Document Identifier: DSP0275

Date: 2019-05-30

Version: 0.9.0

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

Information for Work-in-Progress version:

IMPORTANT: This document is not a standard. It does not necessarily reflect the views of the DMTF or its members. Because this document is a Work in Progress, this document may still change, perhaps profoundly and without notice. This document is available for public review and comment until superseded.

Provide any comments through the DMTF Feedback Portal:
http://www.dmtf.org/standards/feedback

Supersedes: None

Document Class: Normative

Document Status: Work in Progress

Document Language: en-US

CONTENTS

Figures

Tables

Foreword

The *Security Protocol and Data Model (SPDM) over MCTP Binding Specification* (DSP0275) was prepared by the Platform Management Components Intercommunications (PMCI) Working Group.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. For information about the DMTF, see http://www.dmtf.org.

Acknowledgments

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

Editor:

- Mahesh Natu – Intel Corporation

Contributors:

- Richelle Ahlvers – Broadcom Inc.
- Lee Ballard – Dell Technologies
- 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
- Edward Newman – Hewlett Packard Enterprise
- Scott Phuong – Cisco Systems Inc.
- Jeffrey Plank - Microchip
- Viswanath Ponnuru – Dell Technologies
- Hemal Shah – Broadcom Inc.

Introduction

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.

Document conventions

Typographical conventions

The following typographical conventions are used in this document:

- Document titles are marked in *italics*.
- ABNF rules are in monospaced font.

ABNF usage conventions

Format definitions in this document are specified using ABNF (see RFC5234), with the following deviations:

- Literal strings are to be interpreted as case-sensitive Unicode characters, as opposed to the definition in RFC5234 that interprets literal strings as case-insensitive US-ASCII characters.

Deprecated material

Deprecated material is not recommended for use in new development efforts. Existing and new implementations may use this material, but they shall move to the favored approach as soon as possible. CIM service shall implement any deprecated elements as required by this document in order to achieve backwards compatibility. Although CIM clients may use deprecated elements, they are directed to use the favored elements instead.

Deprecated material should contain references to the last published version that included the deprecated material as normative material and to a description of the favored approach.

The following typographical convention indicates deprecated material:

DEPRECATED

Deprecated material appears here.

DEPRECATED

In places where this typographical convention cannot be used (for example, tables or figures), the "DEPRECATED" label is used alone.

Experimental material

Experimental material has yet to receive sufficient review to satisfy the adoption requirements set forth by the DMTF. Experimental material is included in this document as an aid to implementers who are interested in likely future developments. Experimental material may change as implementation experience is gained. It is likely that experimental material will be included in an upcoming revision of the document. Until that time, experimental material is purely informational.

The following typographical convention indicates experimental material:

EXPERIMENTAL

Experimental material appears here.

EXPERIMENTAL

In places where this typographical convention cannot be used (for example, tables or figures), the "EXPERIMENTAL" label is used alone.

121

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

1 Scope

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

This document specifies the following information:

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

2 Normative references

The following referenced documents are indispensable for the application of this document. 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,*
http://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 0.9.0*
https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_0.9.0.pdf

IETF RFC5234, *ABNF: Augmented BNF for Syntax Specifications, January 2008*,
http://tools.ietf.org/html/rfc5234

ISO/IEC Directives, Part 2, *Principles and rules for the structure and drafting of ISO and IEC documents*,
http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype

3 Terms and definitions

In this document, some terms have a specific meaning beyond the normal English meaning. Those terms are defined in this clause.

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.

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

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.

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

4 Symbols and abbreviated terms

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

4.1

SPDM

Security Protocol and Data Model

5 SPDM over MCTP binding

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.

5.1 SPDM over MCTP message fields

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

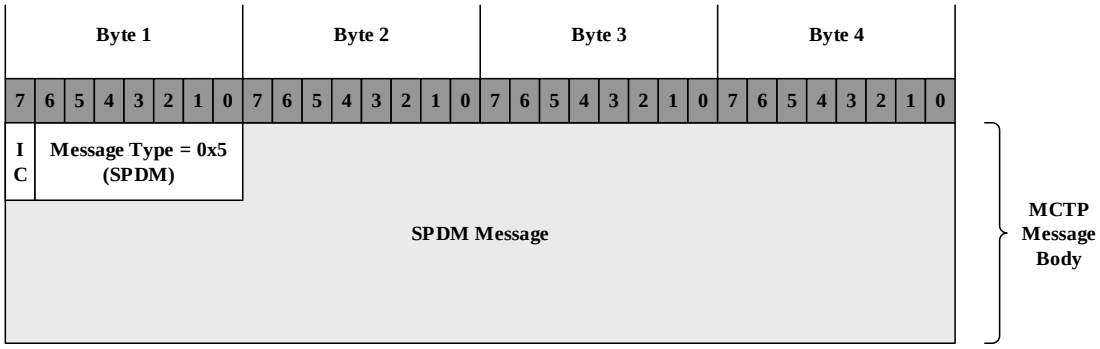

Figure 1 – SPDM over MCTP message fields

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

177 **Table 1 – SPDM over MCTP message field descriptions**

Field Name	Field Size	Description
IC	1 bit	Message Integrity Check bit = `0b` SPDM over MCTP messages do not include an overall Message Integrity check field.
Message Type	7 bits	SPDM = `0x05` (`000_0101b`) This field identifies the MCTP message as carrying a SPDM message.
SPDM Message	Variable	The base SPDM message fields are defined in DSP0274

178

ANNEX A
(**informative**)

Change log

Version	Date	Description
0.9.0	2019-05-30	Work in Progress release.

Bibliography

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