Document Identifier: DSP0276

Date: 2019-03-18

Version: 1.0.0a

Secured MCTP Messages 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 This document is available for public review and comment until superseded.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

Copyright Notice

Copyright © 2020 DMTF. All rights reserved.

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.

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patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a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

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

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

CONTENTS

1 Foreword

The Platform Management Components Intercommunications (PMCI) Working Group prepared the *Security MCTP Messages 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 the DMTF, see https://www.dmtf.org.

2 Acknowledgments

The DMTF acknowledges these individuals' contributions to this document:

Contributors:

- Scott Phuong — Cisco Systems 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.

Secured MCTP Messages over MCTP Binding defines the methodology that MCTP endpoints can use to communicate securely by utilizing SPDM.

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.

4.1 Scope

This document defines the format and other transport requirements for any MCTP message to be sent encrypted and authenticated using SPDM as the basis for a secure channel of communication.

4.2 Normative references

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 1.1.0*, **Add link**
- *ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents*, https://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype
- IETF RFC5234, *Augmented BNF for Syntax Specifications: ABNF*, January 2008, https://tools.ietf.org/html/rfc5234

4.3 Terms and definitions

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

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

4.4 Symbols, Notation and abbreviated terms

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

5 Secured MCTP Messages over MCTP Binding

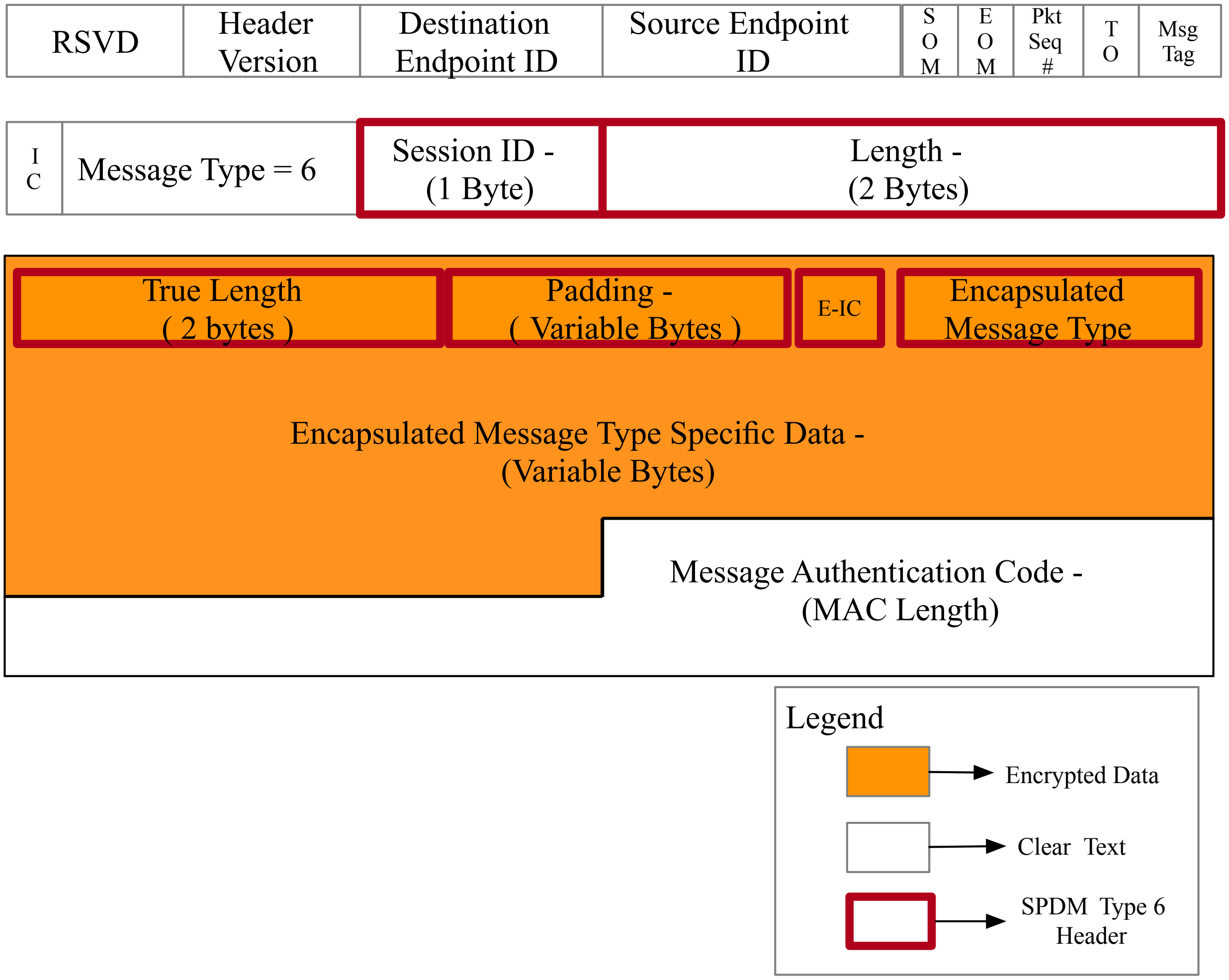
To securely transport MCTP messages over a physical medium, this specification uses SPDM as the foundation for secure communication and defines the necessary details to bind SPDM to the MCTP transport layer. Specifically, a record format based on both TLS 1.3 and DTLS 1.3 is described for encryption and message authentication and a MCTP message type 6 format is defined to encapsulate other MCTP message types. Both these mechanism are necessary to achieve a secure channel of communication for many MCTP message types.

