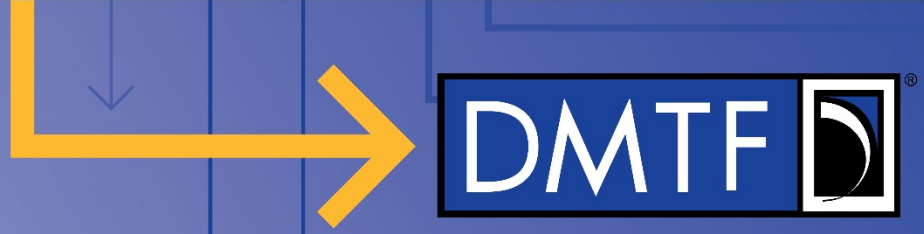


DMTF PMCI
Security Specifications Stack

Phil Hawkes, Jim Panian (Qualcomm)

February 2021

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change without notice. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website.

- This information is a summary of the information that will appear in the specifications. See the specifications for further details.

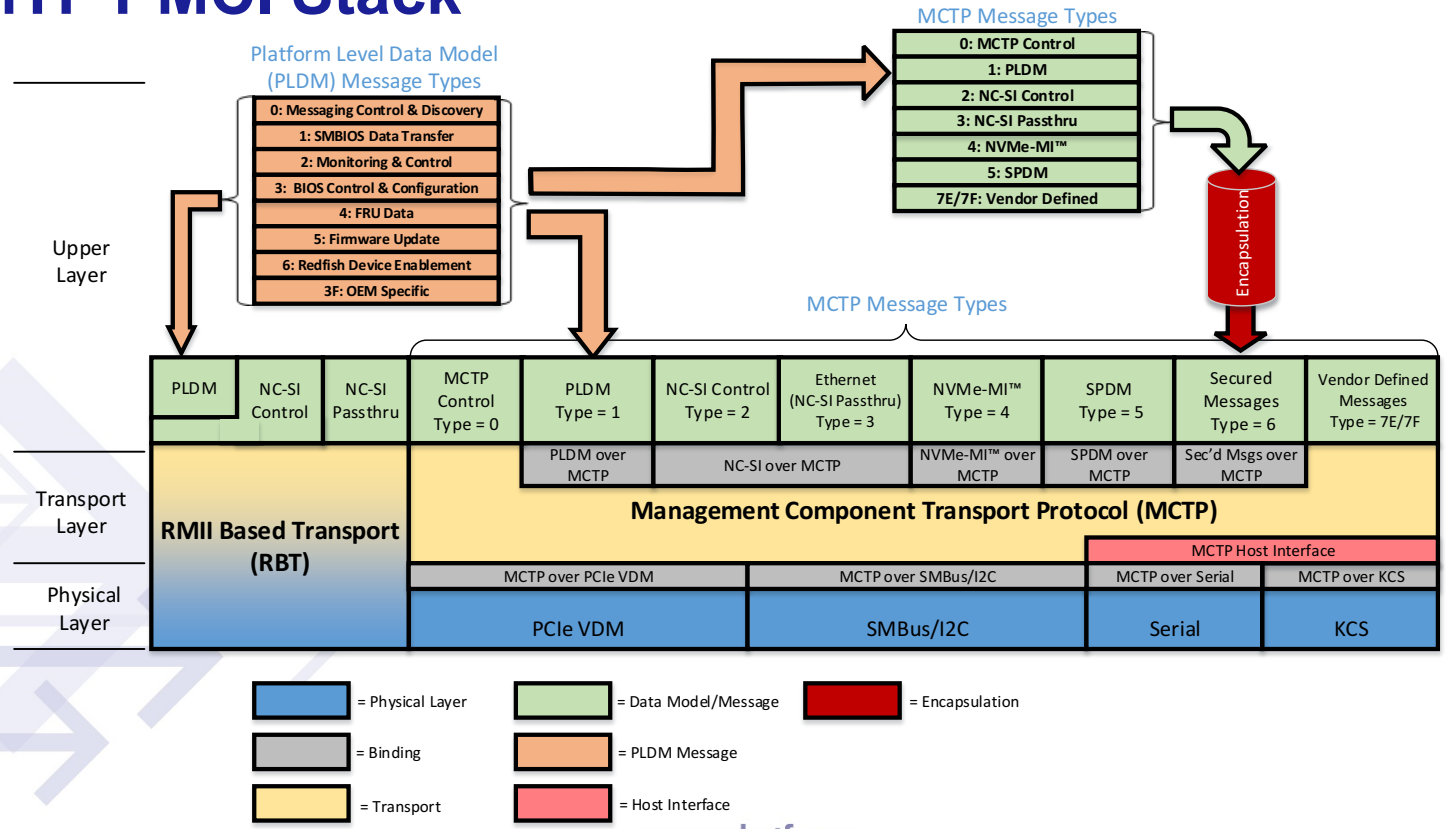
Scope

- Purpose:
  - Explaining how DMTF PMCI Specification are "stacked" to enable securing messages transported by MCTP.
  - Illustrate how MCTP messages are securely encapsulated at a sender and decapsulated at a receiver
  - Protocol Details are out-of-scope.

Introduction

- PMCI provides specifications which combine to enable securing messages transported by MCTP.
- The DMTF PMCI Stack diagram illustrates how various MCTP message types can be transported using MCTP, where MCTP itself can be carried by various physical layers.
  - SPDM messages can be sent using MCTP Type = 0x05
  - MCTP messages can be sent securely by encapsulating them using MCTP Type = 0x06
  - The slide entitled “List of MCTP Message Types” describes the messages associated with each Type

DMTF PMCI Stack



List of MCTP Message Types

This table is copied from DMTF DSP0239 "Management Component Transport Protocol (MCTP) IDs and Codes", v1.7.0. Available at https://www.dmtf.org/standards/pmci

*SPDM and Secured Messages are sent in MCTP using Message Type Codes **0x05** and **0x06** respectively*

