MICROCHIP

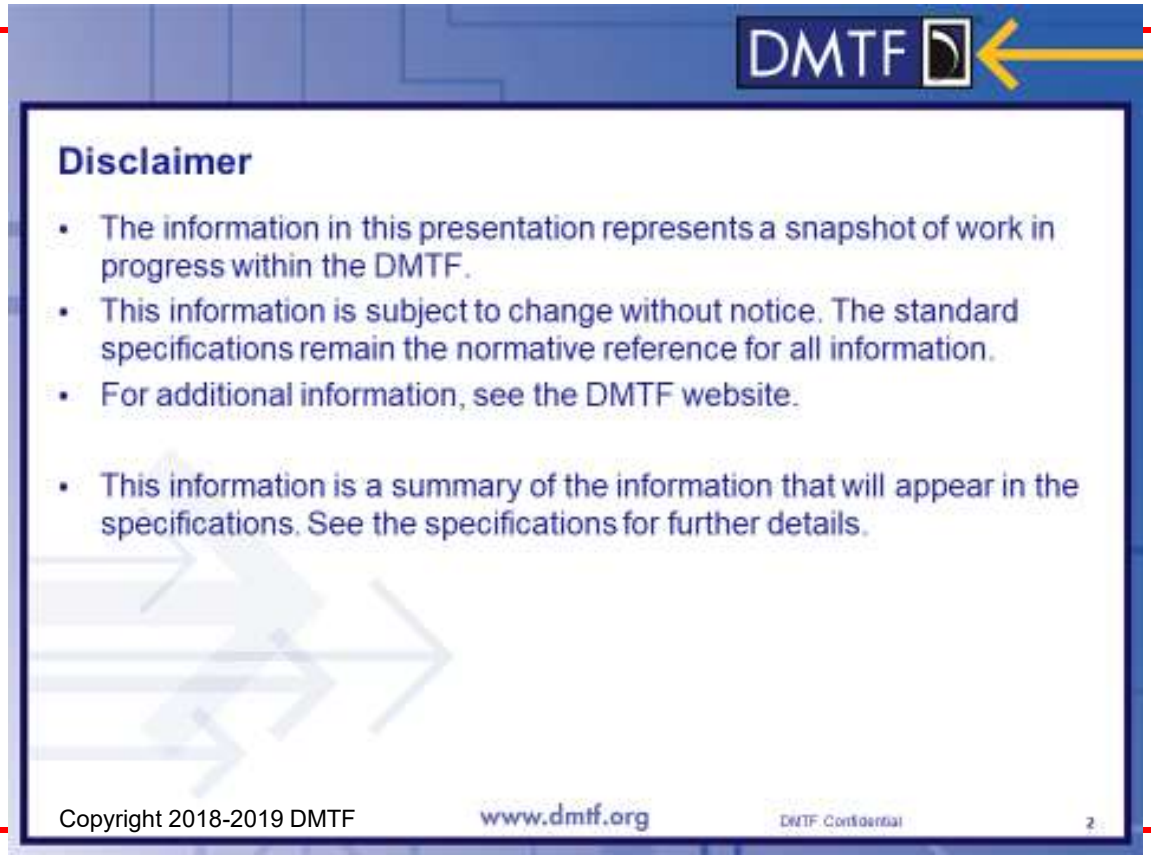
Perspectives in Security Measurement Utilizing the DMTF Security Protocol and Data Model (SPDM)

Jeff Plank, Security Architect, Associate Fellow, October 1, 2019, Platform Security Summit

Disclaimers

- I do not represent the DMFT Organization nor the Security Working Group as I am not an official liaison
- Microchip is a participant in the Security Working Group as a voting member
- Any examples shown in the presentation are for illustrative purposes only and should ***NOT*** be interpreted as supported (current or future) by SPDM, the official released DMTF materials should be observed.
- All DMTF materials found in this presentation are protected by Copyright of the DMTF organization and will be appropriately marked as such
- The DMTF disclaimers apply to presented content regarding SPDM