6 MCTP Encapsulated Format

This clause describes the encapsulated format for the transmission of various MCTP messages over a secured session as described in the main SPDM specification (DSP0274 version 1.1). The figure, SPDM Record over MCTP Type 6, illustrates the general SPDM record format over MCTP. The IC bit shall be 0.

MCTP Message Type 6 contains message-specific headers to associate the message to an SPDM session. The remaining fields of this message type encapsulates other MCTP message types. These two functions work in unison to provide encryption and message authentication for other MCTP message types.

SPDM Record over MCTP Type 6



MCTP endpoints wanting to communicate over an SPDM session shall use MCTP type 6. SPDM endpoints communicating over MCTP Type 6 shall adhere to the format and details described by the SPDM Record over MCTP Table.

SPDM Record over MCTP Table

Offset	Field	Length	Units	Description
1:0	Session ID	2	bytes	The Responder and Requester can use this field to bind all session information such as secrets and keys. This field shall be the same value as the `SessionID` field in either `KEY_EXCHANGE_RES` response or `PSS_KEY_EXCHANGE` response.
3:2	Length	2	bytes	This field shall be the remaining length of data in the MCTP message.
5:4	True Length	2	bytes	This field shall be the remaining length of data minus the padding length.
(5 + A):6	Padding	A	bytes	This field should contain random data of random length. The maximum length shall be 32 bytes and the minimal length shall be 1.
(6 + A)	E-IC	1	bits	This field shall be the integrity check bit for the encapsulated MCTP message.
(6 + A)	Encapsulated Message Type	7	bits	This field shall be the MCTP message type of the encapsulated MCTP message.
(6 + A + B) : (7 + A)	Encapsulated Message Body	B	bytes	This field shall contain data specific to the encapsulated MCTP message, if present.
See Description	Message Authentication Code	Variable	bytes	This field is for illustrative purposes only. The actual location and details of the MAC in the cipher text shall adhere to the AEAD specification for the selected AEAD cipher in `ALGORITHMS` response.

Except for the Encapsulated Message Body and MAC, all fields are in little endian.

6.1 AEAD Requirements

The associated data, `associated_data`, for AEAD shall be the concatenation, in order, of the following fields:

1. Session ID
2. Length
3. True Length
4. Padding
5. E-IC
6. Encapsulated Message Type
7. Encapsulated Message Body

The text to encrypt, `clear_text`, for AEAD shall be the concatenation, in order, of these fields:

1. True Length
2. Padding
3. E-IC
4. Encapsulated Message Type
5. Encapsulated Message Body

6.1.1 Per-Message Nonce Derivation

The nonce used at this layer shall be bound to a single instance of MCTP message type 6.

The nonce shall never be transmitted in the message. This means that both Responder and Requester must internally track the nonce. In order to ensure proper tracking, the Responder shall follow the nonce derivation schedule laid henceforth.

Internally, before the creation of the first record in the session, both Responder and Requester shall start with a 64-bit sequence number with a value of zero. For each record, both SPDM endpoint shall follow the recipe as prescribed:

1. Zero Extend the Sequence Number to `iv_length` according to the selected AEAD cipher suite in `ALGORITHMS` messages.
2. Perform a bitwise XOR of the zero-extended Sequence Number with the respective salt derived in the Key Schedule clauses.
3. The output of the above step is the per-record nonce.
4. Increment the sequence number by a value of one for the next record.

Because different secrets are used for different directions of data transmission, each endpoint would have to track two sequence numbers: one for the reception and the other for the transmission in order to properly process the record.

Lastly, when a `KEY_UPDATE` occurs, the sequence number shall reset to 0 before sending the first record using the new session keys.

6.1.2 Encryption Requirements

A single instance of MCTP message type 6 shall contain the complete cipher text as produced by a single invocation of `AEAD_Encrypt` using the appropriate encryption key for the given direction of transmission, the appropriate per-record nonce and the selected AEAD Cipher Suite in `ALGORITHMS`.

7 Transport Requirements or Allowances

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

7.1 Retries

A retry of this message type shall be defined as the reuse of a sequence number. Record retries shall be expressly prohibited. The MCTP layer may retry the transmission of MCTP message type 6 as long as it does not violate this sequence number requirement.

7.2 Certain SPDM Message Allowances

To take full advantage of asynchronous and bidirectional communication, as allowed by MCTP, both `KEY_UPDATE` and `HEARTBEAT` may be sent directly from a Responder without any other assistance such as a sideband alerting mechanism or SPDM's `GET_ENCAPSULATED_REQUEST` mechanism.

7.3 ERROR Response Message Allowances

Furthermore, the `ERROR` message may be sent without an SPDM request when the error code is an decryption error (`ErrorCode=DecryptError`) to indicate the MCTP message type 6 that was received could not be decrypted. In addition, both SPDM requester and responder may send the `ERROR` message. This is especially useful for data sent at the application layer (i.e. the encapsulated MCTP message). In other words, in this scenario, the `ERROR` response message is behaving as a response to the inability to decrypt or authenticate the received MCTP type 6 message, regardless of the encapsulated MCTP message content.

7.4 ANNEX A (informative)

7.4.1 Change log

Version	Date	Description
1.0.0	2019-10-30	First release.

7.5 Bibliography

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