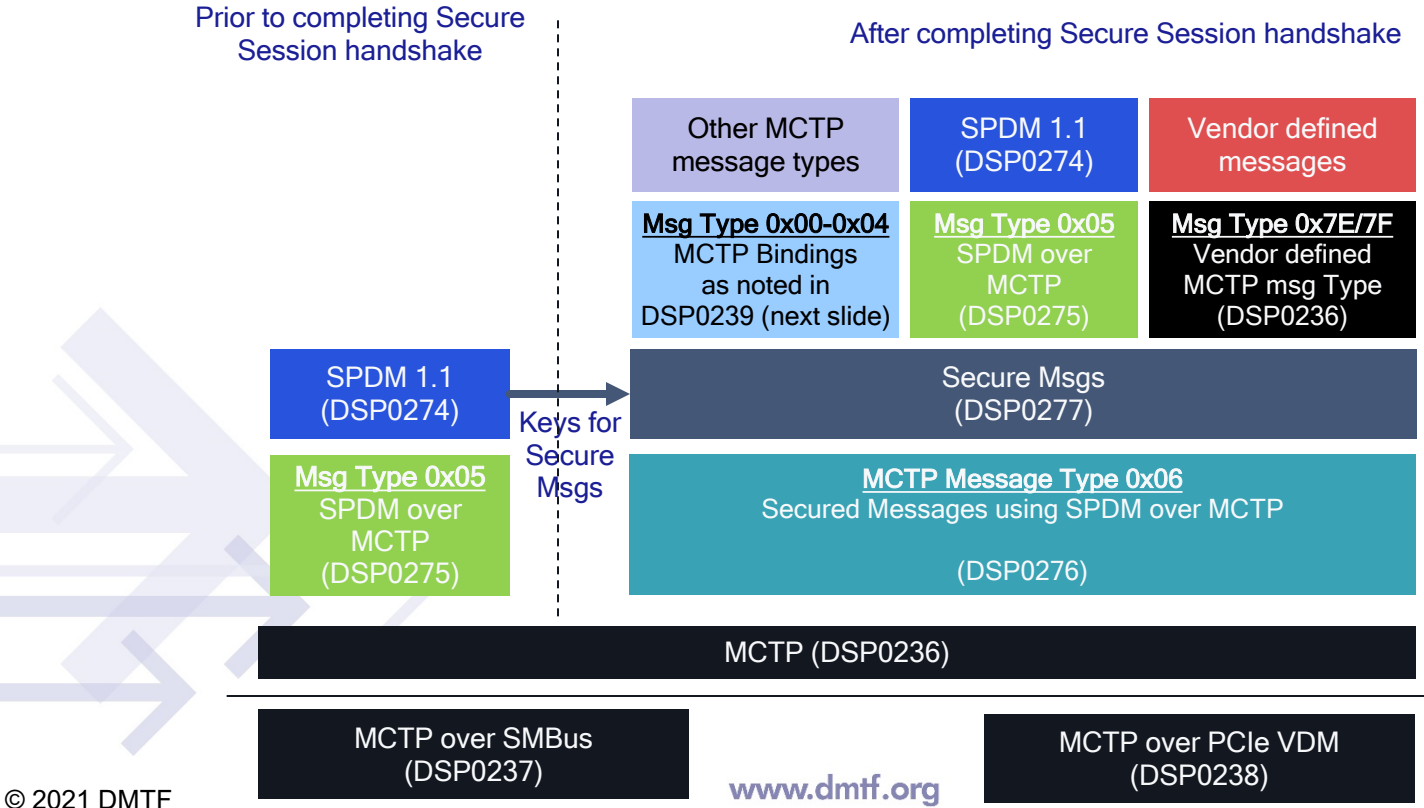
Table 1 – MCTP Message Types

Message Type	Message Type Code	Description
MCTP Control	0x00	Messages used to support initialization and configuration of MCTP communication within an MCTP network, as specified in DSP0236
Platform Level Data Model (PLDM)	0x01	Messages used to convey Platform Level Data Model (PLDM) traffic over MCTP, as specified in DSP0241.
NC-SI over MCTP	0x02	Messages used to convey NC-SI Control traffic over MCTP, as specified in DSP0261.
Ethernet over MCTP	0x03	Messages used to convey Ethernet traffic over MCTP. See DSP0261. This message type can also be used separately by other specifications.
NVM Express Management Messages over MCTP	0x04	Messages used to convey NVM Express (NVMe) Management Messages over MCTP, as specified in DSP0235.
SPDM over MCTP	0x05	Messages used to convey Security Protocol and Data Model Specification (SPDM) traffic over MCTP, as specified in DSP0275.
Secured Messages	0x06	Messages used to convey *Secured Messages using SPDM over MCTP Binding Specification* traffic, as specified in DSP0276.
Vendor Defined – PCI	0x7E	Message type used to support VDMs where the vendor is identifed using a PCI-based vendor ID. The specification of the initial Message Header bytes for this message type is provided within this specification. The specification of the format of this message is given in DSP0236. Otherwise, the message body content is specified by the vendor, company, or organization identified by the given vendor ID.
Vendor Defined – IANA	0x7F	Message type used to support VDMs where the vendor is identifed using an IANA-based vendor ID. This format uses an "Enterprise Number" that is assigned and maintained by the Internet Assigned Numbers Authority (IANA), www.iana.org, as the means of identifying a particular vendor, company, or organization. The specification of the format of this message is given in DSP0236. Otherwise, the message body content is specified by the vendor, company, or organization identified by the given vendor ID.
Reserved	all other	Reserved

How are DMTF PMCI Security Specification "stacked"?

