Secured Messages using SPDM over MCTP Binding Specification

Version: 1.3.0

Document Identifier: DSP0276

Date: 2025-10-31

Version History: https://www.dmtf.org/dsp/DSP0276

Supersedes: 1.2.0

Document Class: Normative

Document Status: Published

Document Language: en-US

10 DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. Members and non-members may reproduce DMTF specifications and documents for uses consistent with this purpose, provided that correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release date should always be noted.

11 Implementation of certain elements of this standard or proposed standard may be subject to third-party patent rights, including provisional patent rights (herein “patent rights”). DMTF makes no representations to users of the standard as to the existence of such rights and is not responsible to recognize, disclose, or identify any or all such third-party patent right owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners, or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third-party patent rights, or for such party’s reliance on the standard or incorporation thereof in its products, protocols, or testing procedures. DMTF shall have no liability to any party implementing such standards, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

12 For information about patents held by third parties which have notified DMTF that, in their opinion, such patents may relate to or impact implementations of DMTF standards, visit https://www.dmtf.org/about/policies/disclosures.

13 IETF® is a registered trademark of IETF Trust. ISO® is a registered trademark of the International Organization for Standardization (ISO). All other marks and brands are the property of their respective owners.

14 This document's normative language is English. Translation into other languages is permitted.

CONTENTS

1 Foreword

The Platform Management Communications Infrastructure (PMCI) Working Group prepared the *Secured Messages using SPDM over MCTP Binding Specification* (DSP0276).

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

1.1 Acknowledgments

DMTF acknowledges the following individuals for their contributions to this document:

Contributors:

- Patrick Caporale — Lenovo
- Nigel Edwards — Hewlett Packard Enterprise
- Daniil Egranov — Arm Limited
- Philip Hawkes — Qualcomm Inc.
- Brett Henning — Broadcom Inc.
- Jeff Hilland — Hewlett Packard Enterprise
- Theo Koulouris — Hewlett Packard Enterprise
- Eliel Louzoun — Intel Corporation
- Donald Matthews — Advanced Micro Devices, Inc.
- Edward Newman — Hewlett Packard Enterprise
- Jim Panian — Qualcomm Inc.
- Scott Phuong — Cisco Systems Inc., Axiado Corporation, Microsoft Corporation
- Viswanath Ponnuru — Dell Technologies
- Xiaoyu Ruan — Intel Corporation
- Nitin Sarangdhar — DMTF
- Bob Stevens — Dell Technologies

21 # 2 Introduction

22 This specification binds Secured Messages using SPDM specification (DSP0277) to MCTP transport.

23 ## 2.1 Document conventions

- Document titles appear in *italics*.
- The first occurrence of each important term appears in *italics* with a link to its definition.
- ABNF rules appear in a monospaced font.

24 # 3 Scope

25 This document binds Secured Messages using SPDM to the MCTP transport and further defines the transport-specific details as outlined in *Secured Messages using SPDM*.

26 ## 3.1 Normative references

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

- DMTF DSP0236, *Management Component Transport Protocol (MCTP) Base Specification* 1.3, https://www.dmtf.org/sites/default/files/standards/documents/DSP0236_1.3.pdf
- DMTF DSP0239, *Management Component Transport Protocol (MCTP) IDs and Codes* 1.7, https://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.7.pdf
- DMTF DSP0274, *Security Protocol and Data Model (SPDM) Specification* 1.1 or later, https://www.dmtf.org/dsp/dsp0274
- DMTF DSP0277, *Secured Messages using SPDM Specification* 1.1, https://www.dmtf.org/sites/default/files/standards/documents/DSP0277_1.1.pdf
- IETF RFC 5234, *Augmented BNF for Syntax Specifications: ABNF* (January 2008), https://datatracker.ietf.org/doc/html/rfc5234
- IETF RFC 9147, *The Datagram Transport Layer Security (DTLS) Protocol* 1.3 (April 2022), https://datatracker.ietf.org/doc/rfc9147
- *ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents* 9th edition (2021), https://www.iso.org/sites/directives/current/part2/index.xhtml

28 ## 3.2 Terms and definitions

29 In this document, some terms have a specific meaning beyond the normal English meaning. This clause defines those terms.

30 The terms "shall" ("required"), "shall not," "should" ("recommended"), "should not" ("not recommended"), "may," "need not" ("not required"), "can," and "cannot" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 7. The terms in parentheses are alternatives for the preceding term, for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that ISO/IEC Directives, Part 2, Clause 7 specifies additional alternatives. Occurrences of such additional alternatives shall be interpreted in their normal English meaning.

31 The terms "clause," "subclause," "paragraph," and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 6.

32 The terms "normative" and "informative" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do not contain normative content. Notes and examples are always informative elements.

