

# Trusted Platform Module Library

## Part 3: Commands

Family “2.0”

Level 00 Revision 01.38

September 29, 2016

Contact: [admin@trustedcomputinggroup.org](mailto:admin@trustedcomputinggroup.org)

**TCG**

**TCG Published**

Copyright © TCG 2006-2016

## Licenses and Notices

### Copyright Licenses:

- Trusted Computing Group (TCG) grants to the user of the source code in this specification (the “Source Code”) a worldwide, irrevocable, nonexclusive, royalty free, copyright license to reproduce, create derivative works, distribute, display and perform the Source Code and derivative works thereof, and to grant others the rights granted herein.
- The TCG grants to the user of the other parts of the specification (other than the Source Code) the rights to reproduce, distribute, display, and perform the specification solely for the purpose of developing products based on such documents.

### Source Code Distribution Conditions:

- Redistributions of Source Code must retain the above copyright licenses, this list of conditions and the following disclaimers.
- Redistributions in binary form must reproduce the above copyright licenses, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.

### Disclaimers:

- THE COPYRIGHT LICENSES SET FORTH ABOVE DO NOT REPRESENT ANY FORM OF LICENSE OR WAIVER, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, WITH RESPECT TO PATENT RIGHTS HELD BY TCG MEMBERS (OR OTHER THIRD PARTIES) THAT MAY BE NECESSARY TO IMPLEMENT THIS SPECIFICATION OR OTHERWISE. Contact TCG Administration ([admin@trustedcomputinggroup.org](mailto:admin@trustedcomputinggroup.org)) for information on specification licensing rights available through TCG membership agreements.
- THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, OR NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.
- Without limitation, TCG and its members and licensors disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Any marks and brands contained herein are the property of their respective owners.

## CONTENTS

1	Scope .....	1
2	Terms and Definitions .....	1
3	Symbols and abbreviated terms.....	1
4	Notation .....	2
4.1	Introduction .....	2
4.2	Table Decorations.....	2
4.3	AuthorizationSize and ParameterSize.....	4
4.4	Return Code Alias.....	4
5	Command Processing.....	5
5.1	Introduction .....	5
5.2	Command Header Validation.....	5
5.3	Mode Checks.....	5
5.4	Handle Area Validation.....	6
5.5	Session Area Validation.....	7
5.6	Authorization Checks.....	8
5.7	Parameter Decryption.....	10
5.8	Parameter Unmarshaling.....	10
5.9	Command Post Processing .....	12
6	Response Values .....	13
6.1	Tag.....	13
6.2	Response Codes .....	13
7	Implementation Dependent .....	16
8	Detailed Actions Assumptions.....	17
8.1	Introduction .....	17
8.2	Pre-processing.....	17
8.3	Post Processing.....	17
9	Start-up.....	18
9.1	Introduction .....	18
9.2	_TPM_Init.....	18
9.3	TPM2_Startup.....	20
9.4	TPM2_Shutdown .....	25
10	Testing.....	28
10.1	Introduction .....	28
10.2	TPM2_SelfTest.....	29
10.3	TPM2_IncrementalSelfTest.....	32
10.4	TPM2_GetTestResult .....	35
11	Session Commands .....	38
11.1	TPM2_StartAuthSession .....	38
11.2	TPM2_PolicyRestart.....	42
12	Object Commands.....	45
12.1	TPM2_Create.....	45
12.2	TPM2_Load .....	50

12.3	TPM2_LoadExternal .....	53
12.4	TPM2_ReadPublic .....	57
12.5	TPM2_ActivateCredential .....	60
12.6	TPM2_MakeCredential .....	63
12.7	TPM2_Unseal .....	66
12.8	TPM2_ObjectChangeAuth .....	69
12.9	TPM2_CreateLoaded .....	72
13	Duplication Commands .....	75
13.1	TPM2_Duplicate .....	75
13.2	TPM2_Rewrap .....	78
13.3	TPM2_Import .....	81
14	Asymmetric Primitives .....	85
14.1	Introduction .....	85
14.2	TPM2_RSA_Encrypt .....	85
14.3	TPM2_RSA_Decrypt .....	89
14.4	TPM2_ECDH_KeyGen .....	92
14.5	TPM2_ECDH_ZGen .....	95
14.6	TPM2_ECC_Parameters .....	98
14.7	TPM2_ZGen_2Phase .....	101
15	Symmetric Primitives .....	104
15.1	Introduction .....	104
15.2	TPM2_EncryptDecrypt .....	106
15.3	TPM2_EncryptDecrypt2 .....	109
15.4	TPM2_Hash .....	112
15.5	TPM2_HMAC .....	115
16	Random Number Generator .....	118
16.1	TPM2_GetRandom .....	118
16.2	TPM2_StirRandom .....	121
17	Hash/HMAC/Event Sequences .....	124
17.1	Introduction .....	124
17.2	TPM2_HMAC_Start .....	124
17.3	TPM2_HashSequenceStart .....	127
17.4	TPM2_SequenceUpdate .....	130
17.5	TPM2_SequenceComplete .....	133
17.6	TPM2_EventSequenceComplete .....	136
18	Attestation Commands .....	139
18.1	Introduction .....	139
18.2	TPM2_Certify .....	141
18.3	TPM2_CertifyCreation .....	144
18.4	TPM2_Quote .....	147
18.5	TPM2_GetSessionAuditDigest .....	150
18.6	TPM2_GetCommandAuditDigest .....	153
18.7	TPM2_GetTime .....	156
19	Ephemeral EC Keys .....	159

- 19.1 Introduction ..... 159
- 19.2 TPM2\_Commit ..... 160
- 19.3 TPM2\_EC\_Ephemeral ..... 163
- 20 Signing and Signature Verification ..... 166
  - 20.1 TPM2\_VerifySignature ..... 166
  - 20.2 TPM2\_Sign ..... 169
- 21 Command Audit ..... 172
  - 21.1 Introduction ..... 172
  - 21.2 TPM2\_SetCommandCodeAuditStatus ..... 173
- 22 Integrity Collection (PCR) ..... 176
  - 22.1 Introduction ..... 176
  - 22.2 TPM2\_PCR\_Extend ..... 177
  - 22.3 TPM2\_PCR\_Event ..... 180
  - 22.4 TPM2\_PCR\_Read ..... 183
  - 22.5 TPM2\_PCR\_Allocate ..... 186
  - 22.6 TPM2\_PCR\_SetAuthPolicy ..... 189
  - 22.7 TPM2\_PCR\_SetAuthValue ..... 192
  - 22.8 TPM2\_PCR\_Reset ..... 195
  - 22.9 \_TPM\_Hash\_Start ..... 198
  - 22.10 \_TPM\_Hash\_Data ..... 200
  - 22.11 \_TPM\_Hash\_End ..... 202
- 23 Enhanced Authorization (EA) Commands ..... 204
  - 23.1 Introduction ..... 204
  - 23.2 Signed Authorization Actions ..... 205
  - 23.3 TPM2\_PolicySigned ..... 209
  - 23.4 TPM2\_PolicySecret ..... 213
  - 23.5 TPM2\_PolicyTicket ..... 216
  - 23.6 TPM2\_PolicyOR ..... 219
  - 23.7 TPM2\_PolicyPCR ..... 222
  - 23.8 TPM2\_PolicyLocality ..... 226
  - 23.9 TPM2\_PolicyNV ..... 229
  - 23.10 TPM2\_PolicyCounterTimer ..... 232
  - 23.11 TPM2\_PolicyCommandCode ..... 235
  - 23.12 TPM2\_PolicyPhysicalPresence ..... 238
  - 23.13 TPM2\_PolicyCpHash ..... 241
  - 23.14 TPM2\_PolicyNameHash ..... 244
  - 23.15 TPM2\_PolicyDuplicationSelect ..... 247
  - 23.16 TPM2\_PolicyAuthorize ..... 250
  - 23.17 TPM2\_PolicyAuthValue ..... 253
  - 23.18 TPM2\_PolicyPassword ..... 256
  - 23.19 TPM2\_PolicyGetDigest ..... 259
  - 23.20 TPM2\_PolicyNvWritten ..... 262
  - 23.21 TPM2\_PolicyTemplate ..... 265
  - 23.22 TPM2\_PolicyAuthorizeNV ..... 268
- 24 Hierarchy Commands ..... 271
  - 24.1 TPM2\_CreatePrimary ..... 271

24.2	TPM2_HierarchyControl .....	274
24.3	TPM2_SetPrimaryPolicy .....	277
24.4	TPM2_ChangePPS .....	280
24.5	TPM2_ChangeEPS .....	283
24.6	TPM2_Clear .....	286
24.7	TPM2_ClearControl .....	289
24.8	TPM2_HierarchyChangeAuth .....	292
25	Dictionary Attack Functions .....	295
25.1	Introduction .....	295
25.2	TPM2_DictionaryAttackLockReset .....	295
25.3	TPM2_DictionaryAttackParameters .....	298
26	Miscellaneous Management Functions .....	301
26.1	Introduction .....	301
26.2	TPM2_PP_Commands .....	301
26.3	TPM2_SetAlgorithmSet .....	304
27	Field Upgrade .....	307
27.1	Introduction .....	307
27.2	TPM2_FieldUpgradeStart .....	309
27.3	TPM2_FieldUpgradeData .....	312
27.4	TPM2_FirmwareRead .....	315
28	Context Management .....	318
28.1	Introduction .....	318
28.2	TPM2_ContextSave .....	318
28.3	TPM2_ContextLoad .....	321
28.4	TPM2_FlushContext .....	324
28.5	TPM2_EvictControl .....	327
29	Clocks and Timers .....	331
29.1	TPM2_ReadClock .....	331
29.2	TPM2_ClockSet .....	334
29.3	TPM2_ClockRateAdjust .....	337
30	Capability Commands .....	340
30.1	Introduction .....	340
30.2	TPM2_GetCapability .....	340
30.3	TPM2_TestParms .....	346
31	Non-volatile Storage .....	349
31.1	Introduction .....	349
31.2	NV Counters .....	351
31.3	TPM2_NV_DefineSpace .....	352
31.4	TPM2_NV_UndefineSpace .....	356
31.5	TPM2_NV_UndefineSpaceSpecial .....	359
31.6	TPM2_NV_ReadPublic .....	362
31.7	TPM2_NV_Write .....	365
31.8	TPM2_NV_Increment .....	368
31.9	TPM2_NV_Extend .....	371

- 31.10 TPM2\_NV\_SetBits ..... 374
- 31.11 TPM2\_NV\_WriteLock ..... 377
- 31.12 TPM2\_NV\_GlobalWriteLock ..... 380
- 31.13 TPM2\_NV\_Read ..... 383
- 31.14 TPM2\_NV\_ReadLock ..... 386
- 31.15 TPM2\_NV\_ChangeAuth ..... 389
- 31.16 TPM2\_NV\_Certify ..... 392
- 32 Vendor Specific ..... 395
  - 32.1 Introduction ..... 395
  - 32.2 TPM2\_Vendor\_TCG\_Test ..... 395

## Tables

Table 1 — Command Modifiers and Decoration .....	2
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_Shutdown Command .....	26
Table 8 — TPM2_Shutdown Response .....	26
Table 9 — TPM2_SelfTest Command .....	30
Table 10 — TPM2_SelfTest Response .....	30
Table 11 — TPM2_IncrementalSelfTest Command .....	33
Table 12 — TPM2_IncrementalSelfTest Response .....	33
Table 13 — TPM2_GetTestResult Command .....	36
Table 14 — TPM2_GetTestResult Response .....	36
Table 15 — TPM2_StartAuthSession Command .....	40
Table 16 — TPM2_StartAuthSession Response .....	40
Table 17 — TPM2_PolicyRestart Command .....	43
Table 18 — TPM2_PolicyRestart Response .....	43
Table 19 — TPM2_Create Command .....	48
Table 20 — TPM2_Create Response .....	48
Table 21 — TPM2_Load Command .....	51
Table 22 — TPM2_Load Response .....	51
Table 23 — TPM2_LoadExternal Command .....	55
Table 24 — TPM2_LoadExternal Response .....	55
Table 25 — TPM2_ReadPublic Command .....	58
Table 26 — TPM2_ReadPublic Response .....	58
Table 27 — TPM2_ActivateCredential Command .....	61
Table 28 — TPM2_ActivateCredential Response .....	61
Table 29 — TPM2_MakeCredential Command .....	64
Table 30 — TPM2_MakeCredential Response .....	64
Table 31 — TPM2_Unseal Command .....	67
Table 32 — TPM2_Unseal Response .....	67
Table 33 — TPM2_ObjectChangeAuth Command .....	70
Table 34 — TPM2_ObjectChangeAuth Response .....	70
Table 35 — TPM2_CreateLoaded Command .....	73
Table 36 — TPM2_CreateLoaded Response .....	73
Table 37 — TPM2_Duplicate Command .....	76



Table 38 — TPM2\_Duplicate Response..... 76

Table 39 — TPM2\_Rewrap Command..... 79

Table 40 — TPM2\_Rewrap Response ..... 79

Table 41 — TPM2\_Import Command ..... 83

Table 42 — TPM2\_Import Response ..... 83

Table 43 — Padding Scheme Selection ..... 85

Table 44 — Message Size Limits Based on Padding..... 86

Table 45 — TPM2\_RSA\_Encrypt Command..... 87

Table 46 — TPM2\_RSA\_Encrypt Response ..... 87

Table 47 — TPM2\_RSA\_Decrypt Command ..... 90

Table 48 — TPM2\_RSA\_Decrypt Response..... 90

Table 49 — TPM2\_ECDH\_KeyGen Command..... 93

Table 50 — TPM2\_ECDH\_KeyGen Response ..... 93

Table 51 — TPM2\_ECDH\_ZGen Command..... 96

Table 52 — TPM2\_ECDH\_ZGen Response ..... 96

Table 53 — TPM2\_ECC\_Parameters Command..... 99

Table 54 — TPM2\_ECC\_Parameters Response ..... 99

Table 55 — TPM2\_ZGen\_2Phase Command..... 102

Table 56 — TPM2\_ZGen\_2Phase Response ..... 102

Table 57 — Symmetric Chaining Process ..... 105

Table 58 — TPM2\_EncryptDecrypt Command..... 107

Table 59 — TPM2\_EncryptDecrypt Response ..... 107

Table 60 — TPM2\_EncryptDecrypt2 Command..... 110

Table 61 — TPM2\_EncryptDecrypt2 Response ..... 110

Table 62 — TPM2\_Hash Command..... 113

Table 63 — TPM2\_Hash Response ..... 113

Table 64 — TPM2\_HMAC Command..... 116

Table 65 — TPM2\_HMAC Response ..... 116

Table 66 — TPM2\_GetRandom Command..... 119

Table 67 — TPM2\_GetRandom Response ..... 119

Table 68 — TPM2\_StirRandom Command ..... 122

Table 69 — TPM2\_StirRandom Response..... 122

Table 70 — Hash Selection Matrix ..... 124

Table 71 — TPM2\_HMAC\_Start Command..... 125

Table 72 — TPM2\_HMAC\_Start Response ..... 125

Table 73 — TPM2\_HashSequenceStart Command..... 128

Table 74 — TPM2\_HashSequenceStart Response ..... 128

Table 75 — TPM2\_SequenceUpdate Command ..... 131

Table 76 — TPM2\_SequenceUpdate Response..... 131

Table 77 — TPM2\_SequenceComplete Command ..... 134

Table 78 — TPM2\_SequenceComplete Response ..... 134

Table 79 — TPM2\_EventSequenceComplete Command ..... 137

Table 80 — TPM2\_EventSequenceComplete Response..... 137

Table 81 — TPM2\_Certify Command..... 142

Table 82 — TPM2\_Certify Response ..... 142

Table 83 — TPM2\_CertifyCreation Command ..... 145

Table 84 — TPM2\_CertifyCreation Response..... 145

Table 85 — TPM2\_Quote Command ..... 148

Table 86 — TPM2\_Quote Response ..... 148

Table 87 — TPM2\_GetSessionAuditDigest Command ..... 151

Table 88 — TPM2\_GetSessionAuditDigest Response ..... 151

Table 89 — TPM2\_GetCommandAuditDigest Command ..... 154

Table 90 — TPM2\_GetCommandAuditDigest Response..... 154

Table 91 — TPM2\_GetTime Command ..... 157

Table 92 — TPM2\_GetTime Response ..... 157

Table 93 — TPM2\_Commit Command..... 161

Table 94 — TPM2\_Commit Response ..... 161

Table 95 — TPM2\_EC\_Ephemeral Command..... 164

Table 96 — TPM2\_EC\_Ephemeral Response ..... 164

Table 97 — TPM2\_VerifySignature Command..... 167

Table 98 — TPM2\_VerifySignature Response ..... 167

Table 99 — TPM2\_Sign Command ..... 170

Table 100 — TPM2\_Sign Response ..... 170

Table 101 — TPM2\_SetCommandCodeAuditStatus Command ..... 174

Table 102 — TPM2\_SetCommandCodeAuditStatus Response ..... 174

Table 103 — TPM2\_PCR\_Extend Command ..... 178

Table 104 — TPM2\_PCR\_Extend Response..... 178

Table 105 — TPM2\_PCR\_Event Command ..... 181

Table 106 — TPM2\_PCR\_Event Response ..... 181

Table 107 — TPM2\_PCR\_Read Command ..... 184

Table 108 — TPM2\_PCR\_Read Response ..... 184

Table 109 — TPM2\_PCR\_Allocate Command..... 187

Table 110 — TPM2\_PCR\_Allocate Response ..... 187

Table 111 — TPM2\_PCR\_SetAuthPolicy Command ..... 190

Table 112 — TPM2\_PCR\_SetAuthPolicy Response ..... 190

Table 113 — TPM2\_PCR\_SetAuthValue Command ..... 193

Table 114 — TPM2\_PCR\_SetAuthValue Response..... 193

Table 115 — TPM2\_PCR\_Reset Command ..... 196

Table 116 — TPM2\_PCR\_Reset Response..... 196

Table 117 — TPM2\_PolicySigned Command ..... 211

Table 118 — TPM2\_PolicySigned Response..... 211

Table 119 — TPM2\_PolicySecret Command ..... 214

Table 120 — TPM2\_PolicySecret Response..... 214

Table 121 — TPM2\_PolicyTicket Command..... 217

Table 122 — TPM2\_PolicyTicket Response ..... 217

Table 123 — TPM2\_PolicyOR Command ..... 220

Table 124 — TPM2\_PolicyOR Response..... 220

Table 125 — TPM2\_PolicyPCR Command..... 224

Table 126 — TPM2\_PolicyPCR Response ..... 224

Table 127 — TPM2\_PolicyLocality Command ..... 227

Table 128 — TPM2\_PolicyLocality Response..... 227

Table 129 — TPM2\_PolicyNV Command..... 230

Table 130 — TPM2\_PolicyNV Response ..... 230

Table 131 — TPM2\_PolicyCounterTimer Command ..... 233

Table 132 — TPM2\_PolicyCounterTimer Response ..... 233

Table 133 — TPM2\_PolicyCommandCode Command ..... 236

Table 134 — TPM2\_PolicyCommandCode Response..... 236

Table 135 — TPM2\_PolicyPhysicalPresence Command..... 239

Table 136 — TPM2\_PolicyPhysicalPresence Response ..... 239

Table 137 — TPM2\_PolicyCpHash Command..... 242

Table 138 — TPM2\_PolicyCpHash Response ..... 242

Table 139 — TPM2\_PolicyNameHash Command..... 245

Table 140 — TPM2\_PolicyNameHash Response ..... 245

Table 141 — TPM2\_PolicyDuplicationSelect Command..... 248

Table 142 — TPM2\_PolicyDuplicationSelect Response ..... 248

Table 143 — TPM2\_PolicyAuthorize Command ..... 251

Table 144 — TPM2\_PolicyAuthorize Response..... 251

Table 145 — TPM2\_PolicyAuthValue Command..... 254

Table 146 — TPM2\_PolicyAuthValue Response ..... 254

Table 147 — TPM2\_PolicyPassword Command..... 257

Table 148 — TPM2\_PolicyPassword Response ..... 257

Table 149 — TPM2\_PolicyGetDigest Command..... 260

Table 150 — TPM2\_PolicyGetDigest Response ..... 260

Table 151 — TPM2\_PolicyNvWritten Command..... 263

Table 152 — TPM2\_PolicyNvWritten Response ..... 263

Table 153 — TPM2\_PolicyTemplate Command..... 266

Table 154 — TPM2\_PolicyTemplate Response ..... 266

Table 155 — TPM2\_PolicyAuthorizeNV Command ..... 269

Table 156 — TPM2\_PolicyAuthorizeNV Response..... 269

Table 157 — TPM2\_CreatePrimary Command..... 272

Table 158 — TPM2\_CreatePrimary Response ..... 272

Table 159 — TPM2\_HierarchyControl Command ..... 275

Table 160 — TPM2\_HierarchyControl Response ..... 275

Table 161 — TPM2\_SetPrimaryPolicy Command..... 278

Table 162 — TPM2\_SetPrimaryPolicy Response ..... 278

Table 163 — TPM2\_ChangePPS Command ..... 281

Table 164 — TPM2\_ChangePPS Response..... 281

Table 165 — TPM2\_ChangeEPS Command ..... 284

Table 166 — TPM2\_ChangeEPS Response..... 284

Table 167 — TPM2\_Clear Command..... 287

Table 168 — TPM2\_Clear Response ..... 287

Table 169 — TPM2\_ClearControl Command..... 290

Table 170 — TPM2\_ClearControl Response ..... 290

Table 171 — TPM2\_HierarchyChangeAuth Command..... 293

Table 172 — TPM2\_HierarchyChangeAuth Response ..... 293

Table 173 — TPM2\_DictionaryAttackLockReset Command..... 296

Table 174 — TPM2\_DictionaryAttackLockReset Response ..... 296

Table 175 — TPM2\_DictionaryAttackParameters Command ..... 299

Table 176 — TPM2\_DictionaryAttackParameters Response..... 299

Table 177 — TPM2\_PP\_Commands Command..... 302

Table 178 — TPM2\_PP\_Commands Response ..... 302

Table 179 — TPM2\_SetAlgorithmSet Command ..... 305

Table 180 — TPM2\_SetAlgorithmSet Response..... 305

Table 181 — TPM2\_FieldUpgradeStart Command..... 310

Table 182 — TPM2\_FieldUpgradeStart Response ..... 310

Table 183 — TPM2\_FieldUpgradeData Command..... 313

Table 184 — TPM2\_FieldUpgradeData Response ..... 313

Table 185 — TPM2\_FirmwareRead Command..... 316

Table 186 — TPM2\_FirmwareRead Response ..... 316

Table 187 — TPM2\_ContextSave Command..... 319

Table 188 — TPM2\_ContextSave Response ..... 319

Table 189 — TPM2\_ContextLoad Command..... 322

Table 190 — TPM2\_ContextLoad Response ..... 322

Table 191 — TPM2\_FlushContext Command..... 325

Table 192 — TPM2\_FlushContext Response ..... 325

Table 193 — TPM2\_EvictControl Command..... 329

Table 194 — TPM2\_EvictControl Response ..... 329

Table 195 — TPM2\_ReadClock Command..... 332

Table 196 — TPM2\_ReadClock Response ..... 332

Table 197 — TPM2\_ClockSet Command..... 335

Table 198 — TPM2\_ClockSet Response ..... 335

Table 199 — TPM2\_ClockRateAdjust Command..... 338

Table 200 — TPM2\_ClockRateAdjust Response ..... 338

Table 201 — TPM2\_GetCapability Command..... 344

Table 202 — TPM2\_GetCapability Response ..... 344

Table 203 — TPM2\_TestParms Command..... 347

Table 204 — TPM2\_TestParms Response ..... 347

Table 205 — TPM2\_NV\_DefineSpace Command ..... 354

Table 206 — TPM2\_NV\_DefineSpace Response ..... 354

Table 207 — TPM2\_NV\_UndefineSpace Command ..... 357

Table 208 — TPM2\_NV\_UndefineSpace Response ..... 357

Table 209 — TPM2\_NV\_UndefineSpaceSpecial Command..... 360

Table 210 — TPM2\_NV\_UndefineSpaceSpecial Response ..... 360

Table 211 — TPM2\_NV\_ReadPublic Command..... 363

Table 212 — TPM2\_NV\_ReadPublic Response ..... 363

Table 213 — TPM2\_NV\_Write Command..... 366

Table 214 — TPM2\_NV\_Write Response ..... 366

Table 215 — TPM2\_NV\_Increment Command ..... 369

Table 216 — TPM2\_NV\_Increment Response..... 369

Table 217 — TPM2\_NV\_Extend Command..... 372

Table 218 — TPM2\_NV\_Extend Response ..... 372

Table 219 — TPM2\_NV\_SetBits Command..... 375

Table 220 — TPM2\_NV\_SetBits Response ..... 375

Table 221 — TPM2\_NV\_WriteLock Command ..... 378

Table 222 — TPM2\_NV\_WriteLock Response..... 378

Table 223 — TPM2\_NV\_GlobalWriteLock Command..... 381

Table 224 — TPM2\_NV\_GlobalWriteLock Response ..... 381

Table 225 — TPM2\_NV\_Read Command..... 384

Table 226 — TPM2\_NV\_Read Response ..... 384

Table 227 — TPM2\_NV\_ReadLock Command ..... 387

Table 228 — TPM2\_NV\_ReadLock Response ..... 387

Table 229 — TPM2\_NV\_ChangeAuth Command ..... 390

Table 230 — TPM2\_NV\_ChangeAuth Response ..... 390

Table 231 — TPM2\_NV\_Certify Command..... 393

Table 232 — TPM2\_NV\_Certify Response ..... 393

Table 233 — TPM2\_Vendor\_TCG\_Test Command..... 396  
Table 234 — TPM2\_Vendor\_TCG\_Test Response ..... 396

## Trusted Platform Module Library Part 3: Commands

### 1 Scope

This TPM 2.0 Part 3 of the *Trusted Platform Module Library* specification contains the definitions of the TPM commands. These commands make use of the constants, flags, structures, and union definitions defined in TPM 2.0 Part 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 TPM 2.0 Part 3 is normative but does not fully describe the behavior of a TPM. The combination of this TPM 2.0 Part 3 and TPM 2.0 Part 4 is sufficient to fully describe the required behavior of a TPM.

The code in parts 3 and 4 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 TPM 2.0 Part 3 would be compliant.

The code in parts 3 and 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.

### 2 Terms and Definitions

For the purposes of this document, the terms and definitions given in TPM 2.0 Part 1 apply.

### 3 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in TPM 2.0 Part 1 apply.

## 4 Notation

### 4.1 Introduction

For the purposes of this document, the notation given in TPM 2.0 Part 1 applies.

Command and response tables use various decorations to indicate the fields of the command and the allowed types. These decorations are described in this clause.

### 4.2 Table Decorations

The symbols and terms in the Notation column of Table 1 are used in the tables for the command schematics. These values indicate various qualifiers for the parameters or descriptions with which they are associated.

**Table 1 — Command Modifiers and Decoration**

Notation	Meaning
+	A Type decoration – When appended to a value in the Type column of a command, this symbol indicates that the parameter is allowed to use the “null” value of the data type (see “Conditional Types” in TPM 2.0 Part 2). The null value is usually TPM_RH_NULL for a handle or TPM_ALG_NULL for an algorithm selector.
@	A Name decoration – When this symbol precedes a handle parameter in the “Name” column, it indicates that an authorization session is required for use of the entity associated with the handle. If a handle does not have this symbol, then an authorization session is not allowed.
+PP	A Description modifier – This modifier may follow TPM_RH_PLATFORM in the “Description” column to indicate that Physical Presence is required when <i>platformAuth/platformPolicy</i> is provided.
+{PP}	A Description modifier – This modifier may follow TPM_RH_PLATFORM to indicate that Physical Presence may be required when <i>platformAuth/platformPolicy</i> is provided. The commands with this notation may be in the <i>setList</i> or <i>clearList</i> of TPM2_PP_Commands().
{NV}	A Description modifier – This modifier may follow the <i>commandCode</i> in the “Description” column to indicate that the command may result in an update of NV memory and be subject to rate throttling by the TPM. If the command code does not have this notation, then a write to NV memory does not occur as part of the command actions.  NOTE Any command that uses authorization may cause a write to NV if there is an authorization failure. A TPM may use the occasion of command execution to update the NV copy of clock.
{F}	A Description modifier – This modifier indicates that the “flushed” attribute will be SET in the TPMA_CC for the command. The modifier may follow the <i>commandCode</i> in the “Description” column to indicate that any transient handle context used by the command will be flushed from the TPM when the command completes. This may be combined with the {NV} modifier but not with the {E} modifier.  EXAMPLE 1 {NV F} EXAMPLE 2 TPM2_SequenceComplete() will flush the context associated with the <i>sequenceHandle</i> .
{E}	A Description modifier – This modifier indicates that the “extensive” attribute will be SET in the TPMA_CC for the command. This modifier may follow the <i>commandCode</i> in the “Description” column to indicate that the command may flush many objects and re-enumeration of the loaded context likely will be required. This may be combined with the {NV} modifier but not with the {F} modifier.  EXAMPLE 1 {NV E} EXAMPLE 2 TPM2_Clear() will flush all contexts associated with the Storage hierarchy and the Endorsement hierarchy.



Notation	Meaning
Auth Index:	<p>A Description modifier – When a handle has a “@” decoration, the “Description” column will contain an “Auth Index:” entry for the handle. This entry indicates the number of the authorization session. The authorization sessions associated with handles will occur in the session area in the order of the handles with the “@” modifier. Sessions used only for encryption/decryption or only for audit will follow the handles used for authorization.</p>
Auth Role:	<p>A Description modifier – This will be in the “Description” column of a handle with the “@” decoration. It may have a value of USER, ADMIN or DUP.</p> <p>If the handle has the Auth Role of USER and the handle is an Object, the type of authorization is determined by the setting of <i>userWithAuth</i> in the Object's attributes. If the handle is TPM_RH_OWNER, TPM_RH_ENDORSEMENT, or TPM_RH_PLATFORM, operation is as if <i>userWithAuth</i> is SET. If the handle references an NV Index, then the allowed authorizations are determined by the settings of the attributes of the NV Index as described in TPM 2.0 Part 2, "TPMA_NV (NV Index Attributes)."</p> <p>If the Auth Role is ADMIN and the handle is an Object, the type of authorization is determined by the setting of <i>adminWithPolicy</i> in the Object's attributes. If the handle is TPM_RH_OWNER, TPM_RH_ENDORSEMENT, or TPM_RH_PLATFORM, operation is as if <i>adminWithPolicy</i> is SET. If the handle is an NV index, operation is as if <i>adminWithPolicy</i> is SET (see 5.6 e)2)).</p> <p>If the DUP role is selected, authorization may only be with a policy session (DUP role only applies to Objects).</p> <p>When either ADMIN or DUP role is selected, a policy command that selects the command being authorized is required to be part of the policy.</p> <p>EXAMPLE      TPM2_Certify requires the ADMIN role for the first handle (<i>objectHandle</i>). The policy authorization for <i>objectHandle</i> is required to contain TPM2_PolicyCommandCode(<i>commandCode</i> == TPM_CC_Certify). This sets the state of the policy so that it can be used for ADMIN role authorization in TPM2_Certify().</p>

### 4.2.1 Handle and Parameter Demarcation

The demarcations between the header, handle, and parameter parts are indicated by:

Table 2 — Separators

Separator	Meaning
#####	the values immediately following are in the handle area
=====	the values immediately following are in the parameter area

### 4.3 AuthorizationSize and ParameterSize

Authorization sessions are not shown in the command or response schematics. When the tag of a command or response is TPM\_ST\_SESSIONS, then a 32-bit value will be present in the command/response buffer to indicate the size of the authorization field or the parameter field. This value shall immediately follow the handle area (which may contain no handles). For a command, this value (*authorizationSize*) indicates the size of the Authorization Area and shall have a value of 9 or more. For a response, this value (*parameterSize*) indicates the size of the parameter area and may have a value of zero.

If the *authorizationSize* field is present in the command, *parameterSize* will be present in the response, but only if the *responseCode* is TPM\_RC\_SUCCESS.

When authorization is required to use the TPM entity associated with a handle, then at least one session will be present. To indicate this, the command *tag Description* field contains TPM\_ST\_SESSIONS. Additional sessions for audit, encrypt, and decrypt may be present.

When the command *tag Description* field contains TPM\_ST\_NO\_SESSIONS, then no sessions are allowed and the *authorizationSize* field is not present.

When a command allows use of sessions when not required, the command *tag Description* field will indicate the types of sessions that may be used with the command.

### 4.4 Return Code Alias

For the RC\_FMT1 return codes that may add a parameter, handle, or session number, the prefix TPM\_RCS\_ is an alias for TPM\_RC\_.

TPM\_RC\_n is added, where n is the parameter, handle, or session number. In addition, TPM\_RC\_H is added for handle, TPM\_RC\_P for parameter, and TPM\_RC\_S for session errors.

**NOTE** TPM\_RCS\_ is a programming convention. Programmers should only add numbers to TPM\_RCS\_ return codes, never TPM\_RC\_ return codes. Only return codes that can have a number added have the TPM\_RCS\_ alias defined. Attempting to use a TPM\_RCS\_ return code that does not have the TPM\_RCS\_ alias will cause a compiler error.

**EXAMPLE 1** Since TPM\_RC\_VALUE can have a number added, TPM\_RCS\_VALUE is defined. A program can use the construct "TPM\_RCS\_VALUE + number". Since TPM\_RC\_SIGNATURE cannot have a number added, TPM\_RCS\_SIGNATURE is not defined. A program using the construct "TPM\_RCS\_SIGNATURE + number" will not compile, alerting the programmer that the construct is incorrect.

By convention, the number to be added is of the form RC\_CommandName\_ParameterName where CommandName is the name of the command with the TPM2\_ prefix removed. The parameter name alone is insufficient because the same parameter name could be in a different position in different commands.

EXAMPLE 2 TPM2\_HMAC\_Start with parameters that result in TPM\_ALG\_NULL as the hash algorithm will return TPM\_RC\_VALUE plus the parameter number. Since *hashAlg* is the second parameter, This code results:

```
#define RC_HMAC_Start_hashAlg      (TPM_RC_P + TPM_RC_2)

return TPM_RCS_VALUE + RC_HMAC_Start_hashAlg;
```

## 5 Command Processing

### 5.1 Introduction

This clause defines the command validations that are required of any implementation and the response code returned if the indicated check fails. Unless stated otherwise, the order of the checks is not normative and different TPM may give different responses when a command has multiple errors.

In the description below, some statements that describe a check may be followed by a response code in parentheses. This is the normative response code should the indicated check fail. A normative response code may also be included in the statement.

### 5.2 Command Header Validation

Before a TPM may begin the actions associated with a command, a set of command format and consistency checks shall be performed. These checks are listed below and should be performed in the indicated order.

- a) The TPM shall successfully unmarshal a TPMI\_ST\_COMMAND\_TAG and verify that it is either TPM\_ST\_SESSIONS or TPM\_ST\_NO\_SESSIONS (TPM\_RC\_BAD\_TAG).
- b) The TPM shall successfully unmarshal a UINT32 as the *commandSize*. If the TPM has an interface buffer that is loaded by some hardware process, the number of octets in the input buffer for the command reported by the hardware process shall exactly match the value in *commandSize* (TPM\_RC\_COMMAND\_SIZE).

NOTE A TPM may have direct access to system memory and unmarshal directly from that memory.

- c) The TPM shall successfully unmarshal a TPM\_CC and verify that the command is implemented (TPM\_RC\_COMMAND\_CODE).

### 5.3 Mode Checks

The following mode checks shall be performed in the order listed:

- a) If the TPM is in Failure mode, then the *commandCode* is TPM\_CC\_GetTestResult or TPM\_CC\_GetCapability (TPM\_RC\_FAILURE) and the command *tag* is TPM\_ST\_NO\_SESSIONS (TPM\_RC\_FAILURE).

NOTE 1 In Failure mode, the TPM has no cryptographic capability and processing of sessions is not supported.

- b) The TPM is in Field Upgrade mode (FUM), the *commandCode* is TPM\_CC\_FieldUpgradeData (TPM\_RC\_UPGRADE).
- c) If the TPM has not been initialized (TPM2\_Startup()), then the *commandCode* is TPM\_CC\_Startup (TPM\_RC\_INITIALIZE).

NOTE 2 The TPM may enter Failure mode during *\_TPM\_Init* processing, before TPM2\_Startup(). Since the platform firmware cannot know that the TPM is in Failure mode without accessing it, and since the first command is required to be TPM2\_Startup(), the expected sequence will be that

platform firmware (the CRTM) will issue TPM2\_Startup() and receive TPM\_RC\_FAILURE indicating that the TPM is in Failure mode.

There may be failures where a TPM cannot record that it received TPM2\_Startup(). In those cases, a TPM in failure mode may process TPM2\_GetTestResult(), TPM2\_GetCapability(), or the field upgrade commands. As a side effect, that TPM may process TPM2\_GetTestResult(), TPM2\_GetCapability() or the field upgrade commands before TPM2\_Startup().

This is a corner case exception to the rule that TPM2\_Startup() must be the first command.

The mode checks may be performed before or after the command header validation.

#### 5.4 Handle Area Validation

After successfully unmarshaling and validating the command header, the TPM shall perform the following checks on the handles and sessions. These checks may be performed in any order.

NOTE 1 A TPM is required to perform the handle area validation before the authorization checks because an authorization cannot be performed unless the authorization values and attributes for the referenced entity are known by the TPM. For them to be known, the referenced entity must be in the TPM and accessible.

- a) The TPM shall successfully unmarshal the number of handles required by the command and validate that the value of the handle is consistent with the command syntax. If not, the TPM shall return TPM\_RC\_VALUE.

NOTE 2 The TPM may unmarshal a handle and validate that it references an entity on the TPM before unmarshaling a subsequent handle.

NOTE 3 If the submitted command contains fewer handles than required by the syntax of the command, the TPM may continue to read into the next area and attempt to interpret the data as a handle.

- b) For all handles in the handle area of the command, the TPM will validate that the referenced entity is present in the TPM.

- 1) If the handle references a transient object, the handle shall reference a loaded object (TPM\_RC\_REFERENCE\_H0 + N where N is the number of the handle in the command).

NOTE 4 If the hierarchy for a transient object is disabled, then the transient objects will be flushed so this check will fail.

- 2) If the handle references a persistent object, then

- i) the hierarchy associated with the object (platform or storage, based on the handle value) is enabled (TPM\_RC\_HANDLE);
- ii) the handle shall reference a persistent object that is currently in TPM non-volatile memory (TPM\_RC\_HANDLE);
- iii) if the handle references a persistent object that is associated with the endorsement hierarchy, that the endorsement hierarchy is not disabled (TPM\_RC\_HANDLE); and

NOTE 5 The reference implementation keeps an internal attribute, passed down from a primary key to its descendents, indicating the object's hierarchy.

- iv) if the TPM implementation moves a persistent object to RAM for command processing then sufficient RAM space is available (TPM\_RC\_OBJECT\_MEMORY).

- 3) If the handle references an NV Index, then

- i) an Index exists that corresponds to the handle (TPM\_RC\_HANDLE); and
- ii) the hierarchy associated with the existing NV Index is not disabled (TPM\_RC\_HANDLE).

- iii) If the command requires write access to the index data then `TPMA_NV_WRITELOCKED` is not SET (`TPM_RC_LOCKED`)
- iv) If the command requires read access to the index data then `TPMA_NV_READLOCKED` is not SET (`TPM_RC_LOCKED`)
- 4) If the handle references a session, then the session context shall be present in TPM memory (`TPM_RC_REFERENCE_H0 + N`).
- 5) If the handle references a primary seed for a hierarchy (`TPM_RH_ENDORSEMENT`, `TPM_RH_OWNER`, or `TPM_RH_PLATFORM`) then the enable for the hierarchy is SET (`TPM_RC_HIERARCHY`).
- 6) If the handle references a PCR, then the value is within the range of PCR supported by the TPM (`TPM_RC_VALUE`)

NOTE 6 In the reference implementation, this `TPM_RC_VALUE` is returned by the unmarshaling code for a `TPMI_DH_PCR`.

### 5.5 Session Area Validation

- a) If the tag is `TPM_ST_SESSIONS` and the command requires `TPM_ST_NO_SESSIONS`, the TPM will return `TPM_RC_AUTH_CONTEXT`.
- b) If the tag is `TPM_ST_NO_SESSIONS` and the command requires `TPM_ST_SESSIONS`, the TPM will return `TPM_RC_AUTH_MISSING`.
- c) If the tag is `TPM_ST_SESSIONS`, the TPM will attempt to unmarshal an *authorizationSize* and return `TPM_RC_AUTHSIZE` if the value is not within an acceptable range.
  - 1) The minimum value is  $(\text{sizeof}(\text{TPM\_HANDLE}) + \text{sizeof}(\text{UINT16}) + \text{sizeof}(\text{TPMA\_SESSION}) + \text{sizeof}(\text{UINT16}))$ .
  - 2) The maximum value of *authorizationSize* is equal to  $\text{commandSize} - (\text{sizeof}(\text{TPM\_ST}) + \text{sizeof}(\text{UINT32}) + \text{sizeof}(\text{TPM\_CC}) + (N * \text{sizeof}(\text{TPM\_HANDLE})) + \text{sizeof}(\text{UINT32}))$  where N is the number of handles associated with the *commandCode* and may be zero.

NOTE 1  $(\text{sizeof}(\text{TPM\_ST}) + \text{sizeof}(\text{UINT32}) + \text{sizeof}(\text{TPM\_CC}))$  is the size of a command header. The last `UINT32` contains the *authorizationSize* octets, which are not counted as being in the authorization session area.

- d) The TPM will unmarshal the authorization sessions and perform the following validations:
  - 1) If the session handle is not a handle for an HMAC session, a handle for a policy session, or, `TPM_RS_PW` then the TPM shall return `TPM_RC_HANDLE`.
  - 2) If the session is not loaded, the TPM will return the warning `TPM_RC_REFERENCE_S0 + N` where N is the number of the session. The first session is session zero,  $N = 0$ .

NOTE 2 If the HMAC and policy session contexts use the same memory, the type of the context must match the type of the handle.

