

# ISO/IEC 11889-4:2009-05 (E)

## Information technology — Trusted Platform Module — Part 4: Commands

---

### 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. Admin Startup and State     | 5  |
| 4.1 TPM_Init                   | 5  |
| 4.2 TPM_Startup                | 6  |
| 4.3 TPM_SaveState              | 8  |
| 5. Admin Testing               | 10 |
| 5.1 TPM_SelfTestFull           | 10 |
| 5.2 TPM_ContinueSelfTest       | 10 |
| 5.3 TPM_GetTestResult          | 12 |
| 6. Admin Opt-in                | 13 |
| 6.1 TPM_SetOwnerInstall        | 13 |
| 6.2 TPM_OwnerSetDisable        | 13 |
| 6.3 TPM_PhysicalEnable         | 14 |
| 6.4 TPM_PhysicalDisable        | 15 |
| 6.5 TPM_PhysicalSetDeactivated | 15 |
| 6.6 TPM_SetTempDeactivated     | 16 |
| 6.7 TPM_SetOperatorAuth        | 17 |
| 7. Admin Ownership             | 18 |
| 7.1 TPM_TakeOwnership          | 18 |
| 7.2 TPM_OwnerClear             | 20 |
| 7.3 TPM_ForceClear             | 22 |
| 7.4 TPM_DisableOwnerClear      | 23 |
| 7.5 TPM_DisableForceClear      | 24 |
| 7.6 TSC_PhysicalPresence       | 24 |
| 7.7 TSC_ResetEstablishmentBit  | 26 |
| 8. The Capability Commands     | 28 |
| 8.1 TPM_GetCapability          | 28 |
| 8.2 TPM_SetCapability          | 29 |
| 8.3 TPM_GetCapabilityOwner     | 30 |
| 9. Auditing                    | 32 |
| 9.1 Audit Generation           | 32 |
| 9.2 Effect of audit failing    | 33 |
| 9.3 TPM_GetAuditDigest         | 34 |

|       |                                       |    |
|-------|---------------------------------------|----|
| 9.4   | TPM_GetAuditDigestSigned              | 35 |
| 9.5   | TPM_SetOrdinalAuditStatus             | 37 |
| 10.   | Administrative Functions - Management | 38 |
| 10.1  | TPM_FieldUpgrade                      | 38 |
| 10.2  | TPM_SetRedirection                    | 40 |
| 10.3  | TPM_ResetLockValue                    | 41 |
| 11.   | Storage functions                     | 43 |
| 11.1  | TPM_Seal                              | 43 |
| 11.2  | TPM_Unseal                            | 46 |
| 11.3  | TPM_UnBind                            | 49 |
| 11.4  | TPM_CreateWrapKey                     | 51 |
| 11.5  | TPM_LoadKey2                          | 53 |
| 11.6  | TPM_GetPubKey                         | 56 |
| 11.7  | TPM_Sealx                             | 57 |
| 12.   | Migration                             | 60 |
| 12.1  | TPM_CreateMigrationBlob               | 60 |
| 12.2  | TPM_ConvertMigrationBlob              | 63 |
| 12.3  | TPM_AuthorizeMigrationKey             | 64 |
| 12.4  | TPM_MigrateKey                        | 66 |
| 12.5  | TPM_CMK_SetRestrictions               | 67 |
| 12.6  | TPM_CMK_ApproveMA                     | 69 |
| 12.7  | TPM_CMK_CreateKey                     | 70 |
| 12.8  | TPM_CMK_CreateTicket                  | 72 |
| 12.9  | TPM_CMK_CreateBlob                    | 74 |
| 12.10 | TPM_CMK_ConvertMigration              | 77 |
| 13.   | Maintenance Functions (optional)      | 80 |
| 13.1  | TPM_CreateMaintenanceArchive          | 81 |
| 13.2  | TPM_LoadMaintenanceArchive            | 83 |
| 13.3  | TPM_KillMaintenanceFeature            | 85 |
| 13.4  | TPM_LoadManuMaintPub                  | 86 |
| 13.5  | TPM_ReadManuMaintPub                  | 87 |
| 14.   | Cryptographic Functions               | 88 |
| 14.1  | TPM_SHA1Start                         | 88 |
| 14.2  | TPM_SHA1Update                        | 89 |
| 14.3  | TPM_SHA1Complete                      | 89 |
| 14.4  | TPM_SHA1CompleteExtend                | 90 |
| 14.5  | TPM_Sign                              | 91 |
| 14.6  | TPM_GetRandom                         | 93 |
| 14.7  | TPM_StirRandom                        | 93 |
| 14.8  | TPM_CertifyKey                        | 94 |

