SPDM Over TCP Binding

Eduardo Cabre, Principal Engineer, Intel
Xiaoyu Ruan, Senior Principal Engineer, Intel
October 15, 2024

Why SPDM

- The *de facto* security protocol for embedded modules. Widely deployed in the industry since its inception in 2019.
- Comprehensive and versatile functionalities
  - Authentication
  - Attestation / measurements
  - Secure session
  - …and growing
- Similar, but different from TLS
  - Lighter weight
  - Dedicated request/response defined for specific use cases, such as attestation
  - Live protocol - new functions added over time
- Runs on various transports defined by individual binding specifications: MCTP, PCIe, CXL, TCP…

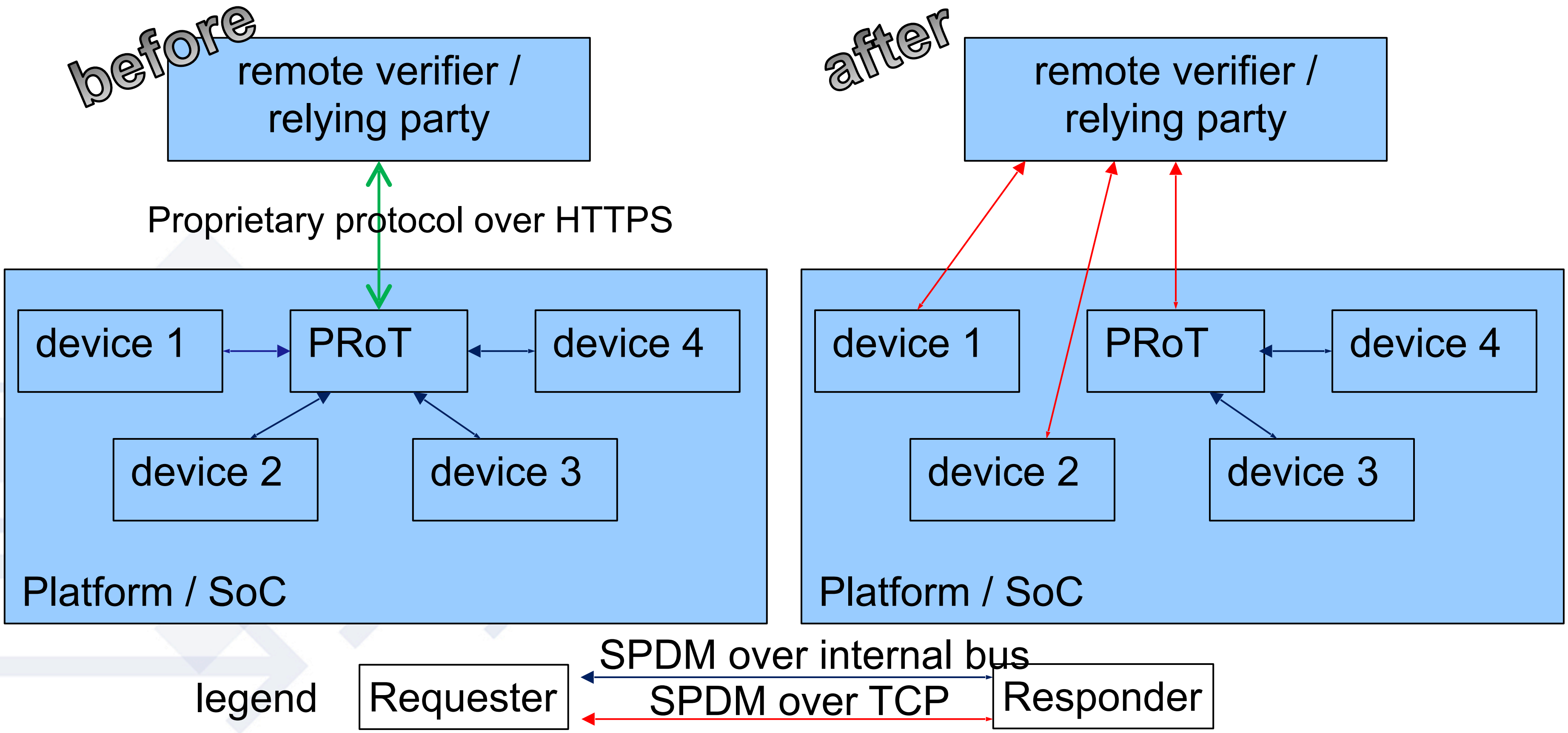
Why SPDM over TCP

- Increasing need for secure communication between an embedded module and a software or service module running on fabric, host, or off-machine (backend), for various use cases.