- 3) If the maximum allowed number of sessions have been unmarshaled and fewer octets than indicated in *authorizationSize* were unmarshaled (that is, *authorizationSize* is too large), the TPM shall return `TPM_RC_AUTHSIZE`.
- 4) The consistency of the authorization session attributes is checked.
  - i) Only one session is allowed for:
    - (a) session auditing (`TPM_RC_ATTRIBUTES`) – this session may be used for encrypt or decrypt but may not be a session that is also used for authorization;

- (b) decrypting a command parameter (TPM\_RC\_ATTRIBUTES) – this may be any of the authorization sessions, or the audit session, or a session may be added for the single purpose of decrypting a command parameter, as long as the total number of sessions does not exceed three; and
- (c) encrypting a response parameter (TPM\_RC\_ATTRIBUTES) – this may be any of the authorization sessions, or the audit session if present, or a session may be added for the single purpose of encrypting a response parameter, as long as the total number of sessions does not exceed three.

NOTE 3            A session used for decrypting a command parameter may also be used for encrypting a response parameter.

- ii) If a session is not being used for authorization, at least one of decrypt, encrypt, or audit must be SET. (TPM\_RC\_ATTRIBUTES).
- 5) An authorization session is present for each of the handles with the “@” decoration (TPM\_RC\_AUTH\_MISSING).

## 5.6 Authorization Checks

After unmarshaling and validating the handles and the consistency of the authorization sessions, the authorizations shall be checked. Authorization checks only apply to handles if the handle in the command schematic has the “@” decoration. Authorization checks must be performed in this order.

- a) The public and sensitive portions of the object shall be present on the TPM (TPM\_RC\_AUTH\_UNAVAILABLE).
- b) If the associated handle is TPM\_RH\_PLATFORM, and the command requires confirmation with physical presence, then physical presence is asserted (TPM\_RC\_PP).
- c) If the object or NV Index is subject to DA protection, and the authorization is with an HMAC or password, then the TPM is not in lockout (TPM\_RC\_LOCKOUT).

NOTE 1            An object is subject to DA protection if its *noDA* attribute is CLEAR. An NV Index is subject to DA protection if its *TPMA\_NV\_NO\_DA* attribute is CLEAR.

NOTE 2            An HMAC or password is required in a policy session when the policy contains *TPM2\_PolicyAuthValue()* or *TPM2\_PolicyPassword()*.

- d) If the command requires a handle to have DUP role authorization, then the associated authorization session is a policy session (TPM\_RC\_AUTH\_TYPE).
- e) If the command requires a handle to have ADMIN role authorization:
  - 1) If the entity being authorized is an object and its *adminWithPolicy* attribute is SET, or a hierarchy, then the authorization session is a policy session (TPM\_RC\_AUTH\_TYPE).

NOTE 3            If *adminWithPolicy* is CLEAR, then any type of authorization session is allowed.

- 2) If the entity being authorized is an NV Index, then the associated authorization session is a policy session.

NOTE 4            The only commands that are currently defined that require use of ADMIN role authorization are commands that operate on objects and NV Indices.

- f) If the command requires a handle to have USER role authorization:
  - 1) If the entity being authorized is an object and its *userWithAuth* attribute is CLEAR, then the associated authorization session is a policy session (TPM\_RC\_POLICY\_FAIL).

NOTE 5            There is no check for a hierarchy, because a hierarchy operates as if *userWithAuth* is SET.

- 2) If the entity being authorized is an NV Index;
  - i) if the authorization session is a policy session;
    - (a) the TPMA\_NV\_POLICYWRITE attribute of the NV Index is SET if the command modifies the NV Index data (TPM\_RC\_AUTH\_UNAVAILABLE);
    - (b) the TPMA\_NV\_POLICYREAD attribute of the NV Index is SET if the command reads the NV Index data (TPM\_RC\_AUTH\_UNAVAILABLE);
  - ii) if the authorization is an HMAC session or a password;
    - (a) the TPMA\_NV\_AUTHWRITE attribute of the NV Index is SET if the command modifies the NV Index data (TPM\_RC\_AUTH\_UNAVAILABLE);
    - (b) the TPMA\_NV\_AUTHREAD attribute of the NV Index is SET if the command reads the NV Index data (TPM\_RC\_AUTH\_UNAVAILABLE).
- g) If the authorization is provided by a policy session, then:
  - 1) if *policySession→timeOut* has been set, the session shall not have expired (TPM\_RC\_EXPIRED);
  - 2) if *policySession→cpHash* has been set, it shall match the *cpHash* of the command (TPM\_RC\_POLICY\_FAIL);
  - 3) if *policySession→commandCode* has been set, then *commandCode* of the command shall match (TPM\_RC\_POLICY\_CC);
  - 4) *policySession→policyDigest* shall match the *authPolicy* associated with the handle (TPM\_RC\_POLICY\_FAIL);
  - 5) if *policySession→pcrUpdateCounter* has been set, then it shall match the value of *pcrUpdateCounter* (TPM\_RC\_PCR\_CHANGED);
  - 6) if *policySession→commandLocality* has been set, it shall match the locality of the command (TPM\_RC\_LOCALITY),
  - 7) if *policySession→cpHash* contains a template, and the command is TPM2\_Create(), TPM2\_CreatePrimary(), or TPM2\_CreateLoaded(), then the *inPublic* parameter matches the contents of *policySession→cpHash*; and
  - 8) if the policy requires that an *authValue* be provided in order to satisfy the policy, then *session.hmac* is not an Empty Buffer.
- h) If the authorization uses an HMAC, then the HMAC is properly constructed using the *authValue* associated with the handle and/or the session secret (TPM\_RC\_AUTH\_FAIL or TPM\_RC\_BAD\_AUTH).

NOTE 6            A policy session may require proof of knowledge of the *authValue* of the object being authorized.

- i) If the authorization uses a password, then the password matches the *authValue* associated with the handle (TPM\_RC\_AUTH\_FAIL or TPM\_RC\_BAD\_AUTH).

If the TPM returns an error other than TPM\_RC\_AUTH\_FAIL then the TPM shall not alter any TPM state. If the TPM return TPM\_RC\_AUTH\_FAIL, then the TPM shall not alter any TPM state other than *lockoutCount*.

NOTE 7            The TPM may decrease failedTries regardless of any other processing performed by the TPM. That is, the TPM may exit Lockout mode, regardless of the return code.

## 5.7 Parameter Decryption

If an authorization session has the TPMA\_SESSION.*decrypt* attribute SET, and the command does not allow a command parameter to be encrypted, then the TPM will return TPM\_RC\_ATTRIBUTES. Otherwise, the TPM will decrypt the parameter using the values associated with the session before parsing parameters.

NOTE                   The size of the parameter to be encrypted can be zero.

## 5.8 Parameter Unmarshaling

### 5.8.1 Introduction

The detailed actions for each command assume that the input parameters of the command have been unmarshaled into a command-specific structure with the structure defined by the command schematic. Additionally, a response-specific output structure is assumed which will receive the values produced by the detailed actions.

NOTE                   An implementation is not required to process parameters in this manner or to separate the parameter parsing from the command actions. This method was chosen for the specification so that the normative behavior described by the detailed actions would be clear and unencumbered.

Unmarshaling is the process of processing the parameters in the input buffer and preparing the parameters for use by the command-specific action code. No data movement need take place but it is required that the TPM validate that the parameters meet the requirements of the expected data type as defined in TPM 2.0 Part 2.



## 5.8.2 Unmarshaling Errors

When an error is encountered while unmarshaling a command parameter, an error response code is returned and no command processing occurs. A table defining a data type may have response codes embedded in the table to indicate the error returned when the input value does not match the parameters of the table.

NOTE In the reference implementation, a parameter number is added to the response code so that the offending parameter can be isolated. This is optional.

In many cases, the table contains no specific response code value and the return code will be determined as defined in Table 3.

**Table 3 — Unmarshaling Errors**

Response Code	Meaning
TPM_RC_ASYMMETRIC	a parameter that should be an asymmetric algorithm selection does not have a value that is supported by the TPM
TPM_RC_BAD_TAG	a parameter that should be a command tag selection has a value that is not supported by the TPM
TPM_RC_COMMAND_CODE	a parameter that should be a command code does not have a value that is supported by the TPM
TPM_RC_HASH	a parameter that should be a hash algorithm selection does not have a value that is supported by the TPM
TPM_RC_INSUFFICIENT	the input buffer did not contain enough octets to allow unmarshaling of the expected data type;
TPM_RC_KDF	a parameter that should be a key derivation scheme (KDF) selection does not have a value that is supported by the TPM
TPM_RC_KEY_SIZE	a parameter that is a key size has a value that is not supported by the TPM
TPM_RC_MODE	a parameter that should be a symmetric encryption mode selection does not have a value that is supported by the TPM
TPM_RC_RESERVED	a non-zero value was found in a reserved field of an attribute structure (TPMA_)
TPM_RC_SCHEME	a parameter that should be signing or encryption scheme selection does not have a value that is supported by the TPM
TPM_RC_SIZE	the value of a size parameter is larger or smaller than allowed
TPM_RC_SYMMETRIC	a parameter that should be a symmetric algorithm selection does not have a value that is supported by the TPM
TPM_RC_TAG	a parameter that should be a structure tag has a value that is not supported by the TPM
TPM_RC_TYPE	The type parameter of a TPMT_PUBLIC or TPMT_SENSITIVE has a value that is not supported by the TPM
TPM_RC_VALUE	a parameter does not have one of its allowed values

In some commands, a parameter may not be used because of various options of that command. However, the unmarshaling code is required to validate that all parameters have values that are allowed by the TPM 2.0 Part 2 definition of the parameter type even if that parameter is not used in the command actions.

## 5.9 Command Post Processing

When the code that implements the detailed actions of the command completes, it returns a response code. If that code is not TPM\_RC\_SUCCESS, the post processing code will not update any session or audit data and will return a 10-octet response packet.

If the command completes successfully, the tag of the command determines if any authorization sessions will be in the response. If so, the TPM will encrypt the first parameter of the response if indicated by the authorization attributes. The TPM will then generate a new nonce value for each session and, if appropriate, generate an HMAC.

If authorization HMAC computations are performed on the response, the HMAC keys used in the response will be the same as the HMAC keys used in processing the HMAC in the command.

NOTE 1 This primarily affects authorizations associated with a first write to an NV Index using a bound session. The computation of the HMAC in the response is performed as if the Name of the Index did not change as a consequence of the command actions. The session binding to the NV Index will not persist to any subsequent command.

NOTE 2 The authorization attributes were validated during the session area validation to ensure that only one session was used for parameter encryption of the response and that the command allowed encryption in the response.

NOTE 3 No session nonce value is used for a password authorization but the session data is present.

Additionally, if the command is being audited by Command Audit, the audit digest is updated with the *cpHash* of the command and *rpHash* of the response.

## 6 Response Values

### 6.1 Tag

When a command completes successfully, the *tag* parameter in the response shall have the same value as the *tag* parameter in the command (TPM\_ST\_SESSIONS or TPM\_ST\_NO\_SESSIONS). When a command fails (the *responseCode* is not TPM\_RC\_SUCCESS), then the *tag* parameter in the response shall be TPM\_ST\_NO\_SESSIONS.

A special case exists when the command *tag* parameter is not an allowed value (TPM\_ST\_SESSIONS or TPM\_ST\_NO\_SESSIONS). For this case, it is assumed that the system software is attempting to send a command formatted for a TPM 1.2 but the TPM is not capable of executing TPM 1.2 commands. So that the TPM 1.2 compatible software will have a recognizable response, the TPM sets *tag* to TPM\_ST\_RSP\_COMMAND, *responseSize* to 00 00 00 0A<sub>16</sub> and *responseCode* to TPM\_RC\_BAD\_TAG. This is the same response as the TPM 1.2 fatal error for TPM\_BADTAG.

### 6.2 Response Codes

The normal response for any command is TPM\_RC\_SUCCESS. Any other value indicates that the command did not complete and the state of the TPM is unchanged. An exception to this general rule is that the logic associated with dictionary attack protection is allowed to be modified when an authorization failure occurs.

Commands have response codes that are specific to that command, and those response codes are enumerated in the detailed actions of each command. The codes associated with the unmarshaling of parameters are documented Table 3. Another set of response code values are not command specific and indicate a problem that is not specific to the command. That is, if the indicated problem is remedied, the same command could be resubmitted and may complete normally.

The response codes that are not command specific are listed and described in

Table 4.

The reference code for the command actions may have code that generates specific response codes associated with a specific check but the listing of responses may not have that response code listed.

Table 4 — Command-Independent Response Codes

Response Code	Meaning
TPM_RC_CANCELED	This response code may be returned by a TPM that supports command cancel. When the TPM receives an indication that the current command should be cancelled, the TPM may complete the command or return this code. If this code is returned, then the TPM state is not changed and the same command may be retried.
TPM_RC_CONTEXT_GAP	This response code can be returned for commands that manage session contexts. It indicates that the gap between the lowest numbered active session and the highest numbered session is at the limits of the session tracking logic. The remedy is to load the session context with the lowest number so that its tracking number can be updated.
TPM_RC_LOCKOUT	This response indicates that authorizations for objects subject to DA protection are not allowed at this time because the TPM is in DA lockout mode. The remedy is to wait or to execute TPM2_DictionaryAttackLockoutReset().
TPM_RC_MEMORY	A TPM may use a common pool of memory for objects, sessions, and other purposes. When the TPM does not have enough memory available to perform the actions of the command, it may return TPM_RC_MEMORY. This indicates that the TPM resource manager may flush either sessions or objects in order to make memory available for the command execution. A TPM may choose to return TPM_RC_OBJECT_MEMORY or TPM_RC_SESSION_MEMORY if it needs contexts of a particular type to be flushed.
TPM_RC_NV_RATE	This response code indicates that the TPM is rate-limiting writes to the NV memory in order to prevent wearout. This response is possible for any command that explicitly writes to NV or commands that incidentally use NV such as a command that uses authorization session that may need to update the dictionary attack logic.
TPM_RC_NV_UNAVAILABLE	This response code is similar to TPM_RC_NV_RATE but indicates that access to NV memory is currently not available and the command is not allowed to proceed until it is. This would occur in a system where the NV memory used by the TPM is not exclusive to the TPM and is a shared system resource.
TPM_RC_OBJECT_HANDLES	This response code indicates that the TPM has exhausted its handle space and no new objects can be loaded unless the TPM is rebooted. This does not occur in the reference implementation because of the way that object handles are allocated. However, other implementations are allowed to assign each object a unique handle each time the object is loaded. A TPM using this implementation would be able to load $2^{24}$ objects before the object space is exhausted.
TPM_RC_OBJECT_MEMORY	This response code can be returned by any command that causes the TPM to need an object 'slot'. The most common case where this might be returned is when an object is loaded (TPM2_Load, TPM2_CreatePrimary(), or TPM2_ContextLoad()). However, the TPM implementation is allowed to use object slots for other reasons. In the reference implementation, the TPM copies a referenced persistent object into RAM for the duration of the command. If all the slots are previously occupied, the TPM may return this value. A TPM is allowed to use object slots for other purposes and return this value. The remedy when this response is returned is for the TPM resource manager to flush a transient object.
TPM_RC_REFERENCE_Hx	This response code indicates that a handle in the handle area of the command is not associated with a loaded object. The value of 'x' is in the range 0 to 6 with a value of 0 indicating the 1 <sup>st</sup> handle and 6 representing the 7 <sup>th</sup> . Upper values are provided for future use. The TPM resource manager needs to find the correct object and load it. It may then adjust the handle and retry the command. NOTE Usually, this error indicates that the TPM resource manager has a corrupted database.

Response Code	Meaning
TPM_RC_REFERENCE_Sx	This response code indicates that a handle in the session area of the command is not associated with a loaded session. The value of 'x' is in the range 0 to 6 with a value of 0 indicating the 1 <sup>st</sup> session handle and 6 representing the 7 <sup>th</sup> . Upper values are provided for future use. The TPM resource manager needs to find the correct session and load it. It may then retry the command. NOTE Usually, this error indicates that the TPM resource manager has a corrupted database.
TPM_RC_RETRY	the TPM was not able to start the command
TPM_RC_SESSION_HANDLES	This response code indicates that the TPM does not have a handle to assign to a new session. This response is only returned by TPM2_StartAuthSession(). It is listed here because the command is not in error and the TPM resource manager can remedy the situation by flushing a session (TPM2_FlushContext()).
TPM_RC_SESSION_MEMORY	This response code can be returned by any command that causes the TPM to need a session 'slot'. The most common case where this might be returned is when a session is loaded (TPM2_StartAuthSession() or TPM2_ContextLoad()). However, the TPM implementation is allowed to use object slots for other purposes. The remedy when this response is returned is for the TPM resource manager to flush a transient object.
TPM_RC_SUCCESS	Normal completion for any command. If the responseCode is TPM_RC_SUCCESS, then the rest of the response has the format indicated in the response schematic. Otherwise, the response is a 10 octet value indicating an error.
TPM_RC_TESTING	This response code indicates that the TPM is performing tests and cannot respond to the request at this time. The command may be retried.
TPM_RC_YIELDED	the TPM has suspended operation on the command; forward progress was made and the command may be retried. See TPM 2.0 Part 1, "Multi-tasking." NOTE This cannot occur on the reference implementation.

## 7 Implementation Dependent

The actions code for each command makes assumptions about the behavior of various sub-systems. There are many possible implementations of the subsystems that would achieve equivalent results. The actions code is not written to anticipate all possible implementations of the sub-systems. Therefore, it is the responsibility of the implementer to ensure that the necessary changes are made to the actions code when the sub-system behavior changes.

## 8 Detailed Actions Assumptions

### 8.1 Introduction

The C code in the Detailed Actions for each command is written with a set of assumptions about the processing performed before the action code is called and the processing that will be done after the action code completes.

### 8.2 Pre-processing

Before calling the command actions code, the following actions have occurred.

- Verification that the handles in the handle area reference entities that are resident on the TPM.
- **NOTE** If a handle is in the parameter portion of the command, the associated entity does not have to be loaded, but the handle is required to be the correct type.
- If use of a handle requires authorization, the Password, HMAC, or Policy session associated with the handle has been verified.
- If a command parameter was encrypted using parameter encryption, it was decrypted before being unmarshaled.
- If the command uses handles or parameters, the calling stack contains a pointer to a data structure (*in*) that holds the unmarshaled values for the handles and command parameters. If the response has handles or parameters, the calling stack contains a pointer to a data structure (*out*) to hold the handles and response parameters generated by the command.
- All parameters of the *in* structure have been validated and meet the requirements of the parameter type as defined in TPM 2.0 Part 2.
- Space set aside for the out structure is sufficient to hold the largest *out* structure that could be produced by the command

### 8.3 Post Processing

When the function implementing the command actions completes,

- response parameters that require parameter encryption will be encrypted after the command actions complete;
- audit and session contexts will be updated if the command response is TPM\_RC\_SUCCESS; and
- the command header and command response parameters will be marshaled to the response buffer.

## 9 Start-up

### 9.1 Introduction

This clause contains the commands used to manage the startup and restart state of a TPM.

### 9.2 `_TPM_Init`

#### 9.2.1 General Description

`_TPM_Init` initializes a TPM.

Initialization actions include testing code required to execute the next expected command. If the TPM is in FUM, the next expected command is `TPM2_FieldUpgradeData()`; otherwise, the next expected command is `TPM2_Startup()`.

NOTE 1 If the TPM performs self-tests after receiving `_TPM_Init()` and the TPM enters Failure mode before receiving `TPM2_Startup()` or `TPM2_FieldUpgradeData()`, then the TPM may be able to accept `TPM2_GetTestResult()` or `TPM2_GetCapability()`.

The means of signaling `_TPM_Init` shall be defined in the platform-specific specifications that define the physical interface to the TPM. The platform shall send this indication whenever the platform starts its boot process and only when the platform starts its boot process.

There shall be no software method of generating this indication that does not also reset the platform and begin execution of the CRTM.

NOTE 2 In the reference implementation, this signal causes an internal flag (*s\_initialized*) to be CLEAR. While this flag is CLEAR, the TPM will only accept the next expected command described above.



## 9.2.2 Detailed Actions

`[[ TPM Init]]`

### 9.3 TPM2\_Startup

#### 9.3.1 General Description

TPM2\_Startup() is always preceded by \_TPM\_Init, which is the physical indication that TPM initialization is necessary because of a system-wide reset. TPM2\_Startup() is only valid after \_TPM\_Init. Additional TPM2\_Startup() commands are not allowed after it has completed successfully. If a TPM requires TPM2\_Startup() and another command is received, or if the TPM receives TPM2\_Startup() when it is not required, the TPM shall return TPM\_RC\_INITIALIZE.

NOTE 1 See 9.2.1 for other command options for a TPM supporting field upgrade mode.

NOTE 2 \_TPM\_Hash\_Start, \_TPM\_Hash\_Data, and \_TPM\_Hash\_End are not commands and a platform-specific specification may allow these indications between \_TPM\_Init and TPM2\_Startup().

If in Failure mode, the TPM shall accept TPM2\_GetTestResult() and TPM2\_GetCapability() even if TPM2\_Startup() is not completed successfully or processed at all.

A platform-specific specification may restrict the localities at which TPM2\_Startup() may be received.

A Shutdown/Startup sequence determines the way in which the TPM will operate in response to TPM2\_Startup(). The three sequences are:

- 1) TPM Reset – This is a Startup(CLEAR) preceded by either Shutdown(CLEAR) or no TPM2\_Shutdown(). On TPM Reset, all variables go back to their default initialization state.

NOTE 3 Only those values that are specified as having a default initialization state are changed by TPM Reset. Persistent values that have no default initialization state are not changed by this command. Values such as seeds have no default initialization state and only change due to specific commands.

- 2) TPM Restart – This is a Startup(CLEAR) preceded by Shutdown(STATE). This preserves much of the previous state of the TPM except that PCR and the controls associated with the Platform hierarchy are all returned to their default initialization state;
- 3) TPM Resume – This is a Startup(STATE) preceded by Shutdown(STATE). This preserves the previous state of the TPM including the static Root of Trust for Measurement (S-RTM) PCR and the platform controls other than the *phEnable*.

If a TPM receives Startup(STATE) and that was not preceded by Shutdown(STATE), the TPM shall return TPM\_RC\_VALUE.

If, during TPM Restart or TPM Resume, the TPM fails to restore the state saved at the last Shutdown(STATE), the TPM shall enter Failure Mode and return TPM\_RC\_FAILURE.

On any TPM2\_Startup(),

- *phEnable* shall be SET;
- all transient contexts (objects, sessions, and sequences) shall be flushed from TPM memory;
- TPMS\_TIME\_INFO.*time* shall be reset to zero; and

NOTE 4 If time is reset to zero at \_TPM\_Init, it need not be reset again here.

- use of *lockoutAuth* shall be enabled if *lockoutRecovery* is zero.

Additional actions are performed based on the Shutdown/Startup sequence.

On TPM Reset

- *platformAuth* and *platformPolicy* shall be set to the Empty Buffer,
- For each NV index with TPMA\_NV\_WRITE\_DEFINE CLEAR or TPMA\_NV\_WRITTEN CLEAR, TPMA\_NV\_WRITELOCKED shall be CLEAR,
- For each NV index with TPMA\_NV\_CLEAR\_STCLEAR SET, TPMA\_NV\_WRITTEN shall be CLEAR,
- tracking data for saved session contexts shall be set to its initial value,
- the object context sequence number is reset to zero,
- a new context encryption key shall be generated,
- TPMS\_CLOCK\_INFO.*restartCount* shall be reset to zero,
- TPMS\_CLOCK\_INFO.*resetCount* shall be incremented,
- the PCR Update Counter shall be clear to zero,

NOTE 5 Because the PCR update counter may be incremented when a PCR is reset, the PCR resets performed as part of this command can result in the PCR update counter being non-zero at the end of this command.

- *phEnableNV*, *shEnable* and *ehEnable* shall be SET, and
- PCR in all banks are reset to their default initial conditions as determined by the relevant platform-specific specification and the H-CRTM state (for exceptions, see TPM 2.0 Part 1, *H-CRTM before TPM2\_Startup()* and *TPM2\_Startup without H-CRTM*)

NOTE 6 PCR may be initialized any time between *\_TPM\_Init* and the end of *TPM2\_Startup()*. PCR that are preserved by TPM Resume will need to be restored during *TPM2\_Startup()*.

NOTE 7 See "Initializing PCR" in TPM 2.0 Part 1 for a description of the default initial conditions for a PCR.

#### On TPM Restart

- TPMS\_CLOCK\_INFO.*restartCount* shall be incremented,
- *phEnableNV*, *shEnable* and *ehEnable* shall be SET,
- *platformAuth* and *platformPolicy* shall be set to the Empty Buffer,
- For each NV index with TPMA\_NV\_WRITE\_DEFINE CLEAR or TPMA\_NV\_WRITTEN CLEAR, TPMA\_NV\_WRITELOCKED shall be CLEAR,
- For each NV index with TPMA\_NV\_CLEAR\_STCLEAR SET, TPMA\_NV\_WRITTEN shall be CLEAR, and
- PCR in all banks are reset to their default initial conditions.
- If an H-CRTM Event Sequence is active, extend the PCR designated by the platform-specific specification.

#### On TPM Resume

- the H-CRTM startup method is the same for this *TPM2\_Startup()* as for the previous *TPM2\_Startup()*; (*TPM\_RC\_LOCALITY*)
- TPMS\_CLOCK\_INFO.*restartCount* shall be incremented; and
- PCR that are specified in a platform-specific specification to be preserved on TPM Resume are restored to their saved state and other PCR are set to their initial value as determined by a platform-specific specification. For constraints, see TPM 2.0 Part 1, *H-CRTM before TPM2\_Startup()* and *TPM2\_Startup without H-CRTM*.

Other TPM state may change as required to meet the needs of the implementation.

If the *startupType* is TPM\_SU\_STATE and the TPM requires TPM\_SU\_CLEAR, then the TPM shall return TPM\_RC\_VALUE.

NOTE 8           The TPM will require TPM\_SU\_CLEAR when no shutdown was performed or after Shutdown(CLEAR).

NOTE 9           If *startupType* is neither TPM\_SU\_STATE nor TPM\_SU\_CLEAR, then the unmarshaling code returns TPM\_RC\_VALUE.

## 9.3.2 Command and Response

Table 5 — TPM2\_Startup Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Startup {NV}
TPM_SU	startupType	TPM_SU_CLEAR or TPM_SU_STATE

Table 6 — TPM2\_Startup Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 9.3.3 Detailed Actions

**[[Startup]]**

## 9.4 TPM2\_Shutdown

### 9.4.1 General Description

This command is used to prepare the TPM for a power cycle. The *shutdownType* parameter indicates how the subsequent TPM2\_Startup() will be processed.

For a *shutdownType* of any type, the volatile portion of Clock is saved to NV memory and the orderly shutdown indication is SET. NV Indexes with the TPMA\_NV\_ORDERLY attribute will be updated.

For a *shutdownType* of TPM\_SU\_STATE, the following additional items are saved:

- tracking information for saved session contexts;
- the session context counter;
- PCR that are designated as being preserved by TPM2\_Shutdown(TPM\_SU\_STATE);
- the PCR Update Counter;
- flags associated with supporting the TPMA\_NV\_WRITESTCLEAR and TPMA\_NV\_READSTCLEAR attributes; and
- the command audit digest and count.

The following items shall not be saved and will not be in TPM memory after the next TPM2\_Startup:

- TPM-memory-resident session contexts;
- TPM-memory-resident transient objects; or
- TPM-memory-resident hash contexts created by TPM2\_HashSequenceStart().

Some values may be either derived from other values or saved to NV memory.

This command saves TPM state but does not change the state other than the internal indication that the context has been saved. The TPM shall continue to accept commands. If a subsequent command changes TPM state saved by this command, then the effect of this command is nullified. The TPM MAY nullify this command for any subsequent command rather than check whether the command changed state saved by this command. If this command is nullified, and if no TPM2\_Shutdown() occurs before the next TPM2\_Startup(), then the next TPM2\_Startup() shall be TPM2\_Startup(CLEAR).

9.4.2 Command and Response

Table 7 — TPM2\_Shutdown Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Shutdown {NV}
TPM_SU	shutdownType	TPM_SU_CLEAR or TPM_SU_STATE

Table 8 — TPM2\_Shutdown Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 9.4.3 Detailed Actions

**[[Shutdown]]**

## 10 Testing

### 10.1 Introduction

Compliance to standards for hardware security modules may require that the TPM test its functions before the results that depend on those functions may be returned. The TPM may perform operations using testable functions before those functions have been tested as long as the TPM returns no value that depends on the correctness of the testable function.

**EXAMPLE**      `TPM2_PCR_Event()` may be executed before the hash algorithms have been tested. However, until the hash algorithms have been tested, the contents of a PCR may not be used in any command if that command may result in a value being returned to the TPM user. This means that `TPM2_PCR_Read()` or `TPM2_PolicyPCR()` could not complete until the hashes have been checked but other `TPM2_PCR_Event()` commands may be executed even though the operation uses previous PCR values.

If a command is received that requires return of a value that depends on untested functions, the TPM shall test the required functions before completing the command.

Once the TPM has received `TPM2_SelfTest()` and before completion of all tests, the TPM is required to return `TPM_RC_TESTING` for any command that uses a function that requires a test.

If a self-test fails at any time, the TPM will enter Failure mode. While in Failure mode, the TPM will return `TPM_RC_FAILURE` for any command other than `TPM2_GetTestResult()` and `TPM2_GetCapability()`. The TPM will remain in Failure mode until the next `_TPM_Init`.

## 10.2 TPM2\_SelfTest

### 10.2.1 General Description

This command causes the TPM to perform a test of its capabilities. If the *fullTest* is YES, the TPM will test all functions. If *fullTest* = NO, the TPM will only test those functions that have not previously been tested.

If any tests are required, the TPM shall either

- return TPM\_RC\_TESTING and begin self-test of the required functions, or

NOTE 1 If *fullTest* is NO, and all functions have been tested, the TPM shall return TPM\_RC\_SUCCESS.

- perform the tests and return the test result when complete. On failure, the TPM shall return TPM\_RC\_FAILURE.

If the TPM uses option a), the TPM shall return TPM\_RC\_TESTING for any command that requires use of a testable function, even if the functions required for completion of the command have already been tested.

NOTE 2 This command may cause the TPM to continue processing after it has returned the response. So that software can be notified of the completion of the testing, the interface may include controls that would allow the TPM to generate an interrupt when the “background” processing is complete. This would be in addition to the interrupt that may be available for signaling normal command completion. It is not necessary that there be two interrupts, but the interface should provide a way to indicate the nature of the interrupt (normal command or deferred command).

10.2.2 Command and Response

**Table 9 — TPM2\_SelfTest Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SelfTest {NV}
TPMI_YES_NO	fullTest	YES if full test to be performed NO if only test of untested functions required

**Table 10 — TPM2\_SelfTest Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 10.2.3 Detailed Actions

**[[SelfTest]]**

## 10.3 TPM2\_IncrementalSelfTest

### 10.3.1 General Description

This command causes the TPM to perform a test of the selected algorithms.

NOTE 1 The *toTest* list indicates the algorithms that software would like the TPM to test in anticipation of future use. This allows tests to be done so that a future commands will not be delayed due to testing.

The implementation may treat algorithms on the *toTest* list as either 'test each completely' or 'test this combination.'

EXAMPLE If the *toTest* list includes AES and CTR mode, it may be interpreted as a request to test only AES in CTR mode. Alternatively, it may be interpreted as a request to test AES in all modes and CTR mode for all symmetric algorithms.

If *toTest* contains an algorithm that has already been tested, it will not be tested again.

NOTE 2 The only way to force retesting of an algorithm is with `TPM2_SelfTest(fullTest = YES)`.

The TPM will return in *toDoList* a list of algorithms that are yet to be tested. This list is not the list of algorithms that are scheduled to be tested but the algorithms/functions that have not been tested. Only the algorithms on the *toTest* list are scheduled to be tested by this command.

NOTE 3 An algorithm remains on the *toDoList* while any part of it remains untested.

EXAMPLE A symmetric algorithm remains untested until it is tested with all its modes.

Making *toTest* an empty list allows the determination of the algorithms that remain untested without triggering any testing.

If *toTest* is not an empty list, the TPM shall return `TPM_RC_SUCCESS` for this command and then return `TPM_RC_TESTING` for any subsequent command (including `TPM2_IncrementalSelfTest()`) until the requested testing is complete.

NOTE 4 If *toDoList* is empty, then no additional tests are required and `TPM_RC_TESTING` will not be returned in subsequent commands and no additional delay will occur in a command due to testing.

NOTE 5 If none of the algorithms listed in *toTest* is in the *toDoList*, then no tests will be performed.

NOTE 6 The TPM cannot return `TPM_RC_TESTING` for the first call to this command even when testing is not complete, because response parameters can only returned with the `TPM_RC_SUCCESS` return code.

If all the parameters in this command are valid, the TPM returns `TPM_RC_SUCCESS` and the *toDoList* (which may be empty).

NOTE 7 An implementation may perform all requested tests before returning `TPM_RC_SUCCESS`, or it may return `TPM_RC_SUCCESS` for this command and then return `TPM_RC_TESTING` for all subsequent commands (including `TPM2_IncrementatSelfTest()`) until the requested tests are complete.

## 10.3.2 Command and Response

Table 11 — TPM2\_IncrementalSelfTest Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_IncrementalSelfTest {NV}
TPML_ALG	toTest	list of algorithms that should be tested

Table 12 — TPM2\_IncrementalSelfTest Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPML_ALG	toDoList	list of algorithms that need testing

### 10.3.3 Detailed Actions

`[[IncrementalSelfTest]]`



## 10.4 TPM2\_GetTestResult

### 10.4.1 General Description

This command returns manufacturer-specific information regarding the results of a self-test and an indication of the test status.

If TPM2\_SelfTest() has not been executed and a testable function has not been tested, *testResult* will be TPM\_RC\_NEEDS\_TEST. If TPM2\_SelfTest() has been received and the tests are not complete, *testResult* will be TPM\_RC\_TESTING. If testing of all functions is complete without functional failures, *testResult* will be TPM\_RC\_SUCCESS. If any test failed, *testResult* will be TPM\_RC\_FAILURE.

This command will operate when the TPM is in Failure mode so that software can determine the test status of the TPM and so that diagnostic information can be obtained for use in failure analysis. If the TPM is in Failure mode, then *tag* is required to be TPM\_ST\_NO\_SESSIONS or the TPM shall return TPM\_RC\_FAILURE.

10.4.2 Command and Response

**Table 13 — TPM2\_GetTestResult Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetTestResult

**Table 14 — TPM2\_GetTestResult Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_MAX_BUFFER	outData	test result data contains manufacturer-specific information
TPM_RC	testResult	

### 10.4.3 Detailed Actions

**[[GetTestResult]]**

## 11 Session Commands

### 11.1 TPM2\_StartAuthSession

#### 11.1.1 General Description

This command is used to start an authorization session using alternative methods of establishing the session key (*sessionKey*). The session key is then used to derive values used for authorization and for encrypting parameters.

This command allows injection of a secret into the TPM using either asymmetric or symmetric encryption. The type of *tpmKey* determines how the value in *encryptedSalt* is encrypted. The decrypted secret value is used to compute the *sessionKey*.

NOTE 1 If *tpmKey* is TPM\_RH\_NULL, then *encryptedSalt* is required to be an Empty Buffer.

The label value of “SECRET” (see “Terms and Definitions” in TPM 2.0 Part 1) is used in the recovery of the secret value.

The TPM generates the *sessionKey* from the recovered secret value.

No authorization is required for *tpmKey* or *bind*.

NOTE 2 The justification for using *tpmKey* without providing authorization is that the result of using the key is not available to the caller, except indirectly through the *sessionKey*. This does not represent a point of attack on the value of the key. If the caller attempts to use the session without knowing the *sessionKey* value, it is an authorization failure that will trigger the dictionary attack logic.

The entity referenced with the *bind* parameter contributes an authorization value to the *sessionKey* generation process.

If both *tpmKey* and *bind* are TPM\_RH\_NULL, then *sessionKey* is set to the Empty Buffer. If *tpmKey* is not TPM\_RH\_NULL, then *encryptedSalt* is used in the computation of *sessionKey*. If *bind* is not TPM\_RH\_NULL, the *authValue* of *bind* is used in the *sessionKey* computation.

If *symmetric* specifies a block cipher, then TPM\_ALG\_CFB is the only allowed value for the *mode* field in the *symmetric* parameter (TPM\_RC\_MODE).

This command starts an authorization session and returns the session handle along with an initial *nonceTPM* in the response.

If the TPM does not have a free slot for an authorization session, it shall return TPM\_RC\_SESSION\_HANDLES.

If the TPM implements a “gap” scheme for assigning *contextID* values, then the TPM shall return TPM\_RC\_CONTEXT\_GAP if creating the session would prevent recycling of old saved contexts (See “Context Management” in TPM 2.0 Part 1).

If *tpmKey* is not TPM\_ALG\_NULL then *encryptedSalt* shall be a TPM2B\_ENCRYPTED\_SECRET of the proper type for *tpmKey*. The TPM shall return TPM\_RC\_HANDLE if the sensitive portion of *tpmKey* is not loaded. The TPM shall return TPM\_RC\_VALUE if:

- a) *tpmKey* references an RSA key and
  - 1) the size of *encryptedSalt* is not the same as the size of the public modulus of *tpmKey*,
  - 2) *encryptedSalt* has a value that is greater than the public modulus of *tpmKey*,
  - 3) *encryptedSalt* is not a properly encoded OAEP value, or
  - 4) the decrypted *salt* value is larger than the size of the digest produced by the *nameAlg* of *tpmKey*,  
or

NOTE 3 The *asymScheme* of the key object is ignored in this case and *TPM\_ALG\_OAEP* is used, even if *asymScheme* is set to *TPM\_ALG\_NULL*.

b) *tpmKey* references an ECC key and *encryptedSalt*

- 1) does not contain a *TPMS\_ECC\_POINT* or
- 2) is not a point on the curve of *tpmKey*;

NOTE 4 When ECC is used, the point multiply process produces a value (Z) that is used in a KDF to produce the final secret value. The size of the secret value is an input parameter to the KDF and the result will be set to be the size of the digest produced by the *nameAlg* of *tpmKey*.

The TPM shall return *TPM\_RC\_KEY* if *tpmkey* does not reference an asymmetric key. The TPM shall return *TPM\_RC\_SCHEME* if the scheme of the key is not *TPM\_ALG\_OAEP* or *TPM\_ALG\_NULL*.

If *bind* references a transient object, then the TPM shall return *TPM\_RC\_HANDLE* if the sensitive portion of the object is not loaded.

For all session types, this command will cause initialization of the *sessionKey* and may establish binding between the session and an object (the *bind* object). If *sessionType* is *TPM\_SE\_POLICY* or *TPM\_SE\_TRIAL*, the additional session initialization is:

- set *policySession*→*policyDigest* to a Zero Digest (the digest size for *policySession*→*policyDigest* is the size of the digest produced by *authHash*);
- authorization may be given at any locality;
- authorization may apply to any command code;
- authorization may apply to any command parameters or handles;
- the authorization has no time limit;
- an *authValue* is not needed when the authorization is used;
- the session is not bound;
- the session is not an audit session; and
- the time at which the policy session was created is recorded.

Additionally, if *sessionType* is *TPM\_SE\_TRIAL*, the session will not be usable for authorization but can be used to compute the *authPolicy* for an object.

NOTE 5 Although this command changes the session allocation information in the TPM, it does not invalidate a saved context. That is, *TPM2\_Shutdown()* is not required after this command in order to re-establish the orderly state of the TPM. This is because the created context will occupy an available slot in the TPM and sessions in the TPM do not survive any *TPM2\_Startup()*. However, if a created session is context saved, the orderly state does change.

The TPM shall return *TPM\_RC\_SIZE* if *nonceCaller* is less than 16 octets or is greater than the size of the digest produced by *authHash*.

## 11.1.2 Command and Response

Table 15 — TPM2\_StartAuthSession Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, decrypt, or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_StartAuthSession
TPMI_DH_OBJECT+	tpmKey	handle of a loaded decrypt key used to encrypt <i>salt</i> may be TPM_RH_NULL Auth Index: None
TPMI_DH_ENTITY+	bind	entity providing the <i>authValue</i> may be TPM_RH_NULL Auth Index: None
TPM2B_NONCE	nonceCaller	initial <i>nonceCaller</i> , sets nonceTPM size for the session shall be at least 16 octets
TPM2B_ENCRYPTED_SECRET	encryptedSalt	value encrypted according to the type of <i>tpmKey</i> If <i>tpmKey</i> is TPM_RH_NULL, this shall be the Empty Buffer.
TPM_SE	sessionType	indicates the type of the session; simple HMAC or policy (including a trial policy)
TPMT_SYM_DEF+	symmetric	the algorithm and key size for parameter encryption may select TPM_ALG_NULL
TPMI_ALG_HASH	authHash	hash algorithm to use for the session Shall be a hash algorithm supported by the TPM and not TPM_ALG_NULL

Table 16 — TPM2\_StartAuthSession Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_SH_AUTH_SESSION	sessionHandle	handle for the newly created session
TPM2B_NONCE	nonceTPM	the initial nonce from the TPM, used in the computation of the <i>sessionKey</i>

### 11.1.3 Detailed Actions

**[[StartAuthSession]]**

## 11.2 TPM2\_PolicyRestart

### 11.2.1 General Description

This command allows a policy authorization session to be returned to its initial state. This command is used after the TPM returns TPM\_RC\_PCR\_CHANGED. That response code indicates that a policy will fail because the PCR have changed after TPM2\_PolicyPCR() was executed. Restarting the session allows the authorizations to be replayed because the session restarts with the same *nonceTPM*. If the PCR are valid for the policy, the policy may then succeed.

This command does not reset the policy ID or the policy start time.



11.2.2 Command and Response

Table 17 — TPM2\_PolicyRestart Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyRestart
TPMI_SH_POLICY	sessionHandle	the handle for the policy session

Table 18 — TPM2\_PolicyRestart Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 11.2.3 Detailed Actions

**[[PolicyRestart]]**

## 12 Object Commands

### 12.1 TPM2\_Create

#### 12.1.1 General Description

This command is used to create an object that can be loaded into a TPM using TPM2\_Load(). If the command completes successfully, the TPM will create the new object and return the object's creation data (*creationData*), its public area (*outPublic*), and its encrypted sensitive area (*outPrivate*). Preservation of the returned data is the responsibility of the caller. The object will need to be loaded (TPM2\_Load()) before it may be used. The only difference between the *inPublic* TPMT\_PUBLIC template and the *outPublic* TPMT\_PUBLIC object is in the *unique* field.

NOTE 1 This command may require temporary use of a transient resource, even though the object does not remain loaded after the command. See Part 1 Transient Resources.