DMTF Disclaimer

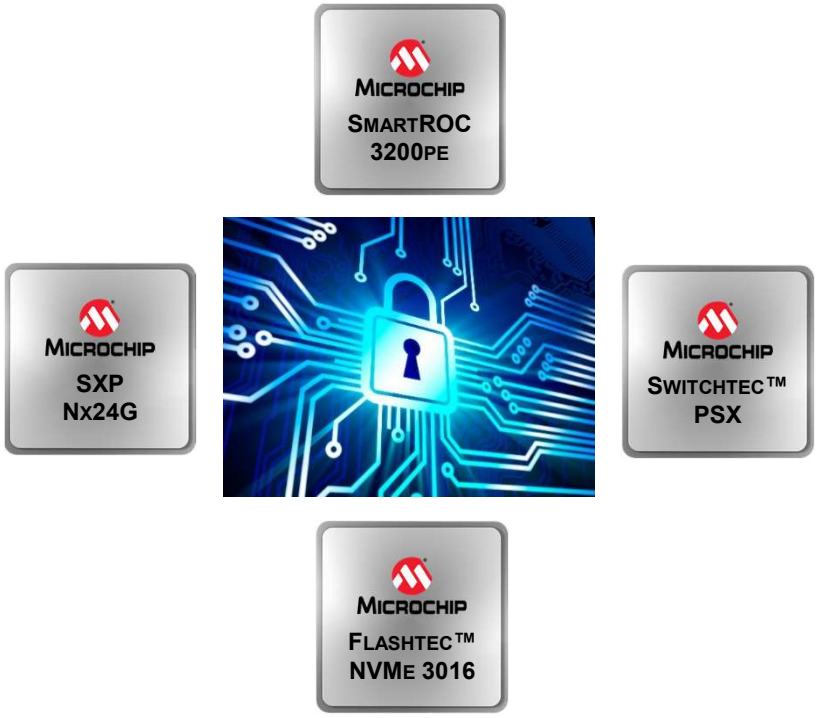


Agenda

- **Microchip Secure Portfolio**
- **Background**
- **Problem Statement**
- **What is SPDM ?**
  - SPDM 1.0 WIP Overview
  - SPDM 1.1 WIP Overview
- **Work Group Information**
- **Observations and Concerns**

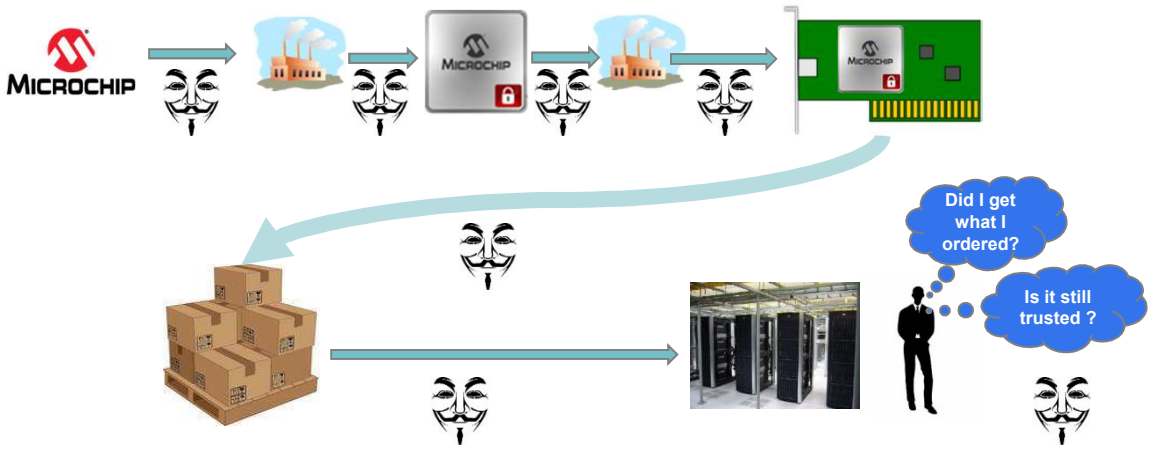
Microchip Data Center Solutions

Leaders in Data Protection and Security



- Data Protection/Encryption
- Hardware Root of Trust
- Programmable Keys
- Secure Firmware Update
- Attestation Measurements
- Authenticated Devices
- Secure Debug

Trusted Platforms – Why the need?



