Document Identifier: DSP0275

Date: 2023-10-08

Version: 1.0.2

Security Protocol and Data Model (SPDM) over MCTP Binding Specification

Supersedes: 1.0.1

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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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 *Security Protocol and Data Model (SPDM) over MCTP Binding Specification* (DSP0275).

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.

2 Acknowledgments

DMTF acknowledges these individuals' contributions to this document:

Contributors:

- Richelle Ahlvers — Broadcom Inc.
- Lee Ballard — Dell Technologies
- Joshua Cahill — Broadcom Inc.
- Patrick Caporale — Lenovo
- Yu-Yuan Chen — Intel Corporation
- Nigel Edwards — Hewlett Packard Enterprise
- Brett Henning — Broadcom Inc.
- Jeff Hilland — Hewlett Packard Enterprise
- Yuval Itkin — Mellanox Technologies
- Theo Koulouris — Hewlett Packard Enterprise
- Luis Luciani — Hewlett Packard Enterprise
- Masoud Manoo — Lenovo
- Mahesh Natu — Intel Corporation
- Edward Newman — Hewlett Packard Enterprise
- Scott Phuong — Cisco Systems Inc.
- Jeffrey Plank — Microchip
- Viswanath Ponnuru — Dell Technologies
- Hemal Shah — Broadcom Inc.

3 Abstract

SPDM is designed to be an effective interface and data model that enables efficient access to low-level security capabilities and operations.

SPDM over MCTP binding defines the format of SPDM messages transported over MCTP.

23 # 4 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 ## 4.1 Scope

25 This document defines the format of Security Protocol and Data Model (SPDM) over MCTP messages.

26 This document describes:

- SPDM over MCTP binding
- Common format for SPDM over MCTP messages

27 ## 4.2 Normative references

28 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 1.6.0*, https://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.6.0.pdf
- DMTF DSP0274, *Security Protocol and Data Model (SPDM) Base Specification, any version*, https://www.dmtf.org/dsp/DSP0274
- *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
- IETF RFC5234, *Augmented BNF for Syntax Specifications: ABNF*, January 2008, https://tools.ietf.org/html/rfc5234

29 ## 4.3 Terms and definitions

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

31 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.

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

33 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.

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

35 4.4 Symbols and abbreviated terms

36 The abbreviations defined in DSP0236, DSP0239, and DSP0274 apply to this document.

37 4.5 SPDM over MCTP binding

38 This specification defines how the Security protocol and data models transported over MCTP communications. SPDM is supported as a message type over MCTP. SPDM over MCTP binding defines the format of SPDM messages transported over MCTP. DSP0274 defines the common fields for SPDM messages and their usage.

39 This specification binds to any version of SPDM.

40 4.5.1 SPDM over MCTP message fields

41 Figure 1 shows the fields of an MCTP message body carrying an SPDM message.

42

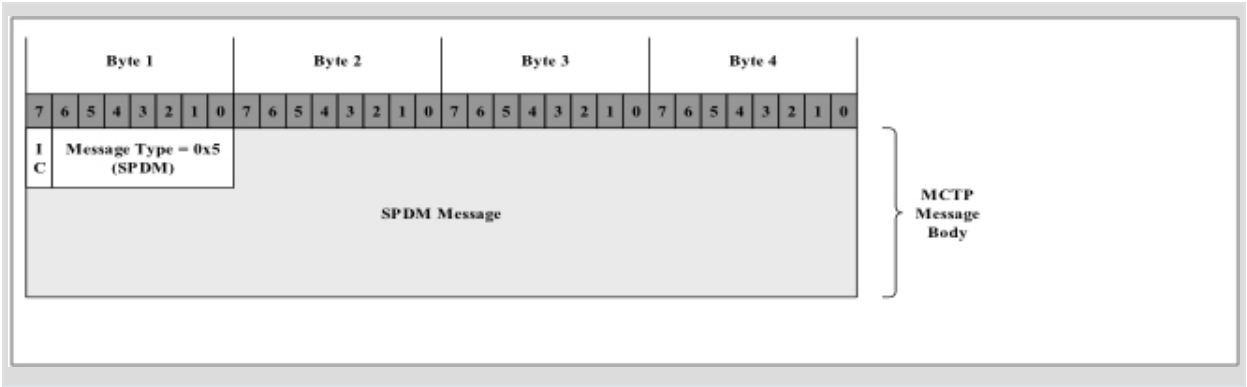

Figure 1 — SPDM over MCTP message fields

43 Table 1 defines the fields for the SPDM over MCTP message.

44 **Table 1 — SPDM over MCTP message field descriptions**

Field name	Field size	Description
IC	One bit	Check bit = `0b` SPDM over MCTP messages do not include an overall message integrity check field.
Message type	Seven bits	SPDM = `0x05` (`000_0101b`) Indicates that the MCTP message contains an SPDM message.
SPDM message	Variable	DSP0274 defines the base SPDM message fields.

45 ### 4.5.2 Requester and responder tracking

46 The Requester and Responder use fields defined in DSP0236 to track Responders and Requesters. The Responder shall use the Source Endpoint ID in the request message to track each SPDM Requester. The Requester shall use the Source Endpoint ID in the response message to track each SPDM Responder.

47 ## 4.6 Message tracking

48 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.

49 SPDM message exchanges, such as `CHUNK_SEND` and `CHUNK_SEND_ACK` , are composed of individual MCTP messages that are assembled into a larger SPDM payload, with the grouping of the chunks tracked by the `Handle` field. For instance, a Requester could send a larger message in three chunks using `CHUNK_SEND` . The Requester could send each chunk using Message Tags of 1, 2, and 3 respectively, but with the `Handle` field (`Param2`) set to the same value for each MCTP message. These chunks would be assembled to form a larger SPDM payload.

50 ## 4.7 Version reporting

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

- The version of the SPDM message type for this specification shall be reported in Version Number Entry 1 as: 1.0.2 [Major version 1, minor version 2, update version 2, no alpha]
  This is reported using the encoding as: `0xF1F0F200` .

5 ANNEX A (informative) Change log

5.1 Version 1.0.0 (2019-12-22)

- Initial release

5.2 Version 1.0.1 (2022-03-28)

- Update reference links to DSP0274.
- Add statement about binding to DSP0274.
- Added requirement for use of the Tag Owner bit and matching Message Tags for Requester and responder tracking.
- Added a section for Message tracking.

5.3 Version 1.0.2 (2023-10-08)

- Add section for Version reporting.
- Fix broken links

56

6 Bibliography

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