TPM2B\_PUBLIC template (*inPublic*) contains all of the fields necessary to define the properties of the new object. The setting for these fields is defined in "Public Area Template" in Part 1 of this specification and in "TPMA\_OBJECT" in Part 2 of this specification. The size of the *unique* field shall not be checked for consistency with the other object parameters.

NOTE 2 For interoperability, the *unique* field should not be set to a value that is larger than allowed by object parameters, so that the unmarshaling will not fail. A size of zero is recommended. After unmarshaling, the TPM does not use the input *unique* field. It is, however, used in TPM2\_CreatePrimary() and TPM2\_CreateLoaded.

EXAMPLE 1 A TPM\_ALG\_RSA object with a *keyBits* of 2048 in the objects parameters should have a *unique* field that is no larger than 256 bytes.

EXAMPLE 2 TPM\_ALG\_KEYEDHASH or a TPM\_ALG\_SYMCIPHER object should have a *unique* field this is no larger than the digest produced by the object's *nameAlg*.

The *parentHandle* parameter shall reference a loaded decryption key that has both the public and sensitive area loaded.

When defining the object, the caller provides a template structure for the object in a TPM2B\_PUBLIC structure (*inPublic*), an initial value for the object's *authValue* (*inSensitive.userAuth*), and, if the object is a symmetric object, an optional initial data value (*inSensitive.data*). The TPM shall validate the consistency of the attributes of *inPublic* according to the Creation rules in "TPMA\_OBJECT" in TPM 2.0 Part 2.

The *inSensitive* parameter may be encrypted using parameter encryption.

The methods in this clause are used by both TPM2\_Create() and TPM2\_CreatePrimary(). When a value is indicated as being TPM-generated, the value is filled in by bits from the RNG if the command is TPM2\_Create() and with values from KDFa() if the command is TPM2\_CreatePrimary(). The parameters of each creation value are specified in TPM 2.0 Part 1.

The *sensitiveDataOrigin* attribute of *inPublic* shall be SET if *inSensitive.data* is an Empty Buffer and CLEAR if *inSensitive.data* is not an Empty Buffer or the TPM shall return TPM\_RC\_ATTRIBUTES.

If the Object is a not a keyedHash object, and the *sign* and *encrypt* attributes are CLEAR, the TPM shall return TPM\_RC\_ATTRIBUTES.

The TPM will create new data for the sensitive area and compute a TPMT\_PUBLIC.*unique* from the sensitive area based on the object type:

a) For a symmetric key:

- 1) If *inSensitive.sensitive.data* is the Empty Buffer, a TPM-generated key value is placed in the new object's *TPMT\_SENSITIVE.sensitive.sym*. The size of the key will be determined by *inPublic.publicArea.parameters*.
- 2) If *inSensitive.sensitive.data* is not the Empty Buffer, the TPM will validate that the size of *inSensitive.data* is no larger than the key size indicated in the *inPublic template* (TPM\_RC\_SIZE) and copy the *inSensitive.data* to *TPMT\_SENSITIVE.sensitive.sym* of the new object.
- 3) A TPM-generated obfuscation value is placed in *TPMT\_SENSITIVE.sensitive.seedValue*. The size of the obfuscation value is the size of the digest produced by the *nameAlg* in *inPublic*. This value prevents the public *unique* value from leaking information about the *sensitive* area.
- 4) The *TPMT\_PUBLIC.unique.sym* value for the new object is then generated, as shown in equation (1) below, by hashing the key and obfuscation values in the *TPMT\_SENSITIVE* with the *nameAlg* of the object.

$$unique := H_{nameAlg}(sensitive.seedValue.buffer || sensitive.any.buffer) \quad (1)$$

b) If the Object is an asymmetric key:

- 1) If *inSensitive.sensitive.data* is not the Empty Buffer, then the TPM shall return TPM\_RC\_VALUE.
- 2) A TPM-generated private key value is created with the size determined by the parameters of *inPublic.publicArea.parameters*.
- 3) If the key is a Storage Key, a TPM-generated *TPMT\_SENSITIVE.seedValue* value is created; otherwise, *TPMT\_SENSITIVE.seedValue.size* is set to zero.

NOTE 3 An Object that is not a storage key has no child Objects to encrypt, so it does not need a symmetric key.

- 4) The public *unique* value is computed from the private key according to the methods of the key type.
- 5) If the key is an ECC key and the scheme required by the *curveID* is not the same as *scheme* in the public area of the template, then the TPM shall return TPM\_RC\_SCHEME.
- 6) If the key is an ECC key and the KDF required by the *curveID* is not the same as *kdf* in the public area of the template, then the TPM shall return TPM\_RC\_KDF.

NOTE 4 There is currently no command in which the caller may specify the KDF to be used with an ECC decryption key. Since there is no use for this capability, the reference implementation requires that the *kdf* in the template be set to TPM\_ALG\_NULL or TPM\_RC\_KDF is returned.

c) If the Object is a keyedHash object:

- 1) If *inSensitive.sensitive.data* is an Empty Buffer, and both *sign* and *decrypt* are CLEAR in the attributes of *inPublic*, the TPM shall return TPM\_RC\_ATTRIBUTES. This would be a data object with no data.
- 2) If *sign* and *decrypt* are both CLEAR, or if *sign* and *decrypt* are both SET and the *scheme* in the public area of the template is not TPM\_ALG\_NULL, the TPM shall return TPM\_RC\_SCHEME.
- 3) If *inSensitive.sensitive.data* is not an Empty Buffer, the TPM will copy the *inSensitive.sensitive.data* to *TPMT\_SENSITIVE.sensitive.bits* of the new object.

NOTE 5 The size of *inSensitive.sensitive.data* is limited to be no larger than the largest value of *TPMT\_SENSITIVE.sensitive.bits* by MAX\_SYM\_DATA.

- 4) If *inSensitive.sensitive.data* is an Empty Buffer, a TPM-generated key value that is the size of the digest produced by the *nameAlg* in *inPublic* is placed in *TPMT\_SENSITIVE.sensitive.bits*.
- 5) A TPM-generated obfuscation value that is the size of the digest produced by the *nameAlg* of *inPublic* is placed in *TPMT\_SENSITIVE.seedValue*.

- 6) The TPMT\_PUBLIC.*unique.keyedHash* value for the new object is then generated, as shown in equation (1) above, by hashing the key and obfuscation values in the TPMT\_SENSITIVE with the *nameAlg* of the object.

For TPM2\_Load(), the TPM will apply normal symmetric protections to the created TPMT\_SENSITIVE to create *outPublic*.

NOTE 6           The encryption key is derived from the symmetric seed in the sensitive area of the parent.

In addition to *outPublic* and *outPrivate*, the TPM will build a TPMS\_CREATION\_DATA structure for the object. TPMS\_CREATION\_DATA.*outsideInfo* is set to *outsideInfo*. This structure is returned in *creationData*. Additionally, the digest of this structure is returned in *creationHash*, and, finally, a TPMT\_TK\_CREATION is created so that the association between the creation data and the object may be validated by TPM2\_CertifyCreation().

If the object being created is a Storage Key and *fixedParent* is SET in the attributes of *inPublic*, then the symmetric algorithms and parameters of *inPublic* are required to match those of the parent. The algorithms that must match are *inPublic.nameAlg*, and the values in *inPublic.parameters* that select the symmetric scheme. If *inPublic.nameAlg* does not match, the TPM shall return TPM\_RC\_HASH. If the symmetric scheme of the key does not match the parent, the TPM shall return TPM\_RC\_SYMMETRIC. The TPM shall not use different response code to differentiate between mismatches of the components of *inPublic.parameters*. However, after this verification, when using the scheme to encrypt child objects, the TPM ignores the symmetric mode and uses TPM\_ALG\_CFB.

NOTE 7           The symmetric scheme is a TPMT\_SYM\_DEF\_OBJECT. In a symmetric block cipher, it is at *inPublic.parameters.symDetail.sym* and in an asymmetric object is at *inPublic.parameters.asymDetail.symmetric*.

## 12.1.2 Command and Response

Table 19 — TPM2\_Create Command

Type	Name	Description
TPML_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Create
TPMI_DH_OBJECT	@parentHandle	handle of parent for new object Auth Index: 1 Auth Role: USER
TPM2B_SENSITIVE_CREATE	inSensitive	the sensitive data
TPM2B_PUBLIC	inPublic	the public template
TPM2B_DATA	outsideInfo	data that will be included in the creation data for this object to provide permanent, verifiable linkage between this object and some object owner data
TPML_PCR_SELECTION	creationPCR	PCR that will be used in creation data

Table 20 — TPM2\_Create Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PRIVATE	outPrivate	the private portion of the object
TPM2B_PUBLIC	outPublic	the public portion of the created object
TPM2B_CREATION_DATA	creationData	contains a TPMS_CREATION_DATA
TPM2B_DIGEST	creationHash	digest of <i>creationData</i> using <i>nameAlg</i> of <i>outPublic</i>
TPMT_TK_CREATION	creationTicket	ticket used by TPM2_CertifyCreation() to validate that the creation data was produced by the TPM

### 12.1.3 Detailed Actions

**[[Create]]**

## 12.2 TPM2\_Load

### 12.2.1 General Description

This command is used to load objects into the TPM. This command is used when both a TPM2B\_PUBLIC and TPM2B\_PRIVATE are to be loaded. If only a TPM2B\_PUBLIC is to be loaded, the TPM2\_LoadExternal command is used.

NOTE 1 Loading an object is not the same as restoring a saved object context.

The object's TPMA\_OBJECT attributes will be checked according to the rules defined in "TPMA\_OBJECT" in TPM 2.0 Part 2 of this specification. If the Object is a not a keyedHash object, and the *sign* and *encrypt* attributes are CLEAR, the TPM shall return TPM\_RC\_ATTRIBUTES.

Objects loaded using this command will have a Name. The Name is the concatenation of *nameAlg* and the digest of the public area using the *nameAlg*.

NOTE 2 *nameAlg* is a parameter in the public area of the inPublic structure.

If *inPrivate.size* is zero, the load will fail.

After *inPrivate.buffer* is decrypted using the symmetric key of the parent, the integrity value shall be checked before the sensitive area is used, or unmarshaled.

NOTE 3 Checking the integrity before the data is used prevents attacks on the sensitive area by fuzzing the data and looking at the differences in the response codes.

The command returns a handle for the loaded object and the Name that the TPM computed for *inPublic.public* (that is, the digest of the TPMT\_PUBLIC structure in *inPublic*).

NOTE 4 The TPM-computed Name is provided as a convenience to the caller for those cases where the caller does not implement the hash algorithms specified in the *nameAlg* of the object.

NOTE 5 The returned handle is associated with the object until the object is flushed (TPM2\_FlushContext) or until the next TPM2\_Startup.

For all objects, the size of the key in the sensitive area shall be consistent with the key size indicated in the public area or the TPM shall return TPM\_RC\_KEY\_SIZE.

Before use, a loaded object shall be checked to validate that the public and sensitive portions are properly linked, cryptographically. Use of an object includes use in any policy command. If the parts of the object are not properly linked, the TPM shall return TPM\_RC\_BINDING. If a weak symmetric key is in the sensitive portion, the TPM shall return TPM\_RC\_KEY.

EXAMPLE 1 For a symmetric object, the unique value in the public area shall be the digest of the sensitive key and the obfuscation value.

EXAMPLE 2 For a two-prime RSA key, the remainder when dividing the public modulus by the private key shall be zero and it shall be possible to form a private exponent from the two prime factors of the public modulus.

EXAMPLE 3 For an ECC key, the public point shall be  $f(x)$  where  $x$  is the private key.



12.2.2 Command and Response

Table 21 — TPM2\_Load Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Load
TPMI_DH_OBJECT	@parentHandle	TPM handle of parent key; shall not be a reserved handle Auth Index: 1 Auth Role: USER
TPM2B_PRIVATE	inPrivate	the private portion of the object
TPM2B_PUBLIC	inPublic	the public portion of the object

Table 22 — TPM2\_Load Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM_HANDLE	objectHandle	handle of type TPM_HT_TRANSIENT for the loaded object
TPM2B_NAME	name	Name of the loaded object

### 12.2.3 Detailed Actions

**[[Load]]**

## 12.3 TPM2\_LoadExternal

### 12.3.1 General Description

This command is used to load an object that is not a Protected Object into the TPM. The command allows loading of a public area or both a public and sensitive area.

NOTE 1 Typical use for loading a public area is to allow the TPM to validate an asymmetric signature. Typical use for loading both a public and sensitive area is to allow the TPM to be used as a crypto accelerator.

Load of a public external object area allows the object be associated with a hierarchy so that the correct algorithms may be used when creating tickets. The *hierarchy* parameter provides this association. If the public and sensitive portions of the object are loaded, *hierarchy* is required to be TPM\_RH\_NULL.

NOTE 2 If both the public and private portions of an object are loaded, the object is not allowed to appear to be part of a hierarchy.

The object's TPMA\_OBJECT attributes will be checked according to the rules defined in "TPMA\_OBJECT" in TPM 2.0 Part 2. In particular, *fixedTPM*, *fixedParent*, and *restricted* shall be CLEAR if *inPrivate* is not the Empty Buffer.

NOTE 3 The duplication status of a public key needs to be able to be the same as the full key which may be resident on a different TPM. If both the public and private parts of the key are loaded, then it is not possible for the key to be either *fixedTPM* or *fixedParent*, since, its private area would not be available in the clear to load.

Objects loaded using this command will have a Name. The Name is the *nameAlg* of the object concatenated with the digest of the public area using the *nameAlg*. The Qualified Name for the object will be the same as its Name. The TPM will validate that the *authPolicy* is either the size of the digest produced by *nameAlg* or the Empty Buffer.

NOTE 4 If *nameAlg* is TPM\_ALG\_NULL, then the Name is the Empty Buffer. When the authorization value for an object with no Name is computed, no Name value is included in the HMAC. To ensure that these unnamed entities are not substituted, they should have an *authValue* that is statistically unique.

NOTE 5 The digest size for TPM\_ALG\_NULL is zero.

If the *nameAlg* is TPM\_ALG\_NULL, the TPM shall not verify the cryptographic binding between the public and sensitive areas, but the TPM will validate that the size of the key in the sensitive area is consistent with the size indicated in the public area. If it is not, the TPM shall return TPM\_RC\_KEY\_SIZE.

NOTE 6 For an ECC object, the TPM will verify that the public key is on the curve of the key before the public area is used.

If *nameAlg* is not TPM\_ALG\_NULL, then the same consistency checks between *inPublic* and *inPrivate* are made as for TPM2\_Load().

NOTE 7 Consistency checks are necessary because an object with a Name needs to have the public and sensitive portions cryptographically bound so that an attacker cannot mix public and sensitive areas.

The command returns a handle for the loaded object and the Name that the TPM computed for *inPublic.public* (that is, the TPMT\_PUBLIC structure in *inPublic*).

NOTE 8 The TPM-computed Name is provided as a convenience to the caller for those cases where the caller does not implement the hash algorithm specified in the *nameAlg* of the object.

The *hierarchy* parameter associates the external object with a hierarchy. External objects are flushed when their associated hierarchy is disabled. If *hierarchy* is TPM\_RH\_NULL, the object is part of no hierarchy, and there is no implicit flush.

If *hierarchy* is TPM\_RH\_NULL or *nameAlg* is TPM\_ALG\_NULL, a ticket produced using the object shall be a NULL Ticket.

EXAMPLE        If a key is loaded with *hierarchy* set to TPM\_RH\_NULL, then TPM2\_VerifySignature() will produce a NULL Ticket of the required type.

External objects are Temporary Objects. The saved external object contexts shall be invalidated at the next TPM Reset.

If a weak symmetric key is in the sensitive area, the TPM shall return TPM\_RC\_KEY.

For an RSA key, the private exponent is computed using the two prime factors of the public modulus. One of the primes is P, and the second prime (Q) is found by dividing the public modulus by P. A TPM may return an error (TPM\_RC\_BINDING) if the bit size of P and Q are not the same.”

12.3.2 Command and Response

Table 23 — TPM2\_LoadExternal Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, encrypt, or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_LoadExternal
TPM2B_SENSITIVE	inPrivate	the sensitive portion of the object (optional)
TPM2B_PUBLIC+	inPublic	the public portion of the object
TPMI_RH_HIERARCHY+	hierarchy	hierarchy with which the object area is associated

Table 24 — TPM2\_LoadExternal Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM_HANDLE	objectHandle	handle of type TPM_HT_TRANSIENT for the loaded object
TPM2B_NAME	name	name of the loaded object

### 12.3.3 Detailed Actions

`[[LoadExternal]]`

## 12.4 TPM2\_ReadPublic

### 12.4.1 General Description

This command allows access to the public area of a loaded object.

Use of the *objectHandle* does not require authorization.

NOTE                Since the caller is not likely to know the public area of the object associated with *objectHandle*, it would not be possible to include the Name associated with *objectHandle* in the *cpHash* computation.

If *objectHandle* references a sequence object, the TPM shall return TPM\_RC\_SEQUENCE.

12.4.2 Command and Response

Table 25 — TPM2\_ReadPublic Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ReadPublic
TPMI_DH_OBJECT	objectHandle	TPM handle of an object Auth Index: None

Table 26 — TPM2\_ReadPublic Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PUBLIC	outPublic	structure containing the public area of an object
TPM2B_NAME	name	name of the object
TPM2B_NAME	qualifiedName	the Qualified Name of the object



### 12.4.3 Detailed Actions

**[[ReadPublic]]**

## 12.5 TPM2\_ActivateCredential

### 12.5.1 General Description

This command enables the association of a credential with an object in a way that ensures that the TPM has validated the parameters of the credentialed object.

If both the public and private portions of *activateHandle* and *keyHandle* are not loaded, then the TPM shall return TPM\_RC\_AUTH\_UNAVAILABLE.

If *keyHandle* is not a Storage Key, then the TPM shall return TPM\_RC\_TYPE.

Authorization for *activateHandle* requires the ADMIN role.

The key associated with *keyHandle* is used to recover a seed from secret, which is the encrypted seed. The Name of the object associated with *activateHandle* and the recovered seed are used in a KDF to recover the symmetric key. The recovered seed (but not the Name) is used in a KDF to recover the HMAC key.

The HMAC is used to validate that the *credentialBlob* is associated with *activateHandle* and that the data in *credentialBlob* has not been modified. The linkage to the object associated with *activateHandle* is achieved by including the Name in the HMAC calculation.

If the integrity checks succeed, *credentialBlob* is decrypted and returned as *certInfo*.

NOTE           The output *certInfo* parameter is an application defined value. It is typically a symmetric key or seed that is used to decrypt a certificate. See the TPM2\_MakeCredential *credential* input parameter.

12.5.2 Command and Response

Table 27 — TPM2\_ActivateCredential Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ActivateCredential
TPMI_DH_OBJECT	@activateHandle	handle of the object associated with certificate in <i>credentialBlob</i> Auth Index: 1 Auth Role: ADMIN
TPMI_DH_OBJECT	@keyHandle	loaded key used to decrypt the TPMS_SENSITIVE in <i>credentialBlob</i> Auth Index: 2 Auth Role: USER
TPM2B_ID_OBJECT	credentialBlob	the credential
TPM2B_ENCRYPTED_SECRET	secret	<i>keyHandle</i> algorithm-dependent encrypted seed that protects <i>credentialBlob</i>

Table 28 — TPM2\_ActivateCredential Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	certInfo	the decrypted certificate information the data should be no larger than the size of the digest of the <i>nameAlg</i> associated with <i>keyHandle</i>

### 12.5.3 Detailed Actions

`[[ActivateCredential]]`

## 12.6 TPM2\_MakeCredential

### 12.6.1 General Description

This command allows the TPM to perform the actions required of a Certificate Authority (CA) in creating a TPM2B\_ID\_OBJECT containing an activation credential.

NOTE           The input *credential* parameter is an application defined value. It is typically a symmetric key or seed that is used to encrypt a certificate. See the TPM2\_ActivateCredential *certInfo* output parameter.

The TPM will produce a TPM2B\_ID\_OBJECT according to the methods in “Credential Protection” in TPM 2.0 Part 1.

The loaded public area referenced by *handle* is required to be the public area of a Storage key, otherwise, the credential cannot be properly sealed.

This command does not use any TPM secrets nor does it require authorization. It is a convenience function, using the TPM to perform cryptographic calculations that could be done externally.

12.6.2 Command and Response

Table 29 — TPM2\_MakeCredential Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, encrypt, or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_MakeCredential
TPMI_DH_OBJECT	handle	loaded public area, used to encrypt the sensitive area containing the credential key Auth Index: None
TPM2B_DIGEST	credential	the credential information
TPM2B_NAME	objectName	Name of the object to which the credential applies

Table 30 — TPM2\_MakeCredential Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ID_OBJECT	credentialBlob	the credential
TPM2B_ENCRYPTED_SECRET	secret	<i>handle</i> algorithm-dependent data that wraps the key that encrypts <i>credentialBlob</i>

### 12.6.3 Detailed Actions

`[[MakeCredential]]`

## 12.7 TPM2\_Unseal

### 12.7.1 General Description

This command returns the data in a loaded Sealed Data Object.

NOTE 1           A random, TPM-generated, Sealed Data Object may be created by the TPM with TPM2\_Create() or TPM2\_CreatePrimary() using the template for a Sealed Data Object.

NOTE 2           TPM 1.2 hard coded PCR authorization. TPM 2.0 PCR authorization requires a policy.

The returned value may be encrypted using authorization session encryption.

If either *restricted*, *decrypt*, or *sign* is SET in the attributes of *itemHandle*, then the TPM shall return TPM\_RC\_ATTRIBUTES. If the *type* of *itemHandle* is not TPM\_ALG\_KEYEDHASH, then the TPM shall return TPM\_RC\_TYPE.



12.7.2 Command and Response

Table 31 — TPM2\_Unseal Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Unseal
TPMI_DH_OBJECT	@itemHandle	handle of a loaded data object Auth Index: 1 Auth Role: USER

Table 32 — TPM2\_Unseal Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_SENSITIVE_DATA	outData	unsealed data Size of <i>outData</i> is limited to be no more than 128 octets.

### 12.7.3 Detailed Actions

**[[Unseal]]**

## 12.8 TPM2\_ObjectChangeAuth

### 12.8.1 General Description

This command is used to change the authorization secret for a TPM-resident object.

If successful, a new private area for the TPM-resident object associated with *objectHandle* is returned, which includes the new authorization value.

This command does not change the authorization of the TPM-resident object on which it operates. Therefore, the old authValue (of the TPM-resident object) is used when generating the response HMAC key if required.

NOTE 1            The returned *outPrivate* will need to be loaded before the new authorization will apply.

NOTE 2            The TPM-resident object may be persistent and changing the authorization value of the persistent object could prevent other users from accessing the object. This is why this command does not change the TPM-resident object.

EXAMPLE          If a persistent key is being used as a Storage Root Key and the authorization of the key is a well-known value so that the key can be used generally, then changing the authorization value in the persistent key would deny access to other users.

This command may not be used to change the authorization value for an NV Index or a Primary Object.

NOTE 3            If an NV Index is to have a new authorization, it is done with TPM2\_NV\_ChangeAuth().

NOTE 4            If a Primary Object is to have a new authorization, it needs to be recreated (TPM2\_CreatePrimary()).

12.8.2 Command and Response

Table 33 — TPM2\_ObjectChangeAuth Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ObjectChangeAuth
TPMI_DH_OBJECT	@objectHandle	handle of the object Auth Index: 1 Auth Role: ADMIN
TPMI_DH_OBJECT	parentHandle	handle of the parent Auth Index: None
TPM2B_AUTH	newAuth	new authorization value

Table 34 — TPM2\_ObjectChangeAuth Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PRIVATE	outPrivate	private area containing the new authorization value

### 12.8.3 Detailed Actions

`[[ObjectChangeAuth]]`

## 12.9 TPM2\_CreateLoaded

### 12.9.1 General Description

This command creates an object and loads it in the TPM. This command allows creation of any type of object (Primary, Ordinary, or Derived) depending on the type of *parentHandle*. If *parentHandle* references a Primary Seed, then a Primary Object is created; if *parentHandle* references a Storage Parent, then an Ordinary Object is created; and if *parentHandle* references a Derivation Parent, then a Derived Object is generated.

The input validation is the same as for TPM2\_Create() and TPM2\_CreatePrimary() with one exception: when *parentHandle* references a Derivation Parent, then *sensitiveDataOrigin* in *inPublic* is required to be CLEAR.

Note 1 In the general descriptions of TPM2\_Create() and TPM2\_CreatePrimary() the validations refer to a TPMT\_PUBLIC structure that is in *inPublic*. For TPM2\_CreateLoaded(), *inPublic* is a TPM2B\_TEMPLATE that may contain a TPMT\_PUBLIC that is used for object creation. For object derivation, the *unique* field can contain a *label* and *context* that are used in the derivation process. To allow both the TPMT\_PUBLIC and the derivation variation, a TPM2B\_TEMPLATE is used. When referring to the checks in TPM2\_Create() and TPM2\_CreatePrimary(), TPM2B\_TEMPLATE should be assumed to contain a TPMT\_PUBLIC.

If *parentHandle* references a Derivation Parent, then the TPM may return TPM\_RC\_TYPE if the key type to be generated is an RSA key.

If *parentHandle* references a Derivation Parent or a Primary Seed, then *outPrivate* will be an Empty Buffer.

NOTE 2 Unlike TPM2\_Create() and TPM2\_CreatePrimary(), this command does not return creation data. If creation data is needed, then TPM2\_Create() or TPM2\_CreatePrimary() should be used.

## 12.9.2 Command and Response

Table 35 — TPM2\_CreateLoaded Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_CreateLoade
TPMI_DH_PARENT+	@parentHandle	Handle of a transient storage key, a persistent storage key, TPM_RH_ENDORSEMENT, TPM_RH_OWNER, TPM_RH_PLATFORM+{PP}, or TPM_RH_NULL Auth Index: 1 Auth Role: USER
TPM2B_SENSITIVE_CREATE	inSensitive	the sensitive data, see TPM 2.0 Part 1 Sensitive Values
TPM2B_TEMPLATE	inPublic	the public template

Table 36 — TPM2\_CreateLoaded Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM_HANDLE	objectHandle	handle of type TPM_HT_TRANSIENT for created object
TPM2B_PRIVATE	outPrivate	the sensitive area of the object (optional)
TPM2B_PUBLIC	outPublic	the public portion of the created object
TPM2B_NAME	name	the name of the created object

### 12.9.3 Detailed Actions

**[[CreateLoaded]]**



## 13 Duplication Commands

### 13.1 TPM2\_Duplicate

#### 13.1.1 General Description

This command duplicates a loaded object so that it may be used in a different hierarchy. The new parent key for the duplicate may be on the same or different TPM or TPM\_RH\_NULL. Only the public area of *newParentHandle* is required to be loaded.

NOTE 1 Since the new parent may only be extant on a different TPM, it is likely that the new parent's sensitive area could not be loaded in the TPM from which *objectHandle* is being duplicated.

If *encryptedDuplication* is SET in the object being duplicated, then the TPM shall return TPM\_RC\_SYMMETRIC if *symmetricAlg.algorithm* is TPM\_ALG\_NULL or TPM\_RC\_HIERARCHY if *newParentHandle* is TPM\_RH\_NULL.

The authorization for this command shall be with a policy session.

If *fixedParent* of *objectHandle→attributes* is SET, the TPM shall return TPM\_RC\_ATTRIBUTES. If *objectHandle→nameAlg* is TPM\_ALG\_NULL, the TPM shall return TPM\_RC\_TYPE.

The *policySession→commandCode* parameter in the policy session is required to be TPM\_CC\_Duplicate to indicate that authorization for duplication has been provided. This indicates that the policy that is being used is a policy that is for duplication, and not a policy that would approve another use. That is, authority to use an object does not grant authority to duplicate the object.

The policy is likely to include cpHash in order to restrict where duplication can occur. If TPM2\_PolicyCpHash() has been executed as part of the policy, the *policySession→cpHash* is compared to the cpHash of the command.

If TPM2\_PolicyDuplicationSelect() has been executed as part of the policy, the *policySession→nameHash* is compared to

$$H_{policyAlg}(objectHandle→Name || newParentHandle→Name) \quad (2)$$

If the compared hashes are not the same, then the TPM shall return TPM\_RC\_POLICY\_FAIL.

NOTE 2 It is allowed that *policySession→nameHash* and *policySession→cpHash* share the same memory space.

NOTE 3 A duplication policy is not required to have either TPM2\_PolicyDuplicationSelect() or TPM2\_PolicyCpHash() as part of the policy. If neither is present, then the duplication policy may be satisfied with a policy that only contains TPM2\_PolicyCommandCode(*code* = TPM\_CC\_Duplicate).

The TPM shall follow the process of encryption defined in the “Duplication” subclause of “Protected Storage Hierarchy” in TPM 2.0 Part 1.

## 13.1.2 Command and Response

Table 37 — TPM2\_Duplicate Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Duplicate
TPMI_DH_OBJECT	@objectHandle	loaded object to duplicate Auth Index: 1 Auth Role: DUP
TPMI_DH_OBJECT+	newParentHandle	shall reference the public area of an asymmetric key Auth Index: None
TPM2B_DATA	encryptionKeyIn	optional symmetric encryption key The size for this key is set to zero when the TPM is to generate the key. This parameter may be encrypted.
TPMT_SYM_DEF_OBJECT+	symmetricAlg	definition for the symmetric algorithm to be used for the inner wrapper may be TPM_ALG_NULL if no inner wrapper is applied

Table 38 — TPM2\_Duplicate Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DATA	encryptionKeyOut	If the caller provided an encryption key or if <i>symmetricAlg</i> was TPM_ALG_NULL, then this will be the Empty Buffer; otherwise, it shall contain the TPM-generated, symmetric encryption key for the inner wrapper.
TPM2B_PRIVATE	duplicate	private area that may be encrypted by <i>encryptionKeyIn</i> ; and may be doubly encrypted
TPM2B_ENCRYPTED_SECRET	outSymSeed	seed protected by the asymmetric algorithms of new parent (NP)

### 13.1.3 Detailed Actions

[[Duplicate]]

## 13.2 TPM2\_Rewrap

### 13.2.1 General Description

This command allows the TPM to serve in the role as a Duplication Authority. If proper authorization for use of the *oldParent* is provided, then an HMAC key and a symmetric key are recovered from *inSymSeed* and used to integrity check and decrypt *inDuplicate*. A new protection seed value is generated according to the methods appropriate for *newParent* and the blob is re-encrypted and a new integrity value is computed. The re-encrypted blob is returned in *outDuplicate* and the symmetric key returned in *outSymKey*.

In the rewrap process, L is “DUPLICATE” (see “Terms and Definitions” in TPM 2.0 Part 1).

If *inSymSeed* has a zero length, then *oldParent* is required to be TPM\_RH\_NULL and no decryption of *inDuplicate* takes place.

If *newParent* is TPM\_RH\_NULL, then no encryption is performed on *outDuplicate*. *outSymSeed* will have a zero length. See TPM 2.0 Part 2 *encryptedDuplication*.

## 13.2.2 Command and Response

Table 39 — TPM2\_Rewrap Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Rewrap
TPMI_DH_OBJECT+	@oldParent	parent of object Auth Index: 1 Auth Role: User
TPMI_DH_OBJECT+	newParent	new parent of the object Auth Index: None
TPM2B_PRIVATE	inDuplicate	an object encrypted using symmetric key derived from <i>inSymSeed</i>
TPM2B_NAME	name	the Name of the object being rewrapped
TPM2B_ENCRYPTED_SECRET	inSymSeed	the seed for the symmetric key and HMAC key needs <i>oldParent</i> private key to recover the seed and generate the symmetric key

Table 40 — TPM2\_Rewrap Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PRIVATE	outDuplicate	an object encrypted using symmetric key derived from <i>outSymSeed</i>
TPM2B_ENCRYPTED_SECRET	outSymSeed	seed for a symmetric key protected by <i>newParent</i> asymmetric key

### 13.2.3 Detailed Actions

[[Rewrap]]

### 13.3 TPM2\_Import

#### 13.3.1 General Description

This command allows an object to be encrypted using the symmetric encryption values of a Storage Key. After encryption, the object may be loaded and used in the new hierarchy. The imported object (*duplicate*) may be singly encrypted, multiply encrypted, or unencrypted.

If *fixedTPM* or *fixedParent* is SET in *objectPublic*, the TPM shall return TPM\_RC\_ATTRIBUTES.

If *encryptedDuplication* is SET in the object referenced by *parentHandle*, then *encryptedDuplication* shall be SET in *objectPublic* (TPM\_RC\_ATTRIBUTES).

If *encryptedDuplication* is SET in *objectPublic*, then *inSymSeed* and *encryptionKey* shall not be Empty buffers (TPM\_RC\_ATTRIBUTES). Recovery of the sensitive data of the object occurs in the TPM in a multi-step process in the following order:

a) If *inSymSeed* has a non-zero size:

- 1) The asymmetric parameters and private key of *parentHandle* are used to recover the seed used in the creation of the HMAC key and encryption keys used to protect the duplication blob.

NOTE 1 When recovering the seed from *inSymSeed*, *L* is "DUPLICATE".

- 2) The integrity value in *duplicate.buffer.integrityOuter* is used to verify the integrity of the data blob, which is the remainder of *duplicate.buffer* (TPM\_RC\_INTEGRITY).

NOTE 2 The data blob will contain a TPMT\_SENSITIVE and may contain a TPM2B\_DIGEST for the *innerIntegrity*.

- 3) The symmetric key recovered in 1) is used to decrypt the data blob.

NOTE 3 Checking the integrity before the data is used prevents attacks on the sensitive area by fuzzing the data and looking at the differences in the response codes.

b) If *encryptionKey* is not an Empty Buffer:

- 1) Use *encryptionKey* to decrypt the inner blob.
- 2) Use the TPM2B\_DIGEST at the start of the inner blob to verify the integrity of the inner blob (TPM\_RC\_INTEGRITY).

c) Unmarshal the sensitive area

NOTE 4 It is not necessary to validate that the sensitive area data is cryptographically bound to the public area other than that the Name of the public area is included in the HMAC. However, if the binding is not validated by this command, the binding must be checked each time the object is loaded. For an object that is imported under a parent with *fixedTPM* SET, binding need only be checked at import. If the parent has *fixedTPM* CLEAR, then the binding needs to be checked each time the object is loaded, or before the TPM performs an operation for which the binding affects the outcome of the operation (for example, TPM2\_PolicySigned() or TPM2\_Certify()).

Similarly, if the new parent's *fixedTPM* is set, the *encryptedDuplication* state need only be checked at import.

If the new parent is not *fixedTPM*, then that object will be loadable on any TPM (including SW versions) on which the new parent exists. This means that, each time an object is loaded under a parent that is not *fixedTPM*, it is necessary to validate all of the properties of that object. If the parent is *fixedTPM*, then the new private blob is integrity protected by the TPM that "owns" the parent. So, it is sufficient to validate the object's properties (attribute and public-private binding) on import and not again.

If a weak symmetric key is being imported, the TPM shall return TPM\_RC\_KEY.

After integrity checks and decryption, the TPM will create a new symmetrically encrypted private area using the encryption key of the parent.

NOTE 5            The symmetric re-encryption is the normal integrity generation and symmetric encryption applied to a child object.



## 13.3.2 Command and Response

Table 41 — TPM2\_Import Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Import
TPMI_DH_OBJECT	@parentHandle	the handle of the new parent for the object Auth Index: 1 Auth Role: USER
TPM2B_DATA	encryptionKey	the optional symmetric encryption key used as the inner wrapper for <i>duplicate</i> If <i>symmetricAlg</i> is TPM_ALG_NULL, then this parameter shall be the Empty Buffer.
TPM2B_PUBLIC	objectPublic	the public area of the object to be imported This is provided so that the integrity value for <i>duplicate</i> and the object attributes can be checked. NOTE Even if the integrity value of the object is not checked on input, the object Name is required to create the integrity value for the imported object.
TPM2B_PRIVATE	duplicate	the symmetrically encrypted duplicate object that may contain an inner symmetric wrapper
TPM2B_ENCRYPTED_SECRET	inSymSeed	the seed for the symmetric key and HMAC key <i>inSymSeed</i> is encrypted/encoded using the algorithms of <i>newParent</i> .
TPMT_SYM_DEF_OBJECT+	symmetricAlg	definition for the symmetric algorithm to use for the inner wrapper If this algorithm is TPM_ALG_NULL, no inner wrapper is present and <i>encryptionKey</i> shall be the Empty Buffer.

Table 42 — TPM2\_Import Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PRIVATE	outPrivate	the sensitive area encrypted with the symmetric key of <i>parentHandle</i>

### 13.3.3 Detailed Actions

`[[Import]]`

## 14 Asymmetric Primitives

### 14.1 Introduction

The commands in this clause provide low-level primitives for access to the asymmetric algorithms implemented in the TPM. Many of these commands are only allowed if the asymmetric key is an unrestricted key.

### 14.2 TPM2\_RSA\_Encrypt

#### 14.2.1 General Description

This command performs RSA encryption using the indicated padding scheme according to IETF RFC 3447. If the *scheme* of *keyHandle* is TPM\_ALG\_NULL, then the caller may use *inScheme* to specify the padding scheme. If *scheme* of *keyHandle* is not TPM\_ALG\_NULL, then *inScheme* shall either be TPM\_ALG\_NULL or be the same as *scheme* (TPM\_RC\_SCHEME).

The key referenced by *keyHandle* is required to be an RSA key (TPM\_RC\_KEY).

The three types of allowed padding are:

- 1) TPM\_ALG\_OAEP – Data is OAEP padded as described in 7.1 of IETF RFC 3447 (PKCS#1). The only supported mask generation is MGF1.
- 2) TPM\_ALG\_RSAES – Data is padded as described in 7.2 of IETF RFC 3447 (PKCS#1).
- 3) TPM\_ALG\_NULL – Data is not padded by the TPM and the TPM will treat *message* as an unsigned integer and perform a modular exponentiation of *message* using the public exponent of the key referenced by *keyHandle*. This scheme is only used if both the *scheme* in the key referenced by *keyHandle* is TPM\_ALG\_NULL, and the *inScheme* parameter of the command is TPM\_ALG\_NULL. The input value cannot be larger than the public modulus of the key referenced by *keyHandle*.

**Table 43 — Padding Scheme Selection**

<i>keyHandle</i> → <i>scheme</i>	<i>inScheme</i>	padding scheme used
TPM_ALG_NULL	TPM_ALG_NULL	none
	TPM_ALG_RSAES	RSAES
	TPM_ALG_OAEP	OAEP
TPM_ALG_RSAES	TPM_ALG_NULL	RSAES
	TPM_ALG_RSAES	RSAES
	TPM_ALG_OAEP	error (TPM_RC_SCHEME)
TPM_ALG_OAEP	TPM_ALG_NULL	OAEP
	TPM_ALG_RSAES	error (TPM_RC_SCHEME)
	TPM_ALG_OAEP	OAEP

After padding, the data is RSAEP encrypted according to 5.1.1 of IETF RFC 3447 (PKCS#1).

If *inScheme* is used, and the scheme requires a hash algorithm it may not be TPM\_ALG\_NULL.

NOTE 1 Because only the public portion of the key needs to be loaded for this command, the caller can manipulate the attributes of the key in any way desired. As a result, the TPM shall not check the consistency of the attributes. The only property checking is that the key is an RSA key and that the padding scheme is supported.

The *message* parameter is limited in size by the padding scheme according to the following table:

**Table 44 — Message Size Limits Based on Padding**

Scheme	Maximum Message Length ( <i>mLen</i> ) in Octets	Comments
TPM_ALG_OAEP	$mLen \leq k - 2hLen - 2$	
TPM_ALG_RSAES	$mLen \leq k - 11$	
TPM_ALG_NULL	$mLen \leq k$	The numeric value of the message must be less than the numeric value of the public modulus ( <i>n</i> ).
NOTES		
1) <i>k</i> := the number of bytes in the public modulus		
2) <i>hLen</i> := the number of octets in the digest produced by the hash algorithm used in the process		

The *label* parameter is optional. If provided (*label.size* != 0) then the TPM shall return TPM\_RC\_VALUE if the last octet in *label* is not zero. If a zero octet occurs before *label.buffer[label.size-1]*, the TPM shall truncate the label at that point. The terminating octet of zero is included in the *label* used in the padding scheme.

NOTE 2            If the scheme does not use a label, the TPM will still verify that label is properly formatted if label is present.

The function returns padded and encrypted value *outData*.

The *message* parameter in the command may be encrypted using parameter encryption.

NOTE 3            Only the public area of *keyHandle* is required to be loaded. A public key may be loaded with any desired scheme. If the scheme is to be changed, a different public area must be loaded.

## 14.2.2 Command and Response

Table 45 — TPM2\_RSA\_Encrypt Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, encrypt, or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_RSA_Encrypt
TPMI_DH_OBJECT	keyHandle	reference to public portion of RSA key to use for encryption Auth Index: None
TPM2B_PUBLIC_KEY_RSA	message	message to be encrypted NOTE 1 The data type was chosen because it limits the overall size of the input to no greater than the size of the largest RSA public key. This may be larger than allowed for <i>keyHandle</i> .
TPMT_RSA_DECRYPT+	inScheme	the padding scheme to use if <i>scheme</i> associated with <i>keyHandle</i> is TPM_ALG_NULL
TPM2B_DATA	label	optional label <i>L</i> to be associated with the message Size of the buffer is zero if no label is present NOTE 2 See description of label above.

Table 46 — TPM2\_RSA\_Encrypt Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PUBLIC_KEY_RSA	outData	encrypted output

### 14.2.3 Detailed Actions

**[[RSA\_Encrypt]]**

## 14.3 TPM2\_RSA\_Decrypt

### 14.3.1 General Description

This command performs RSA decryption using the indicated padding scheme according to IETF RFC 3447 ((PKCS#1).

The scheme selection for this command is the same as for TPM2\_RSA\_Encrypt() and is shown in Table 43.

The key referenced by *keyHandle* shall be an RSA key (TPM\_RC\_KEY) with *restricted* CLEAR and *decrypt* SET (TPM\_RC\_ATTRIBUTES).

This command uses the private key of *keyHandle* for this operation and authorization is required.