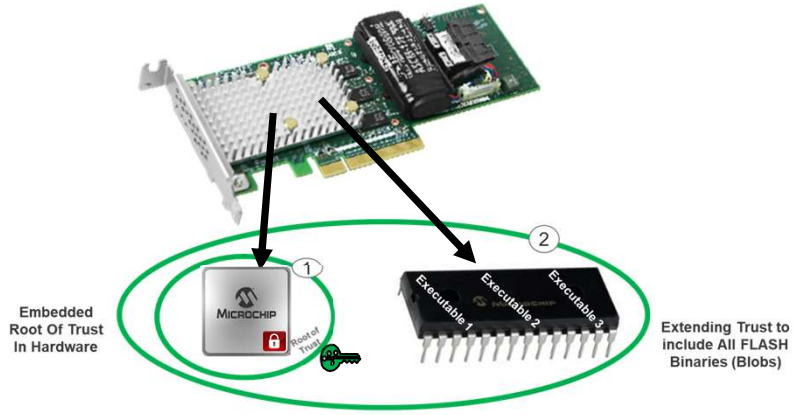
• Various points of entry • Where has the product been? • Is it really the expected product? • Was it intercepted in flight?	• Is it running altered firmware/hardware? • Does it contain the intended components? • Will it stay that way? • Is the product genuine?

Security Threats Along the Way of Manufacturing & Deploying

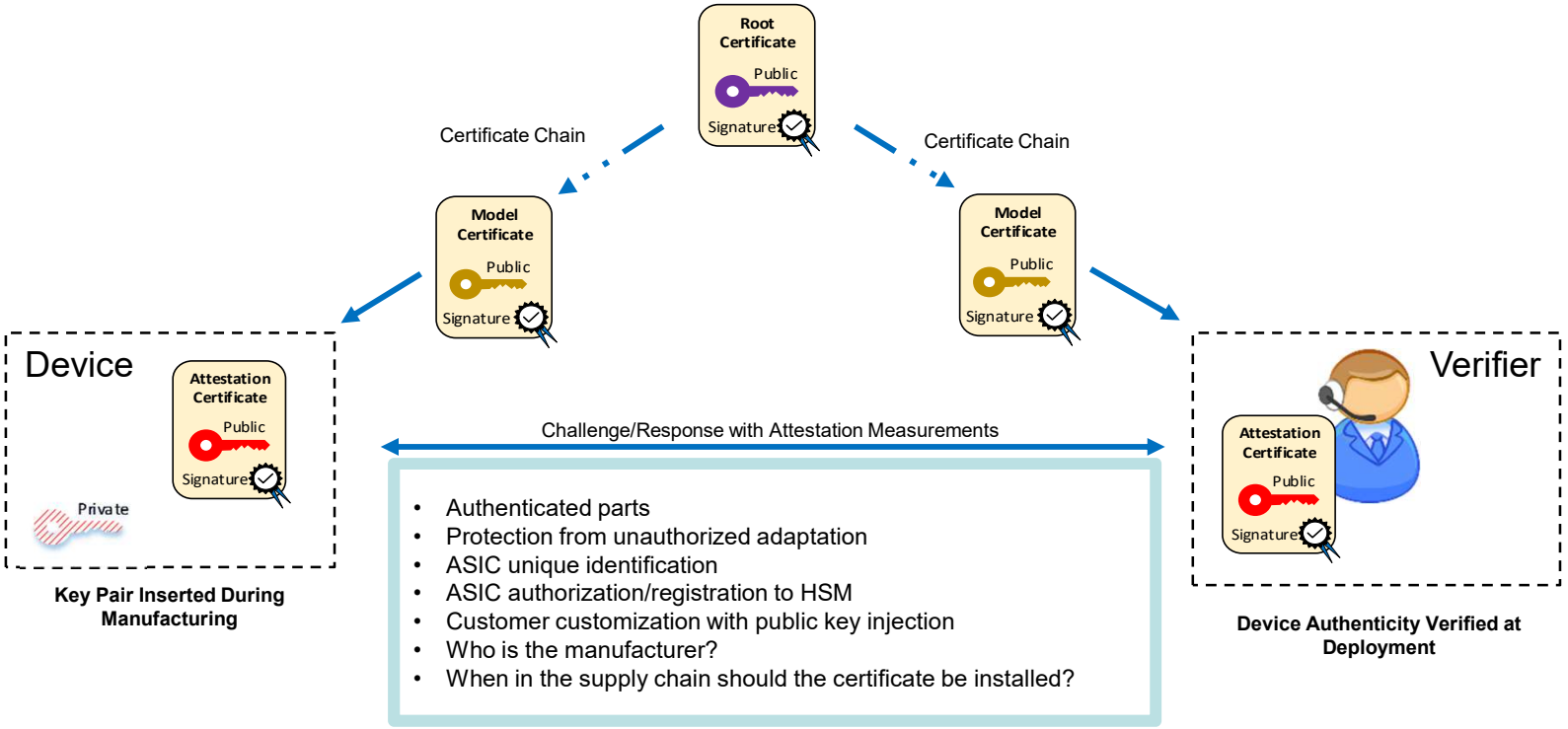
What is Secure Boot?

