SPDM Authorization (Intro and Update)

Raghu Krishnamurthy, NVIDIA
Scott Phuong, Microsoft

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF SPDM WG.
- 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.
- This information is a summary of the information that will appear in the specifications. See the specifications for further details.

Authorization

Definition:

- Determining if the requesting entity has the appropriate privileges to perform protected actions. If yes, to allow them to perform those protected actions.

Scope:

- Provide a general mechanism for any use case (e.g., SPDM, PLDM, other present and future PMCI WG use cases, alliance partners, industry) to perform authorization.
  - Examples:
    - PLDM FW Update, Type 2 and/or Type 6
    - SPDM Set Certs (and other future “set” commands).

Expected publication Q4 2025

Assumptions

- This presentation makes the following assumptions
  - The endpoints in discussion communicate using SPDM (DSP0274) and SPDM Secured Messages (DSP0277)
    - Communication can use any transport that supports the above commands
  - To bootstrap Authorization, there needs to be a provisioning step for initial credential
  - Definition of Policy profiles is out of scope for the Authorization specification

High Level Architectural Components

- Authorization Flow
  - Use SPDM Sessions between Requester/Responder pair (simplifies supported options, baseline security)
  - Specify how to authorize generic messages
- Credential and Policy Management
  - Types of Credentials
    - Asymmetric Key Pair (Focus of initial release)
  - Credential and Credential Policy
    - Standardize provisioning of credentials and associating them with their authorization policy
    - Authorization policy itself should be specified by the protocol leveraging this authorization specification

High Level Architectural Components

- Ownership and Transfer of Ownership
  - Workflow for locking and clearing provisioned authorization data and vendor defined data types to factory defaults.
  - Not the same as OCP Device Ownership Transfer

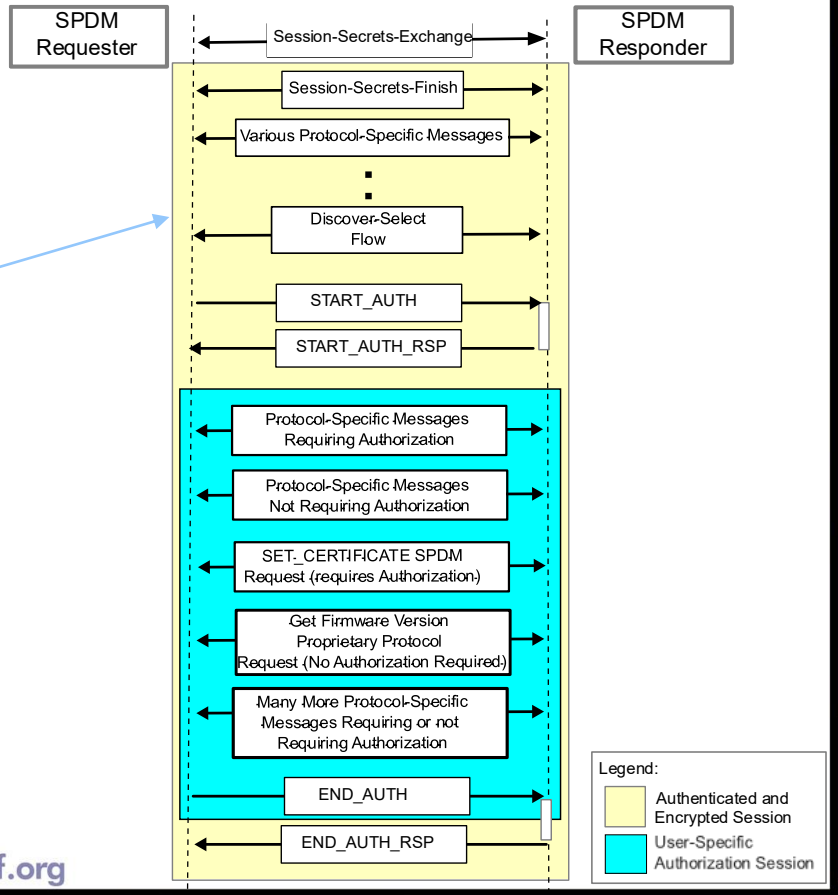
Authorization Processes

- 2 Use Cases – the User is the authorized actor
  - SPDM Requester represents User via SEAP
  - SPDM Requester is a proxy for User via USAP

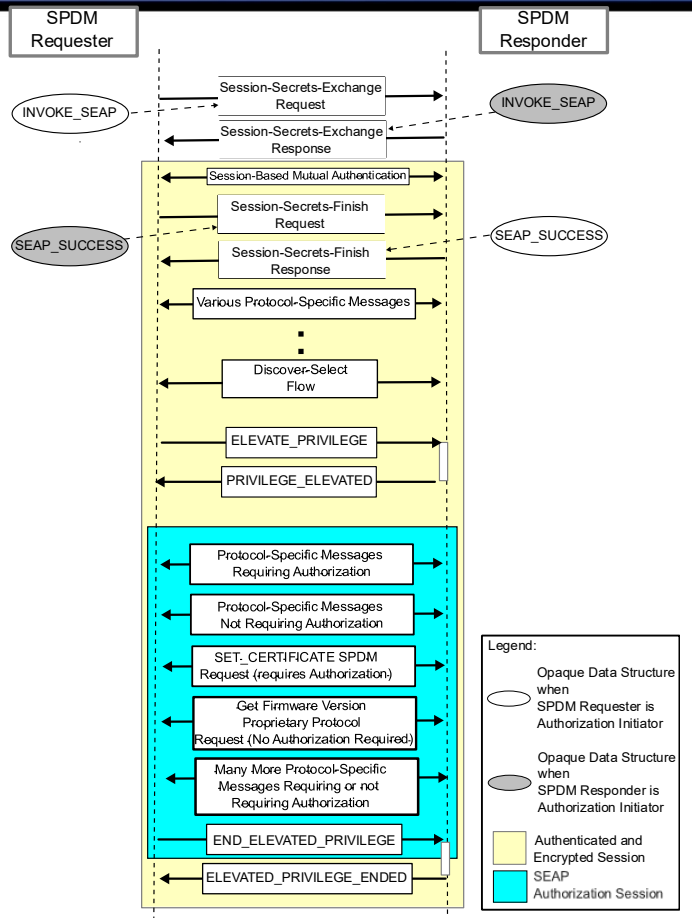
User-Specific Authorization Process (USAP)

Regular SPDM Key exchange (Asym, PSK etc) using endpoint key
Includes negotiating Secured Messages DSP0277 version

AuthTag uses authorization key (separate from key exchange keys)



SPDM Endpoint Authorization Process (SEAP)



Credential Provisioning

- DSP0289 defines 8 persistent Credential Slots, minimum supported is one
  - The ability to clear slot contents will be included in v1.0
- All slots can be provisioned in
  - A trusted environment
  - Authorized via a selected credential(s) already provisioned
- All credentials associated with a policy
  - Defines what the credential can be used to authorize (ex: SET_CERTIFICATE, PLDM FW Activation etc)
- DSP0289 defines credential provisioning commands for credentials and policies

Call to Action

- Get involved in the DMTF Authorization Specification development
- Review the WIP slides from DMTF (https://www.dmtf.org/sites/default/files/SPDM_Authorization_WIP90.pdf)
- Provide feedback to DMTF SPDM (https://www.dmtf.org/standards/feedback)
- Start developing use cases for authorization at the device level
- Is being adopted by other standards bodies.

For more information,
visit dmtf.org

Learn about membership at
dmtf.org/join

Thank you!