The TPM will perform a modular exponentiation of ciphertext using the private exponent associated with *keyHandle* (this is described in IETF RFC 3447 (PKCS#1), clause 5.1.2). It will then validate the padding according to the selected scheme. If the padding checks fail, TPM\_RC\_VALUE is returned. Otherwise, the data is returned with the padding removed. If no padding is used, the returned value is an unsigned integer value that is the result of the modular exponentiation of *cipherText* using the private exponent of *keyHandle*. The returned value may include leading octets zeros so that it is the same size as the public modulus. For the other padding schemes, the returned value will be smaller than the public modulus but will contain all the data remaining after padding is removed and this may include leading zeros if the original encrypted value contained leading zeros.

If a label is used in the padding process of the scheme during encryption, the *label* parameter is required to be present in the decryption process and *label* is required to be the same in both cases. If label is not the same, the decrypt operation is very likely to fail ((TPM\_RC\_VALUE). If *label* is present (*label.size* != 0), it shall be a NULL-terminated string or the TPM will return TPM\_RC\_VALUE.

NOTE 1            The size of *label* includes the terminating null.

The *message* parameter in the response may be encrypted using parameter encryption.

If *inScheme* is used, and the scheme requires a hash algorithm it may not be TPM\_ALG\_NULL.

If the scheme does not require a label, the value in *label* is not used but the size of the label field is checked for consistency with the indicated data type (TPM2B\_DATA). That is, the field may not be larger than allowed for a TPM2B\_DATA.

14.3.2 Command and Response

Table 47 — TPM2\_RSA\_Decrypt Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_RSA_Decrypt
TPMI_DH_OBJECT	@keyHandle	RSA key to use for decryption Auth Index: 1 Auth Role: USER
TPM2B_PUBLIC_KEY_RSA	cipherText	cipher text to be decrypted NOTE An encrypted RSA data block is the size of the public modulus.
TPMT_RSA_DECRYPT+	inScheme	the padding scheme to use if <i>scheme</i> associated with <i>keyHandle</i> is TPM_ALG_NULL
TPM2B_DATA	label	label whose association with the message is to be verified

Table 48 — TPM2\_RSA\_Decrypt Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_PUBLIC_KEY_RSA	message	decrypted output



### 14.3.3 Detailed Actions

`[[RSA_Decrypt]]`

## 14.4 TPM2\_ECDH\_KeyGen

### 14.4.1 General Description

This command uses the TPM to generate an ephemeral key pair  $(d_e, Q_e$  where  $Q_e := [d_e]G$ ). It uses the private ephemeral key and a loaded public key ( $Q_S$ ) to compute the shared secret value ( $P := [hd_e]Q_S$ ).

*keyHandle* shall refer to a loaded, ECC key (TPM\_RC\_KEY). The sensitive portion of this key need not be loaded.

The curve parameters of the loaded ECC key are used to generate the ephemeral key.

NOTE            This function is the equivalent of encrypting data to another object's public key. The *seed* value is used in a KDF to generate a symmetric key and that key is used to encrypt the data. Once the data is encrypted and the symmetric key discarded, only the object with the private portion of the *keyHandle* will be able to decrypt it.

The *zPoint* in the response may be encrypted using parameter encryption.

14.4.2 Command and Response

Table 49 — TPM2\_ECDH\_KeyGen Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ECDH_KeyGen
TPMI_DH_OBJECT	keyHandle	Handle of a loaded ECC key public area. Auth Index: None

Table 50 — TPM2\_ECDH\_KeyGen Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ECC_POINT	zPoint	results of $P := h[d_e]Q_s$
TPM2B_ECC_POINT	pubPoint	generated ephemeral public point ( $Q_e$ )

### 14.4.3 Detailed Actions

**[ [ECDH\_KeyGen] ]**

## 14.5 TPM2\_ECDH\_ZGen

### 14.5.1 General Description

This command uses the TPM to recover the  $Z$  value from a public point ( $Q_B$ ) and a private key ( $d_s$ ). It will perform the multiplication of the provided *inPoint* ( $Q_B$ ) with the private key ( $d_s$ ) and return the coordinates of the resultant point ( $Z = (x_Z, y_Z) := [hd_s]Q_B$ ; where  $h$  is the cofactor of the curve).

*keyHandle* shall refer to a loaded, ECC key (TPM\_RC\_KEY) with the *restricted* attribute CLEAR and the *decrypt* attribute SET (TPM\_RC\_ATTRIBUTES).

NOTE While TPM\_RC\_ATTRIBUTES is preferred, TPM\_RC\_KEY is acceptable.

The *scheme* of the key referenced by *keyHandle* is required to be either TPM\_ALG\_ECDH or TPM\_ALG\_NULL (TPM\_RC\_SCHEME).

*inPoint* is required to be on the curve of the key referenced by *keyHandle* (TPM\_RC\_ECC\_POINT).

The parameters of the key referenced by *keyHandle* are used to perform the point multiplication.

14.5.2 Command and Response

Table 51 — TPM2\_ECDH\_ZGen Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ECDH_ZGen
TPMI_DH_OBJECT	@keyHandle	handle of a loaded ECC key Auth Index: 1 Auth Role: USER
TPM2B_ECC_POINT	inPoint	a public key

Table 52 — TPM2\_ECDH\_ZGen Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ECC_POINT	outPoint	X and Y coordinates of the product of the multiplication $Z = (x_Z, y_Z) := [hd_s]Q_B$

### 14.5.3 Detailed Actions

**[ [ECDH\_ZGen] ]**

## 14.6 TPM2\_ECC\_Parameters

### 14.6.1 General Description

This command returns the parameters of an ECC curve identified by its TCG-assigned *curveID*.



## 14.6.2 Command and Response

Table 53 — TPM2\_ECC\_Parameters Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ECC_Parameters
TPMI_ECC_CURVE	curveID	parameter set selector

Table 54 — TPM2\_ECC\_Parameters Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMS_ALGORITHM_DETAIL_ECC	parameters	ECC parameters for the selected curve

### 14.6.3 Detailed Actions

**[[ECC\_Parameters]]**

## 14.7 TPM2\_ZGen\_2Phase

### 14.7.1 General Description

This command supports two-phase key exchange protocols. The command is used in combination with TPM2\_EC\_Ephemeral(). TPM2\_EC\_Ephemeral() generates an ephemeral key and returns the public point of that ephemeral key along with a numeric value that allows the TPM to regenerate the associated private key.

The input parameters for this command are a static public key ( $inQsU$ ), an ephemeral key ( $inQeU$ ) from party B, and the *commitCounter* returned by TPM2\_EC\_Ephemeral(). The TPM uses the counter value to regenerate the ephemeral private key ( $d_{e,v}$ ) and the associated public key ( $Q_{e,v}$ ). *keyA* provides the static ephemeral elements  $d_{s,v}$  and  $Q_{s,v}$ . This provides the two pairs of ephemeral and static keys that are required for the schemes supported by this command.

The TPM will compute  $Z$  or  $Z_s$  and  $Z_e$  according to the selected scheme. If the scheme is not a two-phase key exchange scheme or if the scheme is not supported, the TPM will return TPM\_RC\_SCHEME.

It is an error if  $inQsB$  or  $inQeB$  are not on the curve of *keyA* (TPM\_RC\_ECC\_POINT).

The two-phase key schemes that were assigned an algorithm ID as of the time of the publication of this specification are TPM\_ALG\_ECDH, TPM\_ALG\_ECMQV, and TPM\_ALG\_SM2.

If this command is supported, then support for TPM\_ALG\_ECDH is required. Support for TPM\_ALG\_ECMQV or TPM\_ALG\_SM2 is optional.

NOTE 1 If SM2 is supported and this command is supported, then the implementation is required to support the key exchange protocol of SM2, part 3.

For TPM\_ALG\_ECDH *outZ1* will be  $Z_s$  and *outZ2* will be  $Z_e$  as defined in 6.1.1.2 of SP800-56A.

NOTE 2 An unrestricted decryption key using ECDH may be used in either TPM2\_ECDH\_ZGen() or TPM2\_ZGen\_2Phase as the computation done with the private part of *keyA* is the same in both cases.

For TPM\_ALG\_ECMQV or TPM\_ALG\_SM2 *outZ1* will be  $Z$  and *outZ2* will be an Empty Point.

NOTE 3 An Empty Point has two Empty Buffers as coordinates meaning the minimum *size* value for *outZ2* will be four.

If the input scheme is TPM\_ALG\_ECDH, then *outZ1* will be  $Z_s$  and *outZ2* will be  $Z_e$ . For schemes like MQV (including SM2), *outZ1* will contain the computed value and *outZ2* will be an Empty Point.

NOTE 4 The  $Z$  values returned by the TPM are a full point and not just an x-coordinate.

If a computation of either  $Z$  produces the point at infinity, then the corresponding  $Z$  value will be an Empty Point.

## 14.7.2 Command and Response

Table 55 — TPM2\_ZGen\_2Phase Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ZGen_2Phase
TPMI_DH_OBJECT	@keyA	handle of an unrestricted decryption key ECC The private key referenced by this handle is used as $d_{S,A}$ Auth Index: 1 Auth Role: USER
TPM2B_ECC_POINT	inQsB	other party's static public key ( $Q_{s,B} = (X_{s,B}, Y_{s,B})$ )
TPM2B_ECC_POINT	inQeB	other party's ephemeral public key ( $Q_{e,B} = (X_{e,B}, Y_{e,B})$ )
TPMI_ECC_KEY_EXCHANGE	inScheme	the key exchange scheme
UINT16	counter	value returned by TPM2_EC_Ephemeral()

Table 56 — TPM2\_ZGen\_2Phase Response

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ECC_POINT	outZ1	X and Y coordinates of the computed value (scheme dependent)
TPM2B_ECC_POINT	outZ2	X and Y coordinates of the second computed value (scheme dependent)

### 14.7.3 Detailed Actions

**[[ZGen\_2Phase]]**

## 15 Symmetric Primitives

### 15.1 Introduction

The commands in this clause provide low-level primitives for access to the symmetric algorithms implemented in the TPM that operate on blocks of data. These include symmetric encryption and decryption as well as hash and HMAC. All of the commands in this group are stateless. That is, they have no persistent state that is retained in the TPM when the command is complete.

For hashing, HMAC, and Events that require large blocks of data with retained state, the sequence commands are provided (see clause 17).

Some of the symmetric encryption/decryption modes use an IV. When an IV is used, it may be an initiation value or a chained value from a previous stage. The chaining for each mode is:

Table 57 — Symmetric Chaining Process

Mode	Chaining process
TPM_ALG_CTR	<p>The TPM will increment the entire IV provided by the caller. The next count value will be returned to the caller as <i>ivOut</i>. This can be the input value to the next encrypt or decrypt operation.</p> <p><i>ivIn</i> is required to be the size of a block encrypted by the selected algorithm and key combination. If the size of <i>ivIn</i> is not correct, the TPM shall return TPM_RC_SIZE.</p> <p>EXAMPLE 1 AES requires that <i>ivIn</i> be 128 bits (16 octets).</p> <p><i>ivOut</i> will be the size of a cipher block and not the size of the last encrypted block.</p> <p>NOTE <i>ivOut</i> will be the value of the counter after the last block is encrypted.</p> <p>EXAMPLE 2 If <i>ivIn</i> were 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<sub>16</sub> and four data blocks were encrypted, <i>ivOut</i> will have a value of 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04<sub>16</sub>.</p> <p>All the bits of the IV are incremented as if it were an unsigned integer.</p>
TPM_ALG_OFB	<p>In Output Feedback (OFB), the output of the pseudo-random function (the block encryption algorithm) is XORed with a plaintext block to produce a ciphertext block. <i>ivOut</i> will be the value that was XORed with the last plaintext block. That value can be used as the <i>ivIn</i> for a next buffer.</p> <p><i>ivIn</i> is required to be the size of a block encrypted by the selected algorithm and key combination. If the size of <i>ivIn</i> is not correct, the TPM shall return TPM_RC_SIZE.</p> <p><i>ivOut</i> will be the size of a cipher block and not the size of the last encrypted block.</p>
TPM_ALG_CBC	<p>For Cipher Block Chaining (CBC), a block of ciphertext is XORed with the next plaintext block and that block is encrypted. The encrypted block is then input to the encryption of the next block. The last ciphertext block then is used as an IV for the next buffer.</p> <p>Even though the last ciphertext block is evident in the encrypted data, it is also returned in <i>ivOut</i>.</p> <p><i>ivIn</i> is required to be the size of a block encrypted by the selected algorithm and key combination. If the size of <i>ivIn</i> is not correct, the TPM shall return TPM_RC_SIZE.</p> <p><i>inData</i> is required to be an even multiple of the block encrypted by the selected algorithm and key combination. If the size of <i>inData</i> is not correct, the TPM shall return TPM_RC_SIZE.</p>
TPM_ALG_CFB	<p>Similar to CBC in that the last ciphertext block is an input to the encryption of the next block. <i>ivOut</i> will be the value that was XORed with the last plaintext block. That value can be used as the <i>ivIn</i> for a next buffer.</p> <p><i>ivIn</i> is required to be the size of a block encrypted by the selected algorithm and key combination. If the size of <i>ivIn</i> is not correct, the TPM shall return TPM_RC_SIZE.</p> <p><i>ivOut</i> will be the size of a cipher block and not the size of the last encrypted block.</p>
TPM_ALG_ECB	<p>Electronic Codebook (ECB) has no chaining. Each block of plaintext is encrypted using the key. ECB does not support chaining and <i>ivIn</i> shall be the Empty Buffer. <i>ivOut</i> will be the Empty Buffer.</p> <p><i>inData</i> is required to be an even multiple of the block encrypted by the selected algorithm and key combination. If the size of <i>inData</i> is not correct, the TPM shall return TPM_RC_SIZE.</p>

## 15.2 TPM2\_EncryptDecrypt

### 15.2.1 General Description

NOTE 1 This command is deprecated, and TPM2\_EncryptDecrypt2() is preferred. This should be reflected in platform-specific specifications.

This command performs symmetric encryption or decryption using the symmetric key referenced by *keyHandle* and the selected mode.

*keyHandle* shall reference a symmetric cipher object (TPM\_RC\_KEY) with the *restricted* attribute CLEAR (TPM\_RC\_ATTRIBUTES).

If the *decrypt* parameter of the command is TRUE, then the *decrypt* attribute of the key is required to be SET (TPM\_RC\_ATTRIBUTES). If the *decrypt* parameter of the command is FALSE, then the *sign* attribute of the key is required to be SET (TPM\_RC\_ATTRIBUTES).

NOTE 2 A key may have both *decrypt* and *sign* SET.

If the mode of the key is not TPM\_ALG\_NULL, then that is the only mode that can be used with the key and the caller is required to set *mode* either to TPM\_ALG\_NULL or to the same mode as the key (TPM\_RC\_MODE). If the mode of the key is TPM\_ALG\_NULL, then the caller may set *mode* to any valid symmetric encryption/decryption mode but may not select TPM\_ALG\_NULL (TPM\_RC\_MODE).

If the TPM allows this command to be canceled before completion, then the TPM may produce incremental results and return TPM\_RC\_SUCCESS rather than TPM\_RC\_CANCELED. In such case, *outData* may be less than *inData*.

NOTE 3 If all the data is encrypted/decrypted, the size of *outData* will be the same as *inData*.



15.2.2 Command and Response

**Table 58 — TPM2\_EncryptDecrypt Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_EncryptDecrypt
TPMI_DH_OBJECT	@keyHandle	the symmetric key used for the operation Auth Index: 1 Auth Role: USER
TPMI_YES_NO	decrypt	if YES, then the operation is decryption; if NO, the operation is encryption
TPMI_ALG_SYM_MODE+	mode	symmetric mode this field shall match the default mode of the key or be TPM_ALG_NULL.
TPM2B_IV	ivIn	an initial value as required by the algorithm
TPM2B_MAX_BUFFER	inData	the data to be encrypted/decrypted

**Table 59 — TPM2\_EncryptDecrypt Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_MAX_BUFFER	outData	encrypted or decrypted output
TPM2B_IV	ivOut	chaining value to use for IV in next round

### 15.2.3 Detailed Actions

`[[EncryptDecrypt]]`

## 15.3 TPM2\_EncryptDecrypt2

### 15.3.1 General Description

This command is identical to TPM2\_EncryptDecrypt(), except that the *inData* parameter is the first parameter. This permits *inData* to be parameter encrypted.

NOTE            In platform specification updates, this command is preferred and TPM2\_EncryptDecrypt() should be deprecated.

## 15.3.2 Command and Response

Table 60 — TPM2\_EncryptDecrypt2 Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_EncryptDecrypt2
TPMI_DH_OBJECT	@keyHandle	the symmetric key used for the operation Auth Index: 1 Auth Role: USER
TPM2B_MAX_BUFFER	inData	the data to be encrypted/decrypted
TPMI_YES_NO	decrypt	if YES, then the operation is decryption; if NO, the operation is encryption
TPMI_ALG_SYM_MODE+	mode	symmetric mode this field shall match the default mode of the key or be TPM_ALG_NULL.
TPM2B_IV	ivIn	an initial value as required by the algorithm

Table 61 — TPM2\_EncryptDecrypt2 Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_MAX_BUFFER	outData	encrypted or decrypted output
TPM2B_IV	ivOut	chaining value to use for IV in next round

### 15.3.3 Detailed Actions

`[[EncryptDecrypt2]]`

## 15.4 TPM2\_Hash

### 15.4.1 General Description

This command performs a hash operation on a data buffer and returns the results.

NOTE If the data buffer to be hashed is larger than will fit into the TPM's input buffer, then the sequence hash commands will need to be used.

If the results of the hash will be used in a signing operation that uses a restricted signing key, then the ticket returned by this command can indicate that the hash is safe to sign.

If the digest is not safe to sign, then the TPM will return a TPMT\_TK\_HASHCHECK with the hierarchy set to TPM\_RH\_NULL and *digest* set to the Empty Buffer.

If *hierarchy* is TPM\_RH\_NULL, then *digest* in the ticket will be the Empty Buffer.

## 15.4.2 Command and Response

Table 62 — TPM2\_Hash Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, decrypt, or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Hash
TPM2B_MAX_BUFFER	data	data to be hashed
TPMI_ALG_HASH	hashAlg	algorithm for the hash being computed – shall not be TPM_ALG_NULL
TPMI_RH_HIERARCHY+	hierarchy	hierarchy to use for the ticket (TPM_RH_NULL allowed)

Table 63 — TPM2\_Hash Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	outHash	results
TPMT_TK_HASHCHECK	validation	ticket indicating that the sequence of octets used to compute <i>outDigest</i> did not start with TPM_GENERATED_VALUE will be a NULL ticket if the digest may not be signed with a restricted key

### 15.4.3 Detailed Actions

[ [HASH] ]



## 15.5 TPM2\_HMAC

### 15.5.1 General Description

This command performs an HMAC on the supplied data using the indicated hash algorithm.

The caller shall provide proper authorization for use of *handle*.

If the *sign* attribute is not SET in the key referenced by *handle* then the TPM shall return TPM\_RC\_KEY. If the key type is not TPM\_ALG\_KEYEDHASH then the TPM shall return TPM\_RC\_TYPE. If the key referenced by *handle* has the *restricted* attribute SET, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE 1 For symmetric signing with a restricted key, see TPM2\_Sign.

If the default scheme of the key referenced by *handle* is not TPM\_ALG\_NULL, then the *hashAlg* parameter is required to be either the same as the key's default or TPM\_ALG\_NULL (TPM\_RC\_VALUE). If the default scheme of the key is TPM\_ALG\_NULL, then *hashAlg* is required to be a valid hash and not TPM\_ALG\_NULL (TPM\_RC\_VALUE). (See hash selection matrix in

Table 70.)

NOTE 2 A key may only have both *sign* and *decrypt* SET if the key is unrestricted. When both *sign* and *decrypt* are set, there is no default scheme for the key and the hash algorithm must be specified.

15.5.2 Command and Response

Table 64 — TPM2\_HMAC Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_HMAC
TPMI_DH_OBJECT	@handle	handle for the symmetric signing key providing the HMAC key Auth Index: 1 Auth Role: USER
TPM2B_MAX_BUFFER	buffer	HMAC data
TPMI_ALG_HASH+	hashAlg	algorithm to use for HMAC

Table 65 — TPM2\_HMAC Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	outHMAC	the returned HMAC in a sized buffer

### 15.5.3 Detailed Actions

[ [HMAC] ]

## 16 Random Number Generator

### 16.1 TPM2\_GetRandom

#### 16.1.1 General Description

This command returns the next *bytesRequested* octets from the random number generator (RNG).

NOTE 1 It is recommended that a TPM implement the RNG in a manner that would allow it to return RNG octets such that, as long as the value of *bytesRequested* is not greater than the maximum digest size, the frequency of *bytesRequested* being more than the number of octets available is an infrequent occurrence.

If *bytesRequested* is more than will fit into a TPM2B\_DIGEST on the TPM, no error is returned but the TPM will only return as much data as will fit into a TPM2B\_DIGEST buffer for the TPM.

NOTE 2 TPM2B\_DIGEST is large enough to hold the largest digest that may be produced by the TPM. Because that digest size changes according to the implemented hashes, the maximum amount of data returned by this command is TPM implementation-dependent.

## 16.1.2 Command and Response

Table 66 — TPM2\_GetRandom Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetRandom
UINT16	bytesRequested	number of octets to return

Table 67 — TPM2\_GetRandom Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	randomBytes	the random octets

### 16.1.3 Detailed Actions

`[[GetRandom]]`

## 16.2 TPM2\_StirRandom

### 16.2.1 General Description

This command is used to add "additional information" to the RNG state.

NOTE           The "additional information" is as defined in SP800-90A.

The *inData* parameter may not be larger than 128 octets.

## 16.2.2 Command and Response

Table 68 — TPM2\_StirRandom Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_StirRandom {NV}
TPM2B_SENSITIVE_DATA	inData	additional information

Table 69 — TPM2\_StirRandom Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 16.2.3 Detailed Actions

**[[StirRandom]]**

## 17 Hash/HMAC/Event Sequences

### 17.1 Introduction

All of the commands in this group are to support sequences for which an intermediate state must be maintained. For a description of sequences, see “Hash, HMAC, and Event Sequences” in TPM 2.0 Part 1.

### 17.2 TPM2\_HMAC\_Start

#### 17.2.1 General Description

This command starts an HMAC sequence. The TPM will create and initialize an HMAC sequence structure, assign a handle to the sequence, and set the *authValue* of the sequence object to the value in *auth*.

NOTE 1 The structure of a sequence object is vendor-dependent.

The caller shall provide proper authorization for use of *handle*.

If the *sign* attribute is not SET in the key referenced by *handle* then the TPM shall return TPM\_RC\_KEY. If the key type is not TPM\_ALG\_KEYEDHASH then the TPM shall return TPM\_RC\_TYPE. If the key referenced by *handle* has the *restricted* attribute SET, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE 2 For symmetric signing with a restricted key, see TPM2\_Sign.

If the default scheme of the key referenced by *handle* is not TPM\_ALG\_NULL, then the *hashAlg* parameter is required to be either the same as the key's default or TPM\_ALG\_NULL (TPM\_RC\_VALUE). If the default scheme of the key is TPM\_ALG\_NULL, then *hashAlg* is required to be a valid hash and not TPM\_ALG\_NULL (TPM\_RC\_VALUE).

**Table 70 — Hash Selection Matrix**

<i>handle</i> → <i>restricted</i> (key's restricted attribute)	<i>handle</i> → <i>scheme</i> (hash algorithm from key's scheme)	<i>hashAlg</i>	hash used
CLEAR (unrestricted)	TPM_ALG_NULL <sup>(1)</sup>	TPM_ALG_NULL	error <sup>(1)</sup> (TPM_RC_VALUE)
CLEAR	TPM_ALG_NULL	valid hash	<i>hashAlg</i>
CLEAR	valid hash	TPM_ALG_NULL or same as <i>handle</i> → <i>scheme</i>	<i>handle</i> → <i>scheme</i>
CLEAR	valid hash	valid hash	error (TPM_RC_VALUE) if <i>hashAlg</i> != <i>handle</i> → <i>scheme</i>
SET (restricted)	don't care	don't care	TPM_RC_ATTRIBUTES
NOTES:			
1) A hash algorithm is required for the HMAC.			

17.2.2 Command and Response

Table 71 — TPM2\_HMAC\_Start Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_HMAC_Start
TPMI_DH_OBJECT	@handle	handle of an HMAC key Auth Index: 1 Auth Role: USER
TPM2B_AUTH	auth	authorization value for subsequent use of the sequence
TPMI_ALG_HASH+	hashAlg	the hash algorithm to use for the HMAC

Table 72 — TPM2\_HMAC\_Start Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_DH_OBJECT	sequenceHandle	a handle to reference the sequence

### 17.2.3 Detailed Actions

`[[HMAC_Start]]`

### 17.3 TPM2\_HashSequenceStart

#### 17.3.1 General Description

This command starts a hash or an Event Sequence. If *hashAlg* is an implemented hash, then a hash sequence is started. If *hashAlg* is TPM\_ALG\_NULL, then an Event Sequence is started. If *hashAlg* is neither an implemented algorithm nor TPM\_ALG\_NULL, then the TPM shall return TPM\_RC\_HASH.

Depending on *hashAlg*, the TPM will create and initialize a Hash Sequence context or an Event Sequence context. Additionally, it will assign a handle to the context and set the *authValue* of the context to the value in *auth*. A sequence context for an Event (*hashAlg* = TPM\_ALG\_NULL) contains a hash context for each of the PCR banks implemented on the TPM.

17.3.2 Command and Response

Table 73 — TPM2\_HashSequenceStart Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_HashSequenceStart
TPM2B_AUTH	auth	authorization value for subsequent use of the sequence
TPMI_ALG_HASH+	hashAlg	the hash algorithm to use for the hash sequence An Event Sequence starts if this is TPM_ALG_NULL.

Table 74 — TPM2\_HashSequenceStart Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_DH_OBJECT	sequenceHandle	a handle to reference the sequence

### 17.3.3 Detailed Actions

**[[HashSequenceStart]]**

## 17.4 TPM2\_SequenceUpdate

### 17.4.1 General Description

This command is used to add data to a hash or HMAC sequence. The amount of data in buffer may be any size up to the limits of the TPM.

NOTE 1 In all TPM, a *buffer* size of 1,024 octets is allowed.

Proper authorization for the sequence object associated with *sequenceHandle* is required. If an authorization or audit of this command requires computation of a *cpHash* and an *rpHash*, the Name associated with *sequenceHandle* will be the Empty Buffer.

If the command does not return TPM\_RC\_SUCCESS, the state of the sequence is unmodified.

If the sequence is intended to produce a digest that will be signed by a restricted signing key, then the first block of data shall contain sizeof(TPM\_GENERATED) octets and the first octets shall not be TPM\_GENERATED\_VALUE.

NOTE 2 This requirement allows the TPM to validate that the first block is safe to sign without having to accumulate octets over multiple calls.



17.4.2 Command and Response

**Table 75 — TPM2\_SequenceUpdate Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SequenceUpdate
TPMI_DH_OBJECT	@sequenceHandle	handle for the sequence object Auth Index: 1 Auth Role: USER
TPM2B_MAX_BUFFER	buffer	data to be added to hash

**Table 76 — TPM2\_SequenceUpdate Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 17.4.3 Detailed Actions

**[[SequenceUpdate]]**

## 17.5 TPM2\_SequenceComplete

### 17.5.1 General Description

This command adds the last part of data, if any, to a hash/HMAC sequence and returns the result.

NOTE 1 This command is not used to complete an Event Sequence. TPM2\_EventSequenceComplete() is used for that purpose.

For a hash sequence, if the results of the hash will be used in a signing operation that uses a restricted signing key, then the ticket returned by this command can indicate that the hash is safe to sign.

If the *digest* is not safe to sign, then *validation* will be a TPMT\_TK\_HASHCHECK with the hierarchy set to TPM\_RH\_NULL and *digest* set to the Empty Buffer.

NOTE 2 Regardless of the contents of the first octets of the hashed message, if the first buffer sent to the TPM had fewer than sizeof(TPM\_GENERATED) octets, then the TPM will operate as if *digest* is not safe to sign.

NOTE 3 The ticket is only required for a signing operation that uses a restricted signing key. It is always returned, but can be ignored if not needed.

If *sequenceHandle* references an Event Sequence, then the TPM shall return TPM\_RC\_MODE.

Proper authorization for the sequence object associated with *sequenceHandle* is required. If an authorization or audit of this command requires computation of a *cpHash* and an *rpHash*, the Name associated with *sequenceHandle* will be the Empty Buffer.

If this command completes successfully, the *sequenceHandle* object will be flushed.

17.5.2 Command and Response

Table 77 — TPM2\_SequenceComplete Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SequenceComplete {F}
TPMI_DH_OBJECT	@sequenceHandle	authorization for the sequence Auth Index: 1 Auth Role: USER
TPM2B_MAX_BUFFER	buffer	data to be added to the hash/HMAC
TPMI_RH_HIERARCHY+	hierarchy	hierarchy of the ticket for a hash

Table 78 — TPM2\_SequenceComplete Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	result	the returned HMAC or digest in a sized buffer
TPMT_TK_HASHCHECK	validation	ticket indicating that the sequence of octets used to compute <i>outDigest</i> did not start with TPM_GENERATED_VALUE This is a NULL Ticket when the sequence is HMAC.

### 17.5.3 Detailed Actions

`[[SequenceComplete]]`

## 17.6 TPM2\_EventSequenceComplete

### 17.6.1 General Description

This command adds the last part of data, if any, to an Event Sequence and returns the result in a digest list. If *pcrHandle* references a PCR and not TPM\_RH\_NULL, then the returned digest list is processed in the same manner as the digest list input parameter to TPM2\_PCR\_Extend() with the *pcrHandle* in each bank extended with the associated digest value.

If *sequenceHandle* references a hash or HMAC sequence, the TPM shall return TPM\_RC\_MODE.

Proper authorization for the sequence object associated with *sequenceHandle* is required. If an authorization or audit of this command requires computation of a *cpHash* and an *rpHash*, the Name associated with *sequenceHandle* will be the Empty Buffer.

If this command completes successfully, the *sequenceHandle* object will be flushed.

17.6.2 Command and Response

**Table 79 — TPM2\_EventSequenceComplete Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_EventSequenceComplete {NV F}
TPMI_DH_PCR+	@pcrHandle	PCR to be extended with the Event data Auth Index: 1 Auth Role: USER
TPMI_DH_OBJECT	@sequenceHandle	authorization for the sequence Auth Index: 2 Auth Role: USER
TPM2B_MAX_BUFFER	buffer	data to be added to the Event

**Table 80 — TPM2\_EventSequenceComplete Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPML_DIGEST_VALUES	results	list of digests computed for the PCR

### 17.6.3 Detailed Actions

`[[EventSequenceComplete]]`



## 18 Attestation Commands

### 18.1 Introduction

The attestation commands cause the TPM to sign an internally generated data structure. The contents of the data structure vary according to the command.

If the *sign* attribute is not SET in the key referenced by *signHandle* then the TPM shall return TPM\_RC\_KEY.

All signing commands include a parameter (typically *inScheme*) for the caller to specify a scheme to be used for the signing operation. This scheme will be applied only if the scheme of the key is TPM\_ALG\_NULL or the key handle is TPM\_RH\_NULL. If the scheme for *signHandle* is not TPM\_ALG\_NULL, then *inScheme.scheme* shall be TPM\_ALG\_NULL or the same as *scheme* in the public area of the key. If the scheme for *signHandle* is TPM\_ALG\_NULL or the key handle is TPM\_RH\_NULL, then *inScheme* will be used for the signing operation and may not be TPM\_ALG\_NULL. The TPM shall return TPM\_RC\_SCHEME to indicate that the scheme is not appropriate.

For a signing key that is not restricted, the caller may specify the scheme to be used as long as the scheme is compatible with the family of the key (for example, TPM\_ALG\_RSAPSS cannot be selected for an ECC key). If the caller sets *scheme* to TPM\_ALG\_NULL, then the default scheme of the key is used. For a restricted signing key, the key's scheme cannot be TPM\_ALG\_NULL and cannot be overridden.

If the handle for the signing key (*signHandle*) is TPM\_RH\_NULL, then all of the actions of the command are performed and the attestation block is "signed" with the NULL Signature.

NOTE 1 This mechanism is provided so that additional commands are not required to access the data that might be in an attestation structure.

NOTE 2 When *signHandle* is TPM\_RH\_NULL, *scheme* is still required to be a valid signing scheme (may be TPM\_ALG\_NULL), but the scheme will have no effect on the format of the signature. It will always be the NULL Signature.

TPM2\_NV\_Certify() is an attestation command that is documented in 31.16. The remaining attestation commands are collected in the remainder of this clause.

Each of the attestation structures contains a TPMS\_CLOCK\_INFO structure and a firmware version number. These values may be considered privacy-sensitive, because they would aid in the correlation of attestations by different keys. To provide improved privacy, the *resetCount*, *restartCount*, and *firmwareVersion* numbers are obfuscated when the signing key is not in the Endorsement or Platform hierarchies.

The obfuscation value is computed by:

$$\text{obfuscation} := \text{KDFa}(\text{signHandle} \rightarrow \text{nameAlg}, \text{shProof}, \text{"OBFUSCATE"}, \text{signHandle} \rightarrow \text{QN}, 0, 128) \quad (3)$$

Of the returned 128 bits, 64 bits are added to the *versionNumber* field of the attestation structure; 32 bits are added to the *clockInfo.resetCount* and 32 bits are added to the *clockInfo.restartCount*. The order in which the bits are added is implementation-dependent.

NOTE 3 The obfuscation value for each signing key will be unique to that key in a specific location. That is, each version of a duplicated signing key will have a different obfuscation value.

When the signing key is TPM\_RH\_NULL, the data structure is produced but not signed; and the values in the signed data structure are obfuscated. When computing the obfuscation value for TPM\_RH\_NULL, the hash used for context integrity is used.

NOTE 4 The QN for TPM\_RH\_NULL is TPM\_RH\_NULL.

If the signing scheme of *signHandle* is an anonymous scheme, then the attestation blocks will not contain the Qualified Name of the *signHandle*.

Each of the attestation structures allows the caller to provide some qualifying data (*qualifyingData*). For most signing schemes, this value will be placed in the TPMS\_ATTEST.*extraData* parameter that is then hashed and signed. However, for some schemes such as ECDA, the *qualifyingData* is used in a different manner (for details, see “ECDA” in TPM 2.0 Part 1).

## 18.2 TPM2\_Certify

### 18.2.1 General Description

The purpose of this command is to prove that an object with a specific Name is loaded in the TPM. By certifying that the object is loaded, the TPM warrants that a public area with a given Name is self-consistent and associated with a valid sensitive area. If a relying party has a public area that has the same Name as a Name certified with this command, then the values in that public area are correct.

NOTE 1 See 18.1 for description of how the signing scheme is selected.

Authorization for *objectHandle* requires ADMIN role authorization. If performed with a policy session, the session shall have a *policySession*→*commandCode* set to TPM\_CC\_Certify. This indicates that the policy that is being used is a policy that is for certification, and not a policy that would approve another use. That is, authority to use an object does not grant authority to certify the object.

The object may be any object that is loaded with TPM2\_Load() or TPM2\_CreatePrimary(). An object that only has its public area loaded cannot be certified.

NOTE 2 The restriction occurs because the Name is used to identify the object being certified. If the TPM has not validated that the public area is associated with a matched sensitive area, then the public area may not represent a valid object and cannot be certified.

The certification includes the Name and Qualified Name of the certified object as well as the Name and the Qualified Name of the certifying object.

NOTE 3 If *signHandle* is TPM\_RH\_NULL, the TPMS\_ATTEST structure is returned and *signature* is a NULL Signature.

18.2.2 Command and Response

Table 81 — TPM2\_Certify Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Certify
TPMI_DH_OBJECT	@objectHandle	handle of the object to be certified Auth Index: 1 Auth Role: ADMIN
TPMI_DH_OBJECT+	@signHandle	handle of the key used to sign the attestation structure Auth Index: 2 Auth Role: USER
TPM2B_DATA	qualifyingData	user provided qualifying data
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL

Table 82 — TPM2\_Certify Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	.
TPM2B_ATTEST	certifyInfo	the structure that was signed
TPMT_SIGNATURE	signature	the asymmetric signature over <i>certifyInfo</i> using the key referenced by <i>signHandle</i>

### 18.2.3 Detailed Actions

**[[Certify]]**

## 18.3 TPM2\_CertifyCreation

### 18.3.1 General Description

This command is used to prove the association between an object and its creation data. The TPM will validate that the ticket was produced by the TPM and that the ticket validates the association between a loaded public area and the provided hash of the creation data (*creationHash*).

NOTE 1 See 18.1 for description of how the signing scheme is selected.

The TPM will create a test ticket using the Name associated with *objectHandle* and *creationHash* as:

$$\mathbf{HMAC}(\mathit{proof}, (\text{TPM\_ST\_CREATION} || \mathit{objectHandle} \rightarrow \mathit{Name} || \mathit{creationHash})) \quad (4)$$

This ticket is then compared to creation ticket. If the tickets are not the same, the TPM shall return TPM\_RC\_TICKET.

If the ticket is valid, then the TPM will create a TPMS\_ATTEST structure and place *creationHash* of the command in the *creationHash* field of the structure. The Name associated with *objectHandle* will be included in the attestation data that is then signed using the key associated with *signHandle*.

NOTE 2 If *signHandle* is TPM\_RH\_NULL, the TPMS\_ATTEST structure is returned and *signature* is a NULL Signature.

*objectHandle* may be any object that is loaded with TPM2\_Load() or TPM2\_CreatePrimary().

## 18.3.2 Command and Response

Table 83 — TPM2\_CertifyCreation Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_CertifyCreation
TPMI_DH_OBJECT+	@signHandle	handle of the key that will sign the attestation block Auth Index: 1 Auth Role: USER
TPMI_DH_OBJECT	objectHandle	the object associated with the creation data Auth Index: None
TPM2B_DATA	qualifyingData	user-provided qualifying data
TPM2B_DIGEST	creationHash	hash of the creation data produced by TPM2_Create() or TPM2_CreatePrimary()
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL
TPMT_TK_CREATION	creationTicket	ticket produced by TPM2_Create() or TPM2_CreatePrimary()

Table 84 — TPM2\_CertifyCreation Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ATTEST	certifyInfo	the structure that was signed
TPMT_SIGNATURE	signature	the signature over <i>certifyInfo</i>

### 18.3.3 Detailed Actions

`[[CertifyCreation]]`



## 18.4 TPM2\_Quote

### 18.4.1 General Description

This command is used to quote PCR values.

The TPM will hash the list of PCR selected by *PCRselect* using the hash algorithm in the selected signing scheme. If the selected signing scheme or the scheme hash algorithm is TPM\_ALG\_NULL, then the TPM shall return TPM\_RC\_SCHEME.

NOTE 1 See 18.1 for description of how the signing scheme is selected.

The digest is computed as the hash of the concatenation of all of the digest values of the selected PCR.

The concatenation of PCR is described in TPM 2.0 Part 1, *Selecting Multiple PCR*.

NOTE 2 If *signHandle* is TPM\_RH\_NULL, the TPMS\_ATTEST structure is returned and *signature* is a NULL Signature.

NOTE 3 A TPM may optionally return TPM\_RC\_SCHEME if *signHandle* is TPM\_RH\_NULL.

NOTE 4 Unlike TPM 1.2, TPM2\_Quote does not return the PCR values. See Part 1, “Attesting to PCR” for a discussion of this issue.

18.4.2 Command and Response

Table 85 — TPM2\_Quote Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Quote
TPMI_DH_OBJECT+	@signHandle	handle of key that will perform signature Auth Index: 1 Auth Role: USER
TPM2B_DATA	qualifyingData	data supplied by the caller
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL
TPML_PCR_SELECTION	PCRselect	PCR set to quote

Table 86 — TPM2\_Quote Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ATTEST	quoted	the quoted information
TPMT_SIGNATURE	signature	the signature over <i>quoted</i>

### 18.4.3 Detailed Actions

[[Quote]]

## 18.5 TPM2\_GetSessionAuditDigest

### 18.5.1 General Description

This command returns a digital signature of the audit session digest.

NOTE 1 See 18.1 for description of how the signing scheme is selected.

If *sessionHandle* is not an audit session, the TPM shall return TPM\_RC\_TYPE.

NOTE 2 A session does not become an audit session until the successful completion of the command in which the session is first used as an audit session.

This command requires authorization from the privacy administrator of the TPM (expressed with Endorsement Authorization) as well as authorization to use the key associated with *signHandle*.

If this command is audited, then the audit digest that is signed will not include the digest of this command because the audit digest is only updated when the command completes successfully.

This command does not cause the audit session to be closed and does not reset the digest value.

NOTE 3 If *sessionHandle* is used as an audit session for this command, the command is audited in the same manner as any other command.

NOTE 4 If *signHandle* is TPM\_RH\_NULL, the TPMS\_ATTEST structure is returned and *signature* is a NULL Signature.

## 18.5.2 Command and Response

Table 87 — TPM2\_GetSessionAuditDigest Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetSessionAuditDigest
TPMI_RH_ENDORSEMENT	@privacyAdminHandle	handle of the privacy administrator (TPM_RH_ENDORSEMENT) Auth Index: 1 Auth Role: USER
TPMI_DH_OBJECT+	@signHandle	handle of the signing key Auth Index: 2 Auth Role: USER
TPMI_SH_HMAC	sessionHandle	handle of the audit session Auth Index: None
TPM2B_DATA	qualifyingData	user-provided qualifying data – may be zero-length
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL

Table 88 — TPM2\_GetSessionAuditDigest Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ATTEST	auditInfo	the audit information that was signed
TPMT_SIGNATURE	signature	the signature over <i>auditInfo</i>

### 18.5.3 Detailed Actions

`[[GetSessionAuditDigest]]`

## 18.6 TPM2\_GetCommandAuditDigest

### 18.6.1 General Description

This command returns the current value of the command audit digest, a digest of the commands being audited, and the audit hash algorithm. These values are placed in an attestation structure and signed with the key referenced by *signHandle*.

NOTE 1 See 18.1 for description of how the signing scheme is selected.

When this command completes successfully, and *signHandle* is not TPM\_RH\_NULL, the audit digest is cleared. If *signHandle* is TPM\_RH\_NULL, *signature* is the Empty Buffer and the audit digest is not cleared.

NOTE 2 The way that the TPM tracks that the digest is clear is vendor-dependent. The reference implementation resets the size of the digest to zero.

If this command is being audited, then the signed digest produced by the command will not include the command. At the end of this command, the audit digest will be extended with *cpHash* and the *rpHash* of the command, which would change the command audit digest signed by the next invocation of this command.

This command requires authorization from the privacy administrator of the TPM (expressed with Endorsement Authorization) as well as authorization to use the key associated with *signHandle*.