- Version 1.0.0 published July 2024 https://www.dmtf.org/sites/default/files/standards/documents/DSP0287_1.0.0.pdf

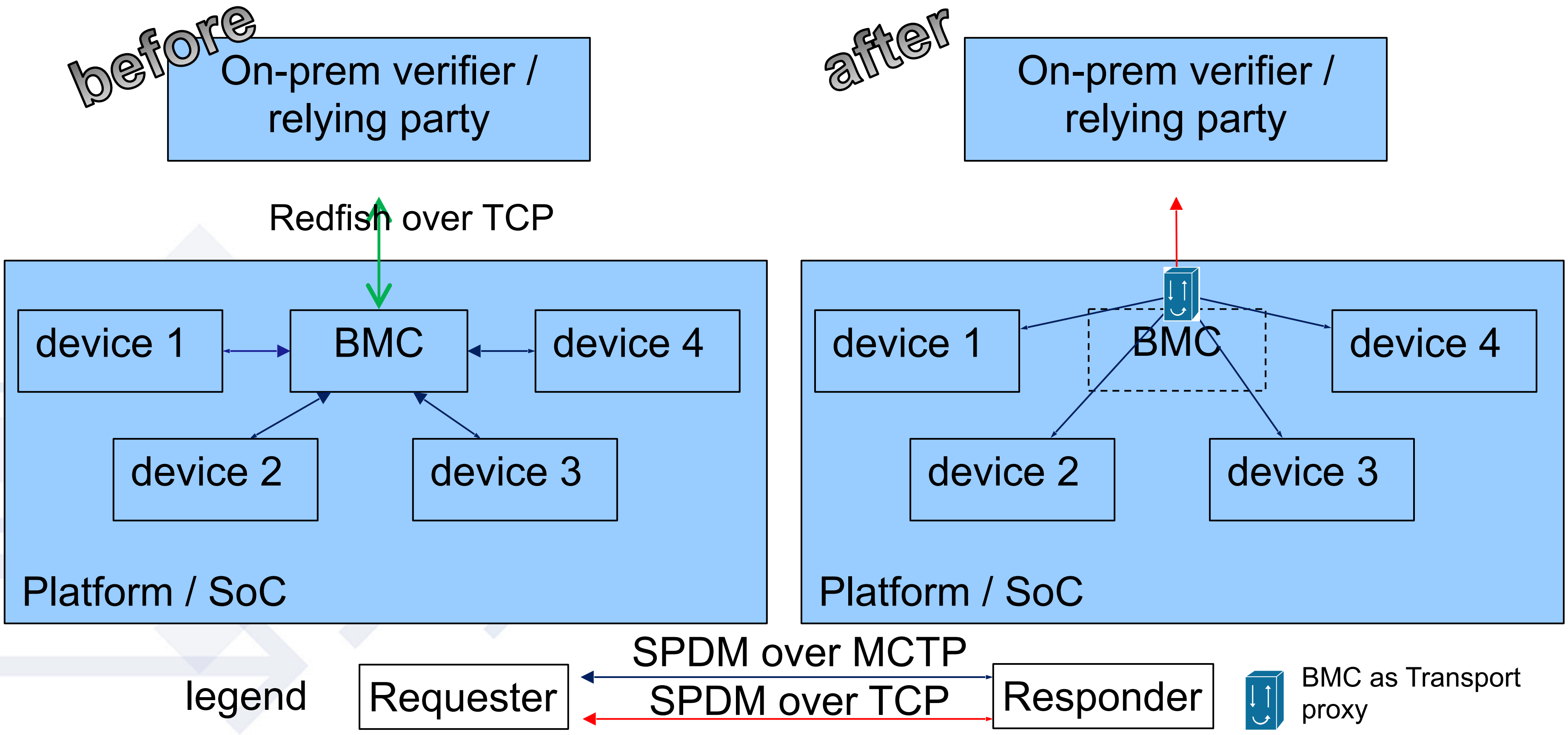
Use Case Example 1 – Client E2E Remote Attestation

- On Client SoC, remote verifier and relying party retrieve attestation of device measurements directly from devices. (GET_CERT, GET_MEASUREMENTS)



