Document Identifier: DSP0276

Date: 2023-10-08

Version: 1.1.1

Secured Messages using SPDM over MCTP Binding Specification

Supersedes: 1.1.0

Document Class: Normative

Document Status: Published

Document Language: en-US

9 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, 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.

10 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 product, protocols, or testing procedures. DMTF shall have no liability to any party implementing such standard, 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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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.

11 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.

12 This document’s normative language is English. Translation into other languages is permitted.

13

CONTENTS

1 Foreword

The Security Protocols and Data Models (SPDM) Working Group of DMTF 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 https://www.dmtf.org.

17

2 Acknowledgments

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

- 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.
- Viswanath Ponnuru — Dell Technologies
- Xiaoyu Ruan — Intel Corporation
- Nitin Sarangdhar — DMTF
- Bob Stevens — Dell Technologies

19 # 3 Introduction

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

21 ## 3.1 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.

22 # 4 Scope

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

24 ## 4.1 Normative references

25 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, *MCTP Base Specification 1.3.0*, https://dmtf.org/sites/default/files/standards/documents/DSP0236_1.3.0.pdf
- DMTF DSP0239, *MCTP IDs and Codes 1.7.0*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.7.0.pdf
- DMTF DSP0274, *Security Protocol and Data Model (SPDM) Base Specification, version 1.1 or later*, https://www.dmtf.org/dsp/DSP0274
- DMTF DSP0277, *Secured Messages using SPDM Specification 1.1.0*, https://www.dmtf.org/dsp/DSP0277
- *ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents - 2018 (8th edition)*
- IETF RFC5234, *Augmented BNF for Syntax Specifications: ABNF*, January 2008, https://tools.ietf.org/html/rfc5234
- *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3, 2020-06-03 Draft*, https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/

26 ## 4.2 Terms and definitions

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

28 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.

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

30 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.

