# ISO/IEC 25706:2026-02 (E)

## Information technology - Security protocol and data model (SPDM) collection

## Contents

Page


1 Foreword . . . 9
2 Introduction . . . 10
2.1 *Security Protocol and Data Model (SPDM) Specification* (DSP0274) . . . 10
2.2 *SPDM over MCTP Binding Specification* (DSP0275) . . . 10
2.3 *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276) . . . 10
2.4 *Secured Messages using SPDM Specification* (DSP0277) . . . 10
2.5 Advice . . . 10
3 Scope . . . 11
3.1 *Security Protocol and Data Model (SPDM) Specification* (DSP0274) . . . 11
3.2 *SPDM over MCTP Binding Specification* (DSP0275) . . . 11
3.3 *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276) . . . 11
3.4 *Secured Messages using SPDM Specification* (DSP0277) . . . 11
4 Normative references . . . 12
5 Terms and definitions . . . 15
6 Symbols and abbreviated terms . . . 19
7 Conventions . . . 20
7.1 Document conventions . . . 20
7.2 Reserved and unassigned values . . . 20
7.3 Byte ordering . . . 20
7.3.1 Hash byte order . . . 20
7.3.2 Encoded ASN.1 byte order . . . 21
7.3.3 Octet string byte order . . . 21
7.3.4 Signature byte order . . . 21
7.3.4.1 ECDSA signatures byte order . . . 21
7.3.4.2 SM2 signatures byte order . . . 21
7.4 Sizes and lengths . . . 22
7.5 SPDM data type conventions . . . 22
7.5.1 SPDM data types . . . 22
7.5.2 Integers . . . 22
7.6 Version encoding . . . 22
7.7 Notations . . . 23
7.8 Text or string encoding . . . 24
7.9 Deprecated material . . . 25
7.10 Figures . . . 25
8 Security Protocol and Data Model (SPDM) Specification (DSP0274) . . . 26
8.1 SPDM message exchanges . . . 26
8.1.1 Security capability discovery and negotiation . . . 26
8.1.2 Identity authentication . . . 26
8.1.2.1 Identity provisioning . . . 27
8.1.2.1.1 Certificate models . . . 27
8.1.2.2 Raw public keys . . . 30
8.1.2.3 Runtime authentication . . . 30
8.1.3 Firmware and configuration measurement . . . 30
8.1.4 Secure sessions . . . 30

8.1.5 Mutual authentication overview . . . 31
8.1.6 Multiple asymmetric key support . . . 31
8.1.7 Custom environments . . . 31
8.1.8 Notification overview . . . 32
8.2 SPDM messaging protocol . . . 32
8.2.1 SPDM connection model . . . 34
8.2.2 SPDM bits-to-bytes mapping . . . 34
8.2.3 Generic SPDM message format . . . 35
8.2.3.1 SPDM version . . . 36
8.2.4 SPDM request codes . . . 36
8.2.5 SPDM response codes . . . 37
8.2.6 SPDM request and response code issuance allowance . . . 39
8.2.7 Concurrent SPDM message processing . . . 41
8.2.8 Requirements for Requesters . . . 41
8.2.9 Requirements for Responders . . . 41
8.2.10 Transcript and transcript hash calculation rules . . . 42
8.3 Timing requirements . . . 42
8.3.1 Timing measurements . . . 42
8.3.2 Timing parameters . . . 43
8.3.3 Timing specification table . . . 43
8.4 SPDM messages . . . 45
8.4.1 Capability discovery and negotiation . . . 45
8.4.1.1 Negotiated state preamble . . . 46
8.4.2 GET_VERSION request and VERSION response messages . . . 46
8.4.3 GET_CAPABILITIES request and CAPABILITIES response messages . . . 49
8.4.3.1 Supported algorithms block . . . 57
8.4.4 NEGOTIATE_ALGORITHMS request and ALGORITHMS response messages . . . 58
8.4.4.1 Connection behavior after VCA . . . 70
8.4.4.2 Multiple asymmetric key negotiation . . . 70
8.4.4.3 Multiple asymmetric key use for Responder authentication . . . 71
8.4.4.4 Multiple asymmetric key use for Requester authentication . . . 71
8.4.4.5 Multiple asymmetric key connection . . . 71
8.4.5 Responder identity authentication . . . 72
8.4.6 Requester identity authentication . . . 74
8.4.6.1 Certificates and certificate chains . . . 74
8.4.7 GET_DIGESTS request and DIGESTS response messages . . . 75
8.4.8 GET_CERTIFICATE request and CERTIFICATE response messages . . . 79
8.4.8.1 Mutual authentication requirements for GET_CERTIFICATE and CERTIFICATE messages . . . 81
8.4.8.2 SPDM certificate requirements and recommendations . . . 81
8.4.8.2.1 Extended Key Usage authentication OIDs . . . 84
8.4.8.2.2 SPDM Non-Critical Certificate Extension OID . . . 84
8.4.9 CHALLENGE request and CHALLENGE_AUTH response messages . . . 85
8.4.9.1 CHALLENGE_AUTH signature generation . . . 88
8.4.9.2 CHALLENGE_AUTH signature verification . . . 89
8.4.9.2.1 Request ordering and message transcript computation rules for M1 and

