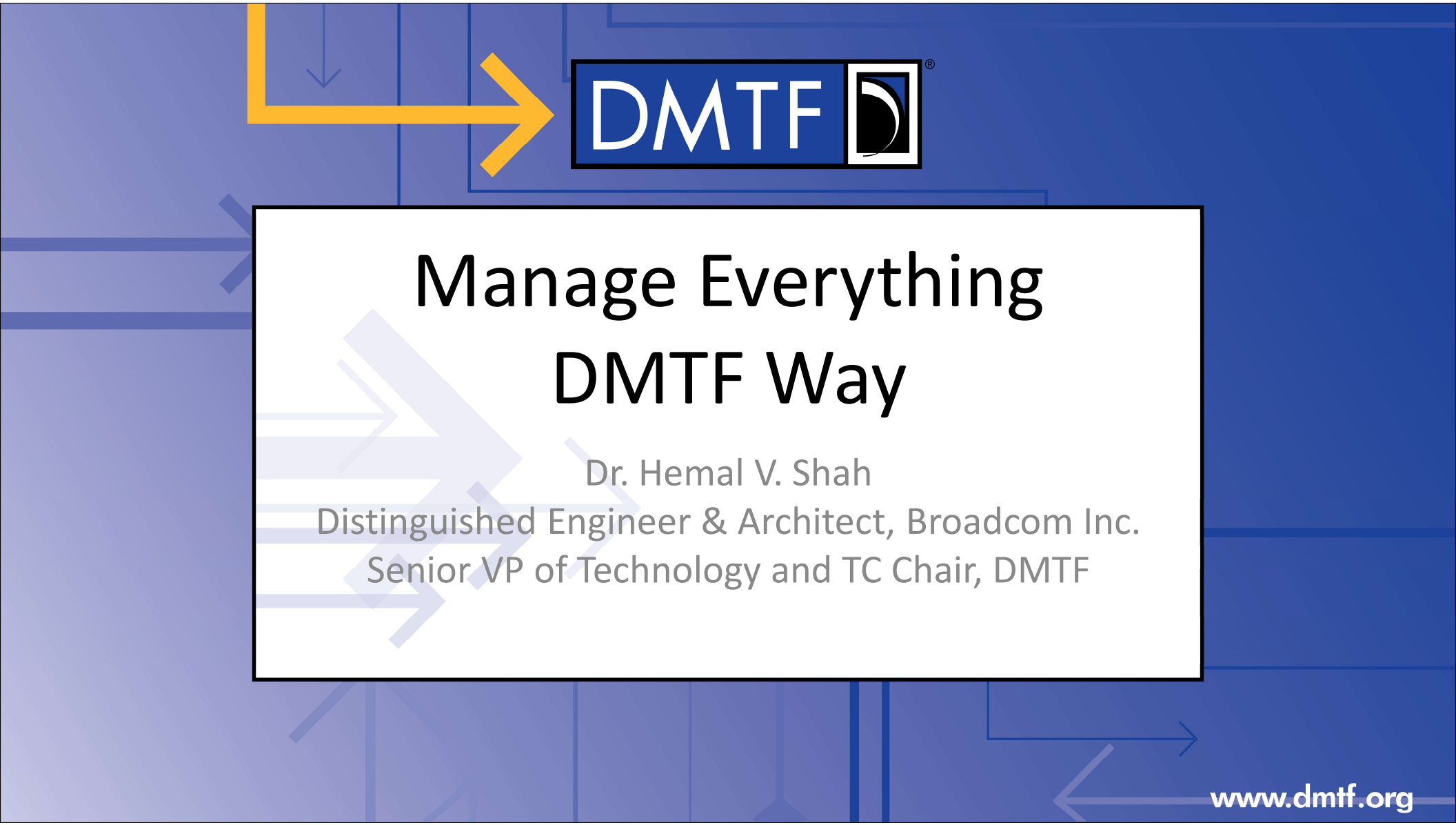

DMTF
Manage Everything
DMTF Way
Dr. Hemal V. Shah
Distinguished Engineer & Architect, Broadcom Inc.
Senior VP of Technology and TC Chair, DMTF
www.dmtf.org

Disclaimers

- Please note this keynote is being recorded
- Recording will be available to the public

Agenda

- DMTF Overview
- DMTF Evolution
- DMTF Technologies
- Redfish Overview
- PMCI Overview
- SPDM Overview

DMTF – An Industry Standards Org

WHO Led by innovative, industry-leading companies, DMTF has a global presence with members in multiple countries.

WHAT DMTF standards support diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. A complete list is available at **www.dmtf.org/standards.**

WHY Nationally and internationally recognized by ANSI and ISO, DMTF standards enable a **more integrated and cost-effective approach to management through interoperable solutions.**

HOW Simultaneous development of Open Source and Open Standards is made possible by DMTF, which has the support, tools and infrastructure for efficient development and collaboration.

DMTF Board Member Companies

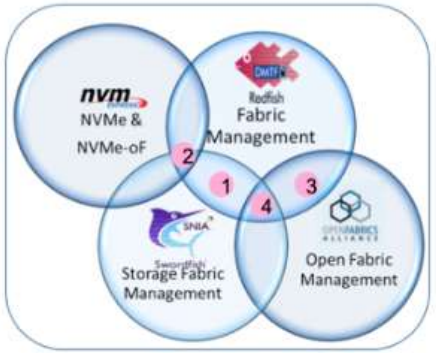
DMTF Alliance Partners (23)

Redfish

Cloud/CIM

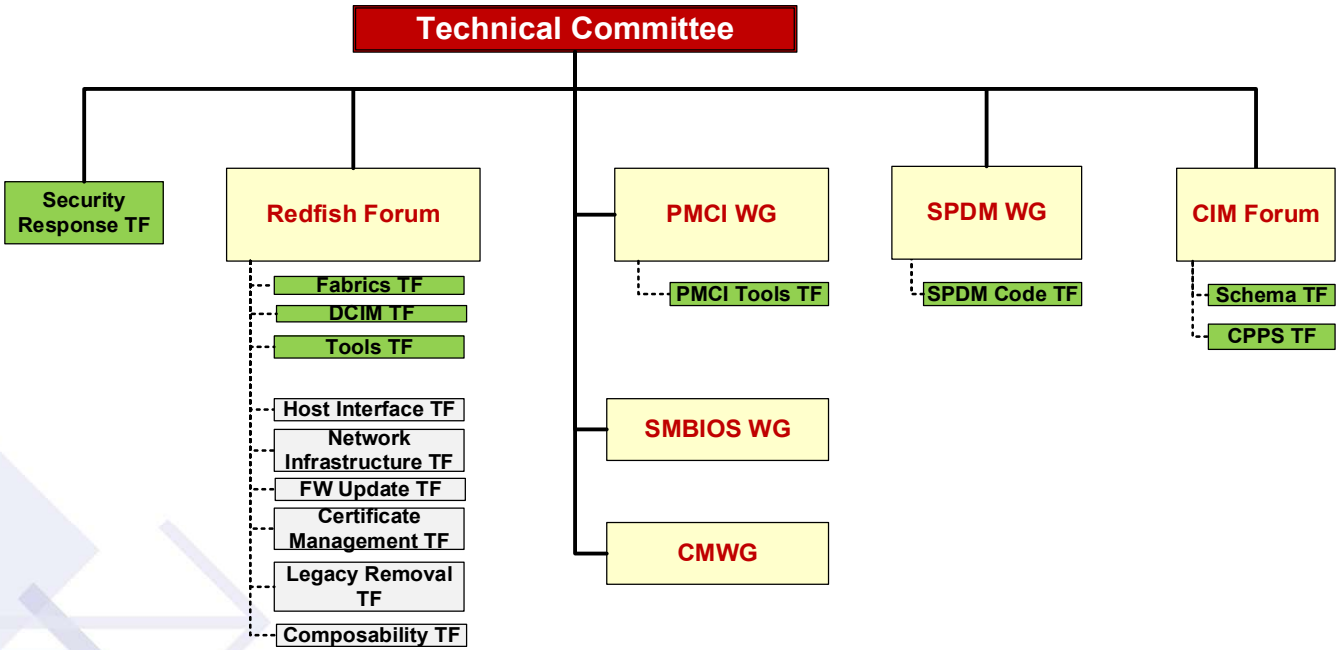
SPDM

MCTP/PLDM



https://www.dmtf.org/about/registers

DMTF TC Organization



CIM – Common Information Model
CMWG – Cloud Management Working Group
CPPS – CIM Profiles for Platforms and Services
DCIM – Data Center Infrastructure Management
PMCI – Platform Management Communications Infrastructure
SPDM – Security Protocol Data Model