- The specifications in the DMTF PMCI Stack specify either
  - a protocol, or
  - a "binding" which describes how protocol messages can be carried inside messages of another protocol or transported by a physical layer.
- A specification "stack" shows the relationships between protocols and physical layers, with protocols higher up the stack being transported by protocols and physical layers lower in the stack
- The relationships between the specifications are illustrated in the Specification Stack for Secured Messages over MCTP:
  - The left-hand side of the figure illustrates the stack of specifications for transporting SPDM over MCTP in the absence of a secured session.
    - The SPDM exchange can include a Secure Session Handshake, resulting in SPDM negotiating algorithms and generating session keys
  - The right-hand side of the figure illustrates the stack of specifications for securing various MCTP message types after SPDM completes a Secure Session Handshake.
  - The full names and versions of the specifications are available on the References slide.

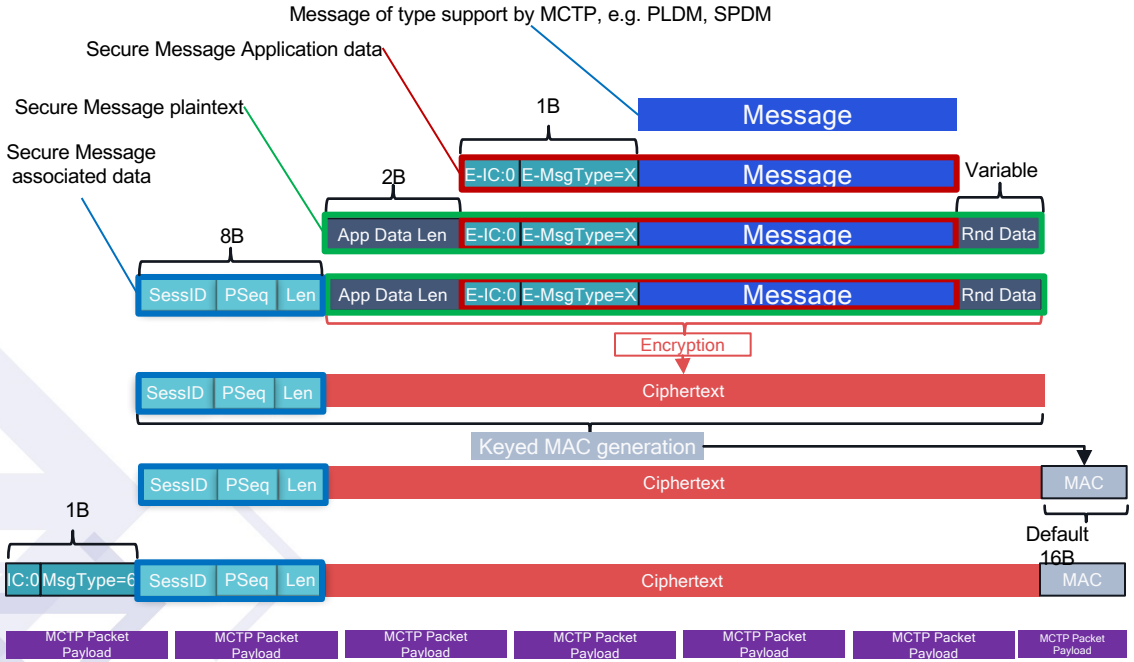
Specification Stack for Secured Messages over MCTP



Message composition

- The next few slides illustrate steps for
  - Encapsulating a MCTP message into a MCTP Type 0x06 Secured Message
  - Decapsulating a MCTP message from a MCTP Type 0x06 Secured Message
- Slides 11 & 12 shows the steps for a generic MCTP message
- Slides 13 & 14 shows the steps for an SPDM message
  - SPDM messages have MCTP message Type 0x05
- The numbers in round brackets refer to the DMTF specification identifier with the preceding "DSP0" removed. The full name and version of the specification is provided in the References slide
  - For example, "(277)" refers to "DSP0277", which has full name *"Secured Messages using SPDM over MCTP Binding Specification", v1.0.0*