33 The terms that DSP0236, DSP0239, and DSP0274 define also apply to this document.

34 3.3 Symbols and abbreviated terms

35 The symbols and abbreviations defined in DSP0236, DSP0239, DSP0274, and DSP0277 apply to this document.

36 3.4 Binding Information

37 This version of this specification binds to these versions of *Secured Messages using SPDM* specification (DSP0277):

- Version 1.3.0 and all 1.3 errata versions

4 Secured Messages over MCTP

To transport Secured Messages over MCTP, this specification utilizes the *Secured Messages using SPDM* specification (DSP0277). The secured message format, as defined by DSP0277, becomes the message payload in MCTP message type 6, as illustrated at a high level in Figure 1 — Secured Message over MCTP.

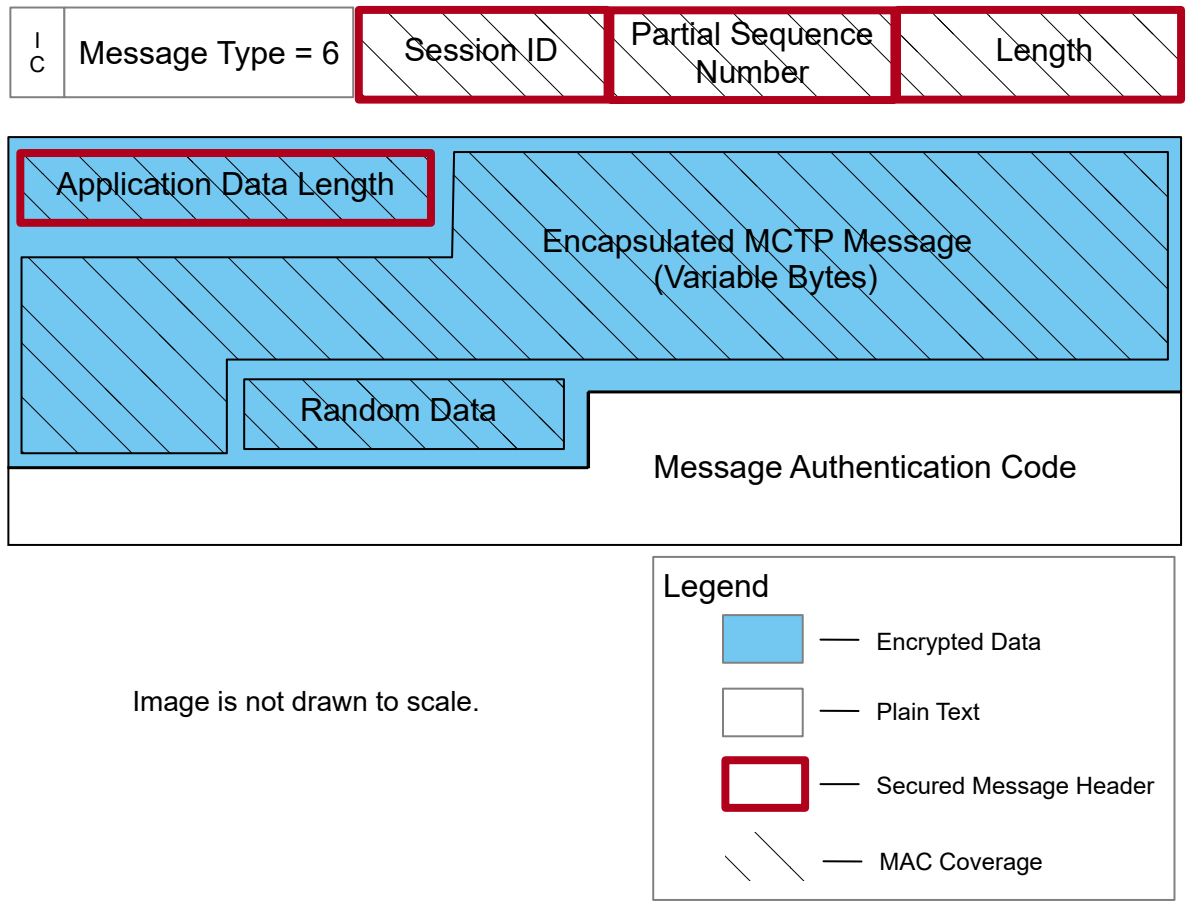

Figure 1 — Secured Message over MCTP

The Partial Sequence Number field shall be 2 bytes in length and shall contain the lower 16 bits of the full Sequence Number as DSP0277 describes. The field presence requirement for Partial Sequence Number shall always be present for Encryption and Message Authentication or Message Authentication Only sessions.

4.1 Sequence number

The sequence number shall be the full width as described in DSP0277. Because only the lower 16 bits of the

sequence number is transmitted in the Partial Sequence Number field, the upper 48 bits of the sequence number shall be internally tracked.

45 Because part of the sequence number is transmitted, there may be additional actions that the receiver of the data needs to take. To avoid replay attacks, the receiver of a Secured Message should discard messages with sequence numbers that have already been successfully authenticated and decrypted. See DTLS 1.3 for further guidance.

