ISO/IEC 11889-2:2009-05 (E)

Information technology — Trusted Platform Module — Part 2: Design principles

Table of Contents

1. Scope 1
   1.1 Key words 1
   1.2 Statement Type 1
2. Normative references 2
3. Abbreviated Terms 3
4. Conformance 5
   4.1 Introduction 5
   4.2 Threat 6
   4.3 Protection of functions 6
   4.4 Protection of information 6
   4.5 Side effects 7
   4.6 Exceptions and clarifications 7
5. TPM Architecture 8
   5.1 Interoperability 8
   5.2 Components 8
      5.2.1 Input and Output 9
      5.2.2 Cryptographic Co-Processor 9
      5.2.3 Key Generation 11
      5.2.4 HMAC Engine 12
      5.2.5 Random Number Generator 13
      5.2.6 SHA-1 Engine 15
      5.2.7 Power Detection 16
      5.2.8 Opt-In 16
      5.2.9 Execution Engine 17
      5.2.10 Non-Volatile Memory 17
   5.3 Data Integrity Register (DIR) 18
   5.4 Platform Configuration Register (PCR) 18
6. Endorsement Key Creation 20
   6.1 Controlling Access to PRIVEK 21
   6.2 Controlling Access to PUBEK 21
7. Attestation Identity Keys 22
8. TPM Ownership 23
   8.1 Platform Ownership and Root of Trust for Storage 23
9. Authentication and Authorization Data 24
   9.1 Dictionary Attack Considerations 25
10. TPM Operation 26
   10.1 TPM Initialization & Operation State Flow 27
      10.1.1 Initialization 27

10.2 Self-Test Modes 28
10.2.1 Operational Self-Test 29
10.3 Startup 32
10.4 Operational Mode 33
10.4.1 Enabling a TPM 34
10.4.2 Activating a TPM 35
10.4.3 Taking TPM Ownership 36
10.4.4 Transitioning Between Operational States 38
10.5 Clearing the TPM 38
11. Physical Presence 40
12. Root of Trust for Reporting (RTR) 42
12.1 Platform Identity 42
12.2 RTR to Platform Binding 43
12.3 Platform Identity and Privacy Considerations 43
12.4 Attestation Identity Keys 43
12.4.1 AIK Creation 44
12.4.2 AIK Storage 45
13. Root of Trust for Storage (RTS) 46
13.1 Loading and Unloading Blobs 46
14. Transport Sessions and Authorization Protocols 47
14.1 Authorization Session Setup 48
14.2 Parameter Declarations for OIAP and OSAP Examples 50
14.2.1 Object-Independent Authorization Protocol (OIAP) 52
14.2.2 Object-Specific Authorization Protocol (OSAP) 56
14.3 Authorization Session Handles 59
14.4 Authorization-Data Insertion Protocol (ADIP) 60
14.5 AuthData Change Protocol (ADCP) 64
14.6 Asymmetric Authorization Change Protocol (AACP) 65
15. ISO/IEC 19790 Evaluations 66
15.1 TPM Profile for successful ISO/IEC 19790 evaluation 66
16. Maintenance 67
16.1 Field Upgrade 69
17. Proof of Locality 70
18. Monotonic Counter 71
19. Transport Protection 74
19.1 Transport encryption and authorization 75
19.1.1 MGF1 parameters 77
19.1.2 HMAC calculation 78
19.1.3 Transport log creation 78
19.1.4 Additional Encryption Mechanisms 78

19.2 Transport Error Handling 79
19.3 Exclusive Transport Sessions 79
19.4 Transport Audit Handling 80
19.4.1 Auditing of wrapped commands 80
20. Audit Commands 81
20.1 Audit Monotonic Counter 83
21. Design Section on Time Stamping 84
21.1 Tick Components 84
21.2 Basic Tick Stamp 85
21.3 Associating a TCV with UTC 85
21.4 Additional Comments and Questions 87
22. Context Management 89
23. Eviction 91
24. Session pool 92
25. Initialization Operations 93
26. HMAC digest rules 94
27. Generic authorization session termination rules 95
28. PCR Grand Unification Theory 96
28.1 Validate Key for use 98
29. Non Volatile Storage 100
29.1 NV storage design principles 101
29.1.1 NV Storage use models 101
29.2 Use of NV storage during manufacturing 103
30. Delegation Model 104
30.1 Table Requirements 104
30.2 How this works 105
30.3 Family Table 106
30.4 Delegate Table 107
30.5 Delegation Administration Control 108
30.5.1 Control in Phase 1 109
30.5.2 Control in Phase 2 110
30.5.3 Control in Phase 3 110
30.6 Family Verification 110
30.7 Use of commands for different states of TPM 112
30.8 Delegation Authorization Values 112
30.8.1 Using the authorization value 112
30.9 DSAP description 113
31. Physical Presence 116
31.1 Use of Physical Presence 116
32. TPM Internal Asymmetric Encryption 117

32.1.1 TPM_ES_RSAESOAEP_SHA1_MGF1 117
32.1.2 TPM_ES_RSAESPKCSV15 118
32.1.3 TPM_ES_SYM_CTR 118
32.1.4 TPM_ES_SYM_OFB 118
32.2 TPM Internal Digital Signatures 118
32.2.1 TPM_SS_RSASSAPKCS1v15_SHA1 119
32.2.2 TPM_SS_RSASSAPKCS1v15_DER 119
32.2.3 TPM_SS_RSASSAPKCS1v15_INFO 120
32.2.4 Use of Signature Schemes 120
33. Key Usage Table 121
34. Direct Anonymous Attestation 123
34.1 TPM_DAA_JOIN 123
34.2 TPM_DAA_Sign 124
34.3 DAA Command summary 125
34.3.1 TPM setup 125
34.3.2 JOIN 126
34.3.3 SIGN 129
35. General Purpose IO 132
36. Redirection 133
37. Structure Versioning 134
38. Certified Migration Key Type 135
38.1 Certified Migration Requirements 135
38.2 Key Creation 136
38.3 Migrate CMK to a MA 136
38.4 Migrate CMK to a MSA 136
39. Revoke Trust 138
40. Mandatory and Optional Functional Blocks 139
41. 1.1a and 1.2 Differences 142
42. Bibliography 143