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 Distributed Management Task Force (DMTF) website.
Goals

• Create specification(s) to provide security for PMCI standards and protocols.
  • Prefer specification that targets the transport layer.
  • MCTP, NC-SI, PLDM, Redfish Device Enablement, Firmware Update, Monitoring and Control, NVMe-MI™ Binding, etc…
  • www.dmtf.org/standards/PMCI
• Specification should be implementable on existing hardware designs.
  • Do not require changes to existing hardware/silicon.
• Referenceable by other industry standards organizations.
  • Examples: Security Project of Open Compute Project (OCP), PCI-SIG, Open Data Center Committee (ODCC), etc…
• Rapid Publication of Standard
  • Detail Architecture Release: October 2018
  • 0.9 Work-in-Progress Release: December 2018
  • Official 1.0 Release: Q1 2019

www.dmtf.org
Requirement Categories

- Functional
- Trust
- Data Protection
- Cryptography
- Out of Scope
- Future Considerations
Functional Requirements

• Endpoint Authentication, Data Confidentiality and Integrity.
  • Security protocol(s) are endpoint-to-endpoint.

• Support Wide Ecosystem
  • Allow resource constrained environments (i.e. low CPU and memory requirements) to choose basic security measures.
  • Allow resource-rich environments to choose stronger security measures.

• Support Layered Security
  • Ensure compatible security methods across layers of PMCI standards and protocols.
  • Should compliment security defined at other layers (i.e. such as the physical layer)

• Interoperable
  • Specify minimal set of capabilities and operations.
  • Define mechanism for protocol endpoints to choose security parameters.
Trust Requirements

- Allows Trust to be determined.
  - When requested, endpoint must provide identity.
  - Support for X.509 certificate
  - Does not exclude other forms of identity.
- Authentication Protocol based on existing art.
  - Example: USB-C authentication
- Define mechanism for passing firmware measurements.
Data Protection Requirements

- Use CIA Triad (Confidentiality, Integrity and Availability) as model for data protection
  - Perform a threat analysis/threat model.
- Allow design/implementation to dynamically choose which data to protect
- Define mechanism for Encryption and Integrity
Cryptography Requirements

• Use Standards (i.e. NIST, FIPS, RFCs, etc…)
  • Use list of algorithms in NIST-SP-800-131A revision 1 (published 2015)
  • Specify a set of cryptography algorithms to balance interoperability and design flexibility.
  • Potentially reference NIST.IR.8105.
  • Don’t invent or use outside of intended design/purpose

• Extensibility
  • Specification must be able to accommodate GEO compliance and support for future algorithms.
Out of Scope for Specification

- How identity and keys are initially provisioned.
- How firmware measurements are performed.
- PMCI Host Interface access to devices
- Security Policies
  - Specification will specify some mechanisms for implementing security policies but will not define those policies.
- Root-of-Trust (RoT)
  - Specification allows for RoT but will neither define nor require a RoT.
Future Considerations (i.e. Post 1.0 release)

• Authorization
  • How does an endpoint determine the remote endpoint has sufficient privilege to perform a specific PMCI operation?

• Identity Lifecycle Management (e.g. Certificate)
  • Do we define a new MCTP ID codes/operations?
  • Or Leverage RDE?
  • Do we do a new PLDM type?
  • What part of the lifecycle needs to be addressed?

• Any PMCI standards and protocols not encompassed in release 1.0.