- **Silicon HW Root of Trust**
- **Security begins with the Root of Trust contained in the ASIC**
  - Embedded Signing Keys
  - Strong Hashing Functions
  - Immutable Authenticating Boot Logic in Silicon Boot ROM

- **Board Components Enablement and Security**
  - Trust is extended by verifying the authenticity and integrity of FLASH content prior to executing it
  - Digital signatures are supplied with all Firmware and Configuration Binaries
  - Validated with Embedded ASIC signing keys
  - *ASIC calculated hashes are computed against the stored images* and compared with stored signatures.

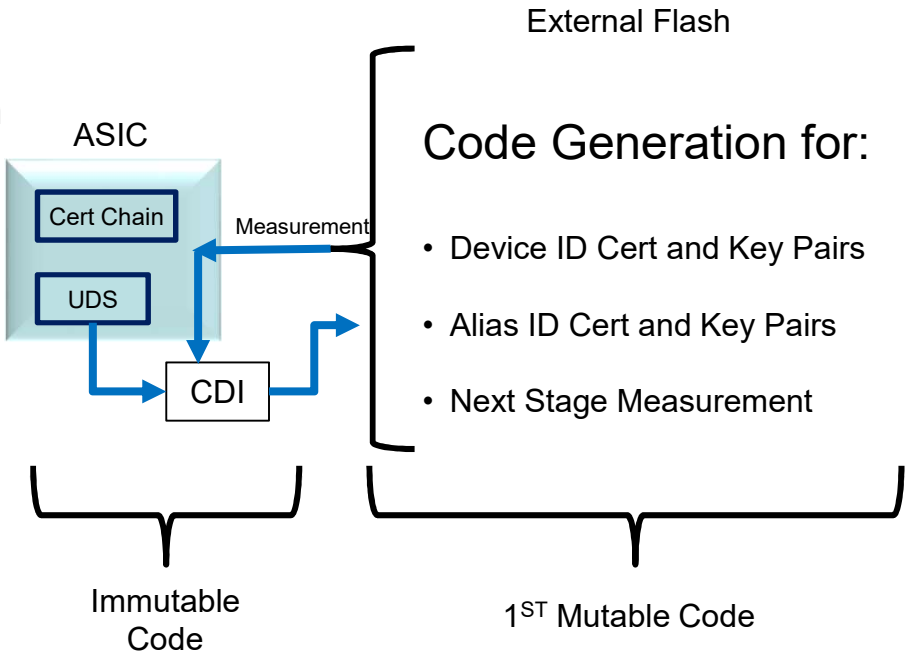


Manufacturing Identification and Authorization