|        |                                     |     |
|--------|-------------------------------------|-----|
| 14.9   | TPM_CertifyKey2                     | 98  |
| 15.    | Endorsement Key Handling            | 101 |
| 15.1   | TPM_CreateEndorsementKeyPair        | 101 |
| 15.2   | TPM_CreateRevocableEK               | 102 |
| 15.3   | TPM_RevokeTrust                     | 104 |
| 15.4   | TPM_ReadPubek                       | 105 |
| 15.5   | TPM_OwnerReadInternalPub            | 106 |
| 16.    | Identity Creation and Activation    | 107 |
| 16.1   | TPM_MakeIdentity                    | 107 |
| 16.2   | TPM_ActivateIdentity                | 110 |
| 17.    | Integrity Collection and Reporting  | 113 |
| 17.1   | TPM_Extend                          | 113 |
| 17.2   | TPM_PCRRead                         | 114 |
| 17.3   | TPM_Quote                           | 115 |
| 17.4   | TPM_PCR_Reset                       | 116 |
| 17.5   | TPM_Quote2                          | 118 |
| 18.    | Changing AuthData                   | 120 |
| 18.1   | TPM_ChangeAuth                      | 120 |
| 18.2   | TPM_ChangeAuthOwner                 | 122 |
| 19.    | Authorization Sessions              | 123 |
| 19.1   | TPM_OIAP                            | 123 |
| 19.1.1 | Actions to validate an OIAP session | 124 |
| 19.2   | TPM_OSAP                            | 125 |
| 19.2.1 | Actions to validate an OSAP session | 128 |
| 19.3   | TPM_DSAP                            | 129 |
| 19.4   | TPM_SetOwnerPointer                 | 132 |
| 20.    | Delegation Commands                 | 134 |
| 20.1   | TPM_Delegate_Manage                 | 134 |
| 20.2   | TPM_Delegate_CreateKeyDelegation    | 137 |
| 20.3   | TPM_Delegate_CreateOwnerDelegation  | 139 |
| 20.4   | TPM_Delegate_LoadOwnerDelegation    | 142 |
| 20.5   | TPM_Delegate_ReadTable              | 144 |
| 20.6   | TPM_Delegate_UpdateVerification     | 145 |
| 20.7   | TPM_Delegate_VerifyDelegation       | 147 |
| 21.    | Non-volatile Storage                | 148 |
| 21.1   | TPM_NV_DefineSpace                  | 149 |
| 21.2   | TPM_NV_WriteValue                   | 152 |
| 21.3   | TPM_NV_WriteValueAuth               | 154 |
| 21.4   | TPM_NV_ReadValue                    | 156 |
| 21.5   | TPM_NV_ReadValueAuth                | 158 |