Use Case Example 2 – Datacenter E2E Off-Machine Attestation

- For datacenter, improve security by minimizing TCB and excluding BMC from SPDM session. (GET_CERT, GET_MEASUREMENTS)



before

On-prem verifier / relying party

Redfish over TCP

device 1

BMC

device 4

device 2

device 3

Platform / SoC

after

On-prem verifier / relying party

device 1

BMC

device 4

device 2

device 3

Platform / SoC

legend

Requester

SPDM over MCTP

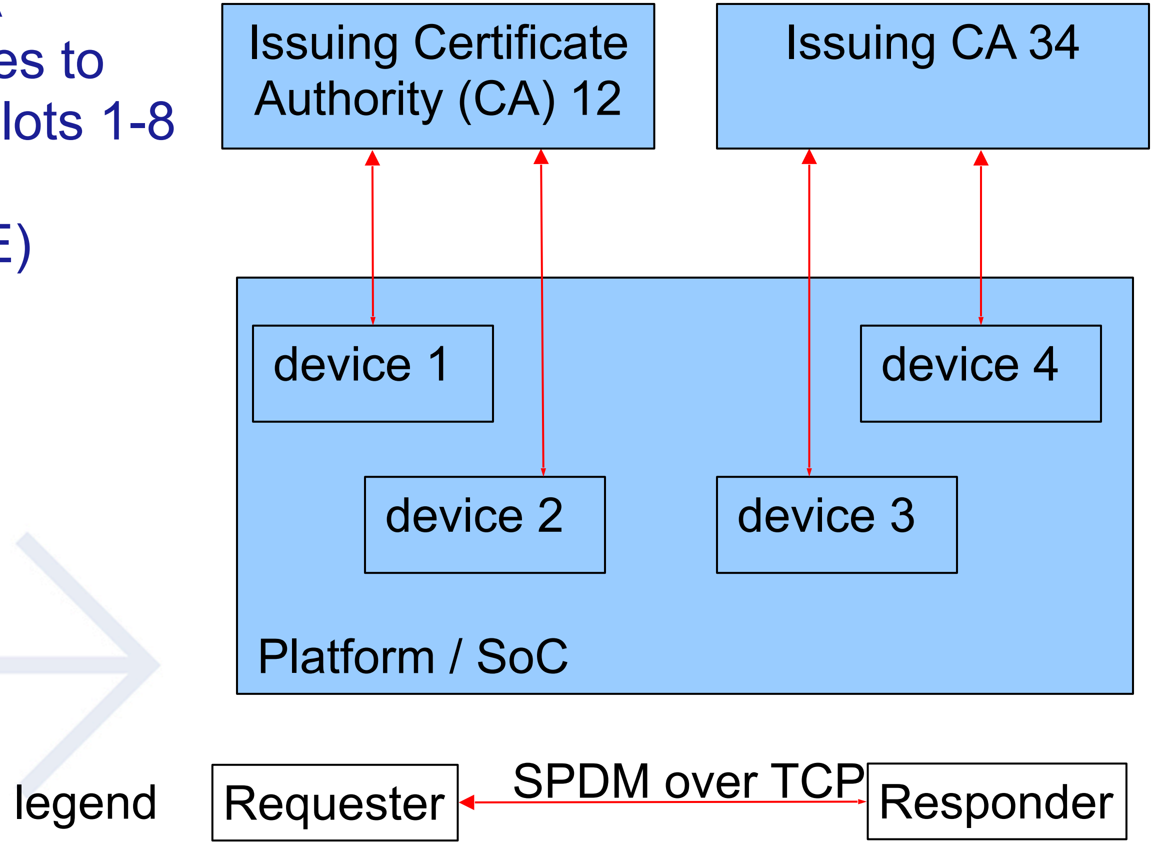
SPDM over TCP

Responder

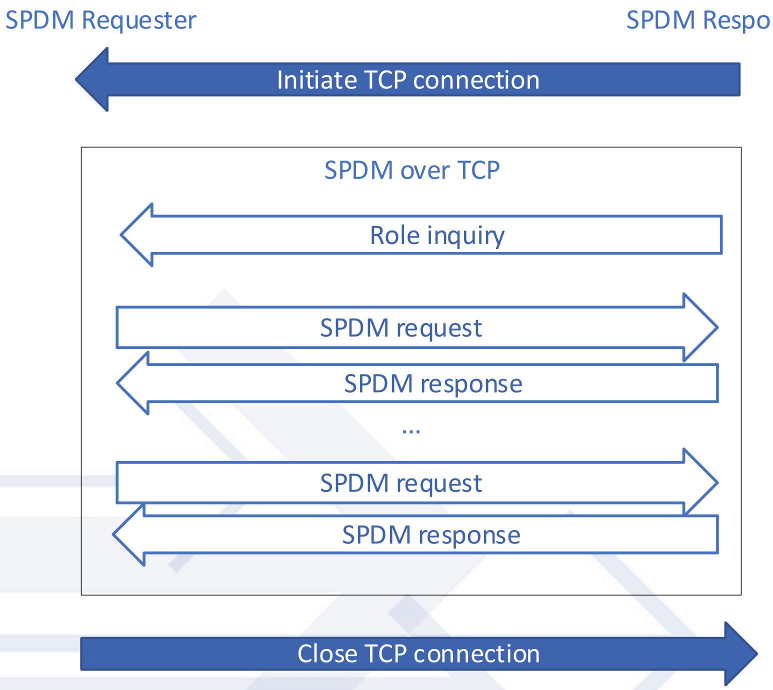
BMC as Transport proxy

Use Case Example 3 – Provisioning Responder Certs

- Device vendor’s or value-added reseller’s CA provisions certificates to devices certificate slots 1-8 (GET_CSR, SET_CERTIFICATE)



