ISO/IEC 11889-1:2015-12 (E)

Information technology - Trusted Platform Module Library - Part 1: Architecture

Contents

Page

Foreword xiv
Introduction xv
1 Scope 1
2 Normative references 2
3 Terms and definitions 3
4 Symbols and Abbreviated Terms 12
4.1 Symbols 12
4.2 Abbreviations 13
5 Conventions 15
5.1 Bit and Octet Numbering and Order 15
5.2 Sized Buffer References 15
5.3 Numbers 16
5.4 KDF Label Parameters 16
6 ISO/IEC 11889 Organization 17
7 Compliance 19
8 Changes from Previous Versions 20
9 Trusted Platforms 21
9.1 Trust 21
9.2 Trust Concepts 21
9.2.1 Trusted Building Block 21
9.2.2 Trusted Computing Base 21
9.2.3 Trust Boundaries 21
9.2.4 Transitive Trust 22
9.2.5 Trust Authority 22
9.3 Trusted Platform Module 23
9.4 Roots of Trust 23
9.4.1 Introduction 23
9.4.2 Root of Trust for Measurement (RTM) 24
9.4.3 Root of Trust for Storage (RTS) 24
9.4.4 Root of Trust for Reporting (RTR) 24
9.5 Basic Trusted Platform Features 25
9.5.1 Introduction 25
9.5.2 Certification 26
9.5.3 Attestation and Authentication 26
9.5.4 Protected Location 29
9.5.5 Integrity Measurement and Reporting 30
10 TPM Protections 31
10.1 Introduction 31
10.2 Protection of Protected Capabilities 31
10.3 Protection of Shielded Locations 31
10.4 Exceptions and Clarifications 31
11 TPM Architecture 33
11.1 Introduction 33
11.2 TPM Command Processing Overview 33

11.3 I/O Buffer 37
11.4 Cryptography Subsystem 37
11.4.1 Introduction 37
11.4.2 Hash Functions 37
11.4.3 HMAC Algorithm 38
11.4.4 Asymmetric Operations 38
11.4.5 Signature Operations 39
11.4.6 Symmetric Encryption 41
11.4.7 Extend 43
11.4.8 Key Generation 43
11.4.9 Key Derivation Function 43
11.4.10 Random Number Generator (RNG) Module 47
11.4.11 Algorithms 49
11.5 Authorization Subsystem 50
11.6 Random Access Memory 51
11.6.1 Introduction 51
11.6.2 Platform Configuration Registers (PCR) 51
11.6.3 Object Store 52
11.6.4 Session Store 52
11.6.5 Size Requirements 52
11.7 Non-Volatile (NV) Memory 53
11.8 Power Detection Module 53
12 TPM Operational States 54
12.1 Introduction 54
12.2 Basic TPM Operational States 54
12.2.1 Power-off State 54
12.2.2 Initialization State 54
12.2.3 Startup State 55
12.2.4 Shutdown State 58
12.2.5 Startup Alternatives 58
12.3 Self-Test Modes 59
12.4 Failure Mode 60
12.5 Field Upgrade 61
12.5.1 Introduction 61
12.5.2 Field Upgrade Mode 61
12.5.3 Preserved TPM State 64
12.5.4 Field Upgrade Implementation Options 65
13 TPM Control Domains 66
13.1 Introduction 66
13.2 Controls 66
13.3 Platform Controls 67
13.4 Owner Controls 68
13.5 Privacy Administrator Controls 68
13.6 Primary Seed Authorizations 69
13.7 Lockout Control 69
13.8 TPM Ownership 70
13.8.1 Taking Ownership 70
13.8.2 Releasing Ownership 70
14 Primary Seeds 72