## 18.6.2 Command and Response

Table 89 — TPM2\_GetCommandAuditDigest Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetCommandAuditDigest {NV}
TPMI_RH_ENDORSEMENT	@privacyHandle	handle of the privacy administrator (TPM_RH_ENDORSEMENT) Auth Index: 1 Auth Role: USER
TPMI_DH_OBJECT+	@signHandle	the handle of the signing key Auth Index: 2 Auth Role: USER
TPM2B_DATA	qualifyingData	other data to associate with this audit digest
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL

Table 90 — TPM2\_GetCommandAuditDigest Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ATTEST	auditInfo	the auditInfo that was signed
TPMT_SIGNATURE	signature	the signature over <i>auditInfo</i>



### 18.6.3 Detailed Actions

`[[GetCommandAuditDigest]]`

## 18.7 TPM2\_GetTime

### 18.7.1 General Description

This command returns the current values of *Time* and *Clock*.

NOTE 1 See 18.1 for description of how the signing scheme is selected.

The values of *Clock*, *resetCount* and *restartCount* appear in two places in *timeInfo*: once in *TPMS\_ATTEST.clockInfo* and again in *TPMS\_ATTEST.attested.time.clockInfo*. The firmware version number also appears in two places (*TPMS\_ATTEST.firmwareVersion* and *TPMS\_ATTEST.attested.time.firmwareVersion*). If *signHandle* is in the endorsement or platform hierarchies, both copies of the data will be the same. However, if *signHandle* is in the storage hierarchy or is *TPM\_RH\_NULL*, the values in *TPMS\_ATTEST.clockInfo* and *TPMS\_ATTEST.firmwareVersion* are obfuscated but the values in *TPMS\_ATTEST.attested.time* are not.

NOTE 2 The purpose of this duplication is to allow an entity who is trusted by the privacy Administrator to correlate the obfuscated values with the clear-text values. This command requires Endorsement Authorization.

NOTE 3 If *signHandle* is *TPM\_RH\_NULL*, the *TPMS\_ATTEST* structure is returned and *signature* is a NULL Signature.

18.7.2 Command and Response

Table 91 — TPM2\_GetTime Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetTime
TPMI_RH_ENDORSEMENT	@privacyAdminHandle	handle of the privacy administrator (TPM_RH_ENDORSEMENT) Auth Index: 1 Auth Role: USER
TPMI_DH_OBJECT+	@signHandle	the <i>keyHandle</i> identifier of a loaded key that can perform digital signatures Auth Index: 2 Auth Role: USER
TPM2B_DATA	qualifyingData	data to tick stamp
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL

Table 92 — TPM2\_GetTime Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	.
TPM2B_ATTEST	timeInfo	standard TPM-generated attestation block
TPMT_SIGNATURE	signature	the signature over <i>timeInfo</i>

### 18.7.3 Detailed Actions

`[[GetTime]]`

## 19 Ephemeral EC Keys

### 19.1 Introduction

The TPM generates keys that have different lifetimes. TPM keys in a hierarchy can be persistent for as long as the seed of the hierarchy is unchanged and these keys may be used multiple times. Other TPM-generated keys are only useful for a single operation. Some of these single-use keys are used in the command in which they are created. Examples of this use are TPM2\_Duplicate() where an ephemeral key is created for a single pass key exchange with another TPM. However, there are other cases, such as anonymous attestation, where the protocol requires two passes where the public part of the ephemeral key is used outside of the TPM before the final command "consumes" the ephemeral key.

For these uses, TPM2\_Commit() or TPM2\_EC\_Ephemeral() may be used to have the TPM create an ephemeral EC key and return the public part of the key for external use. Then in a subsequent command, the caller provides a reference to the ephemeral key so that the TPM can retrieve or recreate the associated private key.

When an ephemeral EC key is created, it is assigned a number and that number is returned to the caller as the identifier for the key. This number is not a handle. A handle is assigned to a key that may be context saved but these ephemeral EC keys may not be saved and do not have a full key context. When a subsequent command uses the ephemeral key, the caller provides the number of the ephemeral key. The TPM uses that number to either look up or recompute the associated private key. After the key is used, the TPM records the fact that the key has been used so that it cannot be used again.

As mentioned, the TPM can keep each assigned private ephemeral key in memory until it is used. However, this could consume a large amount of memory. To limit the memory size, the TPM is allowed to restrict the number of pending private keys – keys that have been allocated but not used.

NOTE            The minimum number of ephemeral keys is determined by a platform specific specification

To further reduce the memory requirements for the ephemeral private keys, the TPM is allowed to use pseudo-random values for the ephemeral keys. Instead of keeping the full value of the key in memory, the TPM can use a counter as input to a KDF. Incrementing the counter will cause the TPM to generate a new pseudo-random value.

Using the counter to generate pseudo-random private ephemeral keys greatly simplifies tracking of key usage. When a counter value is used to create a key, a bit in an array may be set to indicate that the key use is pending. When the ephemeral key is consumed, the bit is cleared. This prevents the key from being used more than once.

Since the TPM is allowed to restrict the number of pending ephemeral keys, the array size can be limited. For example, a 128 bit array would allow 128 keys to be "pending".

The management of the array is described in greater detail in the *Split Operations* clause in Annex C of TPM 2.0 Part 1.

## 19.2 TPM2\_Commit

### 19.2.1 General Description

TPM2\_Commit() performs the first part of an ECC anonymous signing operation. The TPM will perform the point multiplications on the provided points and return intermediate signing values. The *signHandle* parameter shall refer to an ECC key and the signing scheme must be anonymous (TPM\_RC\_SCHEME).

NOTE 1            Currently, TPM\_ALG\_ECDSA is the only defined anonymous scheme.

NOTE 2            This command cannot be used with a sign+decrypt key because that type of key is required to have a scheme of TPM\_ALG\_NULL.

For this command, *p1*, *s2* and *y2* are optional parameters. If *s2* is an Empty Buffer, then the TPM shall return TPM\_RC\_SIZE if *y2* is not an Empty Buffer.

The algorithm is specified in the TPM 2.0 Part 1 Annex for ECC, TPM2\_Commit().

## 19.2.2 Command and Response

Table 93 — TPM2\_Commit Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Commit
TPMI_DH_OBJECT	@signHandle	handle of the key that will be used in the signing operation Auth Index: 1 Auth Role: USER
TPM2B_ECC_POINT	P1	a point ( $M$ ) on the curve used by <i>signHandle</i>
TPM2B_SENSITIVE_DATA	s2	octet array used to derive x-coordinate of a base point
TPM2B_ECC_PARAMETER	y2	y coordinate of the point associated with s2

Table 94 — TPM2\_Commit Response

Type	Name	Description
TPM_ST	tag	see 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ECC_POINT	K	ECC point $K := [d_s](x_2, y_2)$
TPM2B_ECC_POINT	L	ECC point $L := [r](x_2, y_2)$
TPM2B_ECC_POINT	E	ECC point $E := [r]P_1$
UINT16	counter	least-significant 16 bits of <i>commitCount</i>

### 19.2.3 Detailed Actions

`[[Commit]]`



### 19.3 TPM2\_EC\_Ephemeral

#### 19.3.1 General Description

TPM2\_EC\_Ephemeral() creates an ephemeral key for use in a two-phase key exchange protocol.

The TPM will use the commit mechanism to assign an ephemeral key  $r$  and compute a public point  $Q := [r]G$  where  $G$  is the generator point associated with *curveID*.

## 19.3.2 Command and Response

Table 95 — TPM2\_EC\_Ephemeral Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_EC_Ephemeral
TPMI_ECC_CURVE	curveID	The curve for the computed ephemeral point

Table 96 — TPM2\_EC\_Ephemeral Response

Type	Name	Description
TPM_ST	tag	see 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_ECC_POINT	Q	ephemeral public key $Q := [r]G$
UINT16	counter	least-significant 16 bits of <i>commitCount</i>

### 19.3.3 Detailed Actions

[[EC Ephemeral]]

## 20 Signing and Signature Verification

### 20.1 TPM2\_VerifySignature

#### 20.1.1 General Description

This command uses loaded keys to validate a signature on a message with the message digest passed to the TPM.

If the signature check succeeds, then the TPM will produce a TPMT\_TK\_VERIFIED. Otherwise, the TPM shall return TPM\_RC\_SIGNATURE.

NOTE 1           A valid ticket may be used in subsequent commands to provide proof to the TPM that the TPM has validated the signature over the message using the key referenced by *keyHandle*.

If *keyHandle* references an asymmetric key, only the public portion of the key needs to be loaded. If *keyHandle* references a symmetric key, both the public and private portions need to be loaded.

NOTE 2           The sensitive area of the symmetric object is required to allow verification of the symmetric signature (the HMAC).

20.1.2 Command and Response

**Table 97 — TPM2\_VerifySignature Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_VerifySignature
TPMI_DH_OBJECT	keyHandle	handle of public key that will be used in the validation Auth Index: None
TPM2B_DIGEST	digest	digest of the signed message
TPMT_SIGNATURE	signature	signature to be tested

**Table 98 — TPM2\_VerifySignature Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMT_TK_VERIFIED	validation	

### 20.1.3 Detailed Actions

**[[VerifySignature]]**

## 20.2 TPM2\_Sign

### 20.2.1 General Description

This command causes the TPM to sign an externally provided hash with the specified symmetric or asymmetric signing key.

NOTE 1 If *keyhandle* references an unrestricted signing key, a digest can be signed using either this command or an HMAC command.

If *keyHandle* references a restricted signing key, then *validation* shall be provided, indicating that the TPM performed the hash of the data and *validation* shall indicate that hashed data did not start with TPM\_GENERATED\_VALUE.

NOTE 2 If the hashed data did start with TPM\_GENERATED\_VALUE, then the validation will be a NULL ticket.

If the scheme of *keyHandle* is not TPM\_ALG\_NULL, then *inScheme* shall either be the same scheme as *keyHandle* or TPM\_ALG\_NULL. If the *sign* attribute is not SET in the key referenced by *handle* then the TPM shall return TPM\_RC\_KEY.

If the scheme of *keyHandle* is TPM\_ALG\_NULL, the TPM will sign using *inScheme*; otherwise, it will sign using the scheme of *keyHandle*.

NOTE 3 When the signing scheme uses a hash algorithm, the algorithm is defined in the qualifying data of the scheme. This is the same algorithm that is required to be used in producing *digest*. The size of *digest* must match that of the hash algorithm in the scheme.

If *inScheme* is not a valid signing scheme for the type of *keyHandle* (or TPM\_ALG\_NULL), then the TPM shall return TPM\_RC\_SCHEME.

If the scheme of *keyHandle* is an anonymous *scheme*, then *inScheme* shall have the same scheme algorithm as *keyHandle* and *inScheme* will contain a counter value that will be used in the signing process.

If *validation* is provided, then the hash algorithm used in computing the digest is required to be the hash algorithm specified in the scheme of *keyHandle* (TPM\_RC\_TICKET).

If the *validation* parameter is not the Empty Buffer, then it will be checked even if the key referenced by *keyHandle* is not a restricted signing key.

NOTE 4 If *keyHandle* is both a sign and decrypt key, *keyHandle* will have an scheme of TPM\_ALG\_NULL. If *validation* is provided, then it must be a NULL validation ticket or the ticket validation will fail.

20.2.2 Command and Response

Table 99 — TPM2\_Sign Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Sign
TPMI_DH_OBJECT	@keyHandle	Handle of key that will perform signing Auth Index: 1 Auth Role: USER
TPM2B_DIGEST	digest	digest to be signed
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>keyHandle</i> is TPM_ALG_NULL
TPMT_TK_HASHCHECK	validation	proof that digest was created by the TPM If <i>keyHandle</i> is not a restricted signing key, then this may be a NULL Ticket with <i>tag</i> = TPM_ST_CHECKHASH.

Table 100 — TPM2\_Sign Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMT_SIGNATURE	signature	the signature



### 20.2.3 Detailed Actions

**[[Sign]]**

## 21 Command Audit

### 21.1 Introduction

If a command has been selected for command audit, the command audit status will be updated when that command completes successfully. The digest is updated as:

$$commandAuditDigest_{new} := H_{auditAlg}(commandAuditDigest_{old} || cpHash || rpHash) \quad (5)$$

where

$H_{auditAlg}$	hash function using the algorithm of the audit sequence
$commandAuditDigest$	accumulated digest
$cpHash$	the command parameter hash
$rpHash$	the response parameter hash

$auditAlg$ , the hash algorithm, is set using `TPM2_SetCommandCodeAuditStatus()`.

`TPM2_Shutdown()` cannot be audited but `TPM2_Startup()` can be audited. If the  $cpHash$  of the `TPM2_Startup()` is `TPM_SU_STATE`, that would indicate that a `TPM2_Shutdown()` had been successfully executed.

`TPM2_SetCommandCodeAuditStatus()` is always audited, except when it is used to change  $auditAlg$ .

If the TPM is in Failure mode, command audit is not functional.

## 21.2 TPM2\_SetCommandCodeAuditStatus

### 21.2.1 General Description

This command may be used by the Privacy Administrator or platform to change the audit status of a command or to set the hash algorithm used for the audit digest, but not both at the same time.

If the *auditAlg* parameter is a supported hash algorithm and not the same as the current algorithm, then the TPM will check both *setList* and *clearList* are empty (zero length). If so, then the algorithm is changed, and the audit digest is cleared. If *auditAlg* is TPM\_ALG\_NULL or the same as the current algorithm, then the algorithm and audit digest are unchanged and the *setList* and *clearList* will be processed.

NOTE 1            Because the audit digest is cleared, the audit counter will increment the next time that an audited command is executed.

Use of TPM2\_SetCommandCodeAuditStatus() to change the list of audited commands is an audited event. If TPM\_CC\_SetCommandCodeAuditStatus is in *clearList*, the fact that it is in *clearList* is ignored.

NOTE 2            Use of this command to change the audit hash algorithm is not audited and the digest is reset when the command completes. The change in the audit hash algorithm is the evidence that this command was used to change the algorithm.

The commands in *setList* indicate the commands to be added to the list of audited commands and the commands in *clearList* indicate the commands that will no longer be audited. It is not an error if a command in *setList* is already audited or is not implemented. It is not an error if a command in *clearList* is not currently being audited or is not implemented.

If a command code is in both *setList* and *clearList*, then it will not be audited (that is, *setList* shall be processed first).

21.2.2 Command and Response

Table 101 — TPM2\_SetCommandCodeAuditStatus Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SetCommandCodeAuditStatus {NV}
TPMI_RH_PROVISION	@auth	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPMI_ALG_HASH+	auditAlg	hash algorithm for the audit digest; if TPM_ALG_NULL, then the hash is not changed
TPML_CC	setList	list of commands that will be added to those that will be audited
TPML_CC	clearList	list of commands that will no longer be audited

Table 102 — TPM2\_SetCommandCodeAuditStatus Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 21.2.3 Detailed Actions

`[[SetCommandCodeAuditStatus]]`

## 22 Integrity Collection (PCR)

### 22.1 Introduction

In TPM 1.2, an Event was hashed using SHA-1 and then the 20-octet digest was extended to a PCR using TPM\_Extend(). This specification allows the use of multiple PCR at a given Index, each using a different hash algorithm. Rather than require that the external software generate multiple hashes of the Event with each being extended to a different PCR, the Event data may be sent to the TPM for hashing. This ensures that the resulting digests will properly reflect the algorithms chosen for the PCR even if the calling software is unable to implement the hash algorithm.

NOTE 1            There is continued support for software hashing of events with TPM2\_PCR\_Extend().

To support recording of an Event that is larger than the TPM input buffer, the caller may use the command sequence described in clause 17.

Change to a PCR requires authorization. The authorization may be with either an authorization value or an authorization policy. The platform-specific specifications determine which PCR may be controlled by policy. All other PCR are controlled by authorization.

If a PCR may be associated with a policy, then the algorithm ID of that policy determines whether the policy is to be applied. If the algorithm ID is not TPM\_ALG\_NULL, then the policy digest associated with the PCR must match the *policySession*→*policyDigest* in a policy session. If the algorithm ID is TPM\_ALG\_NULL, then no policy is present and the authorization requires an EmptyAuth.

If a platform-specific specification indicates that PCR are grouped, then all the PCR in the group use the same authorization policy or authorization value.

*pcrUpdateCounter* counter will be incremented on the successful completion of any command that modifies (Extends or resets) a PCR unless the platform-specific specification explicitly excludes the PCR from being counted.

NOTE 2            If a command causes PCR in multiple banks to change, the PCR Update Counter may be incremented either once or once for each bank.

A platform-specific specification may designate a set of PCR that are under control of the TCB. These PCR may not be modified without the proper authorization. Updates of these PCR shall not cause the PCR Update Counter to increment.

EXAMPLE           Updates of the TCB PCR will not cause the PCR update counter to increment because these PCR are changed at the whim of the TCB and may not represent the trust state of the platform.

## 22.2 TPM2\_PCR\_Extend

### 22.2.1 General Description

This command is used to cause an update to the indicated PCR. The *digests* parameter contains one or more tagged digest values identified by an algorithm ID. For each digest, the PCR associated with *pcrHandle* is Extended into the bank identified by the tag (*hashAlg*).

EXAMPLE        A SHA1 digest would be Extended into the SHA1 bank and a SHA256 digest would be Extended into the SHA256 bank.

For each list entry, the TPM will check to see if *pcrNum* is implemented for that algorithm. If so, the TPM shall perform the following operation:

$$PCR.digest_{new}[pcrNum][alg] := H_{alg}(PCR.digest_{old}[pcrNum][alg] || data[alg].buffer) \quad (6)$$

where

$H_{alg}()$	hash function using the hash algorithm associated with the PCR instance
<i>PCR.digest</i>	the digest value in a PCR
<i>pcrNum</i>	the PCR numeric selector ( <i>pcrHandle</i> )
<i>alg</i>	the PCR algorithm selector for the digest
<i>data[alg].buffer</i>	the bank-specific data to be extended

If no digest value is specified for a bank, then the PCR in that bank is not modified.

NOTE 1        This allows consistent operation of the digests list for all of the Event recording commands.

If a digest is present and the PCR in that bank is not implemented, the digest value is not used.

NOTE 2        If the caller includes digests for algorithms that are not implemented, then the TPM will fail the call because the unmarshalling of *digests* will fail. Each of the entries in the list is a TPMT\_HA, which is a hash algorithm followed by a digest. If the algorithm is not implemented, unmarshalling of the *hashAlg* will fail and the TPM will return TPM\_RC\_HASH.

If the TPM unmarshals the *hashAlg* of a list entry and the unmarshaled value is not a hash algorithm implemented on the TPM, the TPM shall return TPM\_RC\_HASH.

The *pcrHandle* parameter is allowed to reference TPM\_RH\_NULL. If so, the input parameters are processed but no action is taken by the TPM. This permits the caller to probe for implemented hash algorithms as an alternative to TPM2\_GetCapability.

NOTE 3        This command allows a list of digests so that PCR in all banks may be updated in a single command. While the semantics of this command allow multiple extends to a single PCR bank, this is not the preferred use and the limit on the number of entries in the list make this use somewhat impractical.

22.2.2 Command and Response

Table 103 — TPM2\_PCR\_Extend Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_Extend {NV}
TPMI_DH_PCR+	@pcrHandle	handle of the PCR Auth Handle: 1 Auth Role: USER
TPML_DIGEST_VALUES	digests	list of tagged digest values to be extended

Table 104 — TPM2\_PCR\_Extend Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	.



### 22.2.3 Detailed Actions

[[PCR\_Extend]]

## 22.3 TPM2\_PCR\_Event

### 22.3.1 General Description

This command is used to cause an update to the indicated PCR.

The data in *eventData* is hashed using the hash algorithm associated with each bank in which the indicated PCR has been allocated. After the data is hashed, the *digests* list is returned. If the *pcrHandle* references an implemented PCR and not TPM\_RH\_NULL, the *digests* list is processed as in TPM2\_PCR\_Extend().

A TPM shall support an *Event.size* of zero through 1,024 inclusive (*Event.size* is an octet count). An *Event.size* of zero indicates that there is no data but the indicated operations will still occur,

**EXAMPLE 1** If the command implements PCR[2] in a SHA1 bank and a SHA256 bank, then an extend to PCR[2] will cause *eventData* to be hashed twice, once with SHA1 and once with SHA256. The SHA1 hash of *eventData* will be Extended to PCR[2] in the SHA1 bank and the SHA256 hash of *eventData* will be Extended to PCR[2] of the SHA256 bank.

On successful command completion, *digests* will contain the list of tagged digests of *eventData* that was computed in preparation for extending the data into the PCR. At the option of the TPM, the list may contain a digest for each bank, or it may only contain a digest for each bank in which *pcrHandle* is extant. If *pcrHandle* is TPM\_RH\_NULL, the TPM may return either an empty list or a digest for each bank.

**EXAMPLE 2** Assume a TPM that implements a SHA1 bank and a SHA256 bank and that PCR[22] is only implemented in the SHA1 bank. If *pcrHandle* references PCR[22], then *digests* may contain either a SHA1 and a SHA256 digest or just a SHA1 digest.

22.3.2 Command and Response

Table 105 — TPM2\_PCR\_Event Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_Event {NV}
TPMI_DH_PCR+	@pcrHandle	Handle of the PCR Auth Handle: 1 Auth Role: USER
TPM2B_EVENT	eventData	Event data in sized buffer

Table 106 — TPM2\_PCR\_Event Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	.
TPML_DIGEST_VALUES	digests	

### 22.3.3 Detailed Actions

[[PCR\_Event]]

## 22.4 TPM2\_PCR\_Read

### 22.4.1 General Description

This command returns the values of all PCR specified in *pcrSelectionIn*.

The TPM will process the list of TPMS\_PCR\_SELECTION in *pcrSelectionIn* in order. Within each TPMS\_PCR\_SELECTION, the TPM will process the bits in the *pcrSelect* array in ascending PCR order (see TPM 2.0 Part 1 Selecting Multiple PCR). If a bit is SET, and the indicated PCR is present, then the TPM will add the digest of the PCR to the list of values to be returned in *pcrValues*.

The TPM will continue processing bits until all have been processed or until *pcrValues* would be too large to fit into the output buffer if additional values were added.

The returned *pcrSelectionOut* will have a bit SET in its *pcrSelect* structures for each value present in *pcrValues*.

The current value of the PCR Update Counter is returned in *pcrUpdateCounter*.

The returned list may be empty if none of the selected PCR are implemented.

NOTE If no PCR are returned from a bank, the selector for the bank will be present in *pcrSelectionOut*.

No authorization is required to read a PCR and any implemented PCR may be read from any locality.

## 22.4.2 Command and Response

Table 107 — TPM2\_PCR\_Read Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_Read
TPML_PCR_SELECTION	pcrSelectionIn	The selection of PCR to read

Table 108 — TPM2\_PCR\_Read Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
UINT32	pcrUpdateCounter	the current value of the PCR update counter
TPML_PCR_SELECTION	pcrSelectionOut	the PCR in the returned list
TPML_DIGEST	pcrValues	the contents of the PCR indicated in <i>pcrSelectOut-&gt;pcrSelection[]</i> as tagged digests

### 22.4.3 Detailed Actions

`[[PCR_Read]]`

## 22.5 TPM2\_PCR\_Allocate

### 22.5.1 General Description

This command is used to set the desired PCR allocation of PCR and algorithms. This command requires Platform Authorization.

The TPM will evaluate the request and, if sufficient memory is available for the requested allocation, the TPM will store the allocation request for use during the next TPM2\_Startup(TPM\_SU\_CLEAR) operation. The PCR allocation in place when this command is executed will be retained until the next TPM2\_Startup(TPM\_SU\_CLEAR). If this command is received multiple times before a TPM2\_Startup(TPM\_SU\_CLEAR), each one overwrites the previous stored allocation.

This command will only change the allocations of banks that are listed in *pcrAllocation*.

**EXAMPLE 1** If a TPM supports SHA1 and SHA256, then it maintains an allocation for two banks (one of which could be empty). If a TPM\_PCR\_ALLOCATE() only has a selector for the SHA1 bank, then only the allocation of the SHA1 bank will be changed and the SHA256 bank will remain unchanged. To change the allocation of a TPM from 24 SHA1 PCR and no SHA256 PCR to 24 SHA256 PCR and no SHA1 PCR, the *pcrAllocation* would have to have two selections: one for the empty SHA1 bank and one for the SHA256 bank with 24 PCR.

If a bank is listed more than once, then the last selection in the *pcrAllocation* list is the one that the TPM will attempt to allocate.

**NOTE 1** This does not mean to imply that *pcrAllocation.count* can exceed *HASH\_COUNT*, the number of digests implemented in the TPM.

**EXAMPLE 2** If *HASH\_COUNT* is 2, *pcrAllocation* can specify SHA-256 twice, and the second one is used. However, if *SHA\_256* is specified three times, the unmarshaling may fail and the TPM may return an error.

This command shall not allocate more PCR in any bank than there are PCR attribute definitions. The PCR attribute definitions indicate how a PCR is to be managed – if it is resettable, the locality for update, etc. In the response to this command, the TPM returns the maximum number of PCR allowed for any bank.

When PCR are allocated, if *DRTM\_PCR* is defined, the resulting allocation must have at least one bank with the D-RTM PCR allocated. If *HCRTM\_PCR* is defined, the resulting allocation must have at least one bank with the HCRTM\_PCR allocated. If not, the TPM returns *TPM\_RC\_PCR*.

The TPM may return *TPM\_RC\_SUCCESS* even though the request fails. This is to allow the TPM to return information about the size needed for the requested allocation and the size available. If the *sizeNeeded* parameter in the return is less than or equal to the *sizeAvailable* parameter, then the *allocationSuccess* parameter will be YES. Alternatively, if the request fails, The TPM may return *TPM\_RC\_NO\_RESULT*.

**NOTE 2** An example for this type of failure is a TPM that can only support one bank at a time and cannot support arbitrary distribution of PCR among banks.

After this command, *TPM2\_Shutdown()* is only allowed to have a *startupType* equal to *TPM\_SU\_CLEAR*.

**NOTE 3** Even if this command does not cause the PCR allocation to change, the TPM cannot have its state saved. This is done in order to simplify the implementation. There is no need to optimize this command as it is not expected to be used more than once in the lifetime of the TPM (it can be used any number of times but there is no justification for optimization).



## 22.5.2 Command and Response

Table 109 — TPM2\_PCR\_Allocate Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_Allocate {NV}
TPMI_RH_PLATFORM	@authHandle	TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPML_PCR_SELECTION	pcrAllocation	the requested allocation

Table 110 — TPM2\_PCR\_Allocate Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_YES_NO	allocationSuccess	YES if the allocation succeeded
UINT32	maxPCR	maximum number of PCR that may be in a bank
UINT32	sizeNeeded	number of octets required to satisfy the request
UINT32	sizeAvailable	Number of octets available. Computed before the allocation.

### 22.5.3 Detailed Actions

`[[PCR_Allocate]]`

## 22.6 TPM2\_PCR\_SetAuthPolicy

### 22.6.1 General Description

This command is used to associate a policy with a PCR or group of PCR. The policy determines the conditions under which a PCR may be extended or reset.

A policy may only be associated with a PCR that has been defined by a platform-specific specification as allowing a policy. If the TPM implementation does not allow a policy for *pcrNum*, the TPM shall return TPM\_RC\_VALUE.

A platform-specific specification may group PCR so that they share a common policy. In such case, a *pcrNum* that selects any of the PCR in the group will change the policy for all PCR in the group.

The policy setting is persistent and may only be changed by TPM2\_PCR\_SetAuthPolicy() or by TPM2\_ChangePPS().

Before this command is first executed on a TPM or after TPM2\_ChangePPS(), the access control on the PCR will be set to the default value defined in the platform-specific specification.

NOTE 1 It is expected that the typical default will be with the policy hash set to TPM\_ALG\_NULL and an Empty Buffer for the *authPolicy* value. This will allow an *EmptyAuth* to be used as the authorization value.

If the size of the data buffer in *authPolicy* is not the size of a digest produced by *hashAlg*, the TPM shall return TPM\_RC\_SIZE.

NOTE 2 If *hashAlg* is TPM\_ALG\_NULL, then the size is required to be zero.

This command requires platformAuth/platformPolicy.

NOTE 3 If the PCR is in multiple policy sets, the policy will be changed in only one set. The set that is changed will be implementation dependent.

22.6.2 Command and Response

Table 111 — TPM2\_PCR\_SetAuthPolicy Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_SetAuthPolicy {NV}
TPMI_RH_PLATFORM	@authHandle	TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPM2B_DIGEST	authPolicy	the desired <i>authPolicy</i>
TPMI_ALG_HASH+	hashAlg	the hash algorithm of the policy
TPMI_DH_PCR	pcrNum	the PCR for which the policy is to be set

Table 112 — TPM2\_PCR\_SetAuthPolicy Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 22.6.3 Detailed Actions

`[[PCR_SetAuthPolicy]]`

## 22.7 TPM2\_PCR\_SetAuthValue

### 22.7.1 General Description

This command changes the *authValue* of a PCR or group of PCR.

An *authValue* may only be associated with a PCR that has been defined by a platform-specific specification as allowing an authorization value. If the TPM implementation does not allow an authorization for *pcrNum*, the TPM shall return TPM\_RC\_VALUE. A platform-specific specification may group PCR so that they share a common authorization value. In such case, a *pcrNum* that selects any of the PCR in the group will change the *authValue* value for all PCR in the group.

The authorization setting is set to EmptyAuth on each STARTUP(CLEAR) or by TPM2\_Clear(). The authorization setting is preserved by SHUTDOWN(STATE).

22.7.2 Command and Response

Table 113 — TPM2\_PCR\_SetAuthValue Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_SetAuthValue
TPMI_DH_PCR	@pcrHandle	handle for a PCR that may have an authorization value set Auth Index: 1 Auth Role: USER
TPM2B_DIGEST	auth	the desired authorization value

Table 114 — TPM2\_PCR\_SetAuthValue Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 22.7.3 Detailed Actions

`[[PCR_SetAuthValue]]`



## 22.8 TPM2\_PCR\_Reset

### 22.8.1 General Description

If the attribute of a PCR allows the PCR to be reset and proper authorization is provided, then this command may be used to set the PCR in all banks to zero. The attributes of the PCR may restrict the locality that can perform the reset operation.

NOTE 1            The definition of TPMI\_DH\_PCR in TPM 2.0 Part 2 indicates that if *pcrHandle* is out of the allowed range for PCR, then the appropriate return value is TPM\_RC\_VALUE.

If *pcrHandle* references a PCR that cannot be reset, the TPM shall return TPM\_RC\_LOCALITY.

NOTE 2            TPM\_RC\_LOCALITY is returned because the reset attributes are defined on a per-locality basis.

22.8.2 Command and Response

Table 115 — TPM2\_PCR\_Reset Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PCR_Reset {NV}
TPMI_DH_PCR	@pcrHandle	the PCR to reset Auth Index: 1 Auth Role: USER

Table 116 — TPM2\_PCR\_Reset Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 22.8.3 Detailed Actions

**[[PCR\_Reset]]**

## 22.9 \_TPM\_Hash\_Start

### 22.9.1 Description

This indication from the TPM interface indicates the start of an H-CRTM measurement sequence. On receipt of this indication, the TPM will initialize an H-CRTM Event Sequence context.

If no object memory is available for creation of the sequence context, the TPM will flush the context of an object so that creation of the sequence context will always succeed.

A platform-specific specification may allow this indication before TPM2\_Startup().

**NOTE** If this indication occurs after TPM2\_Startup(), it is the responsibility of software to ensure that an object context slot is available or to deal with the consequences of having the TPM select an arbitrary object to be flushed. If this indication occurs before TPM2\_Startup() then all context slots are available.

## 22.9.2 Detailed Actions

`[[ TPM Hash Start]]`

## 22.10 \_TPM\_Hash\_Data

### 22.10.1 Description

This indication from the TPM interface indicates arrival of one or more octets of data that are to be included in the H-CRTM Event Sequence sequence context created by the \_TPM\_Hash\_Start indication. The context holds data for each hash algorithm for each PCR bank implemented on the TPM.

If no H-CRTM Event Sequence context exists, this indication is discarded and no other action is performed.

### 22.10.2 Detailed Actions

`[[ TPM Hash Data ]]`

## 22.11 \_TPM\_Hash\_End

### 22.11.1 Description

This indication from the TPM interface indicates the end of the H-CRTM measurement. This indication is discarded and no other action performed if the TPM does not contain an H-CRTM Event Sequence context.

NOTE 1 An H-CRTM Event Sequence context is created by `_TPM_Hash_Start()`.

If the H-CRTM Event Sequence occurs after `TPM2_Startup()`, the TPM will set all of the PCR designated in the platform-specific specifications as resettable by this event to the value indicated in the platform specific specification, and increment *restartCount*. The TPM will then Extend the Event Sequence digest/digests into the designated D-RTM PCR (PCR[17]).

$$\text{PCR}[17][\text{hashAlg}] := \mathbf{H}_{\text{hashAlg}}(\text{initial\_value} || \mathbf{H}_{\text{hashAlg}}(\text{hash\_data})) \quad (7)$$

where

<i>hashAlg</i>	hash algorithm associated with a bank of PCR
<i>initial_value</i>	initialization value specified in the platform-specific specification (should be 0...0)
<i>hash_data</i>	all the octets of data received in <code>_TPM_Hash_Data</code> indications

A `_TPM_Hash_End` indication that occurs after `TPM2_Startup()` will increment *pcrUpdateCounter* unless a platform-specific specification excludes modifications of PCR[DRTM] from causing an increment.

A platform-specific specification may allow an H-CRTM Event Sequence before `TPM2_Startup()`. If so, `_TPM_Hash_End` will complete the digest, initialize PCR[0] with a digest-size value of 4, and then extend the H-CRTM Event Sequence data into PCR[0].

$$\text{PCR}[0][\text{hashAlg}] := \mathbf{H}_{\text{hashAlg}}(0\dots04 || \mathbf{H}_{\text{hashAlg}}(\text{hash\_data})) \quad (8)$$

NOTE 2 The entire sequence of `_TPM_Hash_Start`, `_TPM_Hash_Data`, and `_TPM_Hash_End` are required to complete before `TPM2_Startup()` or the sequence will have no effect on the TPM.

NOTE 3 PCR[0] does not need to be updated according to (8) until the end of `TPM2_Startup()`.



### 22.11.2 Detailed Actions

`[ [ TPM Hash End ] ]`

## 23 Enhanced Authorization (EA) Commands

### 23.1 Introduction

The commands in this clause 23 are used for policy evaluation. When successful, each command will update the *policySession*→*policyDigest* in a policy session context in order to establish that the authorizations required to use an object have been provided. Many of the commands will also modify other parts of a policy context so that the caller may constrain the scope of the authorization that is provided.

NOTE 1 Many of the terms used in this clause are described in detail in TPM 2.0 Part 1 and are not redefined in this clause.

The *policySession* parameter of the command is the handle of the policy session context to be modified by the command.

If the *policySession* parameter indicates a trial policy session, then the *policySession*→*policyDigest* will be updated and the indicated validations are not performed. However any authorizations required to perform the policy command will be checked and dictionary attack logic invoked as necessary.

NOTE 2 If software is used to create policies, no authorization values are used. For example, TPM\_PolicySecret requires an authorization in a trial policy session, but not in a policy calculation outside the TPM.

NOTE 3 A policy session is set to a trial policy by TPM2\_StartAuthSession(*sessionType* = TPM\_SE\_TRIAL).

NOTE 4 Unless there is an unmarshaling error in the parameters of the command, these commands will return TPM\_RC\_SUCCESS when *policySession* references a trial session.

NOTE 5 Policy context other than the *policySession*→*policyDigest* may be updated for a trial policy but it is not required.

## 23.2 Signed Authorization Actions

### 23.2.1 Introduction

The TPM2\_PolicySigned, TPM\_PolicySecret, and TPM2\_PolicyTicket commands use many of the same functions. This clause consolidates those functions to simplify the document and to ensure uniformity of the operations.

### 23.2.2 Policy Parameter Checks

These parameter checks will be performed when indicated in the description of each of the commands:

- a) *nonceTPM* – If this parameter is not the Empty Buffer, and it does not match *policySession→nonceTPM*, then the TPM shall return TPM\_RC\_VALUE.
- b) *expiration* – If this parameter is not zero, then:
  - 1) if *nonceTPM* is not an Empty Buffer, then the absolute value of *expiration* is converted to milliseconds and added to *policySession→startTime* to create the *timeout* value and proceed to c).
  - 2) If *nonceTPM* is an Empty Buffer, then the absolute value of *expiration* is converted to milliseconds and used as the *timeout* value and proceed to c).

However, *timeout* can only be changed to a smaller value.

- c) *timeout* – If *timeout* is less than the current value of *Time*, or the current *timeEpoch* is not the same as *policySession→timeEpoch*, the TPM shall return TPM\_RC\_EXPIRED
- d) *cpHashA* – If this parameter is not an Empty Buffer

NOTE 2            *cpHashA* is the hash of the command to be executed using this policy session in the authorization. The algorithm used to compute this hash is required to be the algorithm of the policy session.

- 1) the TPM shall return TPM\_RC\_CPHASH if *policySession→cpHash* is set and the contents of *policySession→cpHash* are not the same as *cpHashA*; or

NOTE 3            cpHash is the expected cpHash value held in the policy session context.

- 2) the TPM shall return TPM\_RC\_SIZE if *cpHashA* is not the same size as *policySession→policyDigest*.

NOTE 4            *policySession→policyDigest* is the size of the digest produced by the hash algorithm used to compute *policyDigest*.

### 23.2.3 Policy Digest Update Function (PolicyUpdate())

This is the update process for  $policySession \rightarrow policyDigest$  used by TPM2\_PolicySigned(), TPM2\_PolicySecret(), TPM2\_PolicyTicket(), and TPM2\_PolicyAuthorize(). The function prototype for the update function is:

$$\mathbf{PolicyUpdate}(commandCode, arg2, arg3) \quad (9)$$

where

$arg2$  a TPM2B\_NAME

$arg3$  a TPM2B

These parameters are used to update  $policySession \rightarrow policyDigest$  by

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || commandCode || arg2.name) \quad (10)$$

followed by

$$policyDigest_{new+1} := H_{policyAlg}(policyDigest_{new} || arg3.buffer) \quad (11)$$

where

$H_{policyAlg}()$  the hash algorithm chosen when the policy session was started

NOTE 1 If  $arg3$  is a TPM2B\_NAME, then  $arg3.buffer$  will actually be an  $arg3.name$ .

NOTE 2 The  $arg2.size$  and  $arg3.size$  fields are not included in the hashes.

NOTE 3 **PolicyUpdate()** uses two hash operations because  $arg2$  and  $arg3$  are variable-sized and the concatenation of  $arg2$  and  $arg3$  in a single hash could produce the same digest even though  $arg2$  and  $arg3$  are different. For example,  $arg2 = 1\ 2\ 3$  and  $arg3 = 4\ 5\ 6$  would produce the same digest as  $arg2 = 1\ 2$  and  $arg3 = 3\ 4\ 5\ 6$ . Processing of the arguments separately in different Extend operation insures that the digest produced by **PolicyUpdate()** will be different if  $arg2$  and  $arg3$  are different.

### 23.2.4 Policy Context Updates

When a policy command modifies some part of the policy session context other than the *policySession*→*policyDigest*, the following rules apply.

- ***cpHash*** – this parameter may only be changed if it contains its initialization value (an Empty Buffer). If *cpHash* is not the Empty Buffer when a policy command attempts to update it, the TPM will return an error (TPM\_RC\_CPHASH) if the current and update values are not the same.
- ***timeOut*** – this parameter may only be changed to a smaller value. If a command attempts to update this value with a larger value (longer into the future), the TPM will discard the update value. This is not an error condition.
- ***commandCode*** – once set by a policy command, this value may not be changed except by TPM2\_PolicyRestart(). If a policy command tries to change this to a different value, an error is returned (TPM\_RC\_POLICY\_CC).
- ***pcrUpdateCounter*** – this parameter is updated by TPM2\_PolicyPCR(). This value may only be set once during a policy. Each time TPM2\_PolicyPCR() executes, it checks to see if *policySession*→*pcrUpdateCounter* has its default state, indicating that this is the first TPM2\_PolicyPCR(). If it has its default value, then *policySession*→*pcrUpdateCounter* is set to the current value of *pcrUpdateCounter*. If *policySession*→*pcrUpdateCounter* does not have its default value and its value is not the same as *pcrUpdateCounter*, the TPM shall return TPM\_RC\_PCR\_CHANGED.

NOTE 1            If this parameter and *pcrUpdateCounter* are not the same, it indicates that PCR have changed since checked by the previous TPM2\_PolicyPCR(). Since they have changed, the previous PCR validation is no longer valid.

- ***commandLocality*** – this parameter is the logical AND of all enabled localities. All localities are enabled for a policy when the policy session is created. TPM2\_PolicyLocalities() selectively disables localities. Once use of a policy for a locality has been disabled, it cannot be enabled except by TPM2\_PolicyRestart().
- ***isPPRequired*** – once SET, this parameter may only be CLEARed by TPM2\_PolicyRestart().
- ***isAuthValueNeeded*** – once SET, this parameter may only be CLEARed by TPM2\_PolicyPassword() or TPM2\_PolicyRestart().
- ***isPasswordNeeded*** – once SET, this parameter may only be CLEARed by TPM2\_PolicyAuthValue() or TPM2\_PolicyRestart(),

NOTE 2            Both TPM2\_PolicyAuthValue() and TPM2\_PolicyPassword() change *policySession*→*policyDigest* in the same way. The different commands simply indicate to the TPM the format used for the *authValue* (HMAC or clear text). Both commands could be in the same policy. The final instance of these commands determines the format.

### 23.2.5 Policy Ticket Creation

For TPM2\_PolicySigned() or TPM2\_PolicySecret(), if the caller specified a negative value for *expiration*, then the TPM will return a ticket that includes a value indicating when the authorization expires. Otherwise, the TPM will return a NULL Ticket.

NOTE 1 If the *authHandle* in TPM2\_PolicySecret() references a PIN Pass Index, then the command may succeed but a NULL Ticket will be returned.