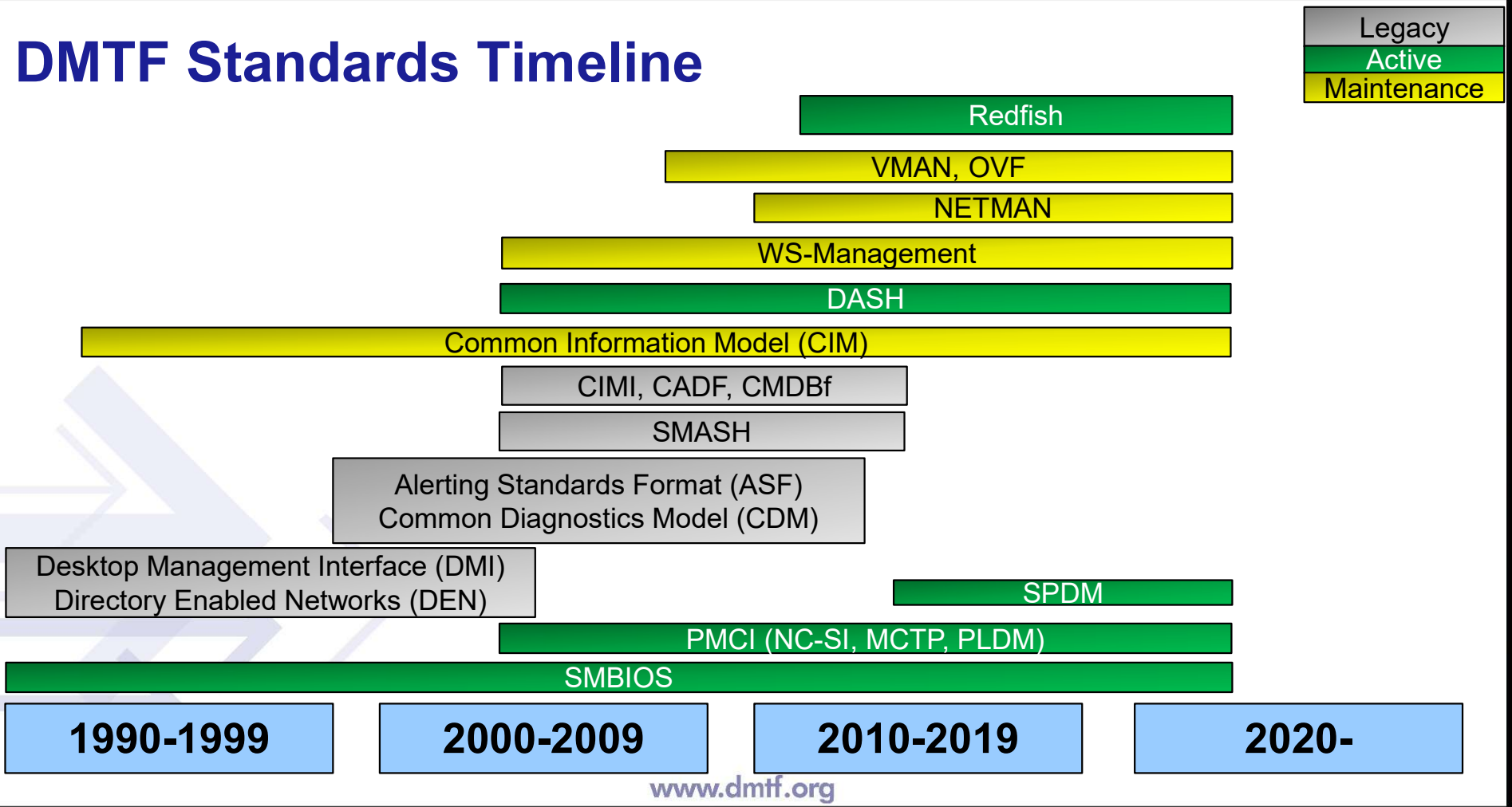
Legend

- Active WG or Forum
- Active TF
- Inactive TF

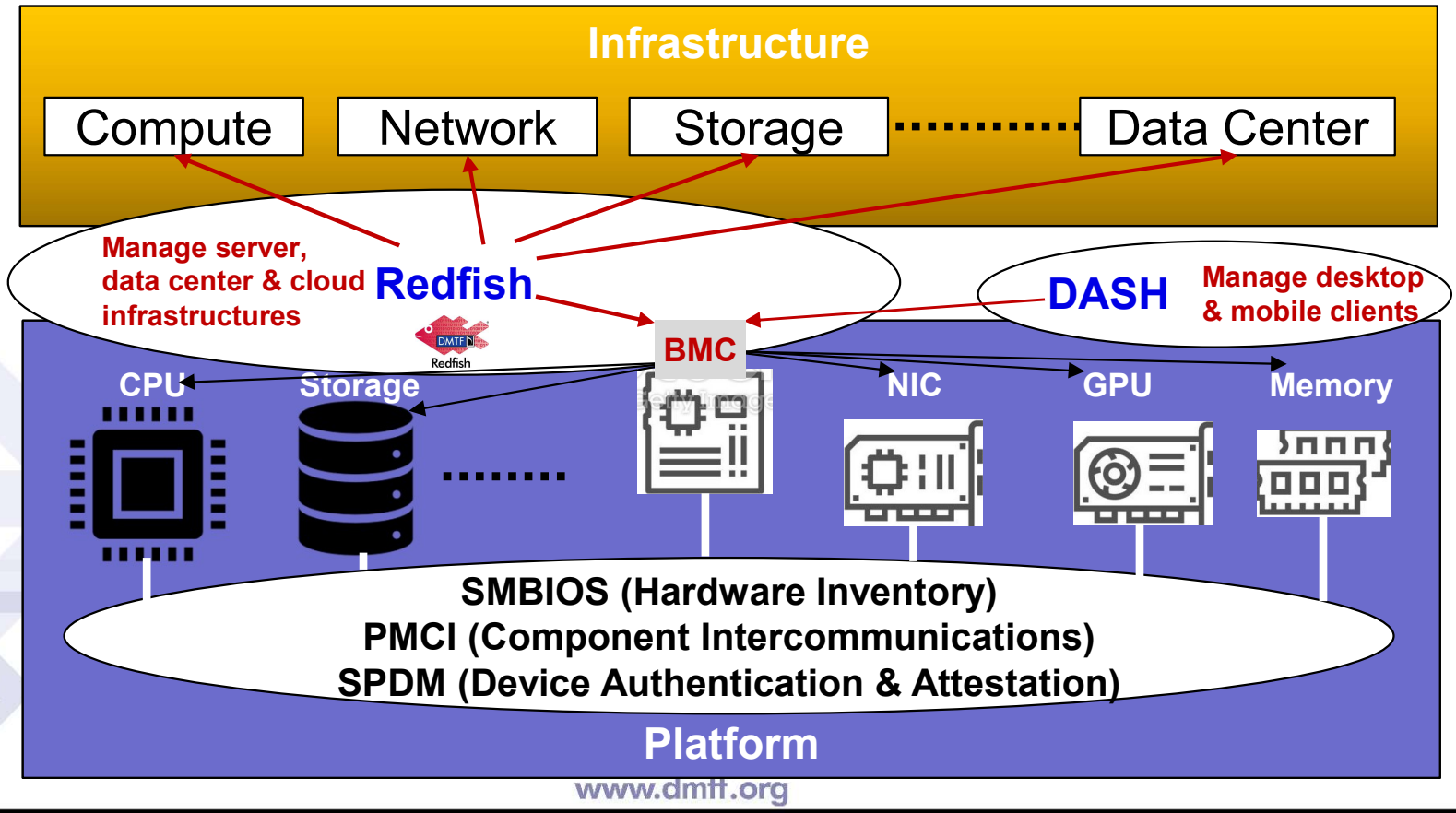
Technical Committee Accomplishments in 2022