14.1 Introduction 72
14.2 Rationale 72
14.3 Primary Seed Properties 73
14.3.1 Introduction 73
14.3.2 Endorsement Primary Seed (EPS) 73
14.3.3 Platform Primary Seed (PPS) 74
14.3.4 Storage Primary Seed (SPS) 74
14.3.5 The Null Seed 74
14.4 Hierarchy Proofs 74
15 TPM Handles 76
15.1 Introduction 76
15.2 PCR Handles (MSO=00_{16}) 76
15.3 NV Index Handles (MSO=01_{16}) 76
15.4 Session Handles (MSO=02_{16} and 03_{16}) 76
15.5 Permanent Resource Handles (MSO=40_{16}) 77
15.6 Transient Object Handles (MSO=80_{16}) 77
15.7 Persistent Object Handles (MSO=81_{16}) 77
16 Names 78
17 PCR Operations 80
17.1 Initializing PCR 80
17.2 Extend of a PCR 80
17.3 Using Extend with PCR Banks 80
17.4 Recording Events 81
17.5 Selecting Multiple PCR 81
17.6 Reporting on PCR 82
17.6.1 Reading PCR 82
17.6.2 Attesting to PCR 82
17.7 PCR Authorizations 83
17.7.1 Introduction 83
17.7.2 PCR Not in a Set 83
17.7.3 Authorization Set 83
17.7.4 Policy Set 84
17.7.5 Order of Checking 84
17.8 PCR Allocation 84
17.9 PCR Change Tracking 84
17.10 Other Uses for PCR 85
18 TPM Command/Response Structure 86
18.1 Introduction 86
18.2 Command/Response Header Fields 88
18.2.1 Introduction 88
18.2.2 *tag* 88
18.2.3 commandSize/responseSize 88
18.2.4 commandCode 88
18.2.5 responseCode 88
18.3 Handles 89
18.4 Parameters 89
18.5 *authorizationSize*/*parameterSize* 90

18.6 Authorization Area 90
18.6.1 Introduction 90
18.6.2 Authorization Structure 92
18.6.3 Session Handles 93
18.6.4 Session Attributes (*sessionAttributes*) 93
18.7 Command Parameter Hash (*cpHash*) 95
18.8 Response Parameter Hash (*rpHash*) 95
18.9 Command Example 96
18.10 Response Example 97
19 Authorizations and Acknowledgments 99
19.1 Introduction 99
19.2 Authorization Roles 99
19.3 Physical Presence Authorization 100
19.4 Password Authorizations 101
19.5 Sessions 102
19.6 Session-Based Authorizations 102
19.6.1 Introduction 102
19.6.2 Authorization Session Formats 103
19.6.3 Session Nonces 103
19.6.4 Authorization Values 105
19.6.5 HMAC Computation 106
19.6.6 Note on Use of Nonces in HMAC Computations 107
19.6.7 Starting an Authorization Session 107
19.6.8 *sessionKey* Creation 108
19.6.9 Unbound and Unsalted Session Key Generation 109
19.6.10 Bound Session Key Generation 110
19.6.11 Salted Session Key Generation 112
19.6.12 Salted and Bound Session Key Generation 113
19.6.13 Encryption of *salt* 114
19.6.14 Caution on use of Unsalted Authorization Sessions 115
19.6.15 No HMAC Authorization 115
19.6.16 Authorization Selection Logic for Objects 116
19.6.17 Authorization Session Termination 116
19.7 Enhanced Authorization 117
19.7.1 Introduction 117
19.7.2 Policy Assertion 118
19.7.3 Policy AND 118
19.7.4 Policy OR 120
19.7.5 Order of Evaluation 122
19.7.6 Policy Assertions (Policy Commands) 122
19.7.7 Policy Session Context Values 125
19.7.8 Policy Example 126
19.7.9 Trial Policy 127
19.7.10 Modification of Policies 127
19.7.11 TPM2_PolicySigned(), TPM2_PolicySecret(), and TPM2_PolicyTicket() 128
19.8 Policy Session Creation 130
19.9 Use of TPM for *authPolicy* Computation 131