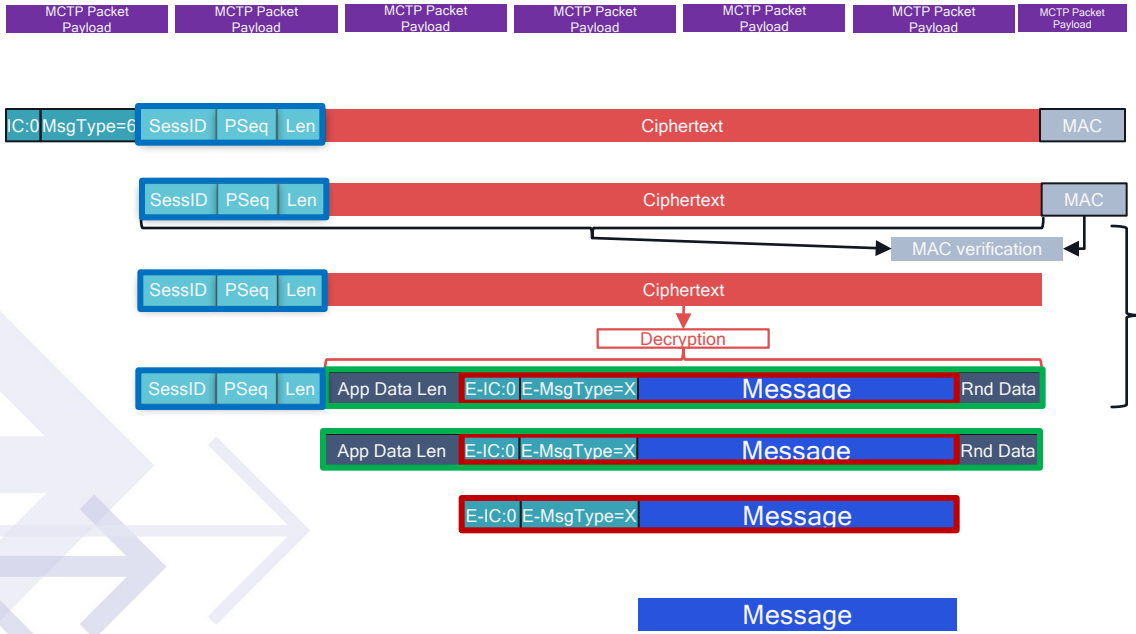
Encapsulating MCTP messages into "Secure Msg over MCTP"



1. Message to be sent
2. Form Sec Msg App Data (277) by adding E-IC and E-MsgType (defined by 239) according to (276)
3. Form Sec Msg Plaintext (277) by prepending App Data Length and appending Random Data
4. Form Sec Msg inputs by adding associated data (277)
5. Apply AEAD Encryption and MAC generation (277)
6. Form MCTP msg by adding IC & MsgType 0x06 for Secured Messages (276)
7. Fragment MCTP Msg into MCTP packet payloads, add MCTP packet headers, and deliver MCTP packet to destination (236)