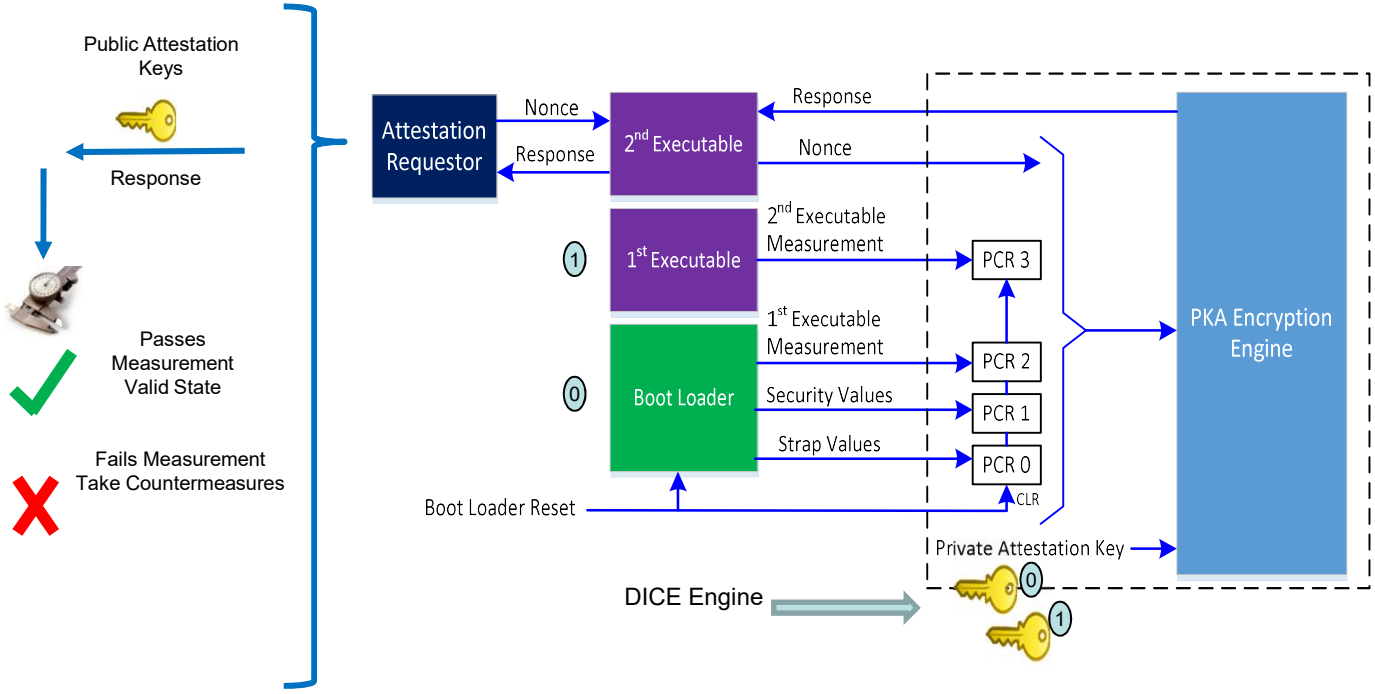


Chain of Trust from Device Identity

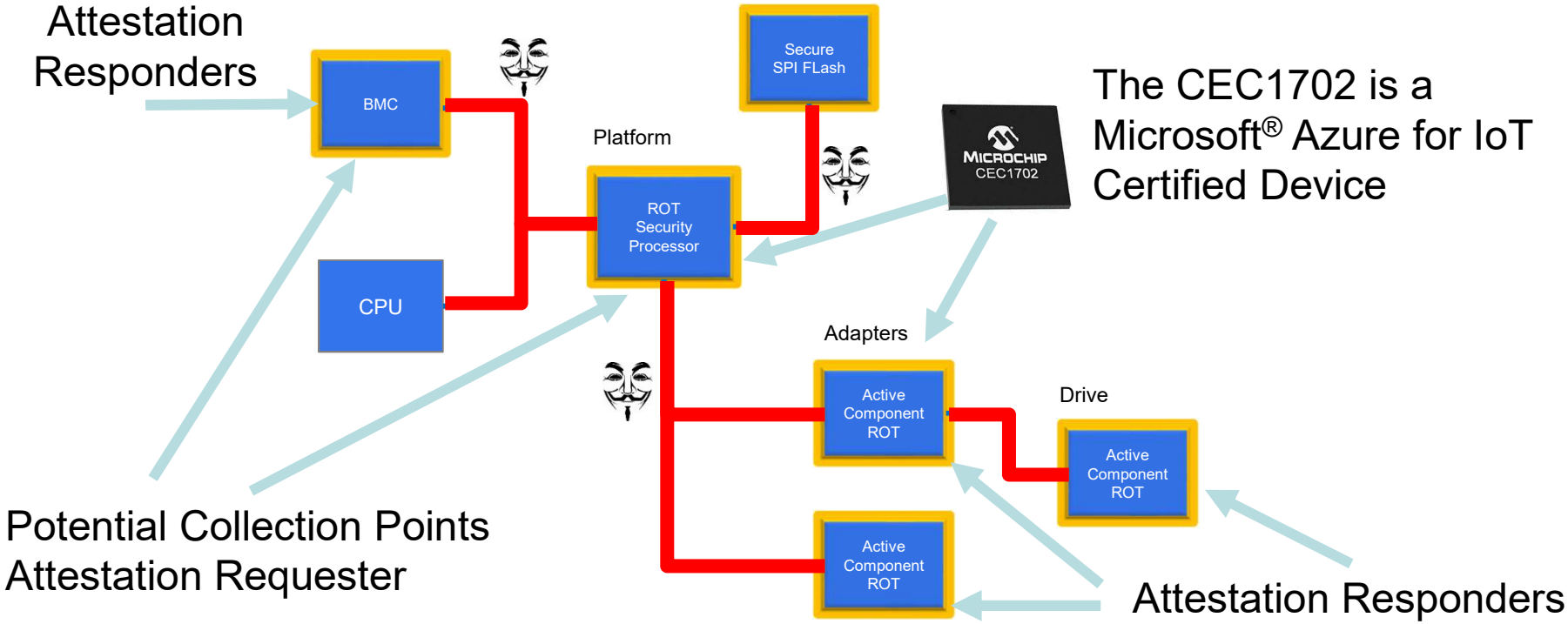
- **Depending on implementation ASIC security state is included in CDI**
  - New Keys, Revoked Keys, Rollback Counters
- **Updates to ASIC state or 1st mutable code can alter the CDI derived keys – desirable ?**
- **Device ID is meant to be enduring**
- **Certificates of the device ID are meant to be issued once (Slot 0)**
- **Factory issuance of 1st mutable code and security state of the device can never change**
- **Device authenticity relies on manufacturing issuance and CA verification**
- **Device keys are used to sign alias keys**
- **Alias keys are used to sign measurements**