19.10 Trial Policy Session 131
19.11 Dictionary Attack Protection 132
19.11.1 Introduction 132
19.11.2 Lockout Mode Configuration Parameters 132
19.11.3 Lockout Mode 133
19.11.4 Recovering from Lockout Mode 133
19.11.5 Authorization Failures Involving lockoutAuth 134
19.11.6 Non-orderly Shutdown 134
19.11.7 Justification for Lockout Due to Session Binding 134
19.11.8 Sample Configurations for Lockout Parameters 135
20 Audit Session 136
20.1 Introduction 136
20.2 Exclusive Audit Sessions 137
20.3 Command Gating Based on Exclusivity 137
20.4 Audit Session Reporting 137
20.5 Audit Establishment Failures 138
21 Session-based encryption 139
21.1 Introduction 139
21.2 XOR Parameter Obfuscation 140
21.3 CFB Mode Parameter Encryption 140
22 Protected Storage 142
22.1 Introduction 142
22.2 Object Protections 142
22.3 Protection Values 142
22.4 Symmetric Encryption 143
22.5 Integrity 144
23 Protected Storage Hierarchy 146
23.1 Introduction 146
23.2 Hierarchical Relationship between Objects 146
23.3 Duplication 147
23.3.1 Definition 147
23.3.2 Protections 148
23.4 Duplication Group 153
23.5 Protection Group 155
23.6 Summary of Hierarchy Attributes 156
23.7 Primary Seed Hierarchies 156
23.8 Hierarchy Attributes Settings Matrix 156
24 Credential Protection 158
24.1 Introduction 158
24.2 Protocol 158
24.3 Protection of Credential 159
24.4 Symmetric Encrypt 159
24.5 HMAC 159
24.6 Summary of Protection Process 161
25 Object Attributes 162
25.1 Base Attributes 162
25.1.1 Introduction 162
25.1.2 *Restricted* Attribute 162
25.1.3 *Sign* Attribute 162

25.1.4 *Decrypt* Attribute 163
25.1.5 Uses 163
25.2 Other Attributes 165
25.2.1 fixedTPM and fixedParent 165
25.2.2 stClear 165
25.2.3 sensitiveDataOrigin 165
25.2.4 userWithAuth 165
25.2.5 adminWithPolicy 165
25.2.6 noDA 166
25.2.7 encryptedDuplication 166
26 Object Structure Elements 167
26.1 Introduction 167
26.2 Public Area 167
26.3 Sensitive Area 168
26.4 Private Area 168
26.5 Qualified Name 169
26.6 Sensitive Area Encryption 169
26.7 Sensitive Area Integrity 170
27 Object Creation 171
27.1 Introduction 171
27.2 Public Area Template 171
27.2.1 Introduction 171
27.2.2 type 171
27.2.3 nameAlg 172
27.2.4 objectAttributes 172
27.2.5 authPolicy 172
27.2.6 parameters 172
27.2.7 unique 172
27.3 Sensitive Values 172
27.3.1 Overview 172
27.3.2 userAuth 173
27.3.3 data 173
27.4 Creation PCR 173
27.5 Public Area Creation 173
27.5.1 Introduction 173
27.5.2 type, nameAlg, objectAttributes, authPolicy, and parameters 173
27.5.3 unique 174
27.6 Sensitive Area Creation 175
27.6.1 Introduction 175
27.6.2 type 175
27.6.3 authValue 175
27.6.4 *seedValue* 175
27.6.5 sensitive 176
27.7 Creation Data and Ticket 177
27.8 Creation Resources 178
28 Object Loading 179

28.1 Introduction 179
28.2 Load of an Ordinary Object 179
28.3 Public-only Load 179
28.4 External Object Load 180
29 Object Creation in Reference Implementation 181
30 Context Management 182
30.1 Introduction 182
30.2 Context Data 183
30.2.1 Introduction 183
30.2.2 Sequence Number 183
30.2.3 Handle 184
30.2.4 Hierarchy 185
30.3 Context Protections 185
30.3.1 Context Confidentiality Protection 185
30.3.2 Context Integrity Protection 186
30.4 Object Context Management 187
30.5 Session Context Management 187
30.6 Eviction 188
30.7 Incidental Use of Object Slots 189
31 Attestation 190
31.1 Introduction 190
31.2 Standard Attestation Structure 190
31.3 Privacy 191
31.4 Qualifying Data 191
31.5 Anonymous Signing 191
32 Cryptographic Support Functions 192
32.1 Introduction 192
32.2 Hash 192
32.3 HMAC 192
32.4 Hash, HMAC, and Event Sequences 193
32.4.1 Introduction 193
32.4.2 Hash Sequence 193
32.4.3 Event Sequence 193
32.4.4 HMAC Sequence 194
32.4.5 Sequence Contexts 194
32.5 Symmetric Encryption 194
32.6 Asymmetric Encryption and Signature Operations 194
33 Locality 195
34 Hardware Core Root of Trust Measurement (H-CRTM) Event Sequence 196
34.1 Introduction 196
34.2 Dynamic Root of Trust Measurement 196
34.3 H-CRTM before TPM2_Startup() 197
35 Command Audit 198
36 Timing Components 200
36.1 Introduction 200
36.2 Clock 201
36.2.1 Introduction 201
36.2.2 *Clock* Implementation 201

