International Standard

ISO/IEC 25706

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

First edition
2026-02

Reference number
ISO/IEC 25706:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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.

CONTENTS

1 Foreword

The Security Protocols and Data Models (SPDM) Working Group of DMTF prepared the *Security Protocol and Data Model (SPDM) Specification* (DSP0274).

The Platform Management Communications Infrastructure (PMCI) Working Group of DMTF prepared the *Security Protocol and Data Model (SPDM) over MCTP Binding Specification* (DSP0275), the *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276), and the *Secured Messages using SPDM Specification* (DSP0277).

DMTF is a not-for-profit association of industry members that promotes enterprise and systems management and interoperability. For information about DMTF, see https://www.dmtf.org.

Table 1 — Component documents lists the specifications that this collection contains.

Table 1 — Component documents

Document number	Document title	Version
DSP0274	Security Protocol and Data Model (SPDM) Specification	1.3.1
DSP0275	Security Protocol and Data Model (SPDM) over MCTP Binding Specification	1.0.2
DSP0276	Secured Messages using SPDM over MCTP Binding Specification	1.2.0
DSP0277	Secured Messages using SPDM Specification	1.2.0

2 Introduction

2.1 *Security Protocol and Data Model (SPDM) Specification* (DSP0274)

DSP0274 defines *messages*, data objects, and sequences for performing message exchanges over a variety of transport and physical media. The description of message exchanges includes *authentication* and provisioning of hardware identities, measurement for firmware identities, session key exchange protocols to enable confidentiality with integrity-protected data communication, and other related capabilities. SPDM enables efficient access to low-level security capabilities and operations. In addition, other mechanisms, including non-DMTF-defined mechanisms, can use the SPDM.

2.2 *SPDM over MCTP Binding Specification* (DSP0275)

DSP0275 defines how SPDM is transported over MCTP communications. SPDM is supported as a message type over MCTP, and the SPDM over MCTP binding defines the format of SPDM messages transported over MCTP.

2.3 *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276)

DSP0276 binds Secured Messages using the SPDM specification (DSP0277) to MCTP transport.

2.4 *Secured Messages using SPDM Specification* (DSP0277)

DSP0277 defines the methodology that various PMCI transports can use to communicate various application data securely by utilizing SPDM. Specifically, DSP0277 defines the transport requirements for SPDM records, which form the basis of encryption and message authentication. Furthermore, DSP0277 contains guidance and certain decisions that it defers to the binding specification, which binds Secured Messages to a specific transport. Thus, the binding specification is expected to finalize those decisions or guidance by way of normalization or recommendation. DSP0277 was written with PMCI transports in mind, but nothing precludes specifying bindings to other transports.

2.5 Advice

The authors of these specifications recommend that readers visit tutorial and educational materials under Security Protocols and Data Models (SPDM) and Platform Management Communications Infrastructure (PMCI) on the DMTF website prior to or during the reading of these specifications to aid in understanding them fully.

3 Scope

3.1 *Security Protocol and Data Model (SPDM) Specification* (DSP0274)

DSP0274 describes how to use messages, data objects, and sequences to exchange messages between two devices over a variety of transports and physical media. DSP0274 contains the message exchanges, sequence diagrams, message formats, and other relevant semantics for such message exchanges, including authentication of hardware identities and firmware measurements.

Other specifications define the mapping of these messages to different transports and physical media. DSP0274 provides information to enable security policy enforcement but does not specify individual policy decisions.

3.2 *SPDM over MCTP Binding Specification* (DSP0275)

DSP0275 defines the format of Security Protocol and Data Model (SPDM) over MCTP messages. DSP0275 describes both SPDM over MCTP binding and the common format for SPDM over MCTP messages.

3.3 *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276)

DSP0276 binds Secured Messages using SPDM to MCTP transport and further defines the transport specific details as outlined in *Secured Messages using SPDM Specification* (DSP0277). DSP0276 1.2.0 (this version) binds to version 1.2.0 and all 1.2 errata versions of DSP0277.

3.4 *Secured Messages using SPDM Specification* (DSP0277)

DSP0277 defines a generic record format used to encrypt and authenticate any application data within SPDM's secure session. Also, relating to encryption, message authentication, and secure sessions, DSP0277 further defines those areas in SPDM that the specification states are the responsibilities of the transport layer. DSP0277 requires SPDM version 1.1 or later.

4 Normative references

The following referenced documents are indispensable for the application of the specifications in this collection. For dated or versioned references, only the edition cited, including any corrigenda or DMTF update versions, applies. For references without date or version, the latest published edition of the referenced document, including any corrigenda or DMTF update versions, applies.