How Do We Measure?



Who Measures?



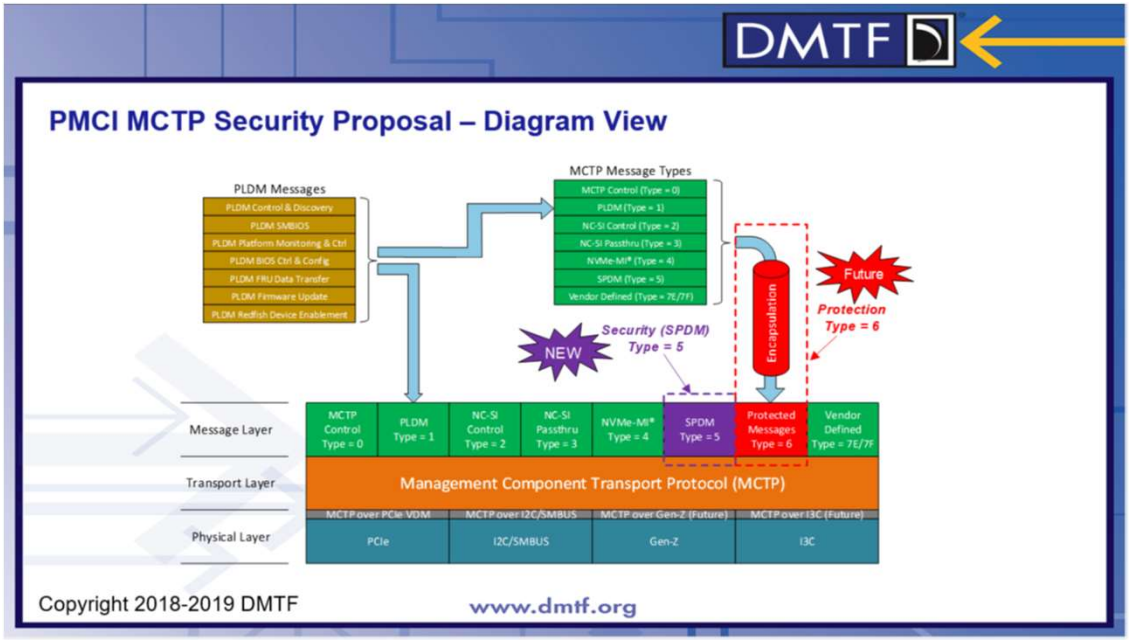
Problem Statements

While individual components can provide secure boot functions, measurement and authentication services, the question remains how to securely interact within a system, to collect and act on the acquired data.