|                                 |     |
|---------------------------------|-----|
| 22. Session Management          | 160 |
| 22.1 TPM_KeyControlOwner        | 160 |
| 22.2 TPM_SaveContext            | 162 |
| 22.3 TPM_LoadContext            | 164 |
| 23. Eviction                    | 167 |
| 23.1 TPM_FlushSpecific          | 167 |
| 24. Timing Ticks                | 169 |
| 24.1 TPM_GetTicks               | 169 |
| 24.2 TPM_TickStampBlob          | 170 |
| 25. Transport Sessions          | 172 |
| 25.1 TPM_EstablishTransport     | 172 |
| 25.2 TPM_ExecuteTransport       | 175 |
| 25.3 TPM_ReleaseTransportSigned | 181 |
| 26. Monotonic Counter           | 184 |
| 26.1 TPM_CreateCounter          | 184 |
| 26.2 TPM_IncrementCounter       | 185 |
| 26.3 TPM_ReadCounter            | 186 |
| 26.4 TPM_ReleaseCounter         | 187 |
| 26.5 TPM_ReleaseCounterOwner    | 188 |
| 27. DAA commands                | 190 |
| 27.1 TPM_DAA_Join               | 190 |
| 27.2 TPM_DAA_Sign               | 205 |
| 28. Deprecated commands         | 215 |
| 28.1 Key commands               | 215 |
| 28.1.1 TPM_EvictKey             | 215 |
| 28.1.2 TPM_Terminate_Handle     | 216 |
| 28.2 Context management         | 217 |
| 28.2.1 TPM_SaveKeyContext       | 217 |
| 28.2.2 TPM_LoadKeyContext       | 218 |
| 28.2.3 TPM_SaveAuthContext      | 219 |
| 28.2.4 TPM_LoadAuthContext      | 220 |
| 28.3 DIR commands               | 220 |
| 28.3.1 TPM_DirWriteAuth         | 221 |
| 28.3.2 TPM_DirRead              | 222 |
| 28.4 Change Auth                | 222 |
| 28.4.1 TPM_ChangeAuthAsymStart  | 223 |
| 28.4.2 TPM_ChangeAuthAsymFinish | 226 |
| 28.5 TPM_Reset                  | 228 |
| 28.6 TPM_OwnerReadPubek         | 229 |
| 28.7 TPM_DisablePubekRead       | 230 |

|      |                           |     |
|------|---------------------------|-----|
| 28.8 | TPM_LoadKey               | 231 |
| 29.  | Deleted Commands          | 234 |
| 29.1 | TPM_GetCapabilitySigned   | 234 |
| 29.2 | TPM_GetOrdinalAuditStatus | 234 |
| 29.3 | TPM_CertifySelfTest       | 235 |
| 30.  | Bibliography              | 237 |

## List of Tables

|  |    |
|--|----|
| Table 1. TPM_Init Incoming Parameters and Sizes                  | 6  |
| Table 2. TPM_Init Outgoing Parameters and Sizes                  | 6  |
| Table 3. TPM_SaveState Incoming Parameters and Sizes             | 9  |
| Table 4. TPM_SaveState Outgoing Parameters and Sizes             | 9  |
| Table 5. TPM_SelfTestFull Incoming Operands and Sizes            | 10 |
| Table 6. TPM_SelfTestFull Outgoing Operands and Sizes            | 10 |
| Table 7. TPM_ContinueSelfTest Incoming Operands and Sizes        | 10 |
| Table 8. TPM_ContinueSelfTest Outgoing Operands and Sizes        | 11 |
| Table 9. TPM_GetTestResult Incoming Operands and Sizes           | 12 |
| Table 10. TPM_GetTestResult Outgoing Operands and Sizes          | 12 |
| Table 11. TPM_SetOwnerInstall Incoming Operands and Sizes        | 13 |
| Table 12. TPM_SetOwnerInstall Outgoing Operands and Sizes        | 13 |
| Table 13. TPM_OwnerSetDisable Incoming Operands and Sizes        | 13 |
| Table 14. TPM_OwnerSetDisable Outgoing Operands and Sizes        | 14 |
| Table 15. TPM_PhysicalEnable Incoming Operands and Sizes         | 14 |
| Table 16. TPM_PhysicalEnable Outgoing Operands and Sizes         | 14 |
| Table 17. TPM_PhysicalDisable Incoming Operands and Sizes        | 15 |
| Table 18. TPM_PhysicalEnable Outgoing Operands and Sizes         | 15 |
| Table 19. TPM_PhysicalSetDeactivated Incoming Operands and Sizes | 15 |
| Table 20. TPM_PhysicalSetDeactivated Outgoing Operands and Sizes | 15 |
| Table 21. TPM_SetTemp Deactivated Incoming Operands and Sizes    | 16 |
| Table 22. TPM_SetTemp Deactivated Outgoing Operands and Sizes    | 16 |
| Table 23. TPM_SetOperatorAuth Incoming Operands and Sizes        | 17 |
| Table 24. TPM_SetOperatorAuth Outgoing Operands and Sizes        | 17 |
| Table 25. TPM_TakeOwnership Incoming Operands and Sizes          | 18 |
| Table 26. TPM_TakeOwnership Outgoing Operands and Sizes          | 19 |
| Table 27. TPM_OwnerClear Incoming Operands and Sizes             | 20 |
| Table 28. TPM_OwnerClear Outgoing Operands and Sizes             | 20 |
| Table 29. TPM_ForceClear Incoming Operands and Sizes             | 22 |
| Table 30. TPM_ForceClear Outgoing Operands and Sizes             | 23 |
| Table 31. TPM_DisableOwnerClear Incoming Operands and Sizes      | 23 |
| Table 32. TPM_DisableOwnerClear Outgoing Operands and Sizes      | 23 |
| Table 33. TPM_DisableForceClear Incoming Operands and Sizes      | 24 |
| Table 34. TPM_DisableForceClear Outgoing Operands and Sizes      | 24 |
| Table 35. TSC_PhysicalPresence Incoming Operands and Sizes       | 25 |
| Table 36. TSC_PhysicalPresence Outgoing Operands and Sizes       | 25 |
| Table 37. TCG_ResetEstablishmentBit Incoming Operands and Sizes  | 27 |
| Table 38. TCG_ResetEstablishmentBit Outgoing Operands and Sizes  | 27 |
| Table 39. TPM_GetCapability Incoming Parameters and Sizes        | 28 |