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

32 4.3 Symbols and abbreviated terms

33 The abbreviations or notations defined in DSP0236, DSP0239, DSP0277, and DSP0274 apply to this document.

34 4.4 Binding Information

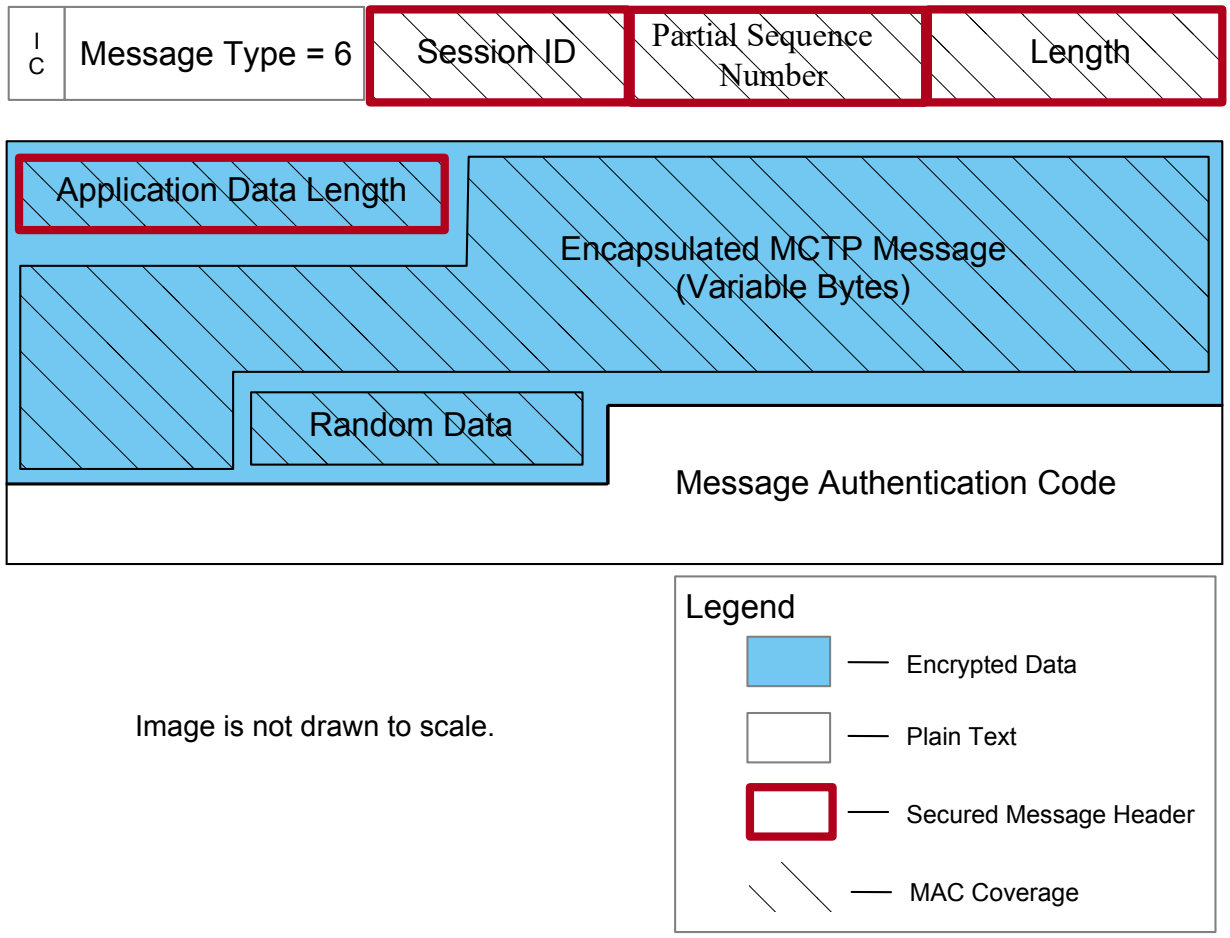
35 This version of this specification binds to these versions of *Secured Messages using SPDM* specification (DSP0277):

- Version 1.0.0 and all 1.0 errata versions
- Version 1.1.0 and all 1.0 errata versions

5 Secured messages over MCTP

To transport Secured Messages over MCTP, this specification utilizes the *Secured Messages using SPDM* specification (DSP0277), version 1.0. The secured message format, as defined by DSP0277, becomes the message payload in MCTP message type 6, as illustrated, at a high level, in the Secured Message over MCTP figure.

Secured Message over MCTP



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

5.1 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.

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.

5.2 MCTP encapsulated format

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 to be encapsulated. This is analogous to self-encapsulation, which has no meaningful use case.

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.

The IC bit for message type 6 shall be zero.

48 # 6 Transport requirements or allowances

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

50 ## 6.1 Transmission retries

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

52 ## 6.2 Certain SPDM message allowances

53 To take full advantage of asynchronous and bidirectional communication, as allowed by MCTP, both `KEY_UPDATE` and `HEARTBEAT` 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.

54 ## 6.3 Key management during key update

55 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 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.

56 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.

57 # 7 Timing requirements

58 **Table 1 — Timing specification for SPDM secured messages over MCTP**

Timing parameter	Ownership	Value	Units	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`.

59 ## 7.1 Version reporting

60 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 of the SPDM Secured message type for this specification shall be reported in Version Number Entry 2 as:
  1.1.1 [Major version 1, minor version 1, update version 1, no alpha]
  This is reported using the encoding as: `0xF1F1F100`.

8 ANNEX A (informative) change log

8.1 Version 1.0.0 (2020-09-18)

- Initial release

8.2 Version 1.1.0 (2022-02-28)

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

8.3 Version 1.1.1 (2023-10-08)

- Added “Key management during key update” and “Timing requirements” clauses.
- Add section for Version reporting.
- Updated reference to DSP0274 to version 1.1 or later.

9 Bibliography

66 DMTF DSP4014, *DMTF Process for Working Bodies 2.6*, https://www.dmtf.org/sites/default/files/standards/documents/DSP4014_2.6.1.pdf