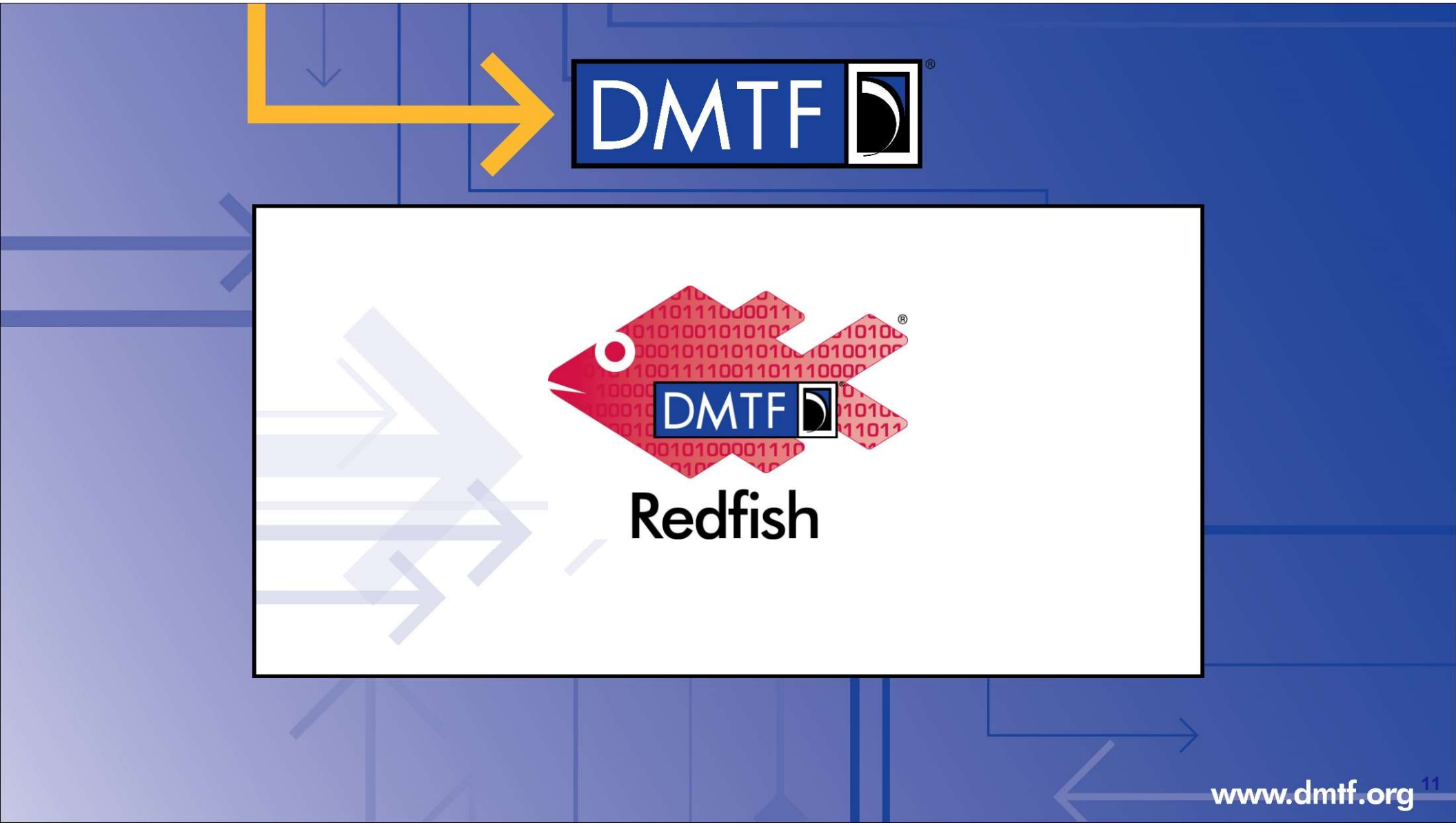
- Continued wide acceptance of DMTF standards in industry, Examples:
  - 2 Billion+ platforms with SMBIOS implementation
  - 340+ certified products in DASH conformance registry
  - Continued traction with Redfish adoption and continuing interest in PMCI and SPDM standards
- Increased adoption of DMTF standards in open source, Examples:
  - OpenBMC https://github.com/openbmc
  - Redfish validators, tools, checkers, etc.: https://github.com/DMTF
  - Open Linux Management Infrastructure (OpenLMI) & Open Management Interface (OMI)
- Expansion of scope continues in the DMTF
  - Redfish expansion into DCIM, Network Infrastructure, OpenAPI...
  - Security Protocol Data Model (SPDM) WG now its own body under the TC
  - The Cloud Management Working Group spun up
  - Security Response Task Force created
- 70 standards and white papers and 15 work-in-progress published in 2022
- International acceptance of DMTF standards via ISO and ANSI adoption
  - **8 ISO** standards published and 4 currently in the submission process
  - 10 published **ANSI standards**