- DMTF DSP0004, *Common Information Model (CIM) Metamodel*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0004_3.0.pdf
- DMTF DSP0223, *Generic Operations*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0223_1.0.pdf
- DMTF DSP0236, *MCTP Base Specification 1.3*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0236_1.3.pdf
- DMTF DSP0239, *MCTP IDs and Codes 1.7*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.7.pdf
- DMTF DSP0240, *Platform Level Data Model (PLDM) Base Specification*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0240_1.0.pdf
- DMTF DSP0274, *Security Protocol and Data Model (SPDM) Specification*, https://www.dmtf.org/dsp/DSP0274
- DMTF DSP0275, *Security Protocol and Data Model (SPDM) over MCTP Binding Specification*, https://www.dmtf.org/dsp/DSP0275
- DMTF DSP0276, *Secured Messages using SPDM over MCTP Binding Specification*, https://www.dmtf.org/dsp/DSP0276
- DMTF DSP0277, *Secured Messages using SPDM Specification*, https://www.dmtf.org/dsp/DSP0277
- DMTF DSP1001, *Management Profile Usage Guide*, https://www.dmtf.org/sites/default/files/standards/documents/DSP1001_1.2.pdf
- GB/T 32905-2016, *Information security technology—SM3 cryptographic hash algorithm*, August 2016
- GB/T 32907-2016, *Information security technology—SM4 block cipher algorithm*, August 2016
- GB/T 32918.1-2016, *Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 1: General*, August 2016
- GB/T 32918.2-2016, *Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 2: Digital signature algorithm*, August 2016
- GB/T 32918.3-2016, *Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 3: Key exchange protocol*, August 2016
- GB/T 32918.4-2016, *Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 4: Public key encryption algorithm*, August 2016
- GB/T 32918.5-2016, *Information security technology—Public key cryptographic algorithm SM2 based on elliptic curves—Part 5: Parameter definition*, August 2016
- IETF RFC 2986, *PKCS #10: Certification Request Syntax Specification*, November 2000, https://tools.ietf.org/html/rfc2986
- IETF RFC 4716, *The Secure Shell (SSH) Public Key File Format*, November 2006, https://tools.ietf.org/html/rfc4716
- IETF RFC 5116, *An Interface and Algorithms for Authenticated Encryption*, January 2008,

https://tools.ietf.org/html/rfc5116

- IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*, January 2008, https://tools.ietf.org/html/rfc5234
- IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008, https://tools.ietf.org/html/rfc5280
- IETF RFC 7250, *Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, June 2014, https://tools.ietf.org/html/rfc7250
- IETF RFC 7919, *Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)*, August 2016, https://tools.ietf.org/html/rfc7919
- IETF RFC 8017, *PKCS #1: RSA Cryptography Specifications Version 2.2*, November 2016, https://tools.ietf.org/html/rfc8017
- IETF RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)*, January 2017, https://tools.ietf.org/html/rfc8032
- IETF RFC 8439, *ChaCha20 and Poly1305 for IETF Protocols*, June 2018, https://tools.ietf.org/html/rfc8439
- IETF RFC 8446, *The Transport Layer Security (TLS) Protocol* Version 1.3, August 2018, https://tools.ietf.org/html/rfc8446
- IETF RFC 8998, *ShangMi (SM) Cipher Suites for TLS 1.3*, March 2021, https://tools.ietf.org/html/rfc8998
- IETF RFC 9147, *The Datagram Transport Layer Security (DTLS) Protocol* Version 1.3, April 2022, https://datatracker.ietf.org/doc/html/rfc9147
- *ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents*, https://www.iso.org/sites/directives/current/part2/index.xhtml
- *ASCII — ISO/IEC 646:1991*, 09/1991, https://www.iso.org/standard/4777.html
- NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, November 2007, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
- *TCG Algorithm Registry, Family "2.0", Level 00 Revision 01.32*, June 25, 2020, https://trustedcomputinggroup.org/resource/tcg-algorithm-registry/
- *USB Authentication Specification Rev 1.0 with ECN and Errata through January 7, 2019*, https://www.usb.org/document-library/usb-authentication-specification-rev-10-ecn-and-errata-through-january-7-2019
- **ASN.1 — ISO-822-1-4, DER — ISO-8825-1**
  - ITU-T X.680, X.681, X.682, X.683, X.690, 08/2015, https://www.itu.int/rec/T-REC-X.680-X.693-201508-S/en
- **ECDSA**
  - Section 6, The Elliptic Curve Digital Signature Algorithm (ECDSA) in FIPS PUB 186-5 Digital Signature Standard (DSS) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
  - IETF RFC 6979, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), August 2013, https://tools.ietf.org/html/rfc6979
  - NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf
- **SHA2-256**, **SHA2-384**, and **SHA2-512**
  - FIPS PUB 180-4 Secure Hash Standard (SHS) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
- **SHA3-256**, **SHA3-384**, and **SHA3-512**

- FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
  https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

17 Bibliography

DMTF DSP4014, *DMTF Process for Working Bodies* 2.6, https://www.dmtf.org/sites/default/files/standards/documents/DSP4014_2.6.pdf