|   |    |
|---|----|
| Table 40. TPM_GetCapability Outgoing Parameters and Sizes         | 28 |
| Table 41. TPM_SetCapability Incoming Parameters and Sizes         | 29 |
| Table 42. TPM_SetCapability Outgoing Parameters and Sizes         | 30 |
| Table 43. TPM_GetCapabilityOwner Incoming Operands and Sizes      | 30 |
| Table 44. TPM_GetCapabilityOwner Outgoing Operands and Sizes      | 31 |
| Table 45. TPM_GetAuditDigest Incoming Parameters and Sizes        | 34 |
| Table 46. TPM_GetAuditDigest Outgoing Parameters and Sizes        | 34 |
| Table 47. TPM_GetAuditDigestSigned Incoming Parameters and Sizes  | 35 |
| Table 48. TPM_GetAuditDigestSigned Outgoing Parameters and Sizes  | 36 |
| Table 49. TPM_SetOrdinalAuditStatus Incoming Parameters and Sizes | 37 |
| Table 50. TPM_SetOrdinalAuditStatus Outgoing Parameters and Sizes | 37 |
| Table 51. TPM_FieldUpgrade Parameters                             | 38 |
| Table 52. TPM_SetRedirection Incoming Operands and Sizes          | 40 |
| Table 53. TPM_SetRedirection Outgoing Operands and Sizes          | 40 |
| Table 54. TPM_ResetLockValue Incoming Operands and Sizes          | 41 |
| Table 55. TPM_ResetLockValue Outgoing Operands and Sizes          | 42 |
| Table 56. TPM_Seal Incoming Operands and Sizes                    | 44 |
| Table 57. TPM_Seal Outgoing Operands and Sizes                    | 44 |
| Table 58. TPM_Unseal Incoming Operands and Sizes                  | 46 |
| Table 59. TPM_Unseal Outgoing Operands and Sizes                  | 47 |
| Table 60. TPM_UnBind Incoming Operands and Sizes                  | 49 |
| Table 61. TPM_UnBind Outgoing Operands and Sizes                  | 50 |
| Table 62. TPM_CreateWrapKey Incoming Operands and Sizes           | 51 |
| Table 63. TPM_CreateWrapKey Outgoing Operands and Sizes           | 51 |
| Table 64. TPM_WrapKey Incoming Operands and Sizes                 | 54 |
| Table 65. TPM_WrapKey Outgoing Operands and Sizes                 | 54 |
| Table 66. TPM_GetPubKey Incoming Operands and Sizes               | 56 |
| Table 67. TPM_GetPubKey Outgoing Operands and Sizes               | 56 |
| Table 68. TPM_Sealx Incoming Operands and Sizes                   | 57 |
| Table 69. TPM_Sealx Outgoing Operands and Sizes                   | 58 |
| Table 70. TPM_CreateMigrationBlob Incoming Operands and Sizes     | 61 |
| Table 71. TPM_CreateMigrationBlob Outgoing Operands and Sizes     | 62 |
| Table 72. TPM_ConvertMigrationBlob Incoming Operands and Sizes    | 63 |
| Table 73. TPM_ConvertMigrationBlob Outgoing Operands and Sizes    | 64 |
| Table 74. TPM_AuthorizeMigrationKey Incoming Operands and Sizes   | 65 |
| Table 75. TPM_AuthorizeMigrationKey Outgoing Operands and Sizes   | 65 |
| Table 76. TPM_MigrateKey Incoming Operands and Sizes              | 66 |
| Table 77. TPM_MigrateKey Outgoing Operands and Sizes              | 67 |
| Table 78. TPM_CMK_SetRestrictions Incoming Operands and Sizes     | 67 |
| Table 79. TPM_CMK_SetRestrictions Outgoing Operands and Sizes     | 68 |