DMTF Standards Timeline

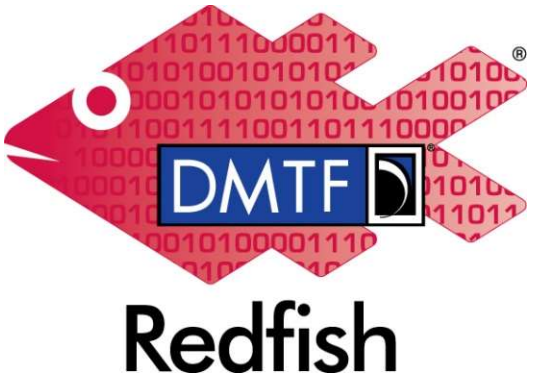


DMTF Technologies



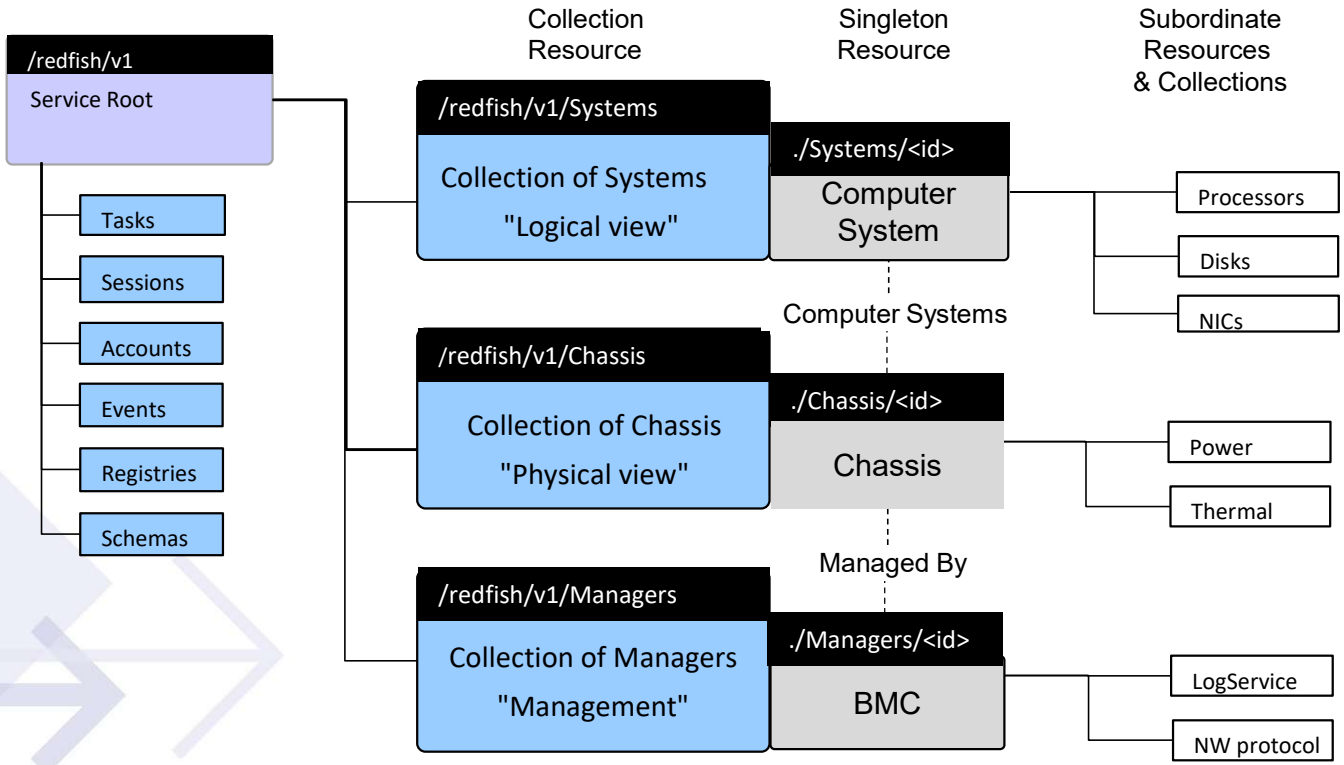

DMTF
DMTF
Redfish

What is Redfish?



- **Industry Standard Software Defined Management for Converged, Hybrid IT**
  - HTTPS in JSON format
  - Schema-backed but human-readable
  - Equally usable by Apps, GUIs and Scripts
  - Extensible, Secure, Interoperable
- **Initial release in 2015 focused on Servers**
  - A secure, multi-node capable replacement for IPMI-over-LAN
  - Represent full server category: Rackmount, Blades, HPC, Racks, Future
  - Intended to meet OCP Remote Machine Management requirement
- **Expanded scope since then to the rest of IT infrastructure**
  - Worked with SNIA to cover more advanced Storage (Swordfish)
  - Worked with OCP, The Green Grid & ASHRAE to cover Facilities (DCIM)
  - Adopted YANG & other models to cover Ethernet Switching
  - Working with CXL & OpenFabrics & others to cover Fabrics
  - Additional features coming out approximately every 4 months

Redfish Resource Map (simplified)



GET http://<ip-addr>/redfish/v1/Systems/{id}/Processors/{id}

Use the Redfish Resource Explorer (redfish.dmtf.org) to explore the resource map

Interoperability Profiles

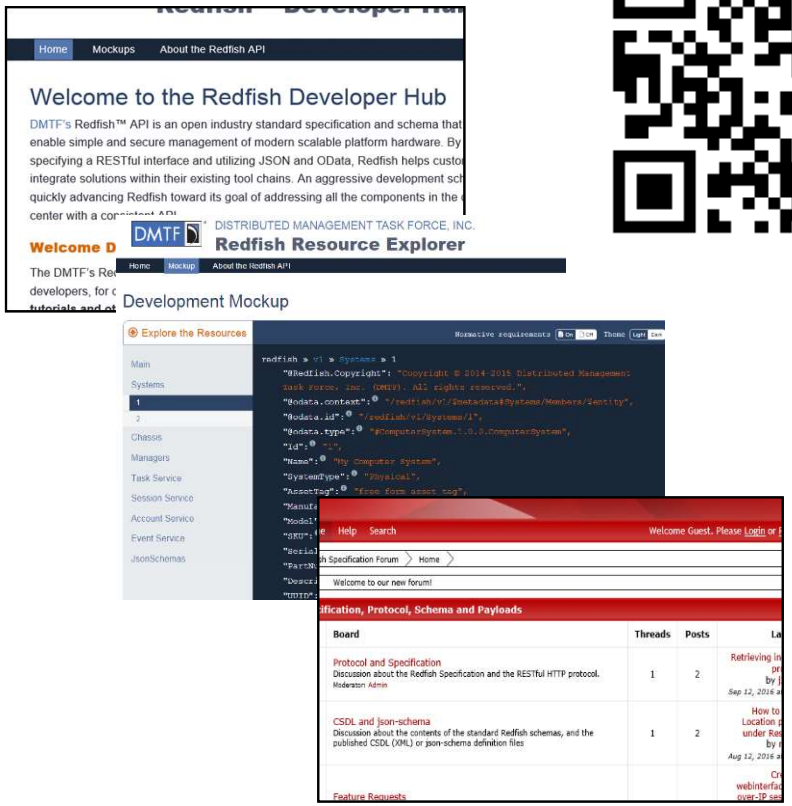
- An “Interoperability Profile” provides a common ground for Service implementers, client software developers, and users
  - A profile would apply to a particular category or class of product (e.g. “Front-end web server”, “NAS”, “Enterprise-class database server”)
  - It specifies Redfish implementation requirements, but **is not** intended to mandate underlying hardware/software features of a product
  - Provides a target for implementers to meet customer requirements
  - Provide baseline expectations for client software developers utilizing Redfish
  - Enable customers to easily specify Redfish functionality / conformance in RFQs
- A machine-readable Profile definition
  - Document must be human-readable
  - Can be created by DevOps personnel and non-CS professionals
- Enable authoring of Profiles by DMTF, partner organizations, and others
  - OCP, OpenStack, and OPAF published profiles for their management domains
- Open-source interop validator developed by the DMTF to test for profile conformance

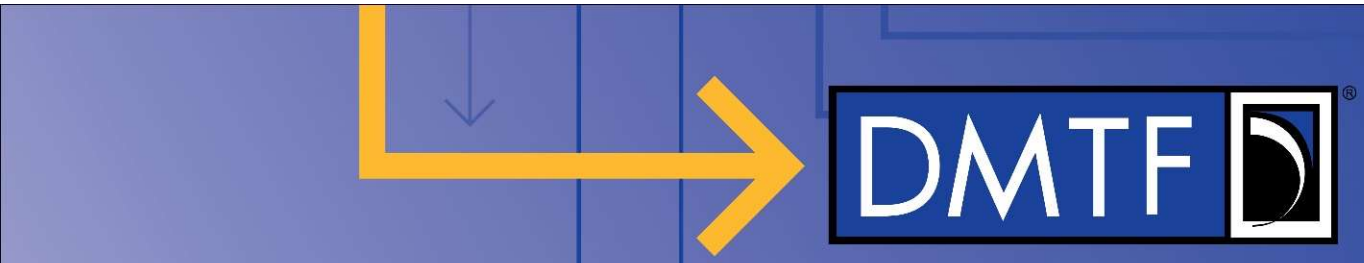
A few of the Open-Source Efforts around Redfish