Roles and Models



SPDM Requester

SPDM Responder

Initiate TCP connection

SPDM over TCP

Role inquiry

SPDM request

SPDM response

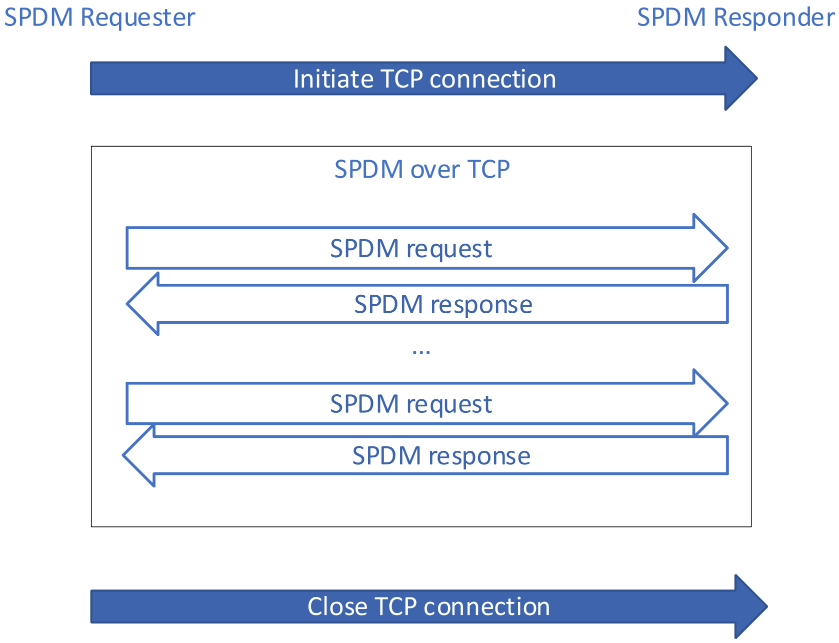
…

SPDM request

SPDM response

Close TCP connection

Reach out model



SPDM Requester

SPDM Responder

Initiate TCP connection

SPDM over TCP

SPDM request

SPDM response

…

SPDM request

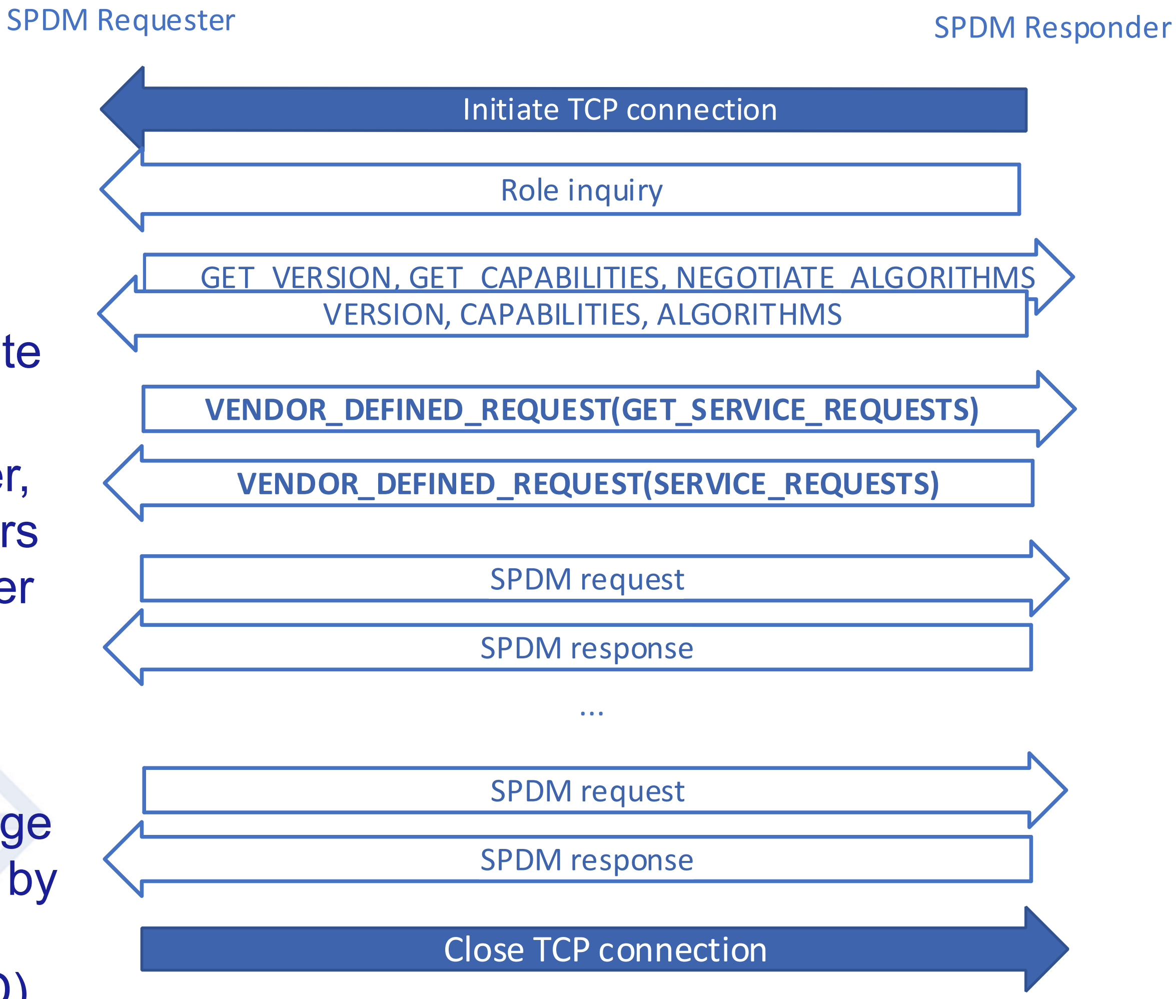
SPDM response

Close TCP connection

Reach down model

Example Flow

1. SPDM Responder (e.g., a device) initiates TCP connection with SPDM Requester (e.g., CA)
2. The two endpoints negotiate V/C/A.
3. Requester asks Responder, and the Responder answers what service the Responder wants, in VENDOR_DEFINED messages.
4. The two endpoints exchange service messages defined by SPDM or the TCP binding spec (VENDOR_DEFINED).



SPDM Requester

SPDM Responder

Initiate TCP connection

Role inquiry

GET_VERSION, GET_CAPABILITIES, NEGOTIATE_ALGORITHMS

VERSION, CAPABILITIES, ALGORITHMS

VENDOR_DEFINED_REQUEST(GET_SERVICE_REQUESTS)

VENDOR_DEFINED_REQUEST(SERVICE_REQUESTS)

SPDM request

