.2. Functions	521
C.8 Platform.h	523
C.8.1. Includes and Defines	523
C.8.2. Power Functions	523
C.8.3. Physical Presence Functions	523
C.8.4. Command Canceling Functions	524
C.8.5. NV memory functions.....	525
C.8.6. Locality Functions.....	527
C.8.7. Clock Constants and Functions.....	527
C.8.8. Entropy Function _plat__GetEntropy().....	529

C.9 PlatformData.h	530
C.10 PlatformData.c	531
C.10.1. Description	531
C.10.2. Includes.....	531
C.11 PPPlat.c.....	532
C.11.1. Description	532
C.11.2. Includes.....	532
C.11.3. Functions	532
C.12 Unique.c.....	534
C.12.1. Introduction	534
C.12.2. Includes.....	534
C.12.3. _plat_GetUnique().....	534
Annex D (informative) Remote Procedure Interface	535
D.1 Introduction	535
D.2 TpmTcpProtocol.h	536
D.2.1. Introduction	536
D.2.2. Defines.....	536
D.2.3. Typedefs	536
D.3 TcpServer.c.....	538
D.3.1. Description	538
D.3.2. Includes, Locals, Defines and Function Prototypes	538
D.3.3. Functions	538
D.4 TPMCmdp.c	548
D.4.1. Description	548
D.4.2. Includes and Data Definitions.....	548
D.4.3. Functions	548
D.5 TPMCmds.c.....	554
D.5.1. Description	554
D.5.2. Includes, Defines, Data Definitions, and Function Prototypes.....	554
D.5.3. Functions	554
Bibliography	556

Tables

Table 1	43
Table 2	44
Table 3	46
Table 4	46
Table 5	47
Table 6	49
Table 7	52
Table 8	54
Table 9	55
Table 10	58
Table 11	61
Table 12	62
Table 13	64
Table 14	64
Table 15	67
Table 16	78
Table 17	80
Table 18	86
Table 19	87
Table 20	88
Table 21	92
Table 22	93
Table 23	94
Table 24	97
Table 25	102
Table 26	104
Table 27	108
Table 28	111
Table 29	114
Table 30	115
Table 31	115
Table 32	116
Table 33	123
Table 34	125
Table 35	128
Table 36	130

Table 37	136
Table 38	136
Table 39	138
Table 40	140
Table 41	141
Table 42	142
Table 43	143
Table 44	146
Table 45	149
Table 46	150
Table 47	154
Table 48	155
Table 49	159
Table 50	160
Table 51	162
Table 52	163
Table 53	166
Table 54	166
Table 55	167
Table 56	168
Table 57	169
Table 58	172
Table 59	172
Table 60	172
Table 61	174
Table 62	175
Table 63	176
Table 64	176
Table 65	178
Table 66	179
Table 67	180
Table 68	181
Table 69	184
Table 70	185
Table 71	186
Table 72	189
Table 73	192
Table 74	193
Table 75	195

ISO/IEC 11889-4:2015(E)

Table 76	195
Table 77	198
Table 78	198
Table 79	202
Table 80	203
Table 81	203
Table 82	204
Table 83	205
Table 84	208
Table 85	209
Table 86	213
Table 87	214
Table 88	219
Table 89	223
Table 90	224
Table 91	231
Table 92	232
Table 93	232
Table 94	233
Table 95	233
Table 96	235
Table 97	237
Table 98	247
Table 99	249
Table 100	250
Table 101— Definition of (TPM_HANDLE) TPML_DH_OBJECT Type from ISO/IEC 11889-2.....	251
Table 102 — Definition of TPML_PUBLIC_PARMS Union <IN/OUT, S> from ISO/IEC 11889-2.....	252
Table 103 — Definition of TPML_PUBLIC Structure from ISO/IEC 11889-2.....	254
Table 104 — Definition of TPML_DIGEST Structure from ISO/IEC 11889-2.....	256
Table 105 — Definition of TPML2B_EVENT Structure from ISO/IEC 11889-2.....	258
Table 106	260
Table 107	262
Table 108	265
Table 109	265
Table 110	272
Table 111	279
Table 112	281
Table 113	282
Table 114	283