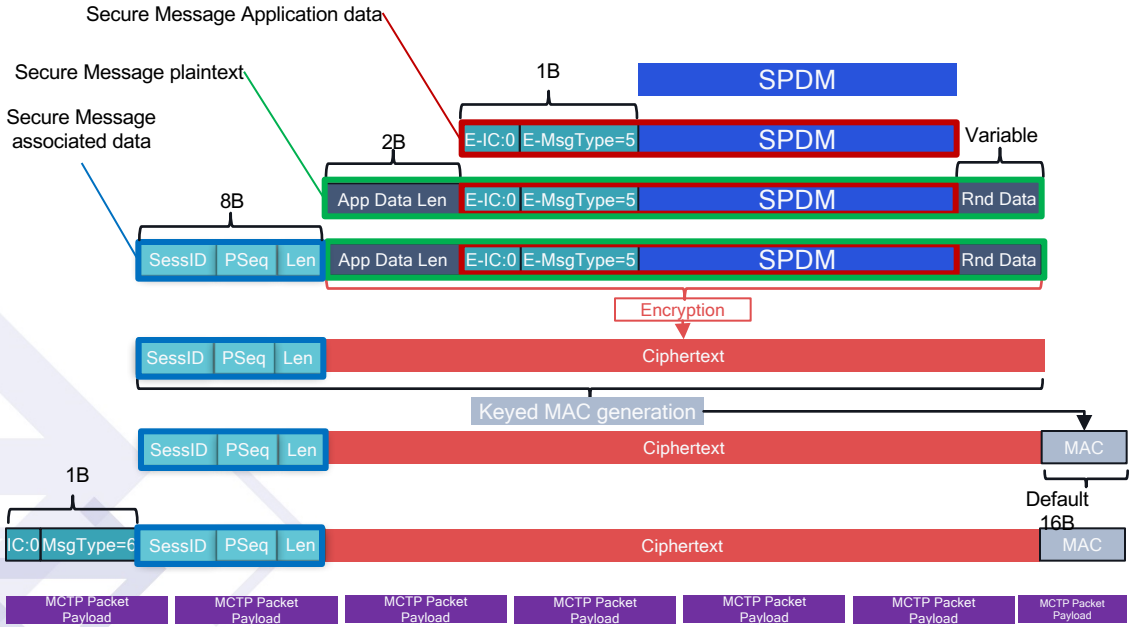
Maximum MCTP Packet payload length depends on the PHY for the delivery path.

Decapsulating MCTP message from "Secure Msg over MCTP"



1. Receive MCTP packets, process MCTP packet headers & reassemble MCTP packet payloads into MCTP Msg (0236)
2. MCTP MsgType=0x06 indicates Sec Msg/MCTP in payload (276)
3. Remove MCTP msg headers leaving Sec Msg outputs (276)
4. Apply AEAD MAC verification and decryption -can occur in parallel (277)
5. Remove associated data, leaving Sec Msg Plaintext (277)
6. Process App Data Len + remove Rnd Data, resulting in Encapsulated MCTP msg App Data (277)
7. Process E-IC & E-MsgType (276) to identify applicable protocol (according to 239)

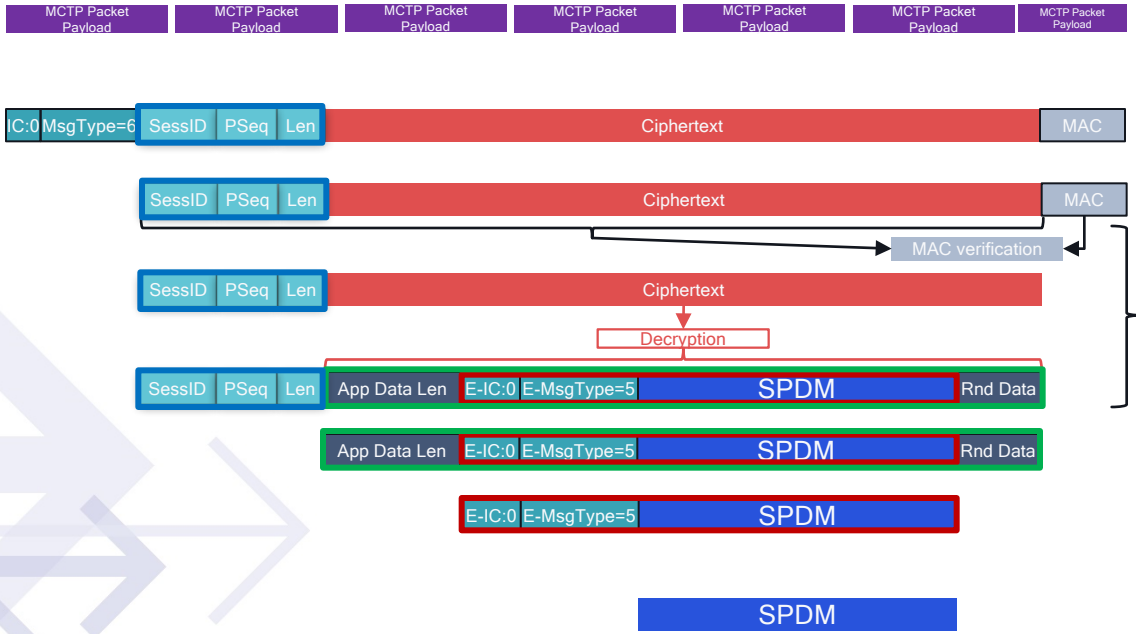
Encapsulating SPDM message into "Secure Msg over MCTP"