- **How do measurements get brokered around the system?**
- **What mechanism protects against man in the middle or fraudulent measurements?**
- **How do the system components authenticate and provision certificates to establish trust?**
- **How does the communication remain confidential?**

DMTF Work in Progress

- Establishes a new MCTP message layer - type (5)
- Proposes a new additional type (6) for encrypting traffic once type 5 is established between devices
- Enables a variety of security features supported by the protocol and data models

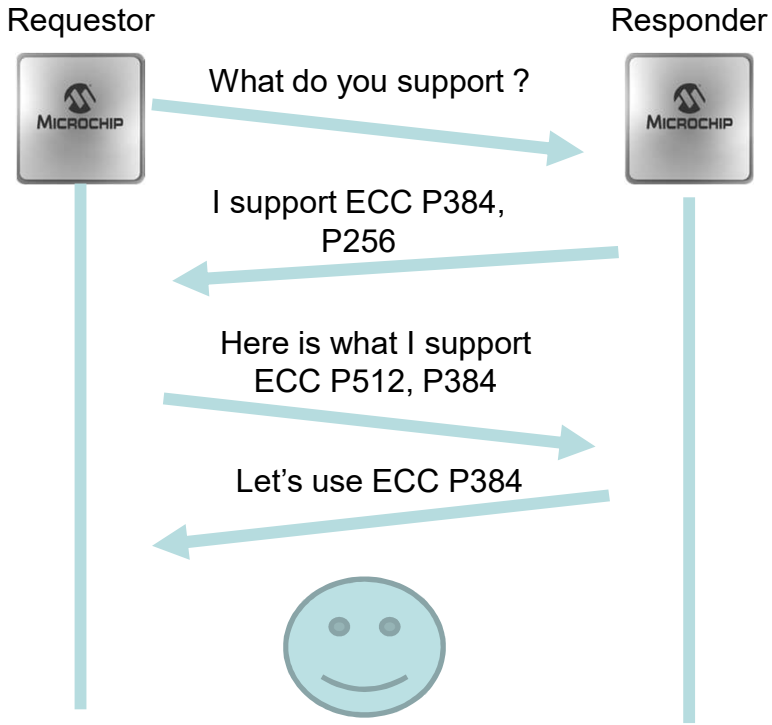


SPDM 1.0 Features

- **Enabling MCTP Type 5**
  - Version
  - Capabilities
  - Negotiate
  - Authenticate
    - Certificate Based
    - Challenge Response
  - Measurement Exchange