Table 115	283
Table 116	284
Table 117	284
Table 118	286
Table 119	287
Table 120	287
Table 121	288
Table 122	288
Table 123	289
Table 124	289
Table 125	290
Table 126	290
Table 127	291
Table 128	291
Table 129	294
Table 130	295
Table 131	296
Table 132	297
Table 133	299
Table 134	300
Table 135	301
Table 136	303
Table 137	304
Table 138	305
Table 139	306
Table 140	307
Table 141	307
Table 142	309
Table 143	310
Table 144	317
Table 145	320
Table 146	322
Table 147	326
Table 148	328
Table 149	330
Table 150	331
Table 151	335
Table 152	337
Table 153	338

ISO/IEC 11889-4:2015(E)

Table 154	339
Table 155	340
Table 156	340
Table 157	341
Table 158	342
Table 159	343
Table 160	347
Table 161	348
Table 162	349
Table B.1	368
Table B.2	371
Table B.3	372
Table B.4	372
Table B.5	373
Table B.6	374
Table B.7	375
Table B.8	377
Table B.9	377
Table B.10	378
Table B.11	380
Table B.12	387
Table B.13	389
Table B.14	389
Table B.15	390
Table B.16	391
Table B.17	392
Table B.18	394
Table B.19	395
Table B.20	396
Table B.21	397
Table B.22	398
Table B.23	400
Table B.24	403
Table B.25	406
Table B.26	409
Table B.27	412
Table B.28	414
Table B.29	416
Table B.30	417

Table B.31	418
Table B.32	419
Table B.33	421
Table B.34	422
Table B.35	422
Table B.36	424
Table B.37	426
Table B.38	427
Table B.39	428
Table B.40	429
Table B.41	430
Table B.42	431
Table B.43	432
Table B.44	439
Table B.45	442
Table B.46	445
Table B.47	451
Table B.48	472
Table B.49	473
Table B.50	475
Table B.51	477
Table B.52	479
Table B.53	481
Table B.54	482
Table B.55	487
Table B.56	489
Table B.57	492
Table B.58	494
Table B.59	495
Table B.60	497
Table B.61	498
Table B.62	500
Table B.63	502
Table B.64	504
Table B.65	507
Table C.1	509
Table C.2	513
Table C.3	516
Table C.4	518

ISO/IEC 11889-4:2015(E)

Table C.5.....	519
Table C.6.....	520
Table C.7.....	524
Table C.8.....	524
Table C.9.....	525
Table C.10.....	525
Table C.11.....	526
Table C.12.....	526
Table C.13.....	529
Table C.14.....	532

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 11889-4 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 11889-4:2009), 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:

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

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 4: Supporting routines

1 Scope

This part of ISO/IEC 11889 contains C code that describes the algorithms and methods used by the command code in ISO/IEC 11889-3. The code in this part of ISO/IEC 11889 augments ISO/IEC 11889-2 and ISO/IEC 11889-3 to provide a complete description of a TPM, including the supporting framework for the code that performs the command actions.

Any code in this part of ISO/IEC 11889 may be replaced by code that provides similar results when interfacing to the action code in ISO/IEC 11889-3. The behavior of code in this part of ISO/IEC 11889 that is not included in an annex is *normative*, as observed at the interfaces with ISO/IEC 11889-3 code. Code in an annex is provided for completeness, that is, to allow a full implementation of ISO/IEC 11889 from the provided code.

The code in ISO/IEC 11889-3 and this part of ISO/IEC 11889 is written to define the behavior of a compliant TPM. In some cases (e.g., firmware update), 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 ISO/IEC 11889-3 would be compliant.

The code in ISO/IEC 11889-3 and this part of ISO/IEC 11889 is not written to meet any particular level of conformance nor does ISO/IEC 11889 require that a TPM meet any particular level of conformance.

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 11889-2, *Information technology — Trusted Platform Module Library — Part 2: Structures*
- ISO/IEC 11889-3, *Information technology — Trusted Platform Module Library — Part 3: Commands*