|   |     |
|---|-----|
| Table 80. TPM_CMK_ApproveMA Incoming Operands and Sizes             | 69  |
| Table 81. TPM_CMK_ApproveMA Outgoing Operands and Sizes             | 69  |
| Table 82. TPM_CMK_CreateKey Incoming Operands and Sizes             | 70  |
| Table 83. TPM_CMK_CreateKey Outgoing Operands and Sizes             | 71  |
| Table 84. TPM_CMK_CreateTicket Incoming Operands and Sizes          | 73  |
| Table 85. TPM_CMK_CreateTicket Outgoing Operands and Sizes          | 73  |
| Table 86. TPM_CMK_CreateBlob Incoming Operands and Sizes            | 74  |
| Table 87. TPM_CMK_CreateBlob Outgoing Operands and Sizes            | 75  |
| Table 88. TPM_CMK_ConvertMigration Incoming Operands and Sizes      | 77  |
| Table 89. TPM_CMK_ConvertMigration Outgoing Operands and Sizes      | 78  |
| Table 90. TPM_CreateMaintenanceArchive Incoming Operands and Sizes  | 81  |
| Table 91. TPM_CreateMaintenanceArchive Outgoing Operands and Sizes  | 81  |
| Table 92. TPM_LoadMaintenanceArchive Incoming Operands and Sizes    | 83  |
| Table 93. TPM_LoadMaintenanceArchive Outgoing Operands and Sizes    | 83  |
| Table 94. TPM_KillMaintenanceFeature Incoming Operands and Sizes    | 85  |
| Table 95. TPM_KillMaintenanceFeature Outgoing Operands and Sizes    | 85  |
| Table 96. TPM_LoadManuMaintPub Incoming Operands and Sizes          | 86  |
| Table 97. TPM_LoadManuMaintPub Outgoing Operands and Sizes          | 86  |
| Table 98. TPM_ReadManuMaintPub Incoming Operands and Sizes          | 87  |
| Table 99. TPM_ReadManuMaintPub Outgoing Operands and Sizes          | 87  |
| Table 100. TPM_SHA1Start Incoming Operands and Sizes                | 88  |
| Table 101. TPM_SHA1Start Outgoing Operands and Sizes                | 88  |
| Table 102. TPM_SHA1Update Incoming Operands and Sizes               | 89  |
| Table 103. TPM_SHA1Update Outgoing Operands and Sizes               | 89  |
| Table 104. TPM_SHA1Complete Incoming Operands and Sizes             | 89  |
| Table 105. TPM_SHA1Complete Outgoing Operands and Sizes             | 90  |
| Table 106. TPM_SHA1CompleteExtend Incoming Operands and Sizes       | 90  |
| Table 107. TPM_SHA1CompleteExtend Outgoing Operands and Sizes       | 90  |
| Table 108. TPM_Sign Incoming Operands and Sizes                     | 91  |
| Table 109. TPM_Sign Outgoing Operands and Sizes                     | 91  |
| Table 110. TPM_GetRandom Incoming Operands and Sizes                | 93  |
| Table 111. TPM_GetRandom Outgoing Operands and Sizes                | 93  |
| Table 112. TPM_StirRandom Incoming Operands and Sizes               | 93  |
| Table 113. TPM_StirRandom Outgoing Operands and Sizes               | 94  |
| Table 114. TPM_CertifyKey Incoming Operands and Sizes               | 95  |
| Table 115. TPM_CertifyKey Outgoing Operands and Sizes               | 95  |
| Table 116. TPM_CertifyKey2 Incoming Operands and Sizes              | 98  |
| Table 117. TPM_CertifyKey2 Outgoing Operands and Sizes              | 99  |
| Table 118. TPM_CreateEndorsementKeyPair Incoming Operands and Sizes | 101 |
| Table 119. TPM_CreateEndorsementKeyPair Outgoing Operands and Sizes | 101 |