36.2.3 Orderly Shutdown of *Clock* 202
36.2.4 *Clock* Initialization at TPM2_Startup() 202
36.2.5 Setting *Clock* 203
36.2.6 *Clock* Periodicity 203
36.3 Time 204
36.4 resetCount 204
36.5 restartCount 204
36.6 Note on the Accuracy and Reliability of *Clock* 205
36.7 Privacy Aspects of Clock 206
37 NV Memory 207
37.1 Introduction 207
37.2 NV Indices 207
37.2.1 Definition 207
37.2.2 NV Index Allocation 208
37.2.3 NV Index Deletion 209
37.2.4 High-Endurance (Hybrid) Indices 209
37.2.5 Reading an NV Index 210
37.2.6 Updating an Index 211
37.2.7 NV Index in a Policy 214
37.3 Owner and Platform Evict Objects 214
37.4 State Saved by TPM2_Shutdown() 215
37.4.1 Background 215
37.4.2 NV Orderly Data 215
37.4.3 NV Clear Data 216
37.4.4 NV Reset Data 217
37.5 Persistent NV Data 218
37.6 NV Rate Limiting 220
37.7 NV Other Considerations 220
37.7.1 Power Interruption 220
37.7.2 External NV 220
37.7.3 PCR in NV 221
38 Multi-Tasking 222
39 Errors and Response Codes 223
39.1 Error Reporting 223
39.2 TPM State After an Error 223
39.3 Resource Exhaustion Warnings 223
39.3.1 Introduction 223
39.3.2 Transient Resources 223
39.3.3 Temporary Resources 224
39.4 Response Code Details 224
40 General Purpose I/O 226
41 Minimums 227
41.1 Introduction 227
41.2 Authorization Sessions 227
41.3 Transient Objects 227
41.4 NV Counters and Bit Fields 227
Annex A (normative) RSA 228

A.1 Introduction 228
A.2 RSAEP 229
A.3 RSADP 229
A.4 RSAES_OAEP 229
A.5 RSAES_PKCSV1_5 229
A.6 RSASSA_PKCS1v1_5 229
A.7 RSASSA_PSS 230
A.8 RSA Cryptographic Primitives 231
A.8.1 Introduction 231
A.8.2 TPM2_RSA_Encrypt() 231
A.8.3 TPM2_RSA_Decrypt() 231
A.9 Secret Sharing 231
A.9.1 Overview 231
A.9.2 RSA Encryption of Salt 231
A.9.3 RSA Secret Sharing for Duplication 232
A.9.4 RSA Secret Sharing for Credentials 232
Annex B (normative) ECC 233
B.1 Introduction 233
B.2 Split Operations 233
B.2.1 Introduction 233
B.2.2 Commit Random Value 233
B.2.3 TPM2_Commit() 234
B.2.4 TPM2_EC_Ephemeral() 235
B.2.5 Recovering the Private Ephemeral Key 236
B.3 ECC-Based Secret Sharing 236
B.4 EC Signing 236
B.4.1 ECDSA 236
B.4.2 ECDAA 236
B.4.3 EC Schnorr 239
B.5 Secret Sharing 240
B.5.1 ECDH 240
B.5.2 ECDH Encryption of Salt 241
B.5.3 ECC Secret Sharing for Duplication 241
B.5.4 ECC Secret Sharing for Credentials 241
B.6 ECC Primitive Operations 241
B.6.1 Introduction 241
B.6.2 TPM2_ECDH_KeyGen() 241
B.6.3 TPM2_ECDH_ZGen() 241
B.6.4 Two-phase Key Exchange 242
Annex C (normative) Support for SMx Family of Algorithms 244
C.1 Introduction 244
C.1 SM2 244
C.1.1 Introduction 244
C.1.2 SM2 Digital Signature Algorithm 245
C.1.3 SM2 Key Exchange 247