46 4.2 MCTP encapsulated format

47 To allow any MCTP message to utilize Secured Messages, this specification encapsulates any MCTP message type other than type 6. This specification shall prohibit message type 6 from being encapsulated. This is analogous to self-encapsulation, which has no meaningful use case.

48 In the figure, the MCTP encapsulated data is the Secured Message's application data in MCTP context and it shall be concatenated in the following order: E-IC, Encapsulated Message Type, and Encapsulated Message Type Specific Data. The encapsulated MCTP message type shall not be message type 6.

49 The IC bit for message type 6 shall be zero.

50 # 5 Transport requirements or allowances

51 This clause and subclauses describe the various requirements or flexibility allowed at the MCTP transport layer.

52 ## 5.1 Transmission retries

53 The MCTP transport should retry the transmission of an MCTP message to ensure reliable delivery or reception of an MCTP message.

54 ## 5.2 Certain SPDM message allowances

55 To take full advantage of asynchronous and bidirectional communication, as allowed by MCTP, `KEY_UPDATE`, `HEARTBEAT`, and `END_SESSION` may be sent directly from an SPDM Responder without any other assistance such as a sideband alerting mechanism or SPDM's `GET_ENCAPSULATED_REQUEST` mechanism. This allowance shall only apply during the Application Phase of a secure session.

56 ## 5.3 Version reporting

57 The version that shall be reported for this message type in the Get MCTP version support response is as follows:

- The Version Number Entry 1 field shall be used to indicate backward compatibility with Version 1.0 of the SPDM Secured message type as:
  1.0.0 [Major version 1, minor version 0, any update version, no alpha]
  This is reported using the encoding as: `0xF1F0FF00`.
- The Version Number Entry 2 field shall be used to indicate backward compatibility with Version 1.1 of the SPDM Secured message type as:
  1.1.0 [Major version 1, minor version 1, any update version, no alpha]
  This is reported using the encoding as: `0xF1F1FF00`.
- The Version Number Entry 3 field shall be used to indicate backward compatibility with Version 1.2 of the SPDM Secured message type as:
  1.2.0 [Major version 1, minor version 2, any update version, no alpha]
  This is reported using the encoding as: `0xF1F2FF00`.
- The version of the SPDM Secured message type for this specification shall be reported in Version Number Entry 4 as:
  1.3.0 [Major version 1, minor version 3, update version 0, no alpha]
  This is reported using the encoding as: `0xF1F3F000`.

5.4 Key management during key update

59 The "Key update allowances" clause of DSP0277 describes how the receiver of `KEY_UPDATE` handles the transition from the old session key to the new session key. Specifically, for a transport like MCTP where the order of message delivery is not guaranteed, the receiver may have to keep the old session key after the key update, for decrypting incoming messages that were sent before the key update but arrived after the key update.

60 This specification recommends that an MCTP receiver should keep the old session key until `KT1` seconds (see Table 1 — Timing specification for SPDM secured messages over MCTP) have elapsed since the arrival of the `KEY_UPDATE` request with Operation of `VerifyNewKey`, which is protected by the new session key. After the old session key is deleted, messages protected by the old session key that have not reached the receiver, if any, are considered lost in transport and cannot be decrypted by the receiver, even if they eventually arrive at the receiver later.

5.5 Message tracking

62 The Requester and Responder use fields defined in DSP0236 to track messages. The Requester and Responder shall use the Source Endpoint ID, Message Tag (`Msg Tag`), and Tag Owner (`TO`) fields to uniquely identify messages and the corresponding responses. Request messages shall set the Tag Owner bit (`TO=1`), and Response messages shall clear the Tag Owner bit (`TO=0`) and shall use the same Message Tag as in the corresponding request message.

63

6 Timing requirements

64

Table 1 — Timing specification for SPDM secured messages over MCTP

Timing parameter	Ownership	Value	Unit	Description
`KT1`	Receiver	10	second	Shall be the number of seconds for which the receiver should retain the old session key after receiving the `KEY_UPDATE` request with `Operation` == `VerifyNewKey`.

7 ANNEX A (informative) Change log

7.1 Version 1.0.0 (2020-09-18)

- Initial release

7.2 Version 1.1.0 (2022-02-28)

- Allowed binding to Secured Messages using SPDM specification version 1.1 in Binding information.
- Change header level for Annex A and Bibliography.

7.3 Version 1.2.0 (2024-07-18)

- Updated reference to DSP0274 to version 1.1 or later.
- Add section for Version reporting.
- Clarify that the Partial Sequence Number in this specification is a portion of the full Sequence Number field in DSP0277.
- Added "Key management during key update" and "Timing requirements" clauses.
- Change binding to DSP0277 to version 1.2 and its errata and removed earlier DSP0277 bindings.

7.4 Version 1.3.0 (2025-10-31)

- Allow the `END_SESSION` request to be sent from the Responder to the Requester.
- Update Version reporting with new version number.
- Add Message tracking guidelines.

8 Bibliography

71 DMTF DSP4014, *DMTF Process for Working Bodies*, https://www.dmtf.org/dsp/DSP4014