|   |     |
|---|-----|
| Table 120. TPM_CreateRevocableEK Incoming Operands and Sizes              | 103 |
| Table 121. TPM_CreateRevocableEK Outgoing Operands and Sizes              | 103 |
| Table 122. TPM_RevokeTrust Incoming Operands and Sizes                    | 104 |
| Table 123. TPM_RevokeTrust Outgoing Operands and Sizes                    | 104 |
| Table 124. TPM_ReadPubek Incoming Operands and Sizes                      | 105 |
| Table 125. TPM_ReadPubek Outgoing Operands and Sizes                      | 105 |
| Table 126. TPM_OwnerReadInternalPub Incoming Operands and Sizes           | 106 |
| Table 127. TPM_OwnerReadInternalPub Outgoing Operands and Sizes           | 106 |
| Table 128. TPM_MakeIdentity Incoming Operands and Sizes                   | 107 |
| Table 129. TPM_MakeIdentity Outgoing Operands and Sizes                   | 108 |
| Table 130. Properties of the new identity                                 | 108 |
| Table 131. TPM_ActivateIdentity Incoming Parameters and Sizes             | 110 |
| Table 132. TPM_ActivateIdentity Outgoing Parameters and Sizes             | 111 |
| Table 133. TPM_Extend Incoming Operands and Sizes                         | 113 |
| Table 134. TPM_Extend Outgoing Operands and Sizes                         | 113 |
| Table 135. TPM_PCRRead Incoming Operands and Sizes                        | 114 |
| Table 136. TPM_PCRRead Outgoing Operands and Sizes                        | 114 |
| Table 137. TPM_Quote Incoming Operands and Sizes                          | 115 |
| Table 138. TPM_Quote Outgoing Operands and Sizes                          | 115 |
| Table 139. TPM_PCR_Reset Incoming Parameters and Sizes                    | 117 |
| Table 140. TPM_PCR_Reset Outgoing Parameters and Sizes                    | 117 |
| Table 141. TPM_Quote2 Incoming Operands and Sizes                         | 118 |
| Table 142. TPM_Quote2 Outgoing Operands and Sizes                         | 118 |
| Table 143. TPM_ChangeAuth Incoming Operands and Sizes                     | 120 |
| Table 144. TPM_ChangeAuth Outgoing Operands and Sizes                     | 121 |
| Table 145. TPM_ChangeAuthOwner Incoming Operands and Sizes                | 122 |
| Table 146. TPM_ChangeAuthOwner Outgoing Operands and Sizes                | 122 |
| Table 147. TPM_OIAP Incoming Operands and Sizes                           | 123 |
| Table 148. TPM-OIAP Outgoing Operands and Sizes                           | 123 |
| Table 149. TPM_OSAP Incoming Operands and Sizes                           | 125 |
| Table 150. TPM_OSAP Outgoing Operands and Sizes                           | 125 |
| Table 151. TPM_DSAP Incoming Operands and Sizes                           | 129 |
| Table 152. TPM_DSAP Outgoing Operands and Sizes                           | 129 |
| Table 153. TPM_SetOwnerPointer Incoming Operands and Sizes                | 132 |
| Table 154. TPM_SetOwnerPointer Outgoing Operands and Sizes                | 133 |
| Table 155. TPM_Delegate_Manage Incoming Operands and Sizes                | 135 |
| Table 156. TPM_Delegate_Manage Outgoing Operands and Sizes                | 135 |
| Table 157. TPM_Delegate_CreateKeyDelegation Incoming Operands and Sizes   | 137 |
| Table 158. TPM_Delegate_CreateKeyDelegation Outgoing Operands and Sizes   | 138 |
| Table 159. TPM_Delegate_CreateOwnerDelegation Incoming Operands and Sizes | 140 |