- DMTF - a suite of validation software, conformance and client tools
- Open Compute Project (OCP) – rack manager & software agent
- Linux Foundation OpenBMC and ODIM projects
- Vertical integrations – OpenStack, Ansible, Puppet
- SNIA Swordfish tools
- Many companies have open-source tools

Redfish Developer Hub: redfish.dmtf.org

- Resources
  - Schema Index
  - Specifications
  - GitHub for Redfish Tools
  - Registries
  - Other Documentation
- Mockups
  - Simple Rack-mounted Server
  - Bladed System
  - Proposed OCP Redfish Profile
  - More being added
- Education/Community
  - Redfish User Forum
  - Whitepapers, Presentations
  - YouTube shorts & Webinars





PMCI

Platform Management Communication Infrastructure

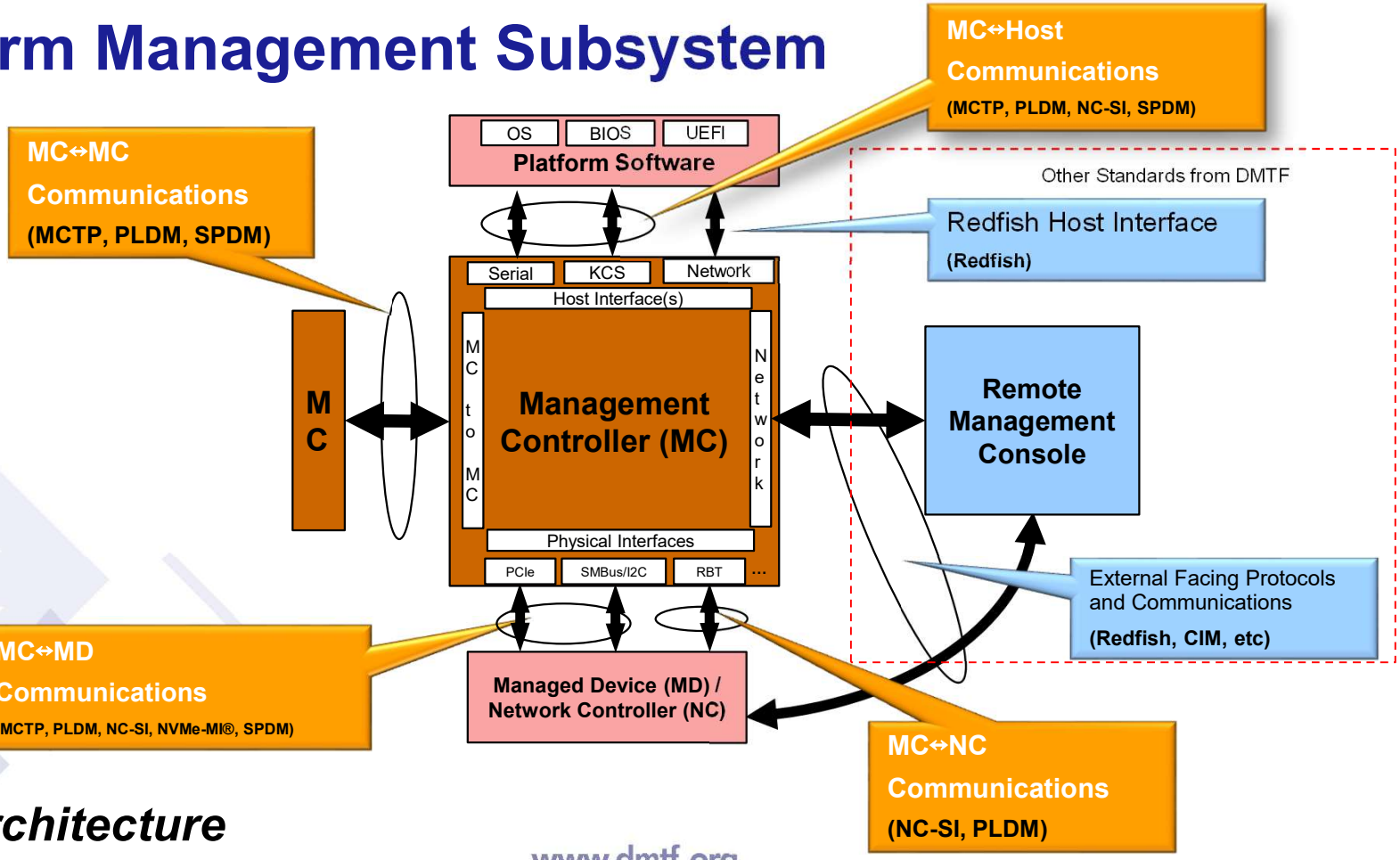
(Was Platform Management Components Intercommunication)

PMCI Working Group

- Platform Management Communications Infrastructure
- PMCI suite of standards provide ‘inside-the-box’ communication and function interfaces between components within the platform management subsystem
  - Management Controller (MC) to Management Controller
  - Management Controller to Network Device (NC)
  - Management Controller to Managed Device (MD)
  - Host Interface to Management Controller
- Formed in 2005, initial standards released in 2007
  - Creates specifications for MCTP, PLDM, and NC-SI
    - PLDM Sensor, FW Update, RDE all done here
    - As are the mapping specs for PCIe, CXL, I2C, I3C, USB, KCS.
- Over a decade of implementations within server and desktops