The required computation for the digest in the authorization ticket is:

$$\text{HMAC}_{\text{contextAlg}}(\text{proof}, (\text{TPM\_ST\_AUTH\_xxx} \parallel \text{cpHash} \parallel \text{policyRef} \parallel \text{authName} \parallel \text{timeout} \parallel [\text{timeEpoch}] \parallel [\text{resetCount}])) \quad (12)$$

where

$\text{HMAC}_{\text{contextAlg}}()$	an HMAC using the context integrity hash
<i>proof</i>	a TPM secret value associated with the hierarchy of the object associated with <i>authName</i>
TPM_ST_AUTH_xxx	either TPM_ST_AUTH_SIGNED or TPM_ST_AUTH_SECRET; used to ensure that the ticket is properly used
<i>cpHash</i>	optional hash of the authorized command
<i>policyRef</i>	optional reference to a policy value
<i>authName</i>	Name of the object that signed the authorization
<i>timeout</i>	implementation-specific value indicating when the authorization expires
<i>timeEpoch</i>	implementation-specific representation of the <i>timeEpoch</i> at the time the ticket was created

NOTE 2 Not included if *timeout* is zero.

*resetCount* implementation-specific representation of the TPM's *totalResetCount*

NOTE 3 Not included if *timeout* is zero or if *nonceTPM* was include in the authorization.

### 23.3 TPM2\_PolicySigned

#### 23.3.1 General Description

This command includes a signed authorization in a policy. The command ties the policy to a signing key by including the Name of the signing key in the *policyDigest*

If *policySession* is a trial session, the TPM will not check the signature and will update *policySession*→*policyDigest* as described in 23.2.3 as if a properly signed authorization was received, but no ticket will be produced.

If *policySession* is not a trial session, the TPM will validate *auth* and only perform the update if it is a valid signature over the fields of the command.

The authorizing entity will sign a digest of the authorization qualifiers: *nonceTPM*, *expiration*, *cpHashA*, and *policyRef*. The digest is computed as:

$$aHash := H_{authAlg}(nonceTPM || expiration || cpHashA || policyRef) \quad (13)$$

where

$H_{authAlg}()$  the hash associated with the auth parameter of this command

NOTE 1 Each signature and key combination indicates the scheme and each scheme has an associated hash.

*nonceTPM* the nonceTPM parameter from the TPM2\_StartAuthSession() response. If the authorization is not limited to this session, the size of this value is zero.

NOTE 2 This parameter must be present if *expiration* is non-zero.

*expiration* time limit on authorization set by authorizing object. This 32-bit value is set to zero if the expiration time is not being set.

*cpHashA* digest of the command parameters for the command being approved using the hash algorithm of the policy session. Set to an EmptyAuth if the authorization is not limited to a specific command.

NOTE 3 This is not the *cpHash* of this TPM2\_PolicySigned() command.

*policyRef* an opaque value determined by the authorizing entity. Set to the Empty Buffer if no value is present.

EXAMPLE The computation for an *aHash* if there are no restrictions is:

$$aHash := H_{authAlg}(00\ 00\ 00\ 00_{16})$$

which is the hash of an expiration time of zero.

The *aHash* is signed by the key associated with a key whose handle is *authObject*. The signature and signing parameters are combined to create the *auth* parameter.

The TPM will perform the parameter checks listed in 23.2.2

If the parameter checks succeed, the TPM will construct a test digest (*tHash*) over the provided parameters using the same formulation as shown in equation (13) above.

If *tHash* does not match the digest of the signed *aHash*, then the authorization fails and the TPM shall return TPM\_RC\_POLICY\_FAIL and make no change to *policySession*→*policyDigest*.

When all validations have succeeded, *policySession*→*policyDigest* is updated by **PolicyUpdate()** (see 23.2.3).

**PolicyUpdate**(TPM\_CC\_PolicySigned, *authObject*→*Name*, *policyRef*) (14)

*policySession* is updated as described in 23.2.4. The TPM will optionally produce a ticket as described in 23.2.5.

Authorization to use *authObject* is not required.



## 23.3.2 Command and Response

Table 117 — TPM2\_PolicySigned Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit, encrypt, or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicySigned
TPMI_DH_OBJECT	authObject	handle for a key that will validate the signature Auth Index: None
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_NONCE	nonceTPM	the policy nonce for the session This can be the Empty Buffer.
TPM2B_DIGEST	cpHashA	digest of the command parameters to which this authorization is limited This is not the <i>cpHash</i> for this command but the <i>cpHash</i> for the command to which this policy session will be applied. If it is not limited, the parameter will be the Empty Buffer.
TPM2B_NONCE	policyRef	a reference to a policy relating to the authorization – may be the Empty Buffer Size is limited to be no larger than the nonce size supported on the TPM.
INT32	expiration	time when authorization will expire, measured in seconds from the time that <i>nonceTPM</i> was generated If <i>expiration</i> is non-negative, a NULL Ticket is returned. See 23.2.5.
TPMT_SIGNATURE	auth	signed authorization (not optional)

Table 118 — TPM2\_PolicySigned Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_TIMEOUT	timeout	implementation-specific time value, used to indicate to the TPM when the ticket expires NOTE If <i>policyTicket</i> is a NULL Ticket, then this shall be the Empty Buffer.
TPMT_TK_AUTH	policyTicket	produced if the command succeeds and <i>expiration</i> in the command was non-zero; this ticket will use the TPMT_ST_AUTH_SIGNED structure tag. See 23.2.5

### 23.3.3 Detailed Actions

`[[PolicySigned]]`

## 23.4 TPM2\_PolicySecret

### 23.4.1 General Description

This command includes a secret-based authorization to a policy. The caller proves knowledge of the secret value using an authorization session using the *authValue* associated with *authHandle*. A password session, an HMAC session, or a policy session containing TPM2\_PolicyAuthValue() or TPM2\_PolicyPassword() will satisfy this requirement.

If a policy session is used and use of the *authValue* of *authHandle* is not required, the TPM will return TPM\_RC\_MODE. That is, the session for *authHandle* must have either *isAuthValueNeeded* or *isPasswordNeeded* SET.

The secret is the *authValue* of the entity whose handle is *authHandle*, which may be any TPM entity with a handle and an associated *authValue*. This includes the reserved handles (for example, Platform, Storage, and Endorsement), NV Indexes, and loaded objects. If *authObject* references an Ordinary object, it must have *userWithAuth* SET.

If *authObject* references a non-PIN Index, TPMA\_NV\_AUTHREAD is required to be SET in the Index. If *authObject* references an NV PIN index, TPMA\_NV\_WRITTEN is required to be SET and *pinCount* must be less than *pinLimit*.

NOTE 1 The authorization value for a hierarchy cannot be used in this command if the hierarchy is disabled.

If the authorization check fails, then the normal dictionary attack logic is invoked.

If the authorization provided by the authorization session is valid, the command parameters are checked as described in 23.2.2.

When all validations have succeeded, *policySession*→*policyDigest* is updated by **PolicyUpdate()** (see 23.2.3).

**PolicyUpdate**(TPM\_CC\_PolicySecret, *authObject*→*Name*, *policyRef*) (15)

*policySession* is updated as described in 23.2.4. The TPM will optionally produce a ticket as described in 23.2.5.

If the session is a trial session, *policySession*→*policyDigest* is updated if the authorization is valid.

NOTE 2 If an HMAC is used to convey the authorization, a separate session is needed for the authorization. Because the HMAC in that authorization will include a nonce that prevents replay of the authorization, the value of the *nonceTPM* parameter in this command is limited. It is retained mostly to provide processing consistency with TPM2\_PolicySigned().

## 23.4.2 Command and Response

Table 119 — TPM2\_PolicySecret Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicySecret
TPMI_DH_ENTITY	@authHandle	handle for an entity providing the authorization Auth Index: 1 Auth Role: USER
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_NONCE	nonceTPM	the policy nonce for the session This can be the Empty Buffer.
TPM2B_DIGEST	cpHashA	digest of the command parameters to which this authorization is limited This not the <i>cpHash</i> for this command but the <i>cpHash</i> for the command to which this policy session will be applied. If it is not limited, the parameter will be the Empty Buffer.
TPM2B_NONCE	policyRef	a reference to a policy relating to the authorization – may be the Empty Buffer Size is limited to be no larger than the nonce size supported on the TPM.
INT32	expiration	time when authorization will expire, measured in seconds from the time that <i>nonceTPM</i> was generated If <i>expiration</i> is non-negative, a NULL Ticket is returned. See 23.2.5.

Table 120 — TPM2\_PolicySecret Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_TIMEOUT	timeout	implementation-specific time value used to indicate to the TPM when the ticket expires; this ticket will use the TPMT_ST_AUTH_SECRET structure tag
TPMT_TK_AUTH	policyTicket	produced if the command succeeds and <i>expiration</i> in the command was non-zero ( See 23.2.5)

### 23.4.3 Detailed Actions

**[[PolicySecret]]**

## 23.5 TPM2\_PolicyTicket

### 23.5.1 General Description

This command is similar to TPM2\_PolicySigned() except that it takes a ticket instead of a signed authorization. The ticket represents a validated authorization that had an expiration time associated with it.

The parameters of this command are checked as described in 23.2.2.

If the checks succeed, the TPM uses the *timeout*, *cpHashA*, *policyRef*, and *authName* to construct a ticket to compare with the value in *ticket*. If these tickets match, then the TPM will create a TPM2B\_NAME (*objectName*) using *authName* and update the context of *policySession* by **PolicyUpdate()** (see 23.2.3).

**PolicyUpdate**(*commandCode*, *authName*, *policyRef*) (16)

If the structure tag of ticket is TPM\_ST\_AUTH\_SECRET, then *commandCode* will be TPM\_CC\_PolicySecret. If the structure tag of ticket is TPM\_ST\_AUTH\_SIGNED, then *commandCode* will be TPM\_CC\_PolicySigned.

*policySession* is updated as described in 23.2.4.

## 23.5.2 Command and Response

Table 121 — TPM2\_PolicyTicket Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyTicket
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_TIMEOUT	timeout	time when authorization will expire The contents are TPM specific. This shall be the value returned when ticket was produced.
TPM2B_DIGEST	cpHashA	digest of the command parameters to which this authorization is limited If it is not limited, the parameter will be the Empty Buffer.
TPM2B_NONCE	policyRef	reference to a qualifier for the policy – may be the Empty Buffer
TPM2B_NAME	authName	name of the object that provided the authorization
TPMT_TK_AUTH	ticket	an authorization ticket returned by the TPM in response to a TPM2_PolicySigned() or TPM2_PolicySecret()

Table 122 — TPM2\_PolicyTicket Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.5.3 Detailed Actions

`[[PolicyTicket]]`



## 23.6 TPM2\_PolicyOR

### 23.6.1 General Description

This command allows options in authorizations without requiring that the TPM evaluate all of the options. If a policy may be satisfied by different sets of conditions, the TPM need only evaluate one set that satisfies the policy. This command will indicate that one of the required sets of conditions has been satisfied.

$policySession \rightarrow policyDigest$  is compared against the list of provided values. If the current  $policySession \rightarrow policyDigest$  does not match any value in the list, the TPM shall return TPM\_RC\_VALUE. Otherwise, the TPM will reset  $policySession \rightarrow policyDigest$  to a Zero Digest. Then  $policySession \rightarrow policyDigest$  is extended by the concatenation of TPM\_CC\_PolicyOR and the concatenation of all of the digests.

If  $policySession$  is a trial session, the TPM will assume that  $policySession \rightarrow policyDigest$  matches one of the list entries and compute the new value of  $policyDigest$ .

The algorithm for computing the new value for  $policyDigest$  of  $policySession$  is:

- a) Concatenate all the digest values in  $pHashList$ :

$$digests := pHashList.digests[1].buffer || \dots || pHashList.digests[n].buffer \quad (17)$$

NOTE 1 The TPM will not return an error if the size of an entry is not the same as the size of the digest of the policy. However, that entry cannot match  $policyDigest$ .

- b) Reset  $policyDigest$  to a Zero Digest.

- c) Extend the command code and the hashes computed in step a) above:

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyOR || digests) \quad (18)$$

NOTE 2 The computation in b) and c) above is equivalent to:

$$policyDigest_{new} := H_{policyAlg}(0 \dots 0 || TPM\_CC\_PolicyOR || digests)$$

A TPM shall support a list with at least eight tagged digest values.

NOTE 3 If policies are to be portable between TPMs, then they should not use more than eight values.

23.6.2 Command and Response

**Table 123 — TPM2\_PolicyOR Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyOR
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPML_DIGEST	pHashList	the list of hashes to check for a match

**Table 124 — TPM2\_PolicyOR Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.6.3 Detailed Actions

**[[PolicyOR]]**

## 23.7 TPM2\_PolicyPCR

### 23.7.1 General Description

This command is used to cause conditional gating of a policy based on PCR. This command together with TPM2\_PolicyOR() allows one group of authorizations to occur when PCR are in one state and a different set of authorizations when the PCR are in a different state.

The TPM will modify the *pcrs* parameter so that bits that correspond to unimplemented PCR are CLEAR. If *policySession* is not a trial policy session, the TPM will use the modified value of *pcrs* to select PCR values to hash according to TPM 2.0 Part 1, *Selecting Multiple PCR*. The hash algorithm of the policy session is used to compute a digest (*digestTPM*) of the selected PCR. If *pcrDigest* does not have a length of zero, then it is compared to *digestTPM*; and if the values do not match, the TPM shall return TPM\_RC\_VALUE and make no change to *policySession*→*policyDigest*. If the values match, or if the length of *pcrDigest* is zero, then *policySession*→*policyDigest* is extended by:

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyPCR || pcrs || digestTPM) \quad (19)$$

where

<i>pcrs</i>	the <i>pcrs</i> parameter with bits corresponding to unimplemented PCR set to 0
<i>digestTPM</i>	the digest of the selected PCR using the hash algorithm of the policy session

NOTE 1 If the caller provides the expected PCR value, the intention is that the policy evaluation stop at that point if the PCR do not match. If the caller does not provide the expected PCR value, then the validity of the settings will not be determined until an attempt is made to use the policy for authorization. If the policy is constructed such that the PCR check comes before user authorization checks, this early termination would allow software to avoid unnecessary prompts for user input to satisfy a policy that would fail later due to incorrect PCR values.

After this command completes successfully, the TPM shall return TPM\_RC\_PCR\_CHANGED if the policy session is used for authorization and the PCR are not known to be correct.

The TPM uses a “generation” number (*pcrUpdateCounter*) that is incremented each time PCR are updated (unless the PCR being changed is specified not to cause a change to this counter). The value of this counter is stored in the policy session context (*policySession*→*pcrUpdateCounter*) when this command is executed. When the policy is used for authorization, the current value of the counter is compared to the value in the policy session context and the authorization will fail if the values are not the same.

When this command is executed, *policySession*→*pcrUpdateCounter* is checked to see if it has been previously set (in the reference implementation, it has a value of zero if not previously set). If it has been set, it will be compared with the current value of *pcrUpdateCounter* to determine if any PCR changes have occurred. If the values are different, the TPM shall return TPM\_RC\_PCR\_CHANGED.

NOTE 2 Since the *pcrUpdateCounter* is updated if any PCR is extended (except those specified not to do so), this means that the command will fail even if a PCR not specified in the policy is updated. This is an optimization for the purposes of conserving internal TPM memory. This would be a rare occurrence, and, if this should occur, the policy could be reset using the TPM2\_PolicyRestart command and rerun.

If *policySession*→*pcrUpdateCounter* has not been set, then it is set to the current value of *pcrUpdateCounter*.

If this command is used for a trial *policySession*, *policySession*→*policyDigest* will be updated using the values from the command rather than the values from a digest of the TPM PCR. If the caller does not provide PCR settings (*pcrDigest* has a length of zero), the TPM may (and it is preferred to) use the

current TPM PCR settings (*digestTPM*) in the calculation for the new *policyDigest*. The TPM may return an error if the caller does not provide a PCR digest for a trial policy session but this is not the preferred behavior.

The TPM will not check any PCR and will compute:

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyPCR || pcrs || pcrDigest) \quad (20)$$

In this computation, *pcrs* is the input parameter without modification.

NOTE 3            The *pcrs* parameter is expected to match the configuration of the TPM for which the policy is being computed which may not be the same as the TPM on which the trial policy is being computed.

NOTE 4            Although no PCR are checked in a trial policy session, *pcrDigest* is expected to correspond to some useful PCR values. It is legal, but pointless, to have the TPM aid in calculating a *policyDigest* corresponding to PCR values that are not useful in practice.

## 23.7.2 Command and Response

Table 125 — TPM2\_PolicyPCR Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyPCR
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_DIGEST	pcrDigest	expected digest value of the selected PCR using the hash algorithm of the session; may be zero length
TPML_PCR_SELECTION	pcrs	the PCR to include in the check digest

Table 126 — TPM2\_PolicyPCR Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.7.3 Detailed Actions

**[[PolicyPCR]]**

## 23.8 TPM2\_PolicyLocality

### 23.8.1 General Description

This command indicates that the authorization will be limited to a specific locality.

*policySession*→*commandLocality* is a parameter kept in the session context. When the policy session is started, this parameter is initialized to a value that allows the policy to apply to any locality.

If *locality* has a value greater than 31, then an extended locality is indicated. For an extended locality, the TPM will validate that *policySession*→*commandLocality* has not previously been set or that the current value of *policySession*→*commandLocality* is the same as *locality* (TPM\_RC\_RANGE).

When *locality* is not an extended locality, the TPM will validate that the *policySession*→*commandLocality* is not set to an extended locality value (TPM\_RC\_RANGE). If not the TPM will disable any locality not SET in the *locality* parameter. If the result of disabling localities results in no locality being enabled, the TPM will return TPM\_RC\_RANGE.

If no error occurred in the validation of *locality*, *policySession*→*policyDigest* is extended with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyLocality || locality) \quad (21)$$

Then *policySession*→*commandLocality* is updated to indicate which localities are still allowed after execution of TPM2\_PolicyLocality().

When the policy session is used to authorize a command, the authorization will fail if the locality used for the command is not one of the enabled localities in *policySession*→*commandLocality*.



23.8.2 Command and Response

**Table 127 — TPM2\_PolicyLocality Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyLocality
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPMA_LOCALITY	locality	the allowed localities for the policy

**Table 128 — TPM2\_PolicyLocality Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.8.3 Detailed Actions

`[[PolicyLocality]]`

## 23.9 TPM2\_PolicyNV

### 23.9.1 General Description

This command is used to cause conditional gating of a policy based on the contents of an NV Index. It is an immediate assertion. The NV index is validated during the TPM2\_PolicyNV() command, not when the session is used for authorization.

The authorization to read the NV Index must succeed even if *policySession* is a trial policy session.

If *policySession* is a trial policy session, the TPM will update *policySession*→*policyDigest* as shown in equations (22) and (23) below and return TPM\_RC\_SUCCESS. It will not perform any further validation. The remainder of this general description would apply only if *policySession* is not a trial policy session.

An authorization session providing authorization to read the NV Index shall be provided.

If TPMA\_NV\_WRITTEN is not SET in the NV Index, the TPM shall return TPM\_RC\_NV\_UNINITIALIZED. If TPMA\_NV\_READLOCKED of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_LOCKED.

For an NV Index with the TPM\_NT\_COUNTER or TPM\_NT\_BITS attribute SET, the TPM may ignore the *offset* parameter and use an offset of 0. Therefore, it is recommended that the caller set the *offset* parameter to 0 for interoperability.

If *offset* and the *size* field of *data* add to a value that is greater than the *dataSize* field of the NV Index referenced by *nvIndex*, the TPM shall return an error (TPM\_RC\_NV\_RANGE). The implementation may return an error (TPM\_RC\_VALUE) if it performs an additional check and determines that *offset* is greater than the *dataSize* field of the NV Index.

*operandA* begins at *offset* into the NV index contents and has a size equal to the size of *operandB*. The TPM will perform the indicated arithmetic check using *operandA* and *operandB*. If the check fails, the TPM shall return TPM\_RC\_POLICY and not change *policySession*→*policyDigest*. If the check succeeds, the TPM will hash the arguments:

$$args := H_{policyAlg}(operandB.buffer || offset || operation) \quad (22)$$

where

$H_{policyAlg}()$	hash function using the algorithm of the policy session
<i>operandB</i>	the value used for the comparison
<i>offset</i>	offset from the start of the NV Index data to start the comparison
<i>operation</i>	the operation parameter indicating the comparison being performed

The value of *args* and the Name of the NV Index are extended to *policySession*→*policyDigest* by

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyNV || args || nvIndex \rightarrow Name) \quad (23)$$

where

$H_{policyAlg}()$	hash function using the algorithm of the policy session
<i>args</i>	value computed in equation (22)
<i>nvIndex</i> → <i>Name</i>	the Name of the NV Index

The signed arithmetic operations are performed using twos-compliment.

Magnitude comparisons assume that the octet at offset zero in the referenced NV location and in *operandB* contain the most significant octet of the data.

23.9.2 Command and Response

**Table 129 — TPM2\_PolicyNV Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyNV
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index of the area to read Auth Index: None
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_OPERAND	operandB	the second operand
UINT16	offset	the offset in the NV Index for the start of operand A
TPM_EO	operation	the comparison to make

**Table 130 — TPM2\_PolicyNV Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.9.3 Detailed Actions

**[[PolicyNV]]**

## 23.10 TPM2\_PolicyCounterTimer

### 23.10.1 General Description

This command is used to cause conditional gating of a policy based on the contents of the TPMS\_TIME\_INFO structure.

If *policySession* is a trial policy session, the TPM will update *policySession*→*policyDigest* as shown in equations (24) and (25) below and return TPM\_RC\_SUCCESS. It will not perform any validation. The remainder of this general description would apply only if *policySession* is not a trial policy session.

The TPM will perform the indicated arithmetic check on the indicated portion of the TPMS\_TIME\_INFO structure. If the check fails, the TPM shall return TPM\_RC\_POLICY and not change *policySession*→*policyDigest*. If the check succeeds, the TPM will hash the arguments:

$$args := H_{policyAlg}(operandB.buffer || offset || operation) \quad (24)$$

where

$H_{policyAlg}()$	hash function using the algorithm of the policy session
<i>operandB.buffer</i>	the value used for the comparison
<i>offset</i>	offset from the start of the TPMS_TIME_INFO structure at which the comparison starts
<i>operation</i>	the operation parameter indicating the comparison being performed

NOTE There is no security related reason for the double hash.

The value of *args* is extended to *policySession*→*policyDigest* by

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyCounterTimer || args) \quad (25)$$

where

$H_{policyAlg}()$	hash function using the algorithm of the policy session
<i>args</i>	value computed in equation (24)

The signed arithmetic operations are performed using twos-compliment. The indicated portion of the TPMS\_TIME\_INFO structure begins at *offset* and has a length of *operandB.size*. If the number of octets to be compared overflows the TPMS\_TIME\_INFO structure, the TPM returns TPM\_RC\_RANGE. If *offset* is greater than the size of the marshaled TPMS\_TIME\_INFO structure, the TPM returns TPM\_RC\_VALUE. The structure is marshaled into its canonical form with no padding. The TPM does not check for alignment of the offset with a TPMS\_TIME\_INFO structure member.

Magnitude comparisons assume that the octet at offset zero in the referenced location and in *operandB* contain the most significant octet of the data.

## 23.10.2 Command and Response

Table 131 — TPM2\_PolicyCounterTimer Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyCounterTimer
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_OPERAND	operandB	the second operand
UINT16	offset	the offset in TPMS_TIME_INFO structure for the start of operand A
TPM_EO	operation	the comparison to make

Table 132 — TPM2\_PolicyCounterTimer Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.10.3 Detailed Actions

`[[PolicyCounterTimer]]`



## 23.11 TPM2\_PolicyCommandCode

### 23.11.1 General Description

This command indicates that the authorization will be limited to a specific command code.

If *policySession*→*commandCode* has its default value, then it will be set to *code*. If *policySession*→*commandCode* does not have its default value, then the TPM will return TPM\_RC\_VALUE if the two values are not the same.

If *code* is not implemented, the TPM will return TPM\_RC\_POLICY\_CC.

If the TPM does not return an error, it will update *policySession*→*policyDigest* by

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyCommandCode || code) \quad (26)$$

NOTE 1 If a previous TPM2\_PolicyCommandCode() had been executed, then it is probable that the policy expression is improperly formed but the TPM does not return an error.

NOTE 2 A TPM2\_PolicyOR() would be used to allow an authorization to be used for multiple commands.

When the policy session is used to authorize a command, the TPM will fail the command if the *commandCode* of that command does not match *policySession*→*commandCode*.

This command, or TPM2\_PolicyDuplicationSelect(), is required to enable the policy to be used for ADMIN role authorization.

EXAMPLE Before TPM2\_Certify() can be executed, TPM2\_PolicyCommandCode() with code set to TPM\_CC\_Certify is required.

23.11.2 Command and Response

**Table 133 — TPM2\_PolicyCommandCode Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyCommandCode
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM_CC	code	the allowed <i>commandCode</i>

**Table 134 — TPM2\_PolicyCommandCode Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.11.3 Detailed Actions

`[[PolicyCommandCode]]`

## 23.12 TPM2\_PolicyPhysicalPresence

### 23.12.1 General Description

This command indicates that physical presence will need to be asserted at the time the authorization is performed.

If this command is successful, *policySession*→*isPPRequired* will be SET to indicate that this check is required when the policy is used for authorization. Additionally, *policySession*→*policyDigest* is extended with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyPhysicalPresence) \quad (27)$$

23.12.2 Command and Response

**Table 135 — TPM2\_PolicyPhysicalPresence Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyPhysicalPresence
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None

**Table 136 — TPM2\_PolicyPhysicalPresence Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.12.3 Detailed Actions

**[[PolicyPhysicalPresence]]**

## 23.13 TPM2\_PolicyCpHash

### 23.13.1 General Description

This command is used to allow a policy to be bound to a specific command and command parameters.

TPM2\_PolicySigned(), TPM2\_PolicySecret(), and TPM2\_PolicyTicket() are designed to allow an authorizing entity to execute an arbitrary command as the *cpHashA* parameter of those commands is not included in *policySession*→*policyDigest*. TPM2\_PolicyCommandCode() allows the policy to be bound to a specific Command Code so that only certain entities may authorize specific command codes. This command allows the policy to be restricted such that an entity may only authorize a command with a specific set of parameters.

If *policySession*→*cpHash* is already set and not the same as *cpHashA*, then the TPM shall return TPM\_RC\_CPHASH. If *cpHashA* does not have the size of the *policySession*→*policyDigest*, the TPM shall return TPM\_RC\_SIZE.

NOTE 1 If a previous TPM2\_PolicyCpHash() had been executed, then it is probable that the policy expression is improperly formed but the TPM does not return an error if *cpHash* is the same.

If the *cpHashA* checks succeed, *policySession*→*cpHash* is set to *cpHashA* and *policySession*→*policyDigest* is updated with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyCpHash || cpHashA) \quad (28)$$

23.13.2 Command and Response

Table 137 — TPM2\_PolicyCpHash Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyCpHash
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_DIGEST	cpHashA	the <i>cpHash</i> added to the policy

Table 138 — TPM2\_PolicyCpHash Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 23.13.3 Detailed Actions

**[[PolicyCpHash]]**

## 23.14 TPM2\_PolicyNameHash

### 23.14.1 General Description

This command allows a policy to be bound to a specific set of TPM entities without being bound to the parameters of the command. This is most useful for commands such as TPM2\_Duplicate() and for TPM2\_PCR\_Event() when the referenced PCR requires a policy.

The *nameHash* parameter should contain the digest of the Names associated with the handles to be used in the authorized command.

EXAMPLE For the TPM2\_Duplicate() command, two handles are provided. One is the handle of the object being duplicated and the other is the handle of the new parent. For that command, *nameHash* would contain:

$$nameHash := H_{policyAlg}(objectHandle \rightarrow Name || newParentHandle \rightarrow Name)$$

If *policySession*→*cpHash* is already set, the TPM shall return TPM\_RC\_CPHASH. If the size of *nameHash* is not the size of *policySession*→*policyDigest*, the TPM shall return TPM\_RC\_SIZE. Otherwise, *policySession*→*cpHash* is set to *nameHash*.

If this command completes successfully, the *cpHash* of the authorized command will not be used for validation. Only the digest of the Names associated with the handles in the command will be used.

NOTE 1 This allows the space normally used to hold *policySession*→*cpHash* to be used for *policySession*→*nameHash* instead.

The *policySession*→*policyDigest* will be updated with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyNameHash || nameHash) \quad (29)$$

NOTE 2 This command will often be used with TPM2\_PolicyAuthorize() where the owner of the object being duplicated provides approval for their object to be migrated to a specific new parent.

23.14.2 Command and Response

**Table 139 — TPM2\_PolicyNameHash Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyNameHash
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_DIGEST	nameHash	the digest to be added to the policy

**Table 140 — TPM2\_PolicyNameHash Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.14.3 Detailed Actions

`[[PolicyNameHash]]`

## 23.15 TPM2\_PolicyDuplicationSelect

### 23.15.1 General Description

This command allows qualification of duplication to allow duplication to a selected new parent.

If this command not used in conjunction with a PolicyAuthorize Command, then only the new parent is selected and *includeObject* should be CLEAR.

EXAMPLE When an object is created when the list of allowed duplication targets is known, the policy would be created with *includeObject* CLEAR.

NOTE 1 Only the new parent may be selected because, without TPM2\_PolicyAuthorize(), the Name of the Object to be duplicated would need to be known at the time that Object's policy is created. However, since the Name of the Object includes its policy, the Name is not known. The Name can be known by the authorizing entity (a PolicyAuthorize Command) in which case *includeObject* may be SET.

If used in conjunction with TPM2\_PolicyAuthorize(), then the authorizer of the new policy has the option of selecting just the new parent or of selecting both the new parent and the duplication Object.

NOTE 2 If the authorizing entity for an TPM2\_PolicyAuthorize() only specifies the new parent, then that authorization may be applied to the duplication of any number of other Objects. If the authorizing entity specifies both a new parent and the duplicated Object, then the authorization only applies to that pairing of Object and new parent.

If either *policySession*→*cpHash* or *policySession*→*nameHash* has been previously set, the TPM shall return TPM\_RC\_CPHASH. Otherwise, *policySession*→*nameHash* will be set to:

$$nameHash := H_{policyAlg}(objectName || newParentName) \quad (30)$$

NOTE 3 It is allowed that *policySession*→*nameHash* and *policySession*→*cpHash* share the same memory space.

The *policySession*→*policyDigest* will be updated according to the setting of *includeObject*. If equal to YES, *policySession*→*policyDigest* is updated by:

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyDuplicationSelect || objectName || newParentName || includeObject) \quad (31)$$

If *includeObject* is NO, *policySession*→*policyDigest* is updated by:

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyDuplicationSelect || newParentName || includeObject) \quad (32)$$

NOTE 4 *policySession*→*cpHash* receives the digest of both Names so that the check performed in TPM2\_Duplicate() may be the same regardless of which Names are included in *policySession*→*policyDigest*. This means that, when TPM2\_PolicyDuplicationSelect() is executed, it is only valid for a specific pair of duplication object and new parent.

If the command succeeds, *policySession*→*commandCode* is set to TPM\_CC\_Duplicate.

NOTE 5 The normal use of this command is before a TPM2\_PolicyAuthorize(). An authorized entity would approve a *policyDigest* that allowed duplication to a specific new parent. The authorizing entity may want to limit the authorization so that the approval allows only a specific object to be duplicated to the new parent. In that case, the authorizing entity would approve the *policyDigest* of equation (31).

## 23.15.2 Command and Response

Table 141 — TPM2\_PolicyDuplicationSelect Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyDuplicationSelect
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_NAME	objectName	the Name of the object to be duplicated
TPM2B_NAME	newParentName	the Name of the new parent
TPMI_YES_NO	includeObject	if YES, the <i>objectName</i> will be included in the value in <i>policySession</i> → <i>policyDigest</i>

Table 142 — TPM2\_PolicyDuplicationSelect Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.15.3 Detailed Actions

`[[PolicyDuplicationSelect]]`

## 23.16 TPM2\_PolicyAuthorize

### 23.16.1 General Description

This command allows policies to change. If a policy were static, then it would be difficult to add users to a policy. This command lets a policy authority sign a new policy so that it may be used in an existing policy.

The authorizing entity signs a structure that contains

$$aHash := H_{aHashAlg}(approvedPolicy || policyRef) \quad (33)$$

The *aHashAlg* is required to be the *nameAlg* of the key used to sign the *aHash*. The *aHash* value is then signed (symmetric or asymmetric) by *keySign*. That signature is then checked by the TPM in `TPM2_VerifySignature()` which produces a ticket by

$$HMAC(proof, (TPM\_ST\_VERIFIED || aHash || keySign \rightarrow Name)) \quad (34)$$

NOTE 1 The reason for the validation is because of the expectation that the policy will be used multiple times and it is more efficient to check a ticket than to load an object each time to check a signature.

The ticket is then used in `TPM2_PolicyAuthorize()` to validate the parameters.

The *keySign* parameter is required to be a valid object name using *nameAlg* other than `TPM_ALG_NULL`. If the first two octets of *keySign* are not a valid hash algorithm, the TPM shall return `TPM_RC_HASH`. If the remainder of the Name is not the size of the indicated digest, the TPM shall return `TPM_RC_SIZE`.

The TPM validates that the *approvedPolicy* matches the current value of *policySession*→*policyDigest* and if not, shall return `TPM_RC_VALUE`.

The TPM then validates that the parameters to `TPM2_PolicyAuthorize()` match the values used to generate the ticket. If so, the TPM will reset *policySession*→*policyDigest* to a Zero Digest. Then it will update *policySession*→*policyDigest* with **PolicyUpdate()** (see 23.2.3).

$$\mathbf{PolicyUpdate}(TPM\_CC\_PolicyAuthorize, keySign, policyRef) \quad (35)$$

If the ticket is not valid, the TPM shall return `TPM_RC_POLICY`.

If *policySession* is a trial session, *policySession*→*policyDigest* is extended as if the ticket is valid without actual verification.

NOTE 2 The unmarshaling process requires that a proper `TPMT_TK_VERIFIED` be provided for *checkTicket* but it may be a NULL Ticket. A NULL ticket is useful in a trial policy, where the caller uses the TPM to perform policy calculations but does not have a valid authorization ticket.



## 23.16.2 Command and Response

Table 143 — TPM2\_PolicyAuthorize Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyAuthorize
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_DIGEST	approvedPolicy	digest of the policy being approved
TPM2B_NONCE	policyRef	a policy qualifier
TPM2B_NAME	keySign	Name of a key that can sign a policy addition
TPMT_TK_VERIFIED	checkTicket	ticket validating that <i>approvedPolicy</i> and <i>policyRef</i> were signed by <i>keySign</i>

Table 144 — TPM2\_PolicyAuthorize Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.16.3 Detailed Actions

`[[PolicyAuthorize]]`

## 23.17 TPM2\_PolicyAuthValue

### 23.17.1 General Description

This command allows a policy to be bound to the authorization value of the authorized entity.

When this command completes successfully, *policySession*→*isAuthValueNeeded* is SET to indicate that the *authValue* will be included in *hmacKey* when the authorization HMAC is computed for the command being authorized using this session. Additionally, *policySession*→*isPasswordNeeded* will be CLEAR.

NOTE If a policy does not use this command, then the *hmacKey* for the authorized command would only use *sessionKey*. If *sessionKey* is not present, then the *hmacKey* is an Empty Buffer and no HMAC would be computed.

If successful, *policySession*→*policyDigest* will be updated with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyAuthValue) \quad (36)$$

23.17.2 Command and Response

**Table 145 — TPM2\_PolicyAuthValue Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyAuthValue
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None

**Table 146 — TPM2\_PolicyAuthValue Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.17.3 Detailed Actions

`[[PolicyAuthValue]]`

## 23.18 TPM2\_PolicyPassword

### 23.18.1 General Description

This command allows a policy to be bound to the authorization value of the authorized object.

When this command completes successfully, *policySession*→*isPasswordNeeded* is SET to indicate that *authValue* of the authorized object will be checked when the session is used for authorization. The caller will provide the *authValue* in clear text in the *hmac* parameter of the authorization. The comparison of *hmac* to *authValue* is performed as if the authorization is a password.

NOTE 1           The parameter field in the policy session where the authorization value is provided is called *hmac*. If TPM2\_PolicyPassword() is part of the sequence, then the field will contain a password and not an HMAC.

If successful, *policySession*→*policyDigest* will be updated with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyAuthValue) \quad (37)$$

NOTE 2           This is the same extend value as used with TPM2\_PolicyAuthValue so that the evaluation may be done using either an HMAC or a password with no change to the *authPolicy* of the object. The reason that two commands are present is to indicate to the TPM if the *hmac* field in the authorization will contain an HMAC or a password value.

When this command is successful, *policySession*→*isAuthValueNeeded* will be CLEAR.

23.18.2 Command and Response

Table 147 — TPM2\_PolicyPassword Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyPassword
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None

Table 148 — TPM2\_PolicyPassword Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.18.3 Detailed Actions

**[[PolicyPassword]]**



## 23.19 TPM2\_PolicyGetDigest

### 23.19.1 General Description

This command returns the current *policyDigest* of the session. This command allows the TPM to be used to perform the actions required to pre-compute the *authPolicy* for an object.

23.19.2 Command and Response

Table 149 — TPM2\_PolicyGetDigest Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyGetDigest
TPMI_SH_POLICY	policySession	handle for the policy session Auth Index: None

Table 150 — TPM2\_PolicyGetDigest Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_DIGEST	policyDigest	the current value of the <i>policySession</i> → <i>policyDigest</i>

### 23.19.3 Detailed Actions

`[[PolicyGetDigest]]`

## 23.20 TPM2\_PolicyNvWritten

### 23.20.1 General Description

This command allows a policy to be bound to the TPMA\_NV\_WRITTEN attributes. This is a deferred assertion. Values are stored in the policy session context and checked when the policy is used for authorization.

If *policySession*→*checkNVWritten* is CLEAR, it is SET and *policySession*→*nvWrittenState* is set to *writtenSet*. If *policySession*→*checkNVWritten* is SET, the TPM will return TPM\_RC\_VALUE if *policySession*→*nvWrittenState* and *writtenSet* are not the same.

If the TPM does not return an error, it will update *policySession*→*policyDigest* by

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyNvWritten || writtenSet) \quad (38)$$

When the policy session is used to authorize a command, the TPM will fail the command if *policySession*→*checkNVWritten* is SET and *nvIndex*→*attributes*→*TPMA\_NV\_WRITTEN* does not match *policySession*→*nvWrittenState*.

NOTE 1            A typical use case is a simple policy for the first write during manufacturing provisioning that would require TPMA\_NV\_WRITTEN CLEAR and a more complex policy for later use that would require TPMA\_NV\_WRITTEN SET.

NOTE 2            When an Index is written, it has a different authorization name than an Index that has not been written. It is possible to use this change in the NV Index to create a write-once Index.

23.20.2 Command and Response

Table 151 — TPM2\_PolicyNvWritten Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyNvWritten
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPMI_YES_NO	writtenSet	YES if NV Index is required to have been written NO if NV Index is required not to have been written

Table 152 — TPM2\_PolicyNvWritten Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.20.3 Detailed Actions

**[[PolicyNvWRitten]]**

## 23.21 TPM2\_PolicyTemplate

### 23.21.1 General Description

This command allows a policy to be bound to a specific creation template. This is most useful for an object creation command such as TPM2\_Create(), TPM2\_CreatePrimary(), or TPM2\_CreateLoaded().

The *templateHash* parameter should contain the digest of the template that will be required for the *inPublic* parameter of an Object creation command. If *policySession→cpHash* is already set, the TPM shall return TPM\_RC\_CPHASH. If the size of *templateHash* is not the size of *policySession→policyDigest*, the TPM shall return TPM\_RC\_SIZE. Otherwise, *policySession→cpHash* is set to *templateHash*.

If this command completes successfully, the *cpHash* of the authorized command will not be used for validation. Only the digest of the *inPublic* parameter will be used.

NOTE This allows the space normally used to hold *policySession→cpHash* to be used for *policySession→templateHash* instead.

The *policySession→policyDigest* will be updated with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyTemplate || templateHash) \quad (39)$$

23.21.2 Command and Response

Table 153 — TPM2\_PolicyTemplate Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyTemplate
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None
TPM2B_DIGEST	templateHash	the digest to be added to the policy

Table 154 — TPM2\_PolicyTemplate Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 23.21.3 Detailed Actions

**[[PolicyTemplate]]**

## 23.22 TPM2\_PolicyAuthorizeNV

### 23.22.1 General Description

This command provides a capability that is the equivalent of a revocable policy. With TPM2\_PolicyAuthorize(), the authorization ticket never expires, so the authorization may not be withdrawn. With this command, the approved policy is kept in an NV Index location so that the policy may be changed as needed to render the old policy unusable.

NOTE 1 This command is useful for Objects but of limited value for other policies that are persistently stored in TPM NV, such as the OwnerPolicy.

An authorization session providing authorization to read the NV Index shall be provided.

The authorization to read the NV Index must succeed even if *policySession* is a trial policy session.

If *policySession* is a trial policy session, the TPM will update *policySession*→*policyDigest* as shown in equation (40) below and return TPM\_RC\_SUCCESS. It will not perform any further validation. The remainder of this general description would apply only if *policySession* is not a trial policy session.

NOTE 2 If read access is controlled by policy, the policy should include a branch that authorizes a TPM2\_PolicyAuthorizeNV().

If TPMA\_NV\_WRITTEN is not SET in the Index referenced by *nvIndex*, the TPM shall return TPM\_RC\_NV\_UNINITIALIZED. If TPMA\_NV\_READLOCKED of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_LOCKED.

The *dataSize* of the NV Index referenced by *nvIndex* is required to be at least large enough to hold a properly formatted TPMT\_HA (TPM\_RC\_INSUFFICIENT).

NOTE 3 A TPMT\_HA contains a TPM\_ALG\_ID followed a digest that is consistent in size with the hash algorithm indicated by the TPM\_ALG\_ID.

It is an error (TPM\_RC\_HASH) if the first two octets of the Index are not a TPM\_ALG\_ID for a hash algorithm implemented on the TPM or if the indicated hash algorithm does not match *policySession*→*authHash*.

NOTE 4 The TPM\_ALG\_ID is stored in the first two octets in big endian format.

The TPM will compare *policySession*→*policyDigest* to the contents of the NV Index, starting at the first octet after the TPM\_ALG\_ID (the third octet) and return TPM\_RC\_VALUE if they are not the same.

NOTE 5 If the Index does not contain enough bytes for the compare, then TPM\_RC\_INSUFFICIENT is generated as indicated above.

NOTE 6 The *dataSize* of the Index may be larger than is required for this command. This permits the Index to include metadata.