|   |     |
|---|-----|
| Table 160. TPM_Delegate_CreateOwnerDelegation Outgoing Operands and Sizes | 140 |
| Table 161. TPM_Delegate_LoadOwnerDelegation Incoming Operands and Sizes   | 142 |
| Table 162. TPM_Delegate_LoadOwnerDelegation Outgoing Operands and Sizes   | 143 |
| Table 163. TPM_Delegate_ReadTable Incoming Operands and Sizes             | 144 |
| Table 164. TPM_Delegate_ReadTable Outgoing Operands and Sizes             | 144 |
| Table 165. TPM_Delegate_UpdateVerification Incoming Operands and Sizes    | 145 |
| Table 166. TPM_Delegate_UpdateVerification Outgoing Operands and Sizes    | 146 |
| Table 167. TPM_Delegate_VerifyDelegation Incoming Operands and Sizes      | 147 |
| Table 168. TPM_Delegate_VerifyDelegation Outgoing Operands and Sizes      | 147 |
| Table 169. TPM_NV_DefineSpace Incoming Operands and Sizes                 | 149 |
| Table 170. TPM_NV_DefineSpace Outgoing Operands and Sizes                 | 149 |
| Table 171. TPM_NV_WriteValue Incoming Operands and Sizes                  | 152 |
| Table 172. TPM_NV_WriteValue Outgoing Operands and Sizes                  | 152 |
| Table 173. TPM_NV_WriteValueAuth Incoming Operands and Sizes              | 154 |
| Table 174. TPM_NV_WriteValueAuth Outgoing Operands and Sizes              | 155 |
| Table 175. TPM_NV_ReadValue Incoming Operands and Sizes                   | 156 |
| Table 176. TPM_NV_ReadValue Outgoing Operands and Sizes                   | 156 |
| Table 177. TPM_NV_ReadValueAuth Incoming Operands and Sizes               | 158 |
| Table 178. TPM_NV_ReadValueAuth Outgoing Operands and Sizes               | 158 |
| Table 179. TPM_KeyControlOwner Incoming Parameters and Sizes              | 161 |
| Table 180. TPM_KeyControlOwner Outgoing Parameters and Sizes              | 161 |
| Table 181. TPM_SaveContext Incoming Parameters and Sizes                  | 162 |
| Table 182. TPM_SaveContext Outgoing Parameters and Sizes                  | 162 |
| Table 183. TPM_LoadContext Incoming Parameters and Sizes                  | 164 |
| Table 184. TPM_LoadContext Outgoing Parameters and Sizes                  | 165 |
| Table 185. TPM_FlushSpecific Incoming Parameters and Sizes                | 167 |
| Table 186. TPM_FlushSpecific Outgoing Parameters and Sizes                | 167 |
| Table 187. TPM_GetTicks Incoming Parameters and Sizes                     | 169 |
| Table 188. TPM_GetTicks Outgoing Parameters and Sizes                     | 169 |
| Table 189. TPM_TickStampBlob Incoming Parameters and Sizes                | 170 |
| Table 190. TPM_TickStampBlob Outgoing Parameters and Sizes                | 171 |
| Table 191. TPM_EstablishTransport Incoming Parameters and Sizes           | 172 |
| Table 192. TPM_EstablishTransport Outgoing Parameters and Sizes           | 173 |
| Table 193. TPM_ExecuteTransport Incoming Parameters and Sizes             | 175 |
| Table 194. TPM_ExecuteTransport Outgoing Parameters and Sizes             | 176 |
| Table 195. TPM_ReleaseTransportSigned Incoming Parameters and Sizes       | 181 |
| Table 196. TPM_ReleaseTransportSigned Outgoing Parameters and Sizes       | 182 |
| Table 197. TPM_CreateCounter Incoming Parameters and Sizes                | 184 |
| Table 198. TPM_CreateCounter Outgoing Parameters and Sizes                | 184 |
| Table 199. TPM_IncrementCounter Incoming Parameters and Sizes             | 185 |

