SPDM Overview and v1.2 Preview
(Work in Progress)

November 2020

Disclaimer

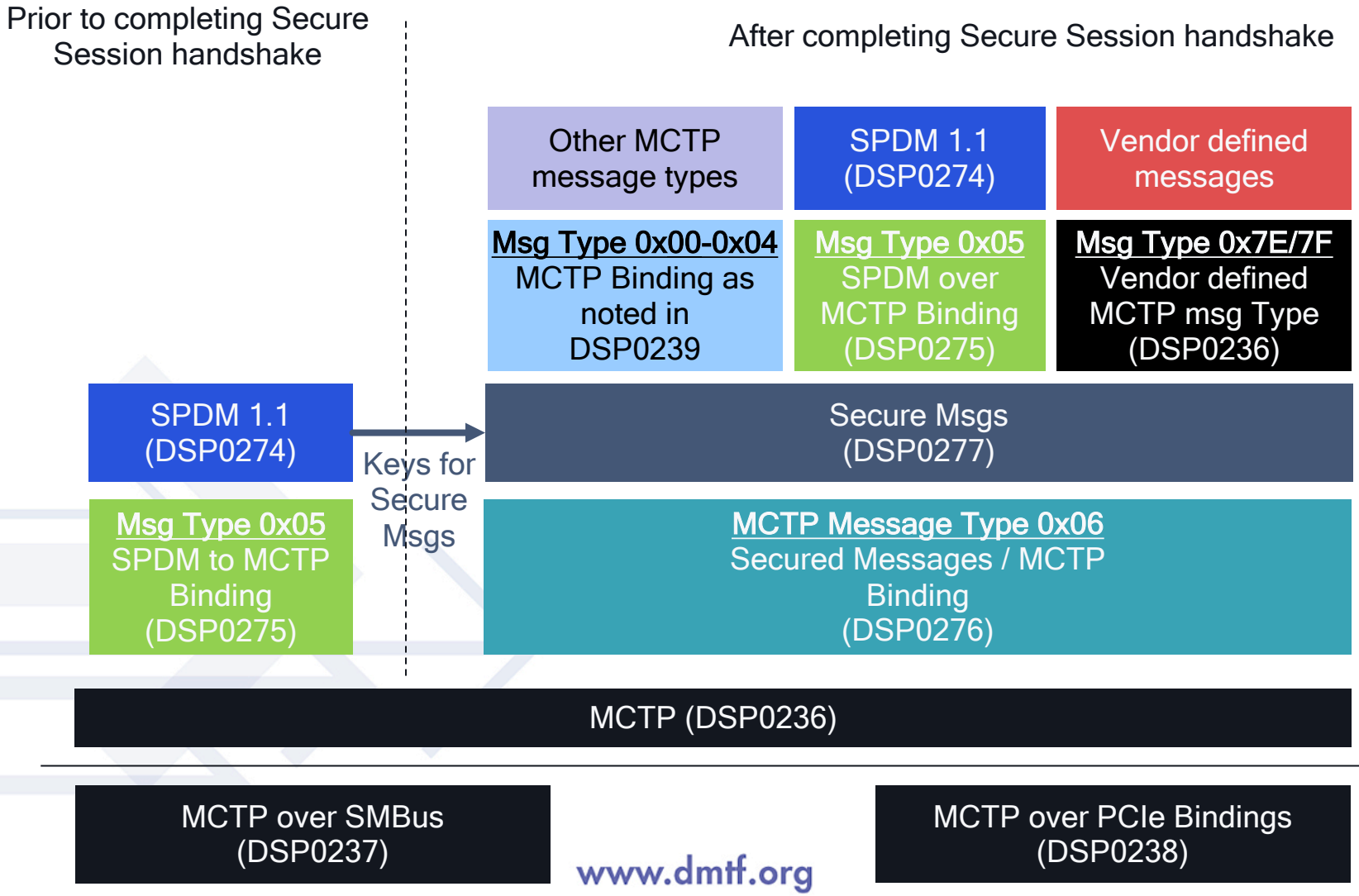
- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change without notice. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website.

SPDM 1.0 and 1.1 Feature Summary

SPDM 1.0 Features	SPDM 1.1 Feature Additions
Certificate Chain Retrieval	Support for Authenticated and Encrypted Messages
Challenge for knowledge of the Device Private Key (Authentication)	Mutual Authentication
Report of Measurements	Session Establishment using a Key Exchange
MCTP Type 5 Messages	Session Establishment using a Preshared Key
	Session Management
	MCTP Type 6 Messages

Working with DMTF Alliance Partners to align industry to a single protocol: PCI-SIG, MIPI, OCP, CXL, GenZ, HD-BaseT

DMTF Security Spec Stack-up using Secured Msgs over MCTP



SPDM 1.2 Key Features under Consideration

Feature	Description
Set Certificate	A set of commands to manage certificate chains in slots 1-7. Could include CSR export and slot policies.
Eventing	Mechanism to send asynchronous events, related to SPDM, to a registered listener.
Multi-tier Authentication	A set of commands to authenticate devices behind non-transparent bridges. Under discussion, does the PA-RoT or intermediate device perform the authentication?
Smaller Certificates	Address the size issue with the current certificate / cert chain.
Measurement Manifests	Define a mechanism to produce a manifest of expected measurements for a given device, and modifications to the MEASUREMENTS command to report measurements in a way that is compatible with the reference manifest.
TCG DICE Support	Support the use of TCG DICE throughout SPDM, including in signature generation, Set Certificate, and events.
Reprovisioning	Mechanism to cause a device to generate a new set of Device Keys and invalidate all elements that depend on the existing Device Keys.