M2 . . . 89
8.4.9.3 Basic mutual authentication . . . 92
8.4.9.3.1 Mutual authentication message transcript . . . 93
8.4.10 Firmware and other measurements . . . 94
8.4.11 GET_MEASUREMENTS request and MEASUREMENTS response messages . . . 95
8.4.11.1 Measurement block . . . 100
8.4.11.1.1 DMTF specification for the Measurement field of a measurement block . . . 101
8.4.11.1.2 Device mode field of a measurement block . . . 103
8.4.11.1.3 Manifest format for a measurement block . . . 104
8.4.11.2 MEASUREMENTS signature generation . . . 104
8.4.11.3 MEASUREMENTS signature verification . . . 106
8.4.12 ERROR response message . . . 107
8.4.12.1 Standards body or vendor-defined header . . . 112
8.4.13 RESPOND_IF_READY request message format . . . 112
8.4.14 VENDOR_DEFINED_REQUEST request message . . . 113
8.4.15 VENDOR_DEFINED_RESPONSE response message . . . 114
8.4.15.1 VendorDefinedReqPayload and VendorDefinedRespPayload defined by DMTF specifications . . . 115
8.4.16 KEY_EXCHANGE request and KEY_EXCHANGE_RSP response messages . . . 115
8.4.16.1 Session-based mutual authentication . . . 123
8.4.16.1.1 Specify Requester certificate for session-based mutual authentication . . . 123
8.4.17 FINISH request and FINISH_RSP response messages . . . 124
8.4.17.1 Transcript and transcript hash calculation rules for KEY_EXCHANGE . . . 125
8.4.18 PSK_EXCHANGE request and PSK_EXCHANGE_RSP response messages . . . 128
8.4.19 PSK_FINISH request and PSK_FINISH_RSP response messages . . . 135
8.4.20 HEARTBEAT request and HEARTBEAT_ACK response messages . . . 136
8.4.20.1 Heartbeat additional information . . . 137
8.4.21 KEY_UPDATE request and KEY_UPDATE_ACK response messages . . . 137
8.4.21.1 Session key update synchronization . . . 138
8.4.21.2 KEY_UPDATE transport allowances . . . 141
8.4.22 GET_ENCAPSULATED_REQUEST request and ENCAPSULATED_REQUEST response messages . . . 144
8.4.22.1 Encapsulated request flow . . . 144
8.4.22.2 Optimized encapsulated request flow . . . 144
8.4.22.3 Triggering GET_ENCAPSULATED_REQUEST . . . 147
8.4.22.4 Additional constraints . . . 147
8.4.23 DELIVER_ENCAPSULATED_RESPONSE request and ENCAPSULATED_RESPONSE_ACK response messages . . . 148
8.4.23.1 Additional information . . . 150
8.4.23.2 Allowance for encapsulated requests . . . 150
8.4.23.3 Certain error handling in encapsulated flows . . . 151
8.4.23.3.1 Response not ready . . . 151
8.4.23.3.2 Timeouts . . . 151
8.4.24 END_SESSION request and END_SESSION_ACK response messages . . . 151
8.4.25 Certificate provisioning . . . 153
8.4.25.1 GET_CSR request and CSR response messages . . . 153

8.4.25.2 SET_CERTIFICATE request and SET_CERTIFICATE_RSP response messages . . . 156
8.4.26 Large SPDM message transfer mechanism . . . 158
8.4.26.1 CHUNK_SEND request and CHUNK_SEND_ACK response message . . . 158
8.4.26.2 CHUNK_GET request and CHUNK_RESPONSE response message . . . 161
8.4.26.3 Additional chunk transfer requirements . . . 163
8.4.27 Key configuration . . . 164
8.4.27.1 GET_KEY_PAIR_INFO request and KEY_PAIR_INFO response . . . 165
8.4.27.2 SET_KEY_PAIR_INFO request and SET_KEY_PAIR_INFO_ACK response . . . 168
8.4.27.3 Key pair ID modification error handling . . . 169
8.4.28 Event mechanism . . . 170
8.4.28.1 GET_SUPPORTED_EVENT_TYPES request and SUPPORTED_EVENT_TYPES response message . . . 172
8.4.28.1.1 Event group format additional information . . . 174
8.4.28.2 SUBSCRIBE_EVENT_TYPES request and SUBSCRIBE_EVENT_TYPES_ACK response message . . . 174
8.4.28.2.1 Additional subscription list information . . . 175
8.4.28.3 SEND_EVENT request and EVENT_ACK response message . . . 176
8.4.28.4 Event Instance ID . . . 177
8.4.29 GET_ENDPOINT_INFO request and ENDPOINT_INFO response messages . . . 178
8.4.29.1 ENDPOINT_INFO signature generation . . . 181
8.4.29.2 ENDPOINT_INFO signature verification . . . 181
8.4.30 Measurement extension log mechanism . . . 182
8.4.30.1 GET_MEASUREMENT_EXTENSION_LOG request and MEASUREMENT_EXTENSION_LOG response messages . . . 183
8.4.30.2 DMTF Measurement Extension Log Format . . . 184
8.4.30.3 Example: Verifying Measurement Extension Log Against Hash-Extend Measurement . . . 185
8.5 Session . . . 187
8.5.1 Session handshake phase . . . 187
8.5.2 Application phase . . . 188
8.5.3 Session termination phase . . . 188
8.5.4 Simultaneous active sessions . . . 188
8.5.5 Records and session ID . . . 189
8.6 Key schedule . . . 189
8.6.1 DHE secret computation . . . 191
8.6.2 Transcript hash in key derivation . . . 192
8.6.3 TH1 definition . . . 192
8.6.4 TH2 definition . . . 192
8.6.5 Key schedule major secrets . . . 193
8.6.5.1 Request-direction handshake secret . . . 193
8.6.5.2 Response-direction handshake secret . . . 193
8.6.5.3 Request-direction data secret . . . 193
8.6.5.4 Response-direction data secret . . . 193
8.6.6 Encryption key and IV derivation . . . 194
8.6.7 finished_key derivation . . . 194