|  |     |
|--|-----|
| Table 200. TPM_IncrementCounter Outgoing Parameters and Sizes      | 186 |
| Table 201. TPM_ReadCounter Incoming Parameters and Sizes           | 186 |
| Table 202. TPM_ReadCounter Outgoing Parameters and Sizes           | 187 |
| Table 203. TPM_ReleaseCounter Incoming Parameters and Sizes        | 187 |
| Table 204. TPM_ReleaseCounter Outgoing Parameters and Sizes        | 188 |
| Table 205. TPM_ReleaseCounterOwner Incoming Parameters and Sizes   | 188 |
| Table 206. TPM_ReleaseCounter Owner Outgoing Parameters and Sizes  | 189 |
| Table 207. TPM_DAA_Join Incoming Parameters and Sizes              | 190 |
| Table 208. TPM_DAA_Join Outgoing Operands and Sizes                | 190 |
| Table 209. Input, Output and Saved Data Associated with Processing | 191 |
| Table 210. TPM_DAA_Sign Incoming Operands and Sizes                | 205 |
| Table 211. TPM_DAA_Sign Outgoing Operands and Sizes                | 205 |
| Table 212. Input, Output and Saved Data Associated with Processing | 206 |
| Table 213. TPM_EvictKey Incoming Operands and Sizes                | 215 |
| Table 214. TPM_EvictKey Outgoing Operands and Sizes                | 215 |
| Table 215. TPM_Terminate_Handle Incoming Operands and Sizes        | 216 |
| Table 216. TPM_Terminate_Handle Outgoing Operands and Sizes        | 216 |
| Table 217. TPM_SaveKeyContext Incoming Operands and Sizes          | 217 |
| Table 218. TPM_SaveKeyContext Outgoing Operands and Sizes          | 217 |
| Table 219. TPM_LoadKeyContext Incoming Operands and Sizes          | 218 |
| Table 220. TPM_LoadKeyContext Outgoing Operands and Sizes          | 218 |
| Table 221. TPM_SaveAuthContext Incoming Operands and Sizes         | 219 |
| Table 222. TPM_SaveAuthContext Outgoing Operands and Sizes         | 219 |
| Table 223. TPM_LoadAuthContext Incoming Operands and Sizes         | 220 |
| Table 224. TPM_LoadAuthContext Outgoing Operands and Sizes         | 220 |
| Table 225. TPM_DirWriteAuth Incoming Operands and Sizes            | 221 |
| Table 226. TPM_DirWriteAuth Outgoing Operands and Sizes            | 221 |
| Table 227. TPM_DirRead Incoming Operands and Sizes                 | 222 |
| Table 228. TPM_DirRead Outgoing Operands and Sizes                 | 222 |
| Table 229. TPM_ChangeAuthAsymStart Incoming Operands and Sizes     | 223 |
| Table 230. TPM_ChangeAuthAsymStart Outgoing Operands and Sizes     | 224 |
| Table 231. Field Descriptions for certifyInfo parameter            | 225 |
| Table 232. TPM_ChangeAuthAsymFinish Incoming Operands and Sizes    | 226 |
| Table 233. TPM_ChangeAuthAsymFinish Outgoing Operands and Sizes    | 227 |
| Table 234. TPM_Reset Incoming Parameters and Sizes                 | 228 |
| Table 235. TPM_Reset Outgoing Parameters and Sizes                 | 228 |
| Table 236. TPM_OwnerReadPubek Incoming Operands and Sizes          | 229 |
| Table 237. TPM_OwnerReadPubek Outgoing Operands and Sizes          | 229 |
| Table 238. TPM_DisablePubekRead Incoming Operands and Sizes        | 230 |
| Table 239. TPM_DisablePubekRead Outgoing Operands and Sizes        | 230 |

|  |     |
|--|-----|
| Table 240. TPM_LoadKey Incoming Operands and Sizes               | 232 |
| Table 241. TPM_LoadKey Outgoing Operands and Sizes               | 232 |
| Table 242. TPM_GetOrdinalAuditStatus Incoming Operands and Sizes | 234 |
| Table 243. TPM_GetOrdinalAuditStatus Outgoing Operands and Sizes | 234 |
| Table 244. TPM_CertifySelfTest Incoming Operands and Sizes       | 235 |
| Table 245. TPM_CertifySelfTest Outgoing Operands and Sizes       | 235 |