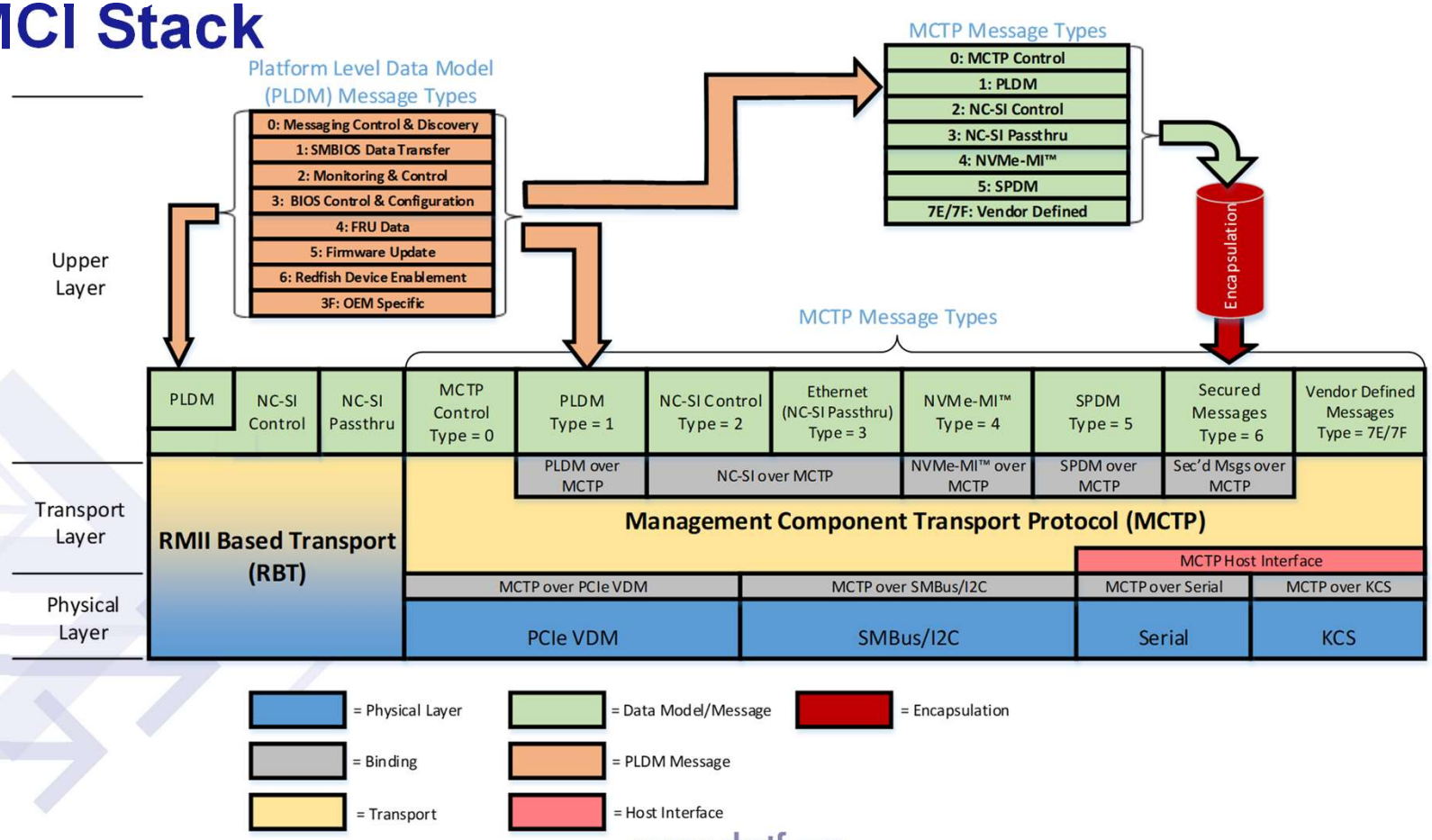
PMCI technologies and interfaces are complementary and enable DMTF external facing data models/remote management protocols

Platform Management Subsystem



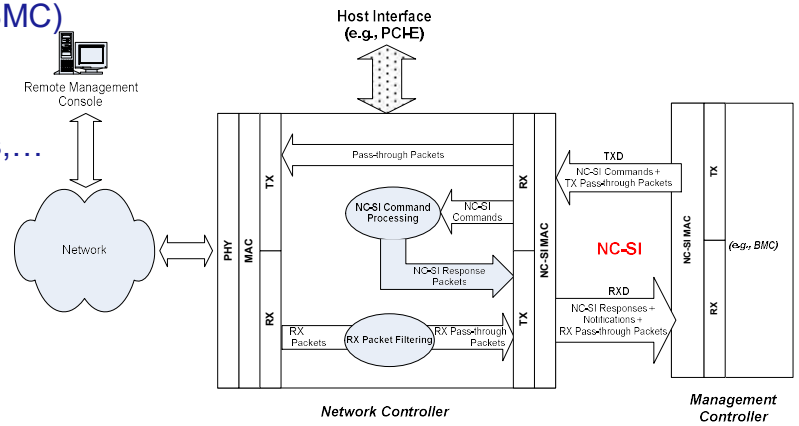
PMCI Architecture

PMCI Stack


Platform Level Data Model (PLDM) Message Types
0: Messaging Control & Discovery
1: SMBIOS Data Transfer
2: Monitoring & Control
3: BIOS Control & Configuration
4: FRU Data
5: Firmware Update
6: Redfish Device Enablement
3F: OEM Specific
MCTP Message Types
0: MCTP Control
1: PLDM
2: NC-SI Control
3: NC-SI Passthru
4: NVMe-MI™
5: SPDM
7E/7F: Vendor Defined
Encapsulation
MCTP Message Types
Upper Layer
PLDM
NC-SI Control
NC-SI Passthru
MCTP Control Type = 0
PLDM Type = 1
NC-SI Control Type = 2
Ethernet (NC-SI Passthru) Type = 3
NVMe-MI™ Type = 4
SPDM Type = 5
Secured Messages Type = 6
Vendor Defined Messages Type = 7E/7F
PLDM over MCTP
NC-SI over MCTP
NVMe-MI™ over MCTP
SPDM over MCTP
Sec'd Msgs over MCTP
Transport Layer
RMII Based Transport (RBT)
Management Component Transport Protocol (MCTP)
MCTP Host Interface
Physical Layer
MCTP over PCIe VDM
MCTP over SMBus/I2C
MCTP over Serial
MCTP over KCS
PCIe VDM
SMBus/I2C
Serial
KCS
= Physical Layer
= Data Model/Message
= Encapsulation
= Binding
= PLDM Message
= Transport
= Host Interface

Network Controller Sideband Interface (NC-SI)

- A common interoperable sideband interface and protocol to transfer management traffic between a Baseboard Management Controller (BMC) & network controller (NC)
- Supports Multiple Types of Management Traffic
  - Pass-Thru Management Traffic enables BMC-Network communication via NC
  - NC-SI Command/Response Packets
    - Command (Response) sent by BMC (NC) to NC (BMC)
    - Request/Response Semantics
    - Functions: Control, Configuration, Status, Statistics,…
  - NC-SI Notification Packets
    - Generated and sent by NC to MC
    - Functions: OS/Link Status Change; NC Soft Reset



Management Component Transport Protocol (MCTP)

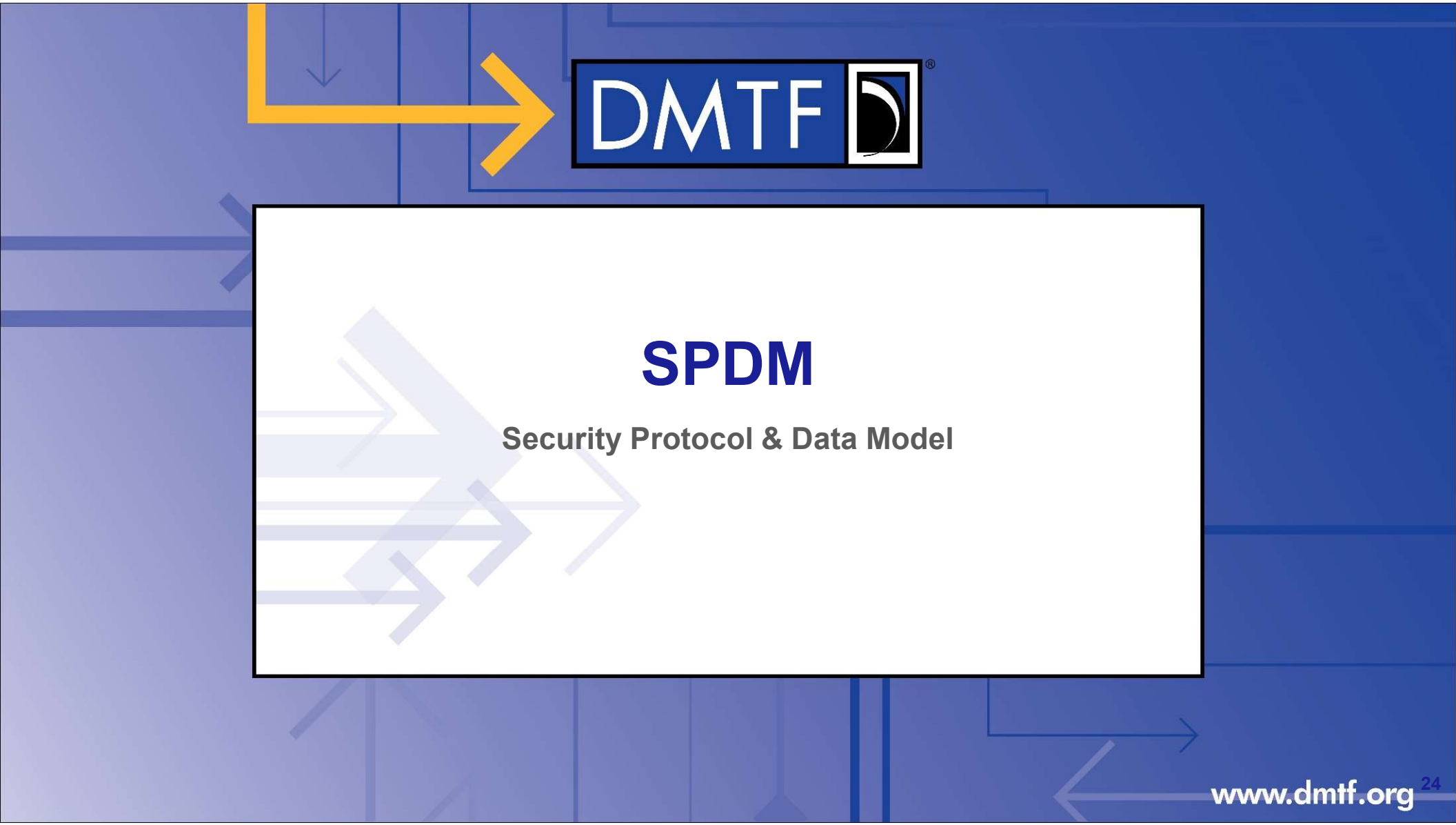
- Base transport for “inside-the-box” communication.
- Suitable for use with multiple media: SMBus/I2C, I3C, PCIe, CXL, etc.
- Suitable for all computer platform types
- Supports logical addressing based on Endpoint IDs
- Provides simple message fragmentation/reassembly
- Built-in capability discovery and supports path transmission unit discovery
- Carries multiple message types: MCTP Ctrl, PLDM, NC-SI, NVMe, SPDM, CXL