8.6.8 Deriving additional keys from the Export Master Secret . . . 195
8.6.9 Major secrets update . . . 195
8.7 Application data . . . 195
8.7.1 Nonce derivation . . . 196
8.8 General opaque data format . . . 196
8.9 Signature generation . . . 197
8.9.1 Signing algorithms in extensions . . . 198
8.9.2 RSA and ECDSA signing algorithms . . . 198
8.9.3 EdDSA signing algorithms . . . 199
8.9.3.1 Ed25519 sign . . . 199
8.9.3.2 Ed448 sign . . . 199
8.9.4 SM2 signing algorithm . . . 199
8.9.5 Signature algorithm references . . . 199
8.10 Signature verification . . . 200
8.10.1 Signature verification algorithms in extensions . . . 201
8.10.2 RSA and ECDSA signature verification algorithms . . . 201
8.10.3 EdDSA signature verification algorithms . . . 201
8.10.3.1 Ed25519 verify . . . 201
8.10.3.2 Ed448 verify . . . 202
8.10.4 SM2 signature verification algorithm . . . 202
8.11 General ordering rules . . . 202
8.12 DMTF event types . . . 203
8.12.1 Event type details . . . 203
8.12.1.1 Event Lost . . . 204
8.12.1.2 Measurement changed event . . . 204
8.12.1.3 Measurement pre-update event . . . 204
8.12.1.4 Certificate changed event . . . 205
9 SPDM over MCTP Binding Specification (DSP0275) . . . 206
9.0.1 SPDM over MCTP binding . . . 206
9.0.1.1 SPDM over MCTP message fields . . . 206
9.0.1.2 Requester and responder tracking . . . 207
9.0.2 Message tracking . . . 207
9.0.3 Version reporting . . . 207
10 Secured Messages using SPDM over MCTP Binding Specification (DSP0276) . . . 208
10.1 Secured messages over MCTP . . . 208
10.1.1 Sequence number . . . 208
10.1.2 MCTP encapsulated format . . . 209
10.2 Transport requirements or allowances . . . 209
10.2.1 Transmission retries . . . 209
10.2.2 Certain SPDM message allowances . . . 209
10.2.3 Version reporting . . . 209
10.2.4 Key management during key update . . . 210
10.3 Timing requirements . . . 210
11 Secured Messages using SPDM Specification (DSP0277) . . . 211
11.1 Secured Message . . . 211
11.1.1 Secured Message format . . . 211
11.1.2 Secured Message protection . . . 214

11.1.2.1 AEAD encryption keys and other secrets . . . 214
11.1.2.2 AEAD requirements . . . 214
11.1.2.2.1 Message Authentication Only session . . . 214
11.1.2.2.2 Encryption and Message Authentication session . . . 215
11.1.2.3 Per-message nonce derivation . . . 215
11.1.2.3.1 Other per-message nonce requirements . . . 216
11.1.2.4 Encryption requirements . . . 216
11.2 Compatibility . . . 216
11.3 Version support . . . 216
11.3.1 Version selection . . . 217
11.4 Transport requirements or allowances . . . 217
11.4.1 Transmission reliability . . . 218
11.4.2 Certain SPDM message allowances . . . 218
11.4.3 ERROR response message allowances . . . 218
11.4.4 Key update allowances . . . 218
11.5 Secured Messages opaque data format . . . 219
11.5.1 Secured Message opaque element data format . . . 220
11.5.1.1 Version selection data format . . . 221
11.5.1.2 Supported version list data format . . . 221
11.6 SPDM general opaque data format . . . 222
12 ANNEX A (informative) TLS 1.3 . . . 223
13 ANNEX B (informative) Device certificate example . . . 224
14 ANNEX C (informative) OID reference . . . 226
15 ANNEX D (informative) Variable name reference . . . 227
16 ANNEX E (informative) Sequence number layout . . . 229
17 Bibliography . . . 230