If the comparison is successful, the TPM will reset *policySession*→*policyDigest* to a Zero Digest. Then it will update *policySession*→*policyDigest* with

$$policyDigest_{new} := H_{policyAlg}(policyDigest_{old} || TPM\_CC\_PolicyAuthorizeNV || nvIndex \rightarrow Name) \quad (40)$$

23.22.2 Command and Response

Table 155 — TPM2\_PolicyAuthorizeNV Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PolicyAuthorizeNV
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index of the area to read Auth Index: None
TPMI_SH_POLICY	policySession	handle for the policy session being extended Auth Index: None

Table 156 — TPM2\_PolicyAuthorizeNV Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 23.22.3 Detailed Actions

`[[PolicyAuthorizeNV]]`

## 24 Hierarchy Commands

### 24.1 TPM2\_CreatePrimary

#### 24.1.1 General Description

This command is used to create a Primary Object under one of the Primary Seeds or a Temporary Object under TPM\_RH\_NULL. The command uses a TPM2B\_PUBLIC as a template for the object to be created. The size of the *unique* field shall not be checked for consistency with the other object parameters. The command will create and load a Primary Object. The sensitive area is not returned.

NOTE 1            Since the sensitive data is not returned, the key cannot be reloaded. It can either be made persistent or it can be recreated.

NOTE 2            For interoperability, the *unique* field should not be set to a value that is larger than allowed by object parameters, so that the unmarshaling will not fail.

NOTE 3            An Empty Buffer is a legal *unique* field value.

EXAMPLE 1        A TPM\_ALG\_RSA object with a *keyBits* of 2048 in the objects parameters should have a *unique* field that is no larger than 256 bytes.

EXAMPLE 2        A TPM\_ALG\_KEYEDHASH or a TPM\_ALG\_SYMCIPHER object should have a *unique* field this is no larger than the digest produced by the object's *nameAlg*.

Any type of object and attributes combination that is allowed by TPM2\_Create() may be created by this command. The constraints on templates and parameters are the same as TPM2\_Create() except that a Primary Storage Key and a Temporary Storage Key are not constrained to use the algorithms of their parents.

For setting of the attributes of the created object, *fixedParent*, *fixedTPM*, *decrypt*, and *restricted* are implied to be SET in the parent (a Permanent Handle). The remaining attributes are implied to be CLEAR.

The TPM will derive the object from the Primary Seed indicated in *primaryHandle* using an approved KDF. All of the bits of the template are used in the creation of the Primary Key. Methods for creating a Primary Object from a Primary Seed are described in TPM 2.0 Part 1 and implemented in TPM 2.0 Part 4.

If this command is called multiple times with the same *inPublic* parameter, *inSensitive.data*, and Primary Seed, the TPM shall produce the same Primary Object.

NOTE 4            If the Primary Seed is changed, the Primary Objects generated with the new seed shall be statistically unique even if the parameters of the call are the same.

This command requires authorization. Authorization for a Primary Object attached to the Platform Primary Seed (PPS) shall be provided by *platformAuth* or *platformPolicy*. Authorization for a Primary Object attached to the Storage Primary Seed (SPS) shall be provided by *ownerAuth* or *ownerPolicy*. Authorization for a Primary Key attached to the Endorsement Primary Seed (EPS) shall be provided by *endorsementAuth* or *endorsementPolicy*.

## 24.1.2 Command and Response

Table 157 — TPM2\_CreatePrimary Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_CreatePrimary
TPMI_RH_HIERARCHY+	@primaryHandle	TPM_RH_ENDORSEMENT, TPM_RH_OWNER, TPM_RH_PLATFORM+{PP}, or TPM_RH_NULL Auth Index: 1 Auth Role: USER
TPM2B_SENSITIVE_CREATE	inSensitive	the sensitive data, see TPM 2.0 Part 1 Sensitive Values
TPM2B_PUBLIC	inPublic	the public template
TPM2B_DATA	outsideInfo	data that will be included in the creation data for this object to provide permanent, verifiable linkage between this object and some object owner data
TPML_PCR_SELECTION	creationPCR	PCR that will be used in creation data

Table 158 — TPM2\_CreatePrimary Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM_HANDLE	objectHandle	handle of type TPM_HT_TRANSIENT for created Primary Object
TPM2B_PUBLIC	outPublic	the public portion of the created object
TPM2B_CREATION_DATA	creationData	contains a TPMT_CREATION_DATA
TPM2B_DIGEST	creationHash	digest of <i>creationData</i> using <i>nameAlg</i> of <i>outPublic</i>
TPMT_TK_CREATION	creationTicket	ticket used by TPM2_CertifyCreation() to validate that the creation data was produced by the TPM
TPM2B_NAME	name	the name of the created object

### 24.1.3 Detailed Actions

**[[CreatePrimary]]**

## 24.2 TPM2\_HierarchyControl

### 24.2.1 General Description

This command enables and disables use of a hierarchy and its associated NV storage. The command allows *phEnable*, *phEnableNV*, *shEnable*, and *ehEnable* to be changed when the proper authorization is provided.

This command may be used to CLEAR *phEnable* and *phEnableNV* if *platformAuth/platformPolicy* is provided. *phEnable* may not be SET using this command.

This command may be used to CLEAR *shEnable* if either *platformAuth/platformPolicy* or *ownerAuth/ownerPolicy* is provided. *shEnable* may be SET if *platformAuth/platformPolicy* is provided.

This command may be used to CLEAR *ehEnable* if either *platformAuth/platformPolicy* or *endorsementAuth/endorsementPolicy* is provided. *ehEnable* may be SET if *platformAuth/platformPolicy* is provided.

When this command is used to CLEAR *phEnable*, *shEnable*, or *ehEnable*, the TPM will disable use of any persistent entity associated with the disabled hierarchy and will flush any transient objects associated with the disabled hierarchy.

When this command is used to CLEAR *shEnable*, the TPM will disable access to any NV index that has TPMA\_NV\_PLATFORMCREATE CLEAR (indicating that the NV Index was defined using Owner Authorization). As long as *shEnable* is CLEAR, the TPM will return an error in response to any command that attempts to operate upon an NV index that has TPMA\_NV\_PLATFORMCREATE CLEAR.

When this command is used to CLEAR *phEnableNV*, the TPM will disable access to any NV index that has TPMA\_NV\_PLATFORMCREATE SET (indicating that the NV Index was defined using Platform Authorization). As long as *phEnableNV* is CLEAR, the TPM will return an error in response to any command that attempts to operate upon an NV index that has TPMA\_NV\_PLATFORMCREATE SET.



24.2.2 Command and Response

Table 159 — TPM2\_HierarchyControl Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_HierarchyControl {NV E}
TPMI_RH_HIERARCHY	@authHandle	TPM_RH_ENDORSEMENT, TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPMI_RH_ENABLES	enable	the enable being modified TPM_RH_ENDORSEMENT, TPM_RH_OWNER, TPM_RH_PLATFORM, or TPM_RH_PLATFORM_NV
TPMI_YES_NO	state	YES if the enable should be SET, NO if the enable should be CLEAR

Table 160 — TPM2\_HierarchyControl Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.2.3 Detailed Actions

**[[HierarchyControl]]**

## 24.3 TPM2\_SetPrimaryPolicy

### 24.3.1 General Description

This command allows setting of the authorization policy for the lockout (*lockoutPolicy*), the platform hierarchy (*platformPolicy*), the storage hierarchy (*ownerPolicy*), and the endorsement hierarchy (*endorsementPolicy*).

The command requires an authorization session. The session shall use the current *authValue* or satisfy the current *authPolicy* for the referenced hierarchy.

The policy that is changed is the policy associated with *authHandle*.

If the enable associated with *authHandle* is not SET, then the associated authorization values (*authValue* or *authPolicy*) may not be used, and the TPM returns TPM\_RC\_HIERARCHY.

When *hashAlg* is not TPM\_ALG\_NULL, if the size of *authPolicy* is not consistent with the hash algorithm, the TPM returns TPM\_RC\_SIZE.

24.3.2 Command and Response

Table 161 — TPM2\_SetPrimaryPolicy Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SetPrimaryPolicy {NV}
TPMI_RH_HIERARCHY_AUTH	@authHandle	TPM_RH_LOCKOUT, TPM_RH_ENDORSEMENT, TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPM2B_DIGEST	authPolicy	an authorization policy digest; may be the Empty Buffer If <i>hashAlg</i> is TPM_ALG_NULL, then this shall be an Empty Buffer.
TPMI_ALG_HASH+	hashAlg	the hash algorithm to use for the policy If the <i>authPolicy</i> is an Empty Buffer, then this field shall be TPM_ALG_NULL.

Table 162 — TPM2\_SetPrimaryPolicy Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.3.3 Detailed Actions

`[[SetPrimaryPolicy]]`

## 24.4 TPM2\_ChangePPS

### 24.4.1 General Description

This replaces the current platform primary seed (PPS) with a value from the RNG and sets *platformPolicy* to the default initialization value (the Empty Buffer).

NOTE 1            A policy that is the Empty Buffer can match no policy.

NOTE 2            Platform Authorization is not changed.

All resident transient and persistent objects in the Platform hierarchy are flushed.

Saved contexts in the Platform hierarchy that were created under the old PPS will no longer be able to be loaded.

The policy hash algorithm for PCR is reset to TPM\_ALG\_NULL.

This command does not clear any NV Index values.

NOTE 3            Index values belonging to the Platform are preserved because the indexes may have configuration information that will be the same after the PPS changes. The Platform may remove the indexes that are no longer needed using TPM2\_NV\_UndefineSpace().

This command requires Platform Authorization.

24.4.2 Command and Response

Table 163 — TPM2\_ChangePPS Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ChangePPS {NV E}
TPMI_RH_PLATFORM	@authHandle	TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER

Table 164 — TPM2\_ChangePPS Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.4.3 Detailed Actions

**[ [ChangePPS] ]**



## 24.5 TPM2\_ChangeEPS

### 24.5.1 General Description

This replaces the current endorsement primary seed (EPS) with a value from the RNG and sets the Endorsement hierarchy controls to their default initialization values: *ehEnable* is SET, *endorsementAuth* and *endorsementPolicy* are both set to the Empty Buffer. It will flush any resident objects (transient or persistent) in the Endorsement hierarchy and not allow objects in the hierarchy associated with the previous EPS to be loaded.

NOTE In the reference implementation, *ehProof* is a non-volatile value from the RNG. It is allowed that the *ehProof* be generated by a KDF using both the EPS and SPS as inputs. If generated with a KDF, the *ehProof* can be generated on an as-needed basis or made a non-volatile value.

This command requires Platform Authorization.

24.5.2 Command and Response

Table 165 — TPM2\_ChangeEPS Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ChangeEPS {NV E}
TPMI_RH_PLATFORM	@authHandle	TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER

Table 166 — TPM2\_ChangeEPS Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.5.3 Detailed Actions

**[ [ChangeEPS] ]**

## 24.6 TPM2\_Clear

### 24.6.1 General Description

This command removes all TPM context associated with a specific Owner.

The clear operation will:

- flush resident objects (persistent and volatile) in the Storage and Endorsement hierarchies;
- delete any NV Index with `TPMA_NV_PLATFORMCREATE == CLEAR`;
- change the storage primary seed (SPS) to a new value from the TPM's random number generator (RNG),
- change *shProof* and *ehProof*,

NOTE 1            The proof values may be set from the RNG or derived from the associated new Primary Seed. If derived from the Primary Seeds, the derivation of *ehProof* shall use both the SPS and EPS. The computation shall use the SPS as an HMAC key and the derived value may then be a parameter in a second HMAC in which the EPS is the HMAC key. The reference design uses values from the RNG.

- SET *shEnable* and *ehEnable*;
- set *ownerAuth*, *endorsementAuth*, and *lockoutAuth* to the Empty Buffer;
- set *ownerPolicy*, *endorsementPolicy*, and *lockoutPolicy* to the Empty Buffer;
- set *Clock* to zero;
- set *resetCount* to zero;
- set *restartCount* to zero; and
- set *Safe* to YES.
- increment *pcrUpdateCounter*

NOTE 2            This permits an application to create a policy session that is invalidated on TPM2\_Clear. The policy needs, ideally as the first term, TPM2\_PolicyPCR(). The session is invalidated even if the PCR selection is empty.

This command requires Platform Authorization or Lockout Authorization. If TPM2\_ClearControl() has disabled this command, the TPM shall return TPM\_RC\_DISABLED.

If this command is authorized using *lockoutAuth*, the HMAC in the response shall use the new *lockoutAuth* value (that is, the Empty Buffer) when computing the response HMAC.

24.6.2 Command and Response

Table 167 — TPM2\_Clear Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Clear {NV E}
TPMI_RH_CLEAR	@authHandle	TPM_RH_LOCKOUT or TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER

Table 168 — TPM2\_Clear Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.6.3 Detailed Actions

**[[Clear]]**

## 24.7 TPM2\_ClearControl

### 24.7.1 General Description

TPM2\_ClearControl() disables and enables the execution of TPM2\_Clear().

The TPM will SET the TPM's TPMA\_PERMANENT.*disableClear* attribute if *disable* is YES and will CLEAR the attribute if *disable* is NO. When the attribute is SET, TPM2\_Clear() may not be executed.

NOTE This is to simplify the logic of TPM2\_Clear(). TPM2\_ClearControl() can be called using Platform Authorization to CLEAR the *disableClear* attribute and then execute TPM2\_Clear().

Lockout Authorization may be used to SET *disableClear* but not to CLEAR it.

Platform Authorization may be used to SET or CLEAR *disableClear*.

24.7.2 Command and Response

Table 169 — TPM2\_ClearControl Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ClearControl {NV}
TPMI_RH_CLEAR	@auth	TPM_RH_LOCKOUT or TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER
TPMI_YES_NO	disable	YES if the <i>disableOwnerClear</i> flag is to be SET, NO if the flag is to be CLEAR.

Table 170 — TPM2\_ClearControl Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 24.7.3 Detailed Actions

`[[ClearControl]]`

## 24.8 TPM2\_HierarchyChangeAuth

### 24.8.1 General Description

This command allows the authorization secret for a hierarchy or lockout to be changed using the current authorization value as the command authorization.

If *authHandle* is TPM\_RH\_PLATFORM, then *platformAuth* is changed. If *authHandle* is TPM\_RH\_OWNER, then *ownerAuth* is changed. If *authHandle* is TPM\_RH\_ENDORSEMENT, then *endorsementAuth* is changed. If *authHandle* is TPM\_RH\_LOCKOUT, then *lockoutAuth* is changed. The HMAC in the response shall use the new authorization value when computing the response HMAC.

If *authHandle* is TPM\_RH\_PLATFORM, then Physical Presence may need to be asserted for this command to succeed (see 26.2, “TPM2\_PP\_Commands”).

The authorization value may be no larger than the digest produced by the hash algorithm used for context integrity.

**EXAMPLE** If SHA384 is used in the computation of the integrity values for saved contexts, then the largest authorization value is 48 octets.

24.8.2 Command and Response

Table 171 — TPM2\_HierarchyChangeAuth Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_HierarchyChangeAuth {NV}
TPMI_RH_HIERARCHY_AUTH	@authHandle	TPM_RH_LOCKOUT, TPM_RH_ENDORSEMENT, TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPM2B_AUTH	newAuth	new authorization value

Table 172 — TPM2\_HierarchyChangeAuth Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 24.8.3 Detailed Actions

**[ [HierarchyChangeAuth] ]**

## 25 Dictionary Attack Functions

### 25.1 Introduction

A TPM is required to have support for logic that will help prevent a dictionary attack on an authorization value. The protection is provided by a counter that increments when a password authorization or an HMAC authorization fails. When the counter reaches a predefined value, the TPM will not accept, for some time interval, further requests that require authorization and the TPM is in Lockout mode. While the TPM is in Lockout mode, the TPM will return `TPM_RC_LOCKED` if the command requires use of an object's or Index's *authValue* unless the authorization applies to an entry in the Platform hierarchy.

NOTE 1 Authorizations for objects and NV Index values in the Platform hierarchy are never locked out. However, a command that requires multiple authorizations will not be accepted when the TPM is in Lockout mode unless all of the authorizations reference objects and indexes in the Platform hierarchy.

If the TPM is continuously powered for the duration of *newRecoveryTime* and no authorization failures occur, the authorization failure counter will be decremented by one. This property is called "self-healing." Self-healing shall not cause the count of failed attempts to decrement below zero.

The count of failed attempts, the lockout interval, and self-healing interval are settable using `TPM2_DictionaryAttackParameters()`. The lockout parameters and the current value of the lockout counter can be read with `TPM2_GetCapability()`.

Dictionary attack protection does not apply to an entity associated with a permanent handle (handle type == `TPM_HT_PERMANENT`) other than `TPM_RH_LOCKOUT`

### 25.2 TPM2\_DictionaryAttackLockReset

#### 25.2.1 General Description

This command cancels the effect of a TPM lockout due to a number of successive authorization failures. If this command is properly authorized, the lockout counter is set to zero.

Only one *lockoutAuth* authorization failure is allowed for this command during a *lockoutRecovery* interval (set using `TPM2_DictionaryAttackParameters()`).

25.2.2 Command and Response

Table 173 — TPM2\_DictionaryAttackLockReset Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_DictionaryAttackLockReset {NV}
TPMI_RH_LOCKOUT	@lockHandle	TPM_RH_LOCKOUT Auth Index: 1 Auth Role: USER

Table 174 — TPM2\_DictionaryAttackLockReset Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 25.2.3 Detailed Actions

**[[DictionaryAttackLockReset]]**

## 25.3 TPM2\_DictionaryAttackParameters

### 25.3.1 General Description

This command changes the lockout parameters.

The command requires Lockout Authorization.

The timeout parameters (*newRecoveryTime* and *lockoutRecovery*) indicate values that are measured with respect to the *Time* and not *Clock*.

NOTE            Use of *Time* means that the TPM shall be continuously powered for the duration of a timeout.

If *newRecoveryTime* is zero, then DA protection is disabled. Authorizations are checked but authorization failures will not cause the TPM to enter lockout.

If *newMaxTries* is zero, the TPM will be in lockout and use of DA protected entities will be disabled.

If *lockoutRecovery* is zero, then the recovery interval is `_TPM_Init` followed by `TPM2_Startup()`.

This command will set the authorization failure count (*failedTries*) to zero.

Only one *lockoutAuth* authorization failure is allowed for this command during a *lockoutRecovery* interval.



## 25.3.2 Command and Response

Table 175 — TPM2\_DictionaryAttackParameters Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_DictionaryAttackParameters {NV}
TPMI_RH_LOCKOUT	@lockHandle	TPM_RH_LOCKOUT Auth Index: 1 Auth Role: USER
UINT32	newMaxTries	count of authorization failures before the lockout is imposed
UINT32	newRecoveryTime	time in seconds before the authorization failure count is automatically decremented A value of zero indicates that DA protection is disabled.
UINT32	lockoutRecovery	time in seconds after a <i>lockoutAuth</i> failure before use of <i>lockoutAuth</i> is allowed A value of zero indicates that a reboot is required.

Table 176 — TPM2\_DictionaryAttackParameters Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 25.3.3 Detailed Actions

`[[DictionaryAttackParameters]]`

## 26 Miscellaneous Management Functions

### 26.1 Introduction

This clause contains commands that do not logically group with any other commands.

### 26.2 TPM2\_PP\_Commands

#### 26.2.1 General Description

This command is used to determine which commands require assertion of Physical Presence (PP) in addition to *platformAuth/platformPolicy*.

This command requires that *auth* is TPM\_RH\_PLATFORM and that Physical Presence be asserted.

After this command executes successfully, the commands listed in *setList* will be added to the list of commands that require that Physical Presence be asserted when the handle associated with the authorization is TPM\_RH\_PLATFORM. The commands in *clearList* will no longer require assertion of Physical Presence in order to authorize a command.

If a command is not in either list, its state is not changed. If a command is in both lists, then it will no longer require Physical Presence (for example, *setList* is processed first).

Only commands with handle types of TPMI\_RH\_PLATFORM, TPMI\_RH\_PROVISION, TPMI\_RH\_CLEAR, or TPMI\_RH\_HIERARCHY can be gated with Physical Presence. If any other command is in either list, it is discarded.

When a command requires that Physical Presence be provided, then Physical Presence shall be asserted for either an HMAC or a Policy authorization.

NOTE Physical Presence may be made a requirement of any policy.

TPM2\_PP\_Commands() always requires assertion of Physical Presence.

26.2.2 Command and Response

Table 177 — TPM2\_PP\_Commands Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_PP_Commands {NV}
TPMI_RH_PLATFORM	@auth	TPM_RH_PLATFORM+PP Auth Index: 1 Auth Role: USER + Physical Presence
TPML_CC	setList	list of commands to be added to those that will require that Physical Presence be asserted
TPML_CC	clearList	list of commands that will no longer require that Physical Presence be asserted

Table 178 — TPM2\_PP\_Commands Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 26.2.3 Detailed Actions

**[[PP\_Commands]]**

## 26.3 TPM2\_SetAlgorithmSet

### 26.3.1 General Description

This command allows the platform to change the set of algorithms that are used by the TPM. The *algorithmSet* setting is a vendor-dependent value.

If the changing of the algorithm set results in a change of the algorithms of PCR banks, then the TPM will need to be reset (`_TPM_Init` and `TPM2_Startup(TPM_SU_CLEAR)`) before the new PCR settings take effect. After this command executes successfully, if *startupType* in the next `TPM2_Startup()` is not `TPM_SU_CLEAR`, the TPM shall return `TPM_RC_VALUE` and enter Failure mode.

This command does not change the algorithms available to the platform.

NOTE           The reference implementation does not have support for this command. In particular, it does not support use of this command to selectively disable algorithms. Proper support would require modification of the unmarshaling code so that each time an algorithm is unmarshaled, it would be verified as being enabled.

26.3.2 Command and Response

Table 179 — TPM2\_SetAlgorithmSet Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SetAlgorithmSet {NV}
TPMI_RH_PLATFORM	@authHandle	TPM_RH_PLATFORM Auth Index: 1 Auth Role: USER
UINT32	algorithmSet	a TPM vendor-dependent value indicating the algorithm set selection

Table 180 — TPM2\_SetAlgorithmSet Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 26.3.3 Detailed Actions

`[[SetAlgorithmSet]]`



## 27 Field Upgrade

### 27.1 Introduction

This clause contains the commands for managing field upgrade of the firmware in the TPM. The field upgrade scheme may be used for replacement or augmentation of the firmware installed in the TPM.

**EXAMPLE 1** If an algorithm is found to be flawed, a patch of that algorithm might be installed using the firmware upgrade process. The patch might be a replacement of a portion of the code or a complete replacement of the firmware.

**EXAMPLE 2** If an additional set of ECC parameters is needed, the firmware process may be used to add the parameters to the TPM data set.

The field upgrade process uses two commands (TPM2\_FieldUpgradeStart() and TPM2\_FieldUpgradeData()). TPM2\_FieldUpgradeStart() validates that a signature on the provided digest is from the TPM manufacturer and that proper authorization is provided using *platformPolicy*.

**NOTE 1** The *platformPolicy* for field upgraded is defined by the PM and may include requirements that the upgrade be signed by the PM or the TPM owner and include any other constraints that are desired by the PM.

If the proper authorization is given, the TPM will retain the signed digest and enter the Field Upgrade mode (FUM). While in FUM, the TPM will accept TPM2\_FieldUpgradeData() commands. It may accept other commands if it is able to complete them using the previously installed firmware. Otherwise, it will return TPM\_RC\_UPGRADE.

Each block of the field upgrade shall contain the digest of the next block of the field upgrade data. That digest shall be included in the digest of the previous block. The digest of the first block is signed by the TPM manufacturer. That signature and first block digest are the parameters for TPM2\_FieldUpgradeStart(). The digest is saved in the TPM as the required digest for the next field upgrade data block and as the identifier of the field upgrade sequence.

For each field upgrade data block that is sent to the TPM by TPM2\_FieldUpgradeData(), the TPM shall validate that the digest matches the required digest and if not, shall return TPM\_RC\_VALUE. The TPM shall extract the digest of the next expected block and return that value to the caller, along with the digest of the first data block of the update sequence.

The system may attempt to abandon the firmware upgrade by using a zero-length buffer in TPM2\_FieldUpgradeData(). If the TPM is able to resume operation using the firmware present when the upgrade started, then the TPM will indicate that it has abandon the update by setting the digest of the next block to the Empty Buffer. If the TPM cannot abandon the update, it will return the expected next digest.

The system may also attempt to abandon the update because of a power interruption. If the TPM is able to resume normal operations, then it will respond normally to TPM2\_Startup(). If the TPM is not able to resume normal operations, then it will respond to any command but TPM2\_FieldUpgradeData() with TPM\_RC\_UPGRADE.

After a \_TPM\_Init, system software may not be able to resume the field upgrade that was in process when the power interruption occurred. In such case, the TPM firmware may be reset to one of two other values:

- the original firmware that was installed at the factory (“initial firmware”); or
- the firmware that was in the TPM when the field upgrade process started (“previous firmware”).

The TPM retains the digest of the first block for these firmware images and checks to see if the first block after \_TPM\_Init matches either of those digests. If so, the firmware update process restarts and the original firmware may be loaded.

NOTE 2           The TPM is required to accept the previous firmware as either a vendor-provided update or as recovered from the TPM using TPM2\_FirmwareRead().

When the last block of the firmware upgrade is loaded into the TPM (indicated to the TPM by data in the data block in a TPM vendor-specific manner), the TPM will complete the upgrade process. If the TPM is able to resume normal operations without a reboot, it will set the hash algorithm of the next block to TPM\_ALG\_NULL and return TPM\_RC\_SUCCESS. If a reboot is required, the TPM shall return TPM\_RC\_REBOOT in response to the last TPM2\_FieldUpgradeData() and all subsequent TPM commands until a \_TPM\_Init is received.

NOTE 3           Because no additional data is allowed when the response code is not TPM\_RC\_SUCCESS, the TPM returns TPM\_RC\_SUCCESS for all calls to TPM2\_FieldUpgradeData() except the last. In this manner, the TPM is able to indicate the digest of the next block. If a \_TPM\_Init occurs while the TPM is in FUM, the next block may be the digest for the first block of the original firmware. If it is not, then the TPM will not accept the original firmware until the next \_TPM\_Init when the TPM is in FUM.

During the field upgrade process, either the one specified in this clause or a vendor proprietary field upgrade process, the TPM shall preserve:

- Primary Seeds;
- Hierarchy *authValue*, *authPolicy*, and *proof* values;
- Lockout *authValue* and authorization failure count values;
- PCR *authValue* and *authPolicy* values;
- NV Index allocations and contents;
- Persistent object allocations and contents; and
- Clock.

NOTE 4           A platform manufacturer may provide a means to change preserved data to accommodate a case where a field upgrade fixes a flaw that might have compromised TPM secrets.

## 27.2 TPM2\_FieldUpgradeStart

### 27.2.1 General Description

This command uses *platformPolicy* and a TPM Vendor Authorization Key to authorize a Field Upgrade Manifest.

If the signature checks succeed, the authorization is valid and the TPM will accept TPM2\_FieldUpgradeData().

This signature is checked against the loaded key referenced by *keyHandle*. This key will have a Name that is the same as a value that is part of the TPM firmware data. If the signature is not valid, the TPM shall return TPM\_RC\_SIGNATURE.

NOTE            A loaded key is used rather than a hard-coded key to reduce the amount of memory needed for this key data in case more than one vendor key is needed.

27.2.2 Command and Response

Table 181 — TPM2\_FieldUpgradeStart Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeStart
TPMI_RH_PLATFORM	@authorization	TPM_RH_PLATFORM+{PP} Auth Index:1 Auth Role: ADMIN
TPMI_DH_OBJECT	keyHandle	handle of a public area that contains the TPM Vendor Authorization Key that will be used to validate <i>manifestSignature</i> Auth Index: None
TPM2B_DIGEST	fuDigest	digest of the first block in the field upgrade sequence
TPMT_SIGNATURE	manifestSignature	signature over <i>fuDigest</i> using the key associated with <i>keyHandle</i> (not optional)

Table 182 — TPM2\_FieldUpgradeStart Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 27.2.3 Detailed Actions

[[FieldUpgradeStart]]

## 27.3 TPM2\_FieldUpgradeData

### 27.3.1 General Description

This command will take the actual field upgrade image to be installed on the TPM. The exact format of *fuData* is vendor-specific. This command is only possible following a successful TPM2\_FieldUpgradeStart(). If the TPM has not received a properly authorized TPM2\_FieldUpgradeStart(), then the TPM shall return TPM\_RC\_FIELDUPGRADE.

The TPM will validate that the digest of *fuData* matches an expected value. If so, the TPM may buffer or immediately apply the update. If the digest of *fuData* does not match an expected value, the TPM shall return TPM\_RC\_VALUE.

## 27.3.2 Command and Response

Table 183 — TPM2\_FieldUpgradeData Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or decrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeData {NV}
TPM2B_MAX_BUFFER	fuData	field upgrade image data

Table 184 — TPM2\_FieldUpgradeData Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMT_HA+	nextDigest	tagged digest of the next block TPM_ALG_NULL if field update is complete
TPMT_HA	firstDigest	tagged digest of the first block of the sequence

### 27.3.3 Detailed Actions

**[[FieldUpgradeData]]**



## 27.4 TPM2\_FirmwareRead

### 27.4.1 General Description

This command is used to read a copy of the current firmware installed in the TPM.

The presumption is that the data will be returned in reverse order so that the last block in the sequence would be the first block given to the TPM in case of a failure recovery. If the TPM2\_FirmwareRead sequence completes successfully, then the data provided from the TPM will be sufficient to allow the TPM to recover from an abandoned upgrade of this firmware.

To start the sequence of retrieving the data, the caller sets *sequenceNumber* to zero. When the TPM has returned all the firmware data, the TPM will return the Empty Buffer as *fuData*.

The contents of *fuData* are opaque to the caller.

NOTE 1           The caller should retain the ordering of the update blocks so that the blocks sent to the TPM have the same size and inverse order as the blocks returned by a sequence of calls to this command.

NOTE 2           Support for this command is optional even if the TPM implements TPM2\_FieldUpgradeStart() and TPM2\_FieldUpgradeData().

27.4.2 Command and Response

**Table 185 — TPM2\_FirmwareRead Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FirmwareRead
UINT32	sequenceNumber	the number of previous calls to this command in this sequence set to 0 on the first call

**Table 186 — TPM2\_FirmwareRead Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_MAX_BUFFER	fuData	field upgrade image data

### 27.4.3 Detailed Actions

**[[FirmwareRead]]**

## 28 Context Management

### 28.1 Introduction

Three of the commands in this clause (TPM2\_ContextSave(), TPM2\_ContextLoad(), and TPM2\_FlushContext()) implement the resource management described in the "Context Management" clause in TPM 2.0 Part 1.

The fourth command in this clause (TPM2\_EvictControl()) is used to control the persistence of loadable objects in TPM memory. Background for this command may be found in the "Owner and Platform Evict Objects" clause in TPM 2.0 Part 1.

### 28.2 TPM2\_ContextSave

#### 28.2.1 General Description

This command saves a session context, object context, or sequence object context outside the TPM.

No authorization sessions of any type are allowed with this command and tag is required to be TPM\_ST\_NO\_SESSIONS.

NOTE This preclusion avoids complex issues of dealing with the same session in *handle* and in the session area. While it might be possible to provide specificity, it would add unnecessary complexity to the TPM and, because this capability would provide no application benefit, use of authorization sessions for audit or encryption is prohibited.

The TPM shall encrypt and integrity protect the TPM2B\_CONTEXT\_SENSITIVE *context* as described in the "Context Protections" clause in TPM 2.0 Part 1.

See the "Context Data" clause in TPM 2.0 Part 2 for a description of the *context* structure in the response.

28.2.2 Command and Response

Table 187 — TPM2\_ContextSave Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ContextSave
TPMI_DH_CONTEXT	saveHandle	handle of the resource to save Auth Index: None

Table 188 — TPM2\_ContextSave Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMS_CONTEXT	context	

### 28.2.3 Detailed Actions

**[[ContextSave]]**

## 28.3 TPM2\_ContextLoad

### 28.3.1 General Description

This command is used to reload a context that has been saved by TPM2\_ContextSave().

No authorization sessions of any type are allowed with this command and tag is required to be TPM\_ST\_NO\_SESSIONS (see note in 28.2.1).

The TPM will return TPM\_RC\_HIERARCHY if the context is associated with a hierarchy that is disabled.

NOTE Contexts for authorization sessions and for sequence objects belong to the NULL hierarchy, which is never disabled.

See the "Context Data" clause in TPM 2.0 Part 2 for a description of the values in the *context* parameter.

If the integrity HMAC of the saved context is not valid, the TPM shall return TPM\_RC\_INTEGRITY.

The TPM shall perform a check on the decrypted context as described in the "Context Confidentiality Protection" clause of TPM 2.0 Part 1 and enter failure mode if the check fails.

28.3.2 Command and Response

Table 189 — TPM2\_ContextLoad Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ContextLoad
TPMS_CONTEXT	context	the context blob

Table 190 — TPM2\_ContextLoad Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_DH_CONTEXT	loadedHandle	the handle assigned to the resource after it has been successfully loaded



### 28.3.3 Detailed Actions

`[[ContextLoad]]`

## 28.4 TPM2\_FlushContext

### 28.4.1 General Description

This command causes all context associated with a loaded object, sequence object, or session to be removed from TPM memory.

This command may not be used to remove a persistent object from the TPM.

A session does not have to be loaded in TPM memory to have its context flushed. The saved session context associated with the indicated handle is invalidated.

No sessions of any type are allowed with this command and tag is required to be TPM\_ST\_NO\_SESSIONS (see note in 28.2.1).

If the handle is for a Transient Object and the handle is not associated with a loaded object, then the TPM shall return TPM\_RC\_HANDLE.

If the handle is for an authorization session and the handle does not reference a loaded or active session, then the TPM shall return TPM\_RC\_HANDLE.

NOTE *flushHandle* is a parameter and not a handle. If it were in the handle area, the TPM would validate that the context for the referenced entity is in the TPM. When a TPM2\_FlushContext references a saved session context, it is not necessary for the context to be in the TPM. When the *flushHandle* is in the parameter area, the TPM does not validate that associated context is actually in the TPM.

## 28.4.2 Command and Response

Table 191 — TPM2\_FlushContext Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FlushContext
TPMI_DH_CONTEXT	flushHandle	the handle of the item to flush NOTE This is a use of a handle as a parameter.

Table 192 — TPM2\_FlushContext Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 28.4.3 Detailed Actions

**[[FlushContext]]**

## 28.5 TPM2\_EvictControl

### 28.5.1 General Description

This command allows certain Transient Objects to be made persistent or a persistent object to be evicted.

NOTE 1 A transient object is one that may be removed from TPM memory using either TPM2\_FlushContext or TPM2\_Startup(). A persistent object is not removed from TPM memory by TPM2\_FlushContext() or TPM2\_Startup().

If *objectHandle* is a Transient Object, then this call makes a persistent copy of the object and assigns *persistentHandle* to the persistent version of the object. If *objectHandle* is a persistent object, then the call evicts the persistent object. The call does not affect the transient object.

Before execution of TPM2\_EvictControl code below, the TPM verifies that *objectHandle* references an object that is resident on the TPM and that *persistentHandle* is a valid handle for a persistent object.

NOTE 2 This requirement simplifies the unmarshaling code so that it only need check that *persistentHandle* is always a persistent object.

If *objectHandle* references a Transient Object:

- a) The TPM shall return TPM\_RC\_ATTRIBUTES if
  - 1) it is in the hierarchy of TPM\_RH\_NULL,
  - 2) only the public portion of the object is loaded, or
  - 3) the *stClear* is SET in the object or in an ancestor key.
- b) The TPM shall return TPM\_RC\_HIERARCHY if the object is not in the proper hierarchy as determined by *auth*.
  - 1) If *auth* is TPM\_RH\_PLATFORM, the proper hierarchy is the Platform hierarchy.
  - 2) If *auth* is TPM\_RH\_OWNER, the proper hierarchy is either the Storage or the Endorsement hierarchy.
- c) The TPM shall return TPM\_RC\_RANGE if *persistentHandle* is not in the proper range as determined by *auth*.
  - 1) If *auth* is TPM\_RH\_OWNER, then *persistentHandle* shall be in the inclusive range of 81 00 00 00<sub>16</sub> to 81 7F FF FF<sub>16</sub>.
  - 2) If *auth* is TPM\_RH\_PLATFORM, then *persistentHandle* shall be in the inclusive range of 81 80 00 00<sub>16</sub> to 81 FF FF FF<sub>16</sub>.
- d) The TPM shall return TPM\_RC\_NV\_DEFINED if a persistent object exists with the same handle as *persistentHandle*.
- e) The TPM shall return TPM\_RC\_NV\_SPACE if insufficient space is available to make the object persistent.
- f) The TPM shall return TPM\_RC\_NV\_SPACE if execution of this command will prevent the TPM from being able to hold two transient objects of any kind.

NOTE 3 This requirement anticipates that a TPM may be implemented such that all TPM memory is non-volatile and not subject to endurance issues. In such case, there is no movement of an object between memory of different types and it is necessary that the TPM ensure that it is always possible for the management software to move objects to/from TPM memory in order to ensure that the objects required for command execution can be context restored.

- g) If the TPM returns TPM\_RC\_SUCCESS, the object referenced by *objectHandle* will not be flushed and both *objectHandle* and *persistentHandle* may be used to access the object.

If *objectHandle* references a persistent object:

- a) The TPM shall return TPM\_RC\_RANGE if *objectHandle* is not in the proper range as determined by *auth*. If *auth* is TPM\_RC\_OWNER, *objectHandle* shall be in the inclusive range of 81 00 00 00<sub>16</sub> to 81 7F FF FF<sub>16</sub>. If *auth* is TPM\_RC\_PLATFORM, *objectHandle* may be any valid persistent object handle.
- b) If *objectHandle* is not the same value as *persistentHandle*, return TPM\_RC\_HANDLE.
- c) If the TPM returns TPM\_RC\_SUCCESS, *objectHandle* will be removed from persistent memory and no longer be accessible.

NOTE 4            The persistent object is not converted to a transient object, as this would prevent the immediate revocation of an object by removing it from persistent memory.

## 28.5.2 Command and Response

Table 193 — TPM2\_EvictControl Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_EvictControl {NV}
TPMI_RH_PROVISION	@auth	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER
TPMI_DH_OBJECT	objectHandle	the handle of a loaded object Auth Index: None
TPMI_DH_PERSISTENT	persistentHandle	if <i>objectHandle</i> is a transient object handle, then this is the persistent handle for the object if <i>objectHandle</i> is a persistent object handle, then it shall be the same value as <i>persistentHandle</i>

Table 194 — TPM2\_EvictControl Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 28.5.3 Detailed Actions

**[[EvictControl]]**



## 29 Clocks and Timers

### 29.1 TPM2\_ReadClock

#### 29.1.1 General Description

This command reads the current TPMS\_TIME\_INFO structure that contains the current setting of *Time*, *Clock*, *resetCount*, and *restartCount*.

## 29.1.2 Command and Response

Table 195 — TPM2\_ReadClock Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ReadClock

Table 196 — TPM2\_ReadClock Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMS_TIME_INFO	currentTime	

### 29.1.3 Detailed Actions

**[[ReadClock]]**

## 29.2 TPM2\_ClockSet

### 29.2.1 General Description

This command is used to advance the value of the TPM's *Clock*. The command will fail if *newTime* is less than the current value of *Clock* or if the new time is greater than FF FF 00 00 00 00 00 00<sub>16</sub>. If both of these checks succeed, *Clock* is set to *newTime*. If either of these checks fails, the TPM shall return TPM\_RC\_VALUE and make no change to *Clock*.

NOTE This maximum setting would prevent *Clock* from rolling over to zero for approximately 8,000 years at the real time *Clock* update rate. If the *Clock* update rate was set so that TPM time was passing 33 percent faster than real time, it would still be more than 6,000 years before *Clock* would roll over to zero. Because *Clock* will not roll over in the lifetime of the TPM, there is no need for external software to deal with the possibility that *Clock* may wrap around.

If the value of *Clock* after the update makes the volatile and non-volatile versions of TPMS\_CLOCK\_INFO.*clock* differ by more than the reported update interval, then the TPM shall update the non-volatile version of TPMS\_CLOCK\_INFO.*clock* before returning.

This command requires Platform Authorization or Owner Authorization.

29.2.2 Command and Response

Table 197 — TPM2\_ClockSet Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ClockSet {NV}
TPMI_RH_PROVISION	@auth	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER
UINT64	newTime	new <i>Clock</i> setting in milliseconds

Table 198 — TPM2\_ClockSet Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 29.2.3 Detailed Actions

`[[ClockSet]]`

## 29.3 TPM2\_ClockRateAdjust

### 29.3.1 General Description

This command adjusts the rate of advance of *Clock* and *Time* to provide a better approximation to real time.

The *rateAdjust* value is relative to the current rate and not the nominal rate of advance.

EXAMPLE 1 If this command had been called three times with *rateAdjust* = TPM\_CLOCK\_COARSE\_SLOWER and once with *rateAdjust* = TPM\_CLOCK\_COARSE\_FASTER, the net effect will be as if the command had been called twice with *rateAdjust* = TPM\_CLOCK\_COARSE\_SLOWER.

The range of adjustment shall be sufficient to allow *Clock* and *Time* to advance at real time but no more. If the requested adjustment would make the rate advance faster or slower than the nominal accuracy of the input frequency, the TPM shall return TPM\_RC\_VALUE.

EXAMPLE 2 If the frequency tolerance of the TPM's input clock is +/-10 percent, then the TPM will return TPM\_RC\_VALUE if the adjustment would make *Clock* run more than 10 percent faster or slower than nominal. That is, if the input oscillator were nominally 100 megahertz (MHz), then 1 millisecond (ms) would normally take 100,000 counts. The update *Clock* should be adjustable so that 1 ms is between 90,000 and 110,000 counts.

The interpretation of “fine” and “coarse” adjustments is implementation-specific.

The nominal rate of advance for *Clock* and *Time* shall be accurate to within 15 percent. That is, with no adjustment applied, *Clock* and *Time* shall be advanced at a rate within 15 percent of actual time.

NOTE If the adjustments are incorrect, it will be possible to make the difference between advance of *Clock/Time* and real time to be as much as  $1.15^2$  or  $\sim 1.33$ .

Changes to the current *Clock* update rate adjustment need not be persisted across TPM power cycles.