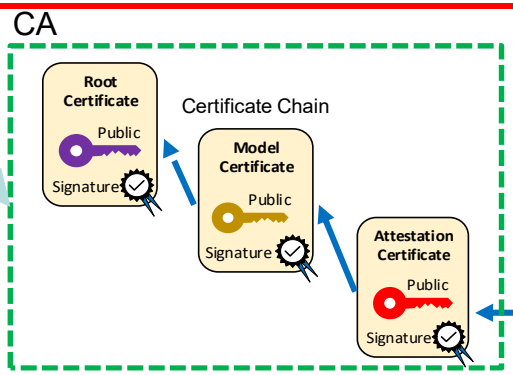
Capabilities Exchange and Negotiate

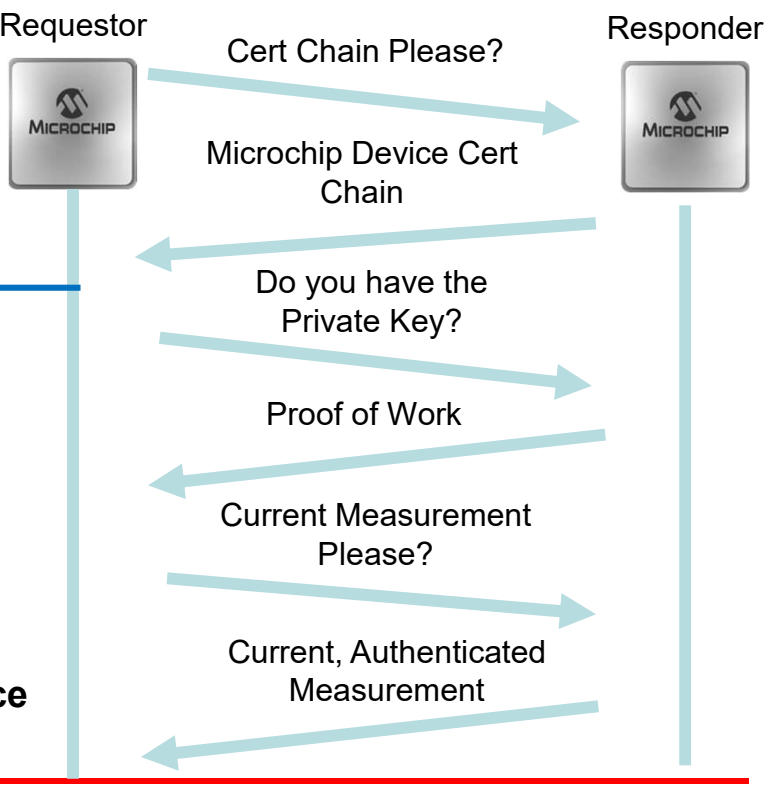
- End points have the ability to exchange cryptographic support
- Establish versions of algorithms willing to support
- Reach agreement , but also have the opportunity to reject at either endpoint
- Intention is to be flexible, and to place the decision making in the hands of the system designer.
- Example, if the use of a fan yields only measurement support and the system design allows, SPDM will support
- However, if an endpoint disallows, the process can stop



Authenticate and Measure

Outside the scope of SPDM 1.0 and implementation dependent





- **Requestor obtains the Responder's Certificate Chain**
- **Requestor can validate with CA or other mechanisms**
- **Requestor supplies content to determine Private Key possession by Responder**
- **Responder provides authenticated reply via proof of work**
- **Requestor confirms the responders work.**
- **Requestor can ask for a current measurement using a nonce**
- **Responder provides the current signed measurement**

System State Post 1.0 Completion and Observations

- Version compatibility will be established at the front end
- Agreed on methods to perform operations by the components
- Authenticated participants in the MCTP network i.e. verified the origin of the components
- Measured participants in the MCTP network i.e. the version and states of firmware and hardware would be known
- At any point, a requestor can “reject” a responder which is implementation dependent, ex. doesn’t support 1.x only 1.y
- System designers can implement flexible varying degrees of security depending on the profile required

SPDM 1.1 Preview Features

- **Provide confidentially to MCTP Communication via session keys**
- **Session Key Exchange Protocols Planned**
  - SIGMA option:
    - Based on ephemeral Diffie-Hellman
    - Digital signatures based
  - Pre-shared secret option
    - Based on a pre-shared secret known to both endpoints
    - Distribution of pre-shared secret is not a part of the SPDM
- **Capabilities and Negotiation apply to the session establishment**
- **Can be serve as a replacement for authentication steps as protocol for Key Establishment contains those security steps**

DMTF Security Task Force

- **DMTF continues its work on the protocol for authentication and measurement exchange between components in a system in support of attestation**
- **The taskforce link is below**
- **The exchange protocol has reached WIP release state targeted for pre-1.0 for DSP0274 and DSP0275**
- **Preview of WIP for 1.1 is also available**

https://www.dmtf.org/content/get-involved-dmtfs-pmci-security-task-force

https://www.dmtf.org/content/dmtf-releases-security-protocol-and-data-model-spdm-architecture-work-progress

https://www.dmtf.org/sites/default/files/PMCI_Security-SPDM_1.1_Preview_WIP_1.pdf

https://www.dmtf.org/content/dmtf-shares-plans-session-keys-spdm-11

Observations

- Provisioning of certificates at the endpoints is not resolved
- CA verification is not resolved
- The methods and security of the responder must still be scrutinized independently. i.e., use of DICE and RIOT are not enforced by the exchange protocol
- Does not inherently detect clones or other security concerns
- Protocol is designed to be flexible and allow many methods of confirmation and capabilities per design
- Intel® PCIe® Secure Device Proposals suggest supporting authentication, measurement and lane encryption for all PCIe attached devices
- MCTP Network comes up “late” in system start but can have important uses cases where PCIe alone can not satisfy, i.e. i2c or downstream device support
- However there is overlap

Thank You