SPDM response

...

SPDM request

SPDM response

Close TCP connection

Services / Use Cases

Service (SPDM Responder asks SPDM Requester to …)	SPDM messages used in service
Establish session	KEY_EXCHANGE PSK_EXCHANGE
Provision certificate	GET_CSR SET_CERTIFICATE
Verify measurements	GET_MEASUREMENTS, VENDOR_DEFINED(VERIFY_RESULTS)
Retrieve measurements	GET_MEASUREMENTS
Retrieve MEL	GET_MEASUREMENTS, GET_MEASUREMENT_EXTENSION_LOG
Provision reference measurements	VENDOR_DEFINED(SET_REFERENCE)
Provision measurement verification policy	VENDOR_DEFINED(SET_POLICY)

Brainstorming for Future Work

- Engage with Alliance Partners, such as OCP and TCG, and explore new use cases and potential adoptions in applications.
- Develop reference implementation for common use cases.
- BMC as proxy performing data transfer - MCTP to TCP and vice versa.

Thank you

Get in touch – comments, case study, new use cases, …

- DMTF Feedback and Technology Submission Portal (https://www.dmtf.org/standards/feedback)
- Eduardo Cabre (eduardo.cabre@intel.com)
- Xiaoyu Ruan (xiaoyu.ruan@intel.com)