MCTP for platform communications ~ TCP/IP for Internet comm

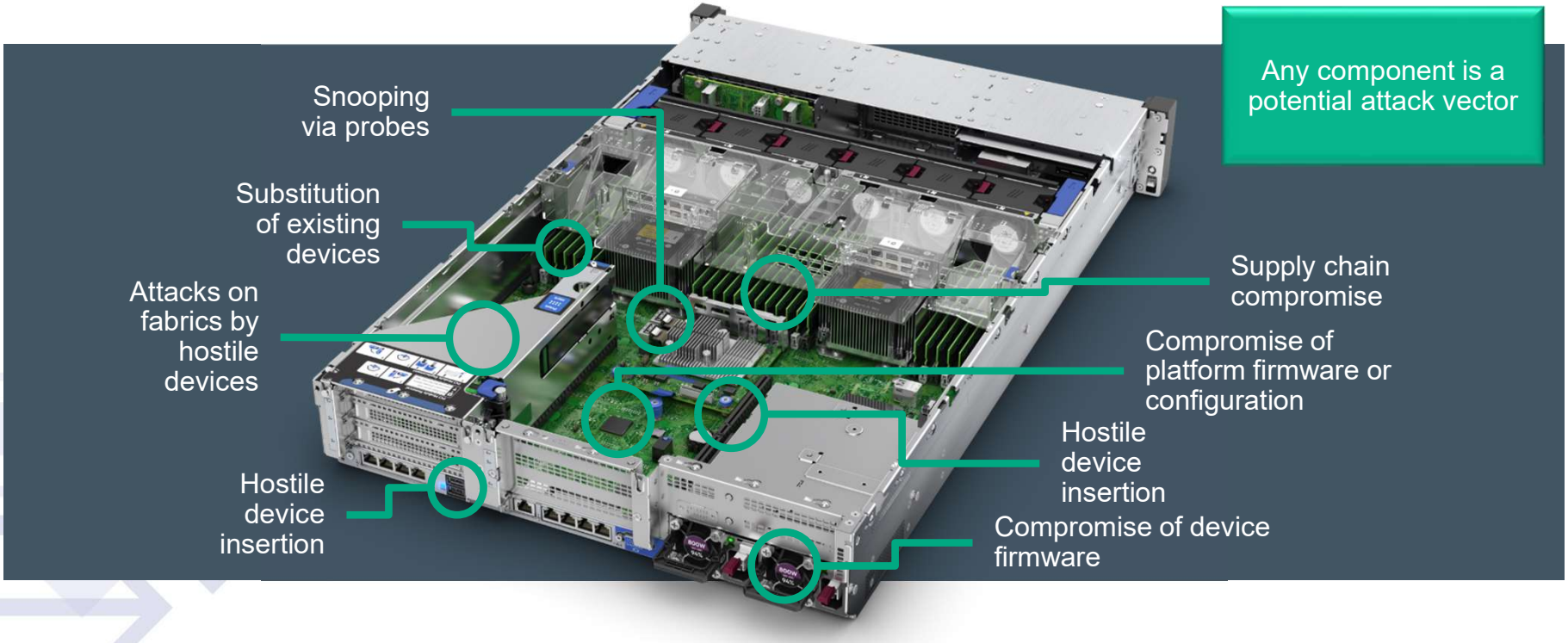
Platform Level Data Model (PLDM)

- An effective interface & data model for efficient access to
  - Low-level platform inventory, BIOS, and config data
  - Platform monitoring/control, alerting, event log, FRU, etc.
  - Firmware Update, Redfish Device Enablement (RDE), File Transfer (future)
- Defines low level data representations and commands
- Provides transport independent Request/Response Model
- Supports a subtype to distinguish types of PLDM Messages
  - Allows messages to be grouped based on the functions
  - Allows the discovery of the functionality supported

PLDM for platform components communications ~ L5-L7 layers of Internet


DMTF
SPDM
Security Protocol & Data Model

Component Security: The Foundation for Zero-Trust



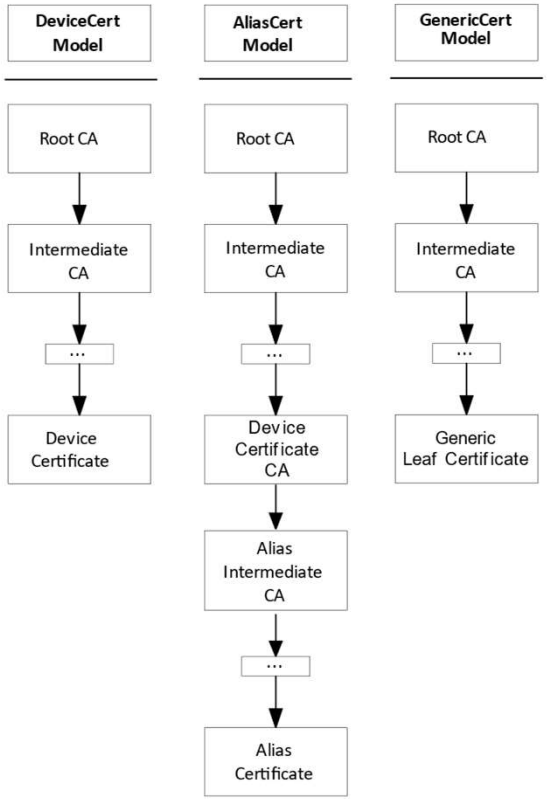
SPDM's Overall Goals

- All SPDM features fall into at least one of these main goals:
  - Device Attestation and Authentication
  - Secure Communication over any transport
- Device Attestation and Authentication
  - Attest aspects of a device such as firmware integrity & device identity
- Secure Communication over any Transport
  - Secure communication of any management traffic over any transport
  - Work with industry partners to ensure data in-flight is secure for all parts of the infrastructure (e.g. storage, network fabrics, etc.)