1. SPDM Message to be sent
2. Form Sec Msg App Data (277) by adding E-IC and E-MsgType=0x05 (239,275) according to (276)
3. Form Sec Msg Plaintext (277) by prepending App Data Length and appending Random Data
4. Form Sec Msg inputs by adding associated data (277)
5. Apply AEAD Encryption and MAC generation (277)
6. Form MCTP msg by adding IC & MsType 0x06 for Secured Messages (276)
7. Fragment MCTP Msg into MCTP packet payloads, add MCTP packet headers, and deliver MCTP packet to destination (236)

Maximum MCTP Packet payload length depends on the PHY for the delivery path.

Decapsulating SPDM message from "Secure Msg over MCTP"



1. Receive MCTP packets, process MCTP packet headers & reassemble MCTP packet payloads into MCTP Msg (236).
2. MCTP MessageType=0x06 indicates Sec Msg/MCTP in payload (276)
3. Remove MCTP msg headers leaving Sec Msg outputs (276)
4. Apply AEAD MAC verification and decryption -can occur in parallel (277)
5. Remove associated data, leaving Sec Msg Plaintext (277)
6. Process App Data Len + Rnd Data, resulting in Encapsulated MCTP msg App Data (277)
7. Process E-IC & E-MsgType=0x05 (276), indicating SPDM message (239,275)

References

These documents are available at https://www.dmtf.org/standards/pmci

1. DMTF DSP0235, *NVMe™ (NVMe Express™) Management Messages over MCTP Binding Specification*, v1.0.1
2. DMTF DSP0236, *Management Component Transport Protocol (MCTP) Base Specification*, v1.3.1
3. DMTF DSP0237, *Management Component Transport Protocol (MCTP) SMBus/I2C Transport Binding Specification*, v1.2.0
4. DMTF DSP0238, *Management Component Transport Protocol (MCTP) PCIe VDM Transport Binding Specification*, v1.1.0
5. DMTF DSP0239, *Management Component Transport Protocol (MCTP) IDs and Codes*, v1.7.0
6. DMTF DSP0241, *Platform Level Data Model (PLDM) Over MCTP Binding Specification*, v1.0.0
7. DMTF DSP0261, *NC-SI over MCTP Binding Specification*, v1.2.2
8. DMTF DSP0274, *Security Protocol and Data Model (SPDM) Specification*, v1.1.0
9. DMTF DSP0275, *Security Protocol and Data Model (SPDM) over MCTP Binding Specification*, v1.0.0
10. DMTF DSP0276, *Secured Messages using SPDM over MCTP Binding Specification*, v1.0.0
11. DMTF DSP0277, *Secured Messages using SPDM Specification*, DRAFT 1.0.0b
12. DMTF DSP2058, *Security Protocol and Data Model (SPDM) Architecture White Paper*, v1.0.0