29.3.2 Command and Response

Table 199 — TPM2\_ClockRateAdjust Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_ClockRateAdjust
TPMI_RH_PROVISION	@auth	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Handle: 1 Auth Role: USER
TPM_CLOCK_ADJUST	rateAdjust	Adjustment to current <i>Clock</i> update rate

Table 200 — TPM2\_ClockRateAdjust Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 29.3.3 Detailed Actions

`[[ClockRateAdjust]]`

## 30 Capability Commands

### 30.1 Introduction

The TPM has numerous values that indicate the state, capabilities, and properties of the TPM. These values are needed for proper management of the TPM. The TPM2\_GetCapability() command is used to access these values.

TPM2\_GetCapability() allows reporting of multiple values in a single call. The values are grouped according to type.

NOTE TPM2\_TestParms() is used to determine if a TPM supports a particular combination of algorithm parameters

### 30.2 TPM2\_GetCapability

#### 30.2.1 General Description

This command returns various information regarding the TPM and its current state.

The *capability* parameter determines the category of data returned. The *property* parameter selects the first value of the selected category to be returned. If there is no property that corresponds to the value of *property*, the next higher value is returned, if it exists.

EXAMPLE 1 The list of handles of transient objects currently loaded in the TPM may be read one at a time. On the first read, set the *property* to TRANSIENT\_FIRST and *propertyCount* to one. If a transient object is present, the lowest numbered handle is returned and *moreData* will be YES if transient objects with higher handles are loaded. On the subsequent call, use returned handle value plus 1 in order to access the next higher handle.

The *propertyCount* parameter indicates the number of capabilities in the indicated group that are requested. The TPM will return no more than the number of requested values (*propertyCount*) or until the last property of the requested type has been returned.

NOTE 1 The type of the capability is derived from a combination of *capability* and *property*.

NOTE 2 If the *property* selects an unimplemented property, the next higher implemented property is returned.

When all of the properties of the requested type have been returned, the *moreData* parameter in the response will be set to NO. Otherwise, it will be set to YES.

NOTE 3 The *moreData* parameter will be YES if there are more properties even if the requested number of capabilities has been returned.

The TPM is not required to return more than one value at a time. It is not required to provide the same number of values in response to subsequent requests.

EXAMPLE 2 A TPM may return 4 properties in response to a TPM2\_GetCapability(*capability* = TPM\_CAP\_TPM\_PROPERTY, *property* = TPM\_PT\_MANUFACTURER, *propertyCount* = 8 ) and for a latter request with the same parameters, the TPM may return as few as one and as many as 8 values.

When the TPM is in Failure mode, a TPM is required to allow use of this command for access of the following capabilities:

- TPM\_PT\_MANUFACTURER
- TPM\_PT\_VENDOR\_STRING\_1
- TPM\_PT\_VENDOR\_STRING\_2 (NOTE 4)
- TPM\_PT\_VENDOR\_STRING\_3 (NOTE 4)
- TPM\_PT\_VENDOR\_STRING\_4 (NOTE 4)
- TPM\_PT\_VENDOR\_TPM\_TYPE
- TPM\_PT\_FIRMWARE\_VERSION\_1
- TPM\_PT\_FIRMWARE\_VERSION\_2

NOTE 4 If the vendor string does not require one of these values, the property type does not need to exist.

A vendor may optionally allow the TPM to return other values.

If in Failure mode and a capability is requested that is not available in Failure mode, the TPM shall return no value.

EXAMPLE 3 Assume the TPM is in Failure mode and the TPM only supports reporting of the minimum required set of properties (the limited set to TPML\_TAGGED\_PCR\_PROPERTY values). If a TPM2\_GetCapability is received requesting a capability that has a property type value greater than TPM\_PT\_FIRMWARE\_VERSION\_2, the TPM will return a zero length list with the moreData parameter set to NO. If the property type is less than TPM\_PT\_MANUFACTURER, the TPM will return properties beginning with TPM\_PT\_MANUFACTURER.

In Failure mode, *tag* is required to be TPM\_ST\_NO\_SESSIONS or the TPM shall return TPM\_RC\_FAILURE.

The capability categories and the types of the return values are:

<i>capability</i>	<i>property</i>	Return Type
TPM_CAP_ALGS	TPM_ALG_ID <sup>(1)</sup>	TPML_ALG_PROPERTY
TPM_CAP_HANDLES	TPM_HANDLE	TPML_HANDLE
TPM_CAP_COMMANDS	TPM_CC	TPML_CCA
TPM_CAP_PP_COMMANDS	TPM_CC	TPML_CC
TPM_CAP_AUDIT_COMMANDS	TPM_CC	TPML_CC
TPM_CAP_PCERS	Reserved	TPML_PCR_SELECTION
TPM_CAP_TPM_PROPERTIES	TPM_PT	TPML_TAGGED_TPM_PROPERTY
TPM_CAP_PCR_PROPERTIES	TPM_PT_PCR	TPML_TAGGED_PCR_PROPERTY
TPM_CAP_ECC_CURVE	TPM_ECC_CURVE <sup>(1)</sup>	TPML_ECC_CURVE
TPM_CAP_AUTH_POLICIES		TPML_TAGGED_POLICY
TPM_CAP_VENDOR_PROPERTY	manufacturer specific	manufacturer-specific values
NOTES: (1) The TPM_ALG_ID or TPM_ECC_CURVE is cast to a UINT32		

- **TPM\_CAP\_ALGS** – Returns a list of TPMS\_ALG\_PROPERTIES. Each entry is an algorithm ID and a set of properties of the algorithm.
- **TPM\_CAP\_HANDLES** – Returns a list of all of the handles within the handle range of the *property* parameter. The range of the returned handles is determined by the handle type (the most-significant octet (MSO) of the *property*). Any of the defined handle types is allowed

EXAMPLE 4      If the MSO of *property* is TPM\_HT\_NV\_INDEX, then the TPM will return a list of NV Index values.

EXAMPLE 5      If the MSO of *property* is TPM\_HT\_PCR, then the TPM will return a list of PCR.

- For this capability, use of TPM\_HT\_LOADED\_SESSION and TPM\_HT\_SAVED\_SESSION is allowed. Requesting handles with a handle type of TPM\_HT\_LOADED\_SESSION will return handles for loaded sessions. The returned handle values will have a handle type of either TPM\_HT\_HMAC\_SESSION or TPM\_HT\_POLICY\_SESSION. If saved sessions are requested, all returned values will have the TPM\_HT\_HMAC\_SESSION handle type because the TPM does not track the session type of saved sessions.

NOTE 5            TPM\_HT\_LOADED\_SESSION and TPM\_HT\_HMAC\_SESSION have the same value, as do TPM\_HT\_SAVED\_SESSION and TPM\_HT\_POLICY\_SESSION. It is not possible to request that the TPM return a list of loaded HMAC sessions without including the policy sessions.

- **TPM\_CAP\_COMMANDS** – Returns a list of the command attributes for all of the commands implemented in the TPM, starting with the TPM\_CC indicated by the *property* parameter. If vendor specific commands are implemented, the vendor-specific command attribute with the lowest *commandIndex*, is returned after the non-vendor-specific (base) command.

NOTE 6            The type of the property parameter is a TPM\_CC while the type of the returned list is TPML\_CCA.

- **TPM\_CAP\_PP\_COMMANDS** – Returns a list of all of the commands currently requiring Physical Presence for confirmation of platform authorization. The list will start with the TPM\_CC indicated by *property*.
- **TPM\_CAP\_AUDIT\_COMMANDS** – Returns a list of all of the commands currently set for command audit.
- **TPM\_CAP\_PCRS** – Returns the current allocation of PCR in a TPML\_PCR\_SELECTION. The *property* parameter shall be zero. The TPM will always respond to this command with the full PCR allocation and *moreData* will be NO.
- **TPM\_CAP\_TPM\_PROPERTIES** – Returns a list of tagged properties. The tag is a TPM\_PT and the property is a 32-bit value. The properties are returned in groups. Each property group is on a 256-value boundary (that is, the boundary occurs when the TPM\_PT is evenly divisible by 256). The TPM will only return values in the same group as the *property* parameter in the command.
- **TPM\_CAP\_PCR\_PROPERTIES** – Returns a list of tagged PCR properties. The tag is a TPM\_PT\_PCR and the property is a TPMS\_PCR\_SELECT.

The input command property is a TPM\_PT\_PCR (see TPM 2.0 Part 2 for PCR properties to be requested) that specifies the first property to be returned. If *propertyCount* is greater than 1, the list of properties begins with that property and proceeds in TPM\_PT\_PCR sequence.

Each item in the list is a TPMS\_PCR\_SELECT structure that contains a bitmap of all PCR.

NOTE 7            A PCR index in all banks (all hash algorithms) has the same properties, so the hash algorithm is not specified here.

- TPM\_CAP\_TPM\_ECC\_CURVES – Returns a list of ECC curve identifiers currently available for use in the TPM.
- TPM\_CAP\_AUTH\_POLICIES - Returns a list of tagged policies reporting the authorization policies for the permanent handles.

The *moreData* parameter will have a value of YES if there are more values of the requested type that were not returned.

If no next capability exists, the TPM will return a zero-length list and *moreData* will have a value of NO.

## 30.2.2 Command and Response

Table 201 — TPM2\_GetCapability Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_GetCapability
TPM_CAP	capability	group selection; determines the format of the response
UINT32	property	further definition of information
UINT32	propertyCount	number of properties of the indicated type to return

Table 202 — TPM2\_GetCapability Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPMI_YES_NO	moreData	flag to indicate if there are more values of this type
TPMS_CAPABILITY_DATA	capabilityData	the capability data

### 30.2.3 Detailed Actions

`[[GetCapability]]`

### 30.3 TPM2\_TestParms

#### 30.3.1 General Description

This command is used to check to see if specific combinations of algorithm parameters are supported.

The TPM will unmarshal the provided TPMT\_PUBLIC\_PARMS. If the parameters unmarshal correctly, then the TPM will return TPM\_RC\_SUCCESS, indicating that the parameters are valid for the TPM. The TPM will return the appropriate unmarshaling error if a parameter is not valid.



30.3.2 Command and Response

**Table 203 — TPM2\_TestParms Command**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_TestParms
TPMT_PUBLIC_PARMS	parameters	algorithm parameters to be validated

**Table 204 — TPM2\_TestParms Response**

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	TPM_RC

### 30.3.3 Detailed Actions

**[[TestParms]]**

## 31 Non-volatile Storage

### 31.1 Introduction

The NV commands are used to create, update, read, and delete allocations of space in NV memory. Before an Index may be used, it must be defined (TPM2\_NV\_DefineSpace()).

An Index may be modified if the proper write authorization is provided or read if the proper read authorization is provided. Different controls are available for reading and writing.

An Index may have an Index-specific *authValue* and *authPolicy*. The *authValue* may be used to authorize reading if TPMA\_NV\_AUTHREAD is SET and writing if TPMA\_NV\_AUTHWRITE is SET. The *authPolicy* may be used to authorize reading if TPMA\_NV\_POLICYREAD is SET and writing if TPMA\_NV\_POLICYWRITE is SET.

For commands that have both *authHandle* and *nvIndex* parameters, *authHandle* can be an NV Index, Platform Authorization, or Owner Authorization. If *authHandle* is an NV Index, it must be the same as *nvIndex* (TPM\_RC\_NV\_AUTHORIZATION).

TPMA\_NV\_PPREAD and TPMA\_NV\_PPWRITE indicate if reading or writing of the NV Index may be authorized by *platformAuth* or *platformPolicy*.

TPMA\_NV\_OWNERREAD and TPMA\_NV\_OWNERWRITE indicate if reading or writing of the NV Index may be authorized by *ownerAuth* or *ownerPolicy*.

If an operation on an NV index requires authorization, and the *authHandle* parameter is the handle of an NV Index, then the *nvIndex* parameter must have the same value or the TPM will return TPM\_RC\_NV\_AUTHORIZATION.

NOTE 1 This check ensures that the authorization that was provided is associated with the NV Index being authorized.

For creating an Index, Owner Authorization may not be used if *shEnable* is CLEAR and Platform Authorization may not be used if *phEnableNV* is CLEAR.

If an Index was defined using Platform Authorization, then that Index is not accessible when *phEnableNV* is CLEAR. If an Index was defined using Owner Authorization, then that Index is not accessible when *shEnable* is CLEAR.

For read access control, any combination of TPMA\_NV\_PPREAD, TPMA\_NV\_OWNERREAD, TPMA\_NV\_AUTHREAD, or TPMA\_NV\_POLICYREAD is allowed as long as at least one is SET.

For write access control, any combination of TPMA\_NV\_PPWRITE, TPMA\_NV\_OWNERWRITE, TPMA\_NV\_AUTHWRITE, or TPMA\_NV\_POLICYWRITE is allowed as long as at least one is SET.

If an Index has been defined and not written, then any operation on the NV Index that requires read authorization will fail (TPM\_RC\_NV\_INITIALIZED). This check may be made before or after other authorization checks but shall be performed before checking the NV Index *authValue*. An authorization failure due to the NV Index not having been written shall not be logged by the dictionary attack logic.

If TPMA\_NV\_CLEAR\_STCLEAR is SET, then the TPMA\_NV\_WRITTEN will be CLEAR on each TPM2\_Startup(TPM\_SU\_CLEAR). TPMA\_NV\_CLEAR\_STCLEAR shall not be SET if the *nvIndexType* is TPM\_NT\_COUNTER.

The code in the “Detailed Actions” clause of each command is written to interface with an implementation-dependent library that allows access to NV memory. The actions assume no specific layout of the structure of the NV data.

Only one NV Index may be directly referenced in a command.

NOTE 2 This means that, if *authHandle* references an NV Index, then *nvIndex* will have the same value. However, this does not limit the number of changes that may occur as side effects. For example, any number of NV Indexes might be relocated as a result of deleting or adding a NV Index.

### 31.2 NV Counters

When an Index has the TPM\_NT\_COUNTER attribute, it behaves as a monotonic counter and may only be updated using TPM2\_NV\_Increment().

When an NV counter is created, the TPM shall initialize the 8-octet counter value with a number that is greater than any count value for any NV counter on the TPM since the time of TPM manufacture.

An NV counter may be defined with the TPMA\_NV\_ORDERLY attribute to indicate that the NV Index is expected to be modified at a high frequency and that the data is only required to persist when the TPM goes through an orderly shutdown process. The TPM may update the counter value in RAM and occasionally update the non-volatile version of the counter. An orderly shutdown is one occasion to update the non-volatile count. If the difference between the volatile and non-volatile version of the counter becomes as large as MAX\_ORDERLY\_COUNT, this shall be another occasion for updating the non-volatile count.

Before an NV counter can be used, the TPM shall validate that the count is not less than a previously reported value. If the TPMA\_NV\_ORDERLY attribute is not SET, or if the TPM experienced an orderly shutdown, then the count is assumed to be correct. If the TPMA\_NV\_ORDERLY attribute is SET, and the TPM shutdown was not orderly, then the TPM shall OR MAX\_ORDERLY\_COUNT to the contents of the non-volatile counter and set that as the current count.

NOTE 1            Because the TPM would have updated the NV Index if the difference between the count values was equal to MAX\_ORDERLY\_COUNT + 1, the highest value that could have been in the NV Index is MAX\_ORDERLY\_COUNT so it is safe to restore that value.

NOTE 2            The TPM may implement the RAM portion of the counter such that the effective value of the NV counter is the sum of both the volatile and non-volatile parts. If so, then the TPM may initialize the RAM version of the counter to MAX\_ORDERLY\_COUNT and no update of NV is necessary.

NOTE 3            When a new NV counter is created, the TPM may search all the counters to determine which has the highest value. In this search, the TPM would use the sum of the non-volatile and RAM portions of the counter. The RAM portion of the counter shall be properly initialized to reflect shutdown process (orderly or not) of the TPM.

### 31.3 TPM2\_NV\_DefineSpace

#### 31.3.1 General Description

This command defines the attributes of an NV Index and causes the TPM to reserve space to hold the data associated with the NV Index. If a definition already exists at the NV Index, the TPM will return TPM\_RC\_NV\_DEFINED.

The TPM will return TPM\_RC\_ATTRIBUTES if *nvIndexType* has a reserved value in *publicInfo*.

NOTE 1 It is not required that any of these three attributes be set.

The TPM shall return TPM\_RC\_ATTRIBUTES if TPMA\_NV\_WRITTEN, TPMA\_NV\_READLOCKED, or TPMA\_NV\_WRITELOCKED is SET.

If *nvIndexType* is TPM\_NT\_COUNTER, TPM\_NT\_BITS, TPM\_NT\_PIN\_FAIL, or TPM\_NT\_PIN\_PASS, then *publicInfo*→*dataSize* shall be set to eight (8) or the TPM shall return TPM\_RC\_SIZE.

If *nvIndexType* is TPM\_NT\_EXTEND, then *publicInfo*→*dataSize* shall match the digest size of the *publicInfo.nameAlg* or the TPM shall return TPM\_RC\_SIZE.

NOTE 2 TPM\_RC\_ATTRIBUTES could be returned by a TPM that is based on the reference code of older versions of the specification but the correct response for this error is TPM\_RC\_SIZE.

If the NV Index is an ordinary Index and *publicInfo*→*dataSize* is larger than supported by the TPM implementation then the TPM shall return TPM\_RC\_SIZE.

NOTE 3 The limit for the data size may vary according to the type of the index. For example, if the index has TPMA\_NV\_ORDERLY SET, then the maximum size of an ordinary NV Index may be less than the size of an ordinary NV Index that has TPMA\_NV\_ORDERLY CLEAR.

At least one of TPMA\_NV\_PPREAD, TPMA\_NV\_OWNERREAD, TPMA\_NV\_AUTHREAD, or TPMA\_NV\_POLICYREAD shall be SET or the TPM shall return TPM\_RC\_ATTRIBUTES.

At least one of TPMA\_NV\_PPWRITE, TPMA\_NV\_OWNERWRITE, TPMA\_NV\_AUTHWRITE, or TPMA\_NV\_POLICYWRITE shall be SET or the TPM shall return TPM\_RC\_ATTRIBUTES.

If TPMA\_NV\_CLEAR\_STCLEAR is SET, then *nvIndexType* shall not be TPM\_NT\_COUNTER or the TPM shall return TPM\_RC\_ATTRIBUTES.

If *platformAuth/platformPolicy* is used for authorization, then TPMA\_NV\_PLATFORMCREATE shall be SET in *publicInfo*. If *ownerAuth/ownerPolicy* is used for authorization, TPMA\_NV\_PLATFORMCREATE shall be CLEAR in *publicInfo*. If TPMA\_NV\_PLATFORMCREATE is not set correctly for the authorization, the TPM shall return TPM\_RC\_ATTRIBUTES.

If TPMA\_NV\_POLICY\_DELETE is SET, then the authorization shall be with Platform Authorization or the TPM shall return TPM\_RC\_ATTRIBUTES.

If *nvIndexType* is TPM\_NT\_PIN\_FAIL, then TPMA\_NV\_NO\_DA shall be SET. Otherwise, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE 4 The intent of a PIN Fail index is that its DA protection is on a per-index basis, not based on the global DA protection. This avoids conflict over which type of dictionary attack protection is in use.

If *nvIndexType* is TPM\_NT\_PIN\_FAIL or TPM\_NT\_PIN\_PASS, then at least one of TPMA\_NV\_PPWRITE, TPMA\_NV\_OWNERWRITE, or TPMA\_NV\_POLICYWRITE shall be SET or the TPM shall return TPM\_RC\_ATTRIBUTES. TPMA\_NV\_AUTHWRITE shall be CLEAR. Otherwise, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE 5 If TPMA\_NV\_AUTHWRITE was SET for a PIN Pass index, a user knowing the authorization value could decrease pinCount or increase pinLimit, defeating the purpose of a PIN Pass index. The requirement is also enforced for a PIN Fail index for consistency.

If the implementation does not support TPM2\_NV\_Increment(), the TPM shall return TPM\_RC\_ATTRIBUTES if *nvIndexType* is TPM\_NT\_COUNTER.

If the implementation does not support TPM2\_NV\_SetBits(), the TPM shall return TPM\_RC\_ATTRIBUTES if *nvIndexType* is TPM\_NT\_BITS.

If the implementation does not support TPM2\_NV\_Extend(), the TPM shall return TPM\_RC\_ATTRIBUTES if *nvIndexType* is TPM\_NT\_EXTEND.

If the implementation does not support TPM2\_NV\_UndefineSpaceSpecial(), the TPM shall return TPM\_RC\_ATTRIBUTES if TPMA\_NV\_POLICY\_DELETE is SET.

After the successful completion of this command, the NV Index exists but TPMA\_NV\_WRITTEN will be CLEAR. Any access of the NV data will return TPM\_RC\_NV\_UNINITIALIZED.

In some implementations, an NV Index with the TPM\_NT\_COUNTER attribute may require special TPM resources that provide higher endurance than regular NV. For those implementations, if this command fails because of lack of resources, the TPM will return TPM\_RC\_NV\_SPACE.

The value of *auth* is saved in the created structure. The size of *auth* is limited to be no larger than the size of the digest produced by the NV Index's *nameAlg* (TPM\_RC\_SIZE).

31.3.2 Command and Response

Table 205 — TPM2\_NV\_DefineSpace Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_DefineSpace {NV}
TPMI_RH_PROVISION	@authHandle	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPM2B_AUTH	auth	the authorization value
TPM2B_NV_PUBLIC	publicInfo	the public parameters of the NV area

Table 206 — TPM2\_NV\_DefineSpace Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 31.3.3 Detailed Actions

`[[NV_DefineSpace]]`

## 31.4 TPM2\_NV\_UndefineSpace

### 31.4.1 General Description

This command removes an Index from the TPM.

If *nvIndex* is not defined, the TPM shall return TPM\_RC\_HANDLE.

If *nvIndex* references an Index that has its TPMA\_NV\_PLATFORMCREATE attribute SET, the TPM shall return TPM\_RC\_NV\_AUTHORIZATION unless Platform Authorization is provided.

If *nvIndex* references an Index that has its TPMA\_NV\_POLICY\_DELETE attribute SET, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE            An Index with TPMA\_NV\_PLATFORMCREATE CLEAR may be deleted with Platform Authorization as long as shEnable is SET. If shEnable is CLEAR, indexes created using Owner Authorization are not accessible even for deletion by the platform.

31.4.2 Command and Response

Table 207 — TPM2\_NV\_UndefineSpace Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_UndefineSpace {NV}
TPMI_RH_PROVISION	@authHandle	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index to remove from NV space Auth Index: None

Table 208 — TPM2\_NV\_UndefineSpace Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.4.3 Detailed Actions

[[NV\_UndefineSpace]]

## 31.5 TPM2\_NV\_UndefineSpaceSpecial

### 31.5.1 General Description

This command allows removal of a platform-created NV Index that has TPMA\_NV\_POLICY\_DELETE SET.

This command requires that the policy of the NV Index be satisfied before the NV Index may be deleted. Because administrative role is required, the policy must contain a command that sets the policy command code to TPM\_CC\_NV\_UndefineSpaceSpecial. This indicates that the policy that is being used is a policy that is for this command, and not a policy that would approve another use. That is, authority to use an entity does not grant authority to undefine the entity.

Since the index is deleted, the Empty Buffer is used as the authValue when generating the response HMAC.

If *nvIndex* is not defined, the TPM shall return TPM\_RC\_HANDLE.

If *nvIndex* references an Index that has its TPMA\_NV\_PLATFORMCREATE or TPMA\_NV\_POLICY\_DELETE attribute CLEAR, the TPM shall return TPM\_RC\_ATTRIBUTES.

NOTE An Index with TPMA\_NV\_PLATFORMCREATE CLEAR may be deleted with TPM2\_UndefineSpace() as long as shEnable is SET. If shEnable is CLEAR, indexes created using Owner Authorization are not accessible even for deletion by the platform.

31.5.2 Command and Response

Table 209 — TPM2\_NV\_UndefineSpaceSpecial Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_UndefineSpaceSpecial {NV}
TPMI_RH_NV_INDEX	@nvIndex	Index to be deleted Auth Index: 1 Auth Role: ADMIN
TPMI_RH_PLATFORM	@platform	TPM_RH_PLATFORM + {PP} Auth Index: 2 Auth Role: USER

Table 210 — TPM2\_NV\_UndefineSpaceSpecial Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.5.3 Detailed Actions

`[[NV_UndefineSpaceSpecial]]`

## 31.6 TPM2\_NV\_ReadPublic

### 31.6.1 General Description

This command is used to read the public area and Name of an NV Index. The public area of an Index is not privacy-sensitive and no authorization is required to read this data.



31.6.2 Command and Response

Table 211 — TPM2\_NV\_ReadPublic Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit or encrypt session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_ReadPublic
TPMI_RH_NV_INDEX	nvIndex	the NV Index Auth Index: None

Table 212 — TPM2\_NV\_ReadPublic Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_NV_PUBLIC	nvPublic	the public area of the NV Index
TPM2B_NAME	nvName	the Name of the <i>nvIndex</i>

### 31.6.3 Detailed Actions

`[[NV_ReadPublic]]`

## 31.7 TPM2\_NV\_Write

### 31.7.1 General Description

This command writes a value to an area in NV memory that was previously defined by TPM2\_NV\_DefineSpace().

Proper authorizations are required for this command as determined by TPMA\_NV\_PPWRITE; TPMA\_NV\_OWNERWRITE; TPMA\_NV\_AUTHWRITE; and, if TPMA\_NV\_POLICY\_WRITE is SET, the *authPolicy* of the NV Index.

If the TPMA\_NV\_WRITELOCKED attribute of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_LOCKED.

NOTE 1 If authorization sessions are present, they are checked before checks to see if writes to the NV Index are locked.

If *nvIndexType* is TPM\_NT\_COUNTER, TPM\_NT\_BITS or TPM\_NT\_EXTEND, then the TPM shall return TPM\_RC\_ATTRIBUTES.

If *offset* and the *size* field of *data* add to a value that is greater than the *dataSize* field of the NV Index referenced by *nvIndex*, the TPM shall return an error (TPM\_RC\_NV\_RANGE). The implementation may return an error (TPM\_RC\_VALUE) if it performs an additional check and determines that *offset* is greater than the *dataSize* field of the NV Index.

If the TPMA\_NV\_WRITEALL attribute of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_RANGE if the size of the *data* parameter of the command is not the same as the *data* field of the NV Index.

If all checks succeed, the TPM will merge the *data.size* octets of *data.buffer* value into the *nvIndex*→*data* starting at *nvIndex*→*data[offset]*. If the NV memory is implemented with a technology that has endurance limitations, the TPM shall check that the merged data is different from the current contents of the NV Index and only perform a write to NV memory if they differ.

After successful completion of this command, TPMA\_NV\_WRITTEN for the NV Index will be SET.

NOTE 2 Once SET, TPMA\_NV\_WRITTEN remains SET until the NV Index is undefined or the NV Index is cleared.

31.7.2 Command and Response

Table 213 — TPM2\_NV\_Write Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_Write {NV}
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index of the area to write Auth Index: None
TPM2B_MAX_NV_BUFFER	data	the data to write
UINT16	offset	the offset into the NV Area

Table 214 — TPM2\_NV\_Write Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.7.3 Detailed Actions

`[[NV_Write]]`

## 31.8 TPM2\_NV\_Increment

### 31.8.1 General Description

This command is used to increment the value in an NV Index that has the TPM\_NT\_COUNTER attribute. The data value of the NV Index is incremented by one.

NOTE 1 The NV Index counter is an unsigned value.

If *nvIndexType* is not TPM\_NT\_COUNTER in the indicated NV Index, the TPM shall return TPM\_RC\_ATTRIBUTES.

If TPMA\_NV\_WRITELOCKED is SET, the TPM shall return TPM\_RC\_NV\_LOCKED.

If TPMA\_NV\_WRITTEN is CLEAR, it will be SET.

If TPMA\_NV\_ORDERLY is SET, and the difference between the volatile and non-volatile versions of this field is greater than MAX\_ORDERLY\_COUNT, then the non-volatile version of the counter is updated.

NOTE 2 If a TPM implements TPMA\_NV\_ORDERLY and an Index is defined with TPMA\_NV\_ORDERLY and TPM\_NT\_COUNTER both SET, then in the Event of a non-orderly shutdown, the non-volatile value for the counter Index will be advanced by MAX\_ORDERLY\_COUNT at the next TPM2\_Startup().

NOTE 3 An allowed implementation would keep a counter value in NV and a resettable counter in RAM. The reported value of the NV Index would be the sum of the two values. When the RAM count increments past the maximum allowed value (MAX\_ORDERLY\_COUNT), the non-volatile version of the count is updated with the sum of the values and the RAM count is reset to zero.

31.8.2 Command and Response

Table 215 — TPM2\_NV\_Increment Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_Increment {NV}
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index to increment Auth Index: None

Table 216 — TPM2\_NV\_Increment Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.8.3 Detailed Actions

`[[NV_Increment]]`



## 31.9 TPM2\_NV\_Extend

### 31.9.1 General Description

This command extends a value to an area in NV memory that was previously defined by TPM2\_NV\_DefineSpace.

If *nvIndexType* is not TPM\_NT\_EXTEND, then the TPM shall return TPM\_RC\_ATTRIBUTES.

Proper write authorizations are required for this command as determined by TPMA\_NV\_PPWRITE, TPMA\_NV\_OWNERWRITE, TPMA\_NV\_AUTHWRITE, and the *authPolicy* of the NV Index.

After successful completion of this command, TPMA\_NV\_WRITTEN for the NV Index will be SET.

NOTE 1 Once SET, TPMA\_NV\_WRITTEN remains SET until the NV Index is undefined, unless the TPMA\_NV\_CLEAR\_STCLEAR attribute is SET and a TPM Reset or TPM Restart occurs.

If the TPMA\_NV\_WRITELOCKED attribute of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_LOCKED.

NOTE 2 If authorization sessions are present, they are checked before checks to see if writes to the NV Index are locked.

The *data.buffer* parameter may be larger than the defined size of the NV Index.

The Index will be updated by:

$$nvIndex \rightarrow data_{new} := H_{nameAlg}(nvIndex \rightarrow data_{old} || data.buffer) \quad (41)$$

where

$H_{nameAlg}()$	the hash algorithm indicated in <i>nvIndex</i> → <i>nameAlg</i>
<i>nvIndex</i> → <i>data</i>	the value of the data field in the NV Index
<i>data.buffer</i>	the data buffer of the command parameter

NOTE 3 If TPMA\_NV\_WRITTEN is CLEAR, then *nvIndex*→*data* is a Zero Digest.

31.9.2 Command and Response

Table 217 — TPM2\_NV\_Extend Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_Extend {NV}
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index to extend Auth Index: None
TPM2B_MAX_NV_BUFFER	data	the data to extend

Table 218 — TPM2\_NV\_Extend Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.9.3 Detailed Actions

**[[NV\_Extend]]**

## 31.10 TPM2\_NV\_SetBits

### 31.10.1 General Description

This command is used to SET bits in an NV Index that was created as a bit field. Any number of bits from 0 to 64 may be SET. The contents of *bits* are ORed with the current contents of the NV Index.

If TPMA\_NV\_WRITTEN is not SET, then, for the purposes of this command, the NV Index is considered to contain all zero bits and *data* is ORed with that value.

If TPM\_NT\_BITS is not SET, then the TPM shall return TPM\_RC\_ATTRIBUTES.

After successful completion of this command, TPMA\_NV\_WRITTEN for the NV Index will be SET.

NOTE TPMA\_NV\_WRITTEN will be SET even if no bits were SET.

31.10.2 Command and Response

Table 219 — TPM2\_NV\_SetBits Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_SetBits {NV}
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	NV Index of the area in which the bit is to be set Auth Index: None
UINT64	bits	the data to OR with the current contents

Table 220 — TPM2\_NV\_SetBits Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.10.3 Detailed Actions

`[[NV_SetBits]]`

## 31.11 TPM2\_NV\_WriteLock

### 31.11.1 General Description

If the TPMA\_NV\_WRITEDEFINE or TPMA\_NV\_WRITE\_STCLEAR attributes of an NV location are SET, then this command may be used to inhibit further writes of the NV Index.

Proper write authorization is required for this command as determined by TPMA\_NV\_PPWRITE, TPMA\_NV\_OWNERWRITE, TPMA\_NV\_AUTHWRITE, and the *authPolicy* of the NV Index.

It is not an error if TPMA\_NV\_WRITELOCKED for the NV Index is already SET.

If neither TPMA\_NV\_WRITEDEFINE nor TPMA\_NV\_WRITE\_STCLEAR of the NV Index is SET, then the TPM shall return TPM\_RC\_ATTRIBUTES.

If the command is properly authorized and TPMA\_NV\_WRITE\_STCLEAR or TPMA\_NV\_WRITEDEFINE is SET, then the TPM shall SET TPMA\_NV\_WRITELOCKED for the NV Index. TPMA\_NV\_WRITELOCKED will be clear on the next TPM2\_Startup(TPM\_SU\_CLEAR) unless TPMA\_NV\_WRITEDEFINE is SET or if TPMA\_NV\_WRITTEN is CLEAR.

31.11.2 Command and Response

Table 221 — TPM2\_NV\_WriteLock Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_WriteLock {NV}
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index of the area to lock Auth Index: None

Table 222 — TPM2\_NV\_WriteLock Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	



### 31.11.3 Detailed Actions

`[[NV_WriteLock]]`

## 31.12 TPM2\_NV\_GlobalWriteLock

### 31.12.1 General Description

The command will SET TPMA\_NV\_WRITELOCKED for all indexes that have their TPMA\_NV\_GLOBALLOCK attribute SET.

If an Index has both TPMA\_NV\_WRITELOCKED and TPMA\_NV\_WRITEDEFINE SET, then this command will permanently lock the NV Index for writing unless TPMA\_NV\_WRITTEN is CLEAR.

**NOTE** If an Index is defined with TPMA\_NV\_GLOBALLOCK SET, then the global lock does not apply until the next time this command is executed.

This command requires either platformAuth/platformPolicy or ownerAuth/ownerPolicy.

31.12.2 Command and Response

Table 223 — TPM2\_NV\_GlobalWriteLock Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_GlobalWriteLock {NV}
TPMI_RH_PROVISION	@authHandle	TPM_RH_OWNER or TPM_RH_PLATFORM+{PP} Auth Index: 1 Auth Role: USER

Table 224 — TPM2\_NV\_GlobalWriteLock Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.12.3 Detailed Actions

`[[NV_GlobalWriteLock]]`

### 31.13 TPM2\_NV\_Read

#### 31.13.1 General Description

This command reads a value from an area in NV memory previously defined by TPM2\_NV\_DefineSpace().

Proper authorizations are required for this command as determined by TPMA\_NV\_PPREAD, TPMA\_NV\_OWNERREAD, TPMA\_NV\_AUTHREAD, and the *authPolicy* of the NV Index.

If TPMA\_NV\_READLOCKED of the NV Index is SET, then the TPM shall return TPM\_RC\_NV\_LOCKED.

If *offset* and the *size* field of *data* add to a value that is greater than the *dataSize* field of the NV Index referenced by *nvIndex*, the TPM shall return an error (TPM\_RC\_NV\_RANGE). The implementation may return an error (TPM\_RC\_VALUE) if it performs an additional check and determines that *offset* is greater than the *dataSize* field of the NV Index.

For an NV Index with the TPM\_NT\_COUNTER or TPM\_NT\_BITS attribute SET, the TPM may ignore the *offset* parameter and use an offset of 0. Therefore, it is recommended that the caller set the *offset* parameter to 0 for interoperability.

NOTE 1            If authorization sessions are present, they are checked before the read-lock status of the NV Index is checked.

If the NV Index has been defined but the TPMA\_NV\_WRITTEN attribute is CLEAR, then this command shall return TPM\_RC\_NV\_UNINITIALIZED even if *size* is zero.

The *data* parameter in the response may be encrypted using parameter encryption.

31.13.2 Command and Response

Table 225 — TPM2\_NV\_Read Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_Read
TPMI_RH_NV_AUTH	@authHandle	the handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index to be read Auth Index: None
UINT16	size	number of octets to read
UINT16	offset	octet offset into the area This value shall be less than or equal to the size of the <i>nvIndex</i> data.

Table 226 — TPM2\_NV\_Read Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	
TPM2B_MAX_NV_BUFFER	data	the data read

### 31.13.3 Detailed Actions

**[[NV\_Read]]**

## 31.14 TPM2\_NV\_ReadLock

### 31.14.1 General Description

If TPMA\_NV\_READ\_STCLEAR is SET in an Index, then this command may be used to prevent further reads of the NV Index until the next TPM2\_Startup (TPM\_SU\_CLEAR).

Proper authorizations are required for this command as determined by TPMA\_NV\_PPREAD, TPMA\_NV\_OWNERREAD, TPMA\_NV\_AUTHREAD, and the *authPolicy* of the NV Index.

NOTE Only an entity that may read an Index is allowed to lock the NV Index for read.

If the command is properly authorized and TPMA\_NV\_READ\_STCLEAR of the NV Index is SET, then the TPM shall SET TPMA\_NV\_READLOCKED for the NV Index. If TPMA\_NV\_READ\_STCLEAR of the NV Index is CLEAR, then the TPM shall return TPM\_RC\_ATTRIBUTES. TPMA\_NV\_READLOCKED will be CLEAR by the next TPM2\_Startup(TPM\_SU\_CLEAR).

It is not an error to use this command for an Index that is already locked for reading.

An Index that had not been written may be locked for reading.



31.14.2 Command and Response

Table 227 — TPM2\_NV\_ReadLock Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_ReadLock {NV}
TPMI_RH_NV_AUTH	@authHandle	the handle indicating the source of the authorization value Auth Index: 1 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	the NV Index to be locked Auth Index: None

Table 228 — TPM2\_NV\_ReadLock Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.14.3 Detailed Actions

`[[NV_ReadLock]]`

## 31.15 TPM2\_NV\_ChangeAuth

### 31.15.1 General Description

This command allows the authorization secret for an NV Index to be changed.

If successful, the authorization secret (*authValue*) of the NV Index associated with *nvIndex* is changed.

This command requires that a policy session be used for authorization of *nvIndex* so that the ADMIN role may be asserted and that *commandCode* in the policy session context shall be TPM\_CC\_NV\_ChangeAuth. That is, the policy must contain a specific authorization for changing the authorization value of the referenced entity.

**NOTE** The reason for this restriction is to ensure that the administrative actions on *nvIndex* require explicit approval while other commands may use policy that is not command-dependent.

The size of the *newAuth* value may be no larger than the size of authorization indicated when the NV Index was defined.

Since the NV Index authorization is changed before the response HMAC is calculated, the *newAuth* value is used when generating the response HMAC key if required. See TPM 2.0 Part 4 ComputeResponseHMAC().

31.15.2 Command and Response

Table 229 — TPM2\_NV\_ChangeAuth Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_ChangeAuth {NV}
TPMI_RH_NV_INDEX	@nvIndex	handle of the entity Auth Index: 1 Auth Role: ADMIN
TPM2B_AUTH	newAuth	new authorization value

Table 230 — TPM2\_NV\_ChangeAuth Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	

### 31.15.3 Detailed Actions

`[[NV_ChangeAuth]]`

## 31.16 TPM2\_NV\_Certify

### 31.16.1 General Description

The purpose of this command is to certify the contents of an NV Index or portion of an NV Index.

If the *sign* attribute is not SET in the key referenced by *signHandle* then the TPM shall return TPM\_RC\_KEY.

If the NV Index has been defined but the TPMA\_NV\_WRITTEN attribute is CLEAR, then this command shall return TPM\_RC\_NV\_UNINITIALIZED even if *size* is zero.

If proper authorization for reading the NV Index is provided, the portion of the NV Index selected by *size* and *offset* are included in an attestation block and signed using the key indicated by *signHandle*. The attestation includes *size* and *offset* so that the range of the data can be determined. It also includes the NV index Name.

For an NV Index with the TPM\_NT\_COUNTER or TPM\_NT\_BITS attribute SET, the TPM may ignore the *offset* parameter and use an offset of 0. Therefore, it is recommended that the caller set the *offset* parameter to 0 for interoperability.

If *offset* and *size* add to a value that is greater than the *dataSize* field of the NV Index referenced by *nvIndex*, the TPM shall return an error (TPM\_RC\_NV\_RANGE). The implementation may return an error (TPM\_RC\_VALUE) if it performs an additional check and determines that *offset* is greater than the *dataSize* field of the NV Index, or if *size* is greater than MAX\_NV\_BUFFER\_SIZE.

NOTE 1            See 18.1 for description of how the signing scheme is selected.

NOTE 2            If *signHandle* is TPM\_RH\_NULL, the TPMS\_ATTEST structure is returned and *signature* is a NULL Signature.

## 31.16.2 Command and Response

Table 231 — TPM2\_NV\_Certify Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_NV_Certify
TPMI_DH_OBJECT+	@signHandle	handle of the key used to sign the attestation structure Auth Index: 1 Auth Role: USER
TPMI_RH_NV_AUTH	@authHandle	handle indicating the source of the authorization value for the NV Index Auth Index: 2 Auth Role: USER
TPMI_RH_NV_INDEX	nvIndex	Index for the area to be certified Auth Index: None
TPM2B_DATA	qualifyingData	user-provided qualifying data
TPMT_SIG_SCHEME+	inScheme	signing scheme to use if the <i>scheme</i> for <i>signHandle</i> is TPM_ALG_NULL
UINT16	size	number of octets to certify
UINT16	offset	octet offset into the area This value shall be less than or equal to the size of the <i>nvIndex</i> data.

Table 232 — TPM2\_NV\_Certify Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	.
TPM2B_ATTEST	certifyInfo	the structure that was signed
TPMT_SIGNATURE	signature	the asymmetric signature over <i>certifyInfo</i> using the key referenced by <i>signHandle</i>

### 31.16.3 Detailed Actions

`[[NV_Certify]]`



## 32 Vendor Specific

### 32.1 Introduction

This section contains commands that are vendor specific but made public in order to prevent proliferation. This specification does define TPM2\_Vendor\_TCG\_Test() in order to have at least one command that can be used to insure the proper operation of the command dispatch code when processing a vendor-specific command.

### 32.2 TPM2\_Vendor\_TCG\_Test

#### 32.2.1 General Description

This is a placeholder to allow testing of the dispatch code.

32.2.2 Command and Response

Table 233 — TPM2\_Vendor\_TCG\_Test Command

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS if an audit session is present; otherwise, TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_Vendor_TCG_Test
TPM2B_DATA	inputData	dummy data

Table 234 — TPM2\_Vendor\_TCG\_Test Response

Type	Name	Description
TPM_ST	tag	see clause 6
UINT32	responseSize	
TPM_RC	responseCode	TPM_RC_SUCCESS
TPM2B_DATA	outputData	dummy data

### 32.2.3 Detailed Actions

`[[Vendor_TCG_Test]]`