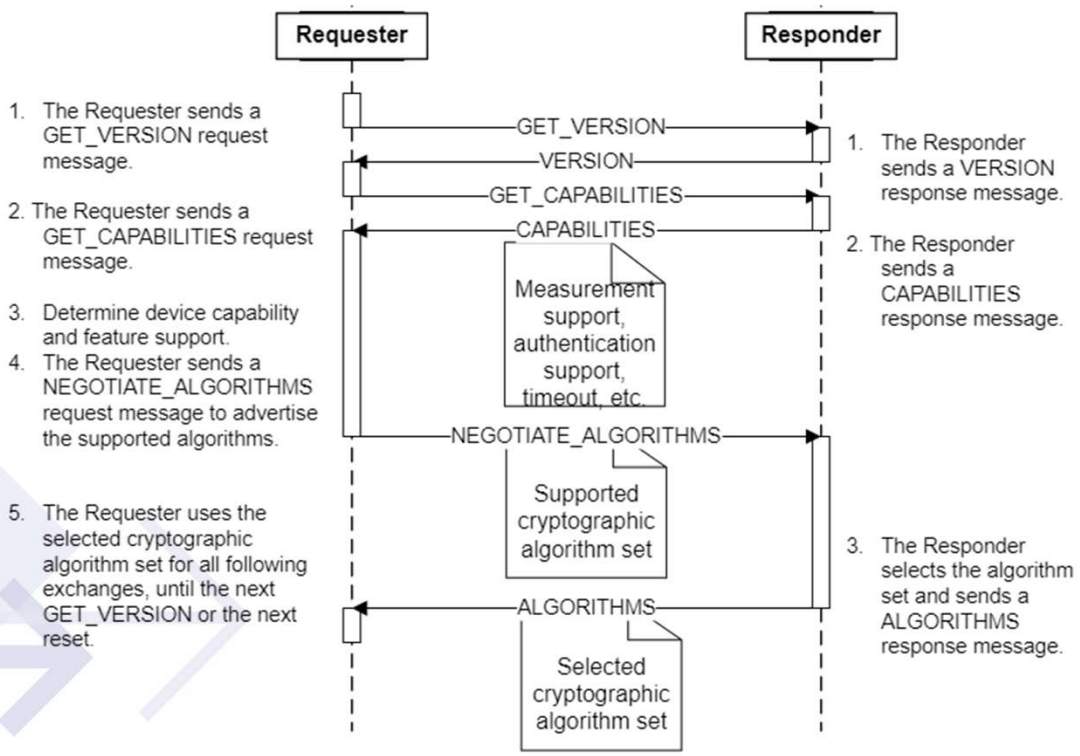
SPDM Feature Summary

- Version 1.0:
  - Measurement Support
  - Device Attestation and Authentication
- Version 1.1:
  - Secure Session
    - Public Key Exchange
    - Symmetric Key Exchange
  - Mutual Authentication
- Version 1.2:
  - Supports installation of certificates
  - Allows for alias certificates derived from device certificates
  - Send and receive large SPDM messages (chunks)
- Version 1.3:
  - Eventing Mechanism
  - Multiple Keys support
  - Measurement Enhancements
  - Miscellaneous

SPDM Certificate Models

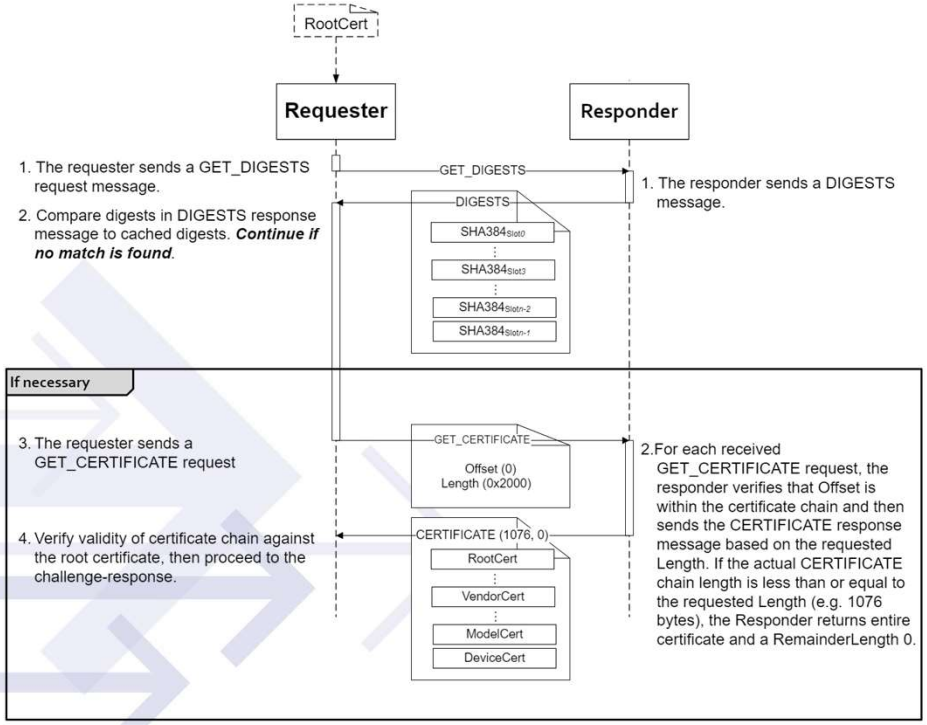


SPDM Discovery and Negotiation

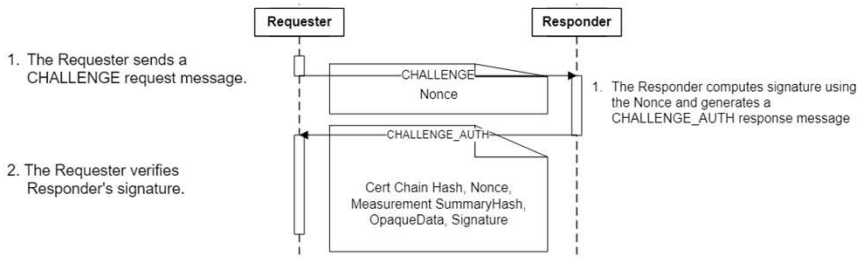


SPDM Endpoint Authentication

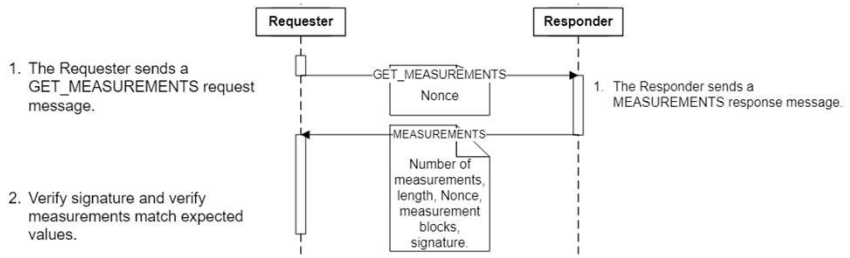
Certificate Retrieval



Challenge/Response



Firmware Measurement Retrieval



Summary

- DMTF standards for managing HW & infrastructures
- DMTF continues to evolve to meet industry needs
- Redfish – de jure standard for IT, server, cloud, and data center infrastructure management
- PMCI – for components comm inside the platform
- SPDM – for device auth, attestation & encrypted comm

Q & A