



**International
Standard**

ISO/IEC 25706

**Information technology — Security
protocol and data model (SPDM)
collection**

**First edition
2026-02**

**iTeh Standards
(<https://standards.iteh.ai>)
Document Preview**

[ISO/IEC 25706:2026](https://standards.iteh.ai/catalog/standards/iso/a1b689c2-23dd-49e0-a2e2-32a6aa0b80fc/iso-iec-25706-2026)

<https://standards.iteh.ai/catalog/standards/iso/a1b689c2-23dd-49e0-a2e2-32a6aa0b80fc/iso-iec-25706-2026>

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC 25706:2026

<https://standards.itih.ai/catalog/standards/iso/a1b689c2-23dd-49e0-a2e2-32a6aa0b80fc/iso-iec-25706-2026>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by DMTF [as Security Protocol and Data Model (SPDM) Collection] and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC 25706:2026](https://standards.itih.ai/catalog/standards/iso/a1b689c2-23dd-49e0-a2e2-32a6aa0b80fc/iso-iec-25706-2026)

<https://standards.itih.ai/catalog/standards/iso/a1b689c2-23dd-49e0-a2e2-32a6aa0b80fc/iso-iec-25706-2026>

CONTENTS

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