C.2 SM3 248
C.3 SM4 248
Annex D (informative) Key Generation 249
D.1 Introduction 249
D.2 RSA Key Generation 249
D.2.1 Background 249
D.2.2 Prime Generation 249
D.2.3 Key Generation Algorithm 250
D.3 ECC Ordinary Keys 251
D.4 ECC Primary key 251
Annex E (informative) Policy Examples 252
E.1 Introduction 252
E.2 ISO/IEC 11889 (first edition) Compatible Authorization 252
Annex F (informative) Acknowledgements and contributors 254
F.1 Acknowledgements 254
F.2 Contributors 254
Bibliography 256

Tables

Table 1 — KDF Label Parameters 16
Table 2 — Block Cipher Parameters 41
Table 3 — Hierarchy Control Setting Combinations 67
Table 4 — Equations for Computing Entity Names 78
Table 5 — Separators 87
Table 6 — *Tag* Values 88
Table 7 — Use of Authorization/Session Blocks 91
Table 8 — Description of *sessionAttributes* 93
Table 9 — Command Layout for Example Command 96
Table 10 — Example Command Showing *authorizationSize* 97
Table 11 — Response Layout for Example Command 97
Table 12 — Example Response Showing *parameterSize* 98
Table 13 — Password Authorization of Command 101
Table 14 — Password Acknowledgment in Response 101
Table 15 — Session-Based Authorization of Command 103
Table 16 — Session-Based Acknowledgment in Response 103
Table 17 — Schematic of TPM2_StartAuthSession Command 107
Table 18 — Handle Parameters for TPM2_StartAuthSession 108
Table 19 — Format to Start Unbounded, Unsalted Session 109
Table 20 — Format to Start Bound Session 111

Table 21 — Format to Start Salted Session 112
Table 22 — Format to Start Salted and Bound Session 113
Table 23 — Mapping of Hierarchy Attributes 156
Table 24 — Allowed Hierarchy Settings 156
Table 25 — Mapping of Functional Attributes 163
Table 26 — ISO/IEC 11889 (first edition) Correspondence 164
Table 27 — Public Area Parameters 167
Table 28 — Sensitive Area Parameters 168
Table 29 — Standard Attestation Structure 190
Table 30 — Contents of the ORDERLY_DATA Structure 216
Table 31 — Contents of the STATE_CLEAR_DATA Structure 216
Table 32 — Contents of the STATE_RESET_DATA Structure 217
Table 33 — Contents of the PERSISTENT_DATA Structure 218

Figures

Figure 1 — Attestation Hierarchy 30
Figure 2 — Architectural Overview 36
Figure 3 — Command Execution Flow 40
Figure 4 — Random Number Generation 51
Figure 5 — TPM Startup Sequences 60
Figure 6 — On-Demand Self-Test 62
Figure 7 — Failure Mode Behavior 64
Figure 8 — Resuming FUM after _TPM_Init 66
Figure 9 — Field Upgrade Mode 67
Figure 10 — Command Structure 90
Figure 11 — Response Structure 90
Figure 12 — Command/Response Header Structure 91
Figure 13 — Authorization Layout for Command 95
Figure 14 — Authorization Layout for Response 95
Figure 15 — A Policy Evaluation 121
Figure 16 — Two Different Policy Expressions 122
Figure 17 — A Four-Term Policy 122
Figure 18 — Policy with an OR 123
Figure 19 — Policy where only one OR Branch is Evaluated 124
Figure 20 — A 12-input OR Policy 124
Figure 21 — Use of TPM2_PolicyAuthorize() to Avoid PCR Brittleness 131
Figure 22 — Creating a Private Structure 148
Figure 23 — Symmetric Protection of Hierarchy 150
Figure 24 — Duplication Process with Inner and Outer Wrapper 154
Figure 25 — Duplication Process with Outer Wrapper and No Inner Wrapper 155
Figure 26 — Duplication Process with Inner Wrapper and TPM_RH_NULL as NP 156
Figure 27 — Duplication Process with no Inner Wrapper and TPM_RH_NULL as NP 156
Figure 28 — Duplication Groups 158
Figure 29 — Protection Groups 158
Figure 30 — Creating a Identity Structure 164
Figure 31 — Response Code Evaluation 228