SPDM 1.1: Session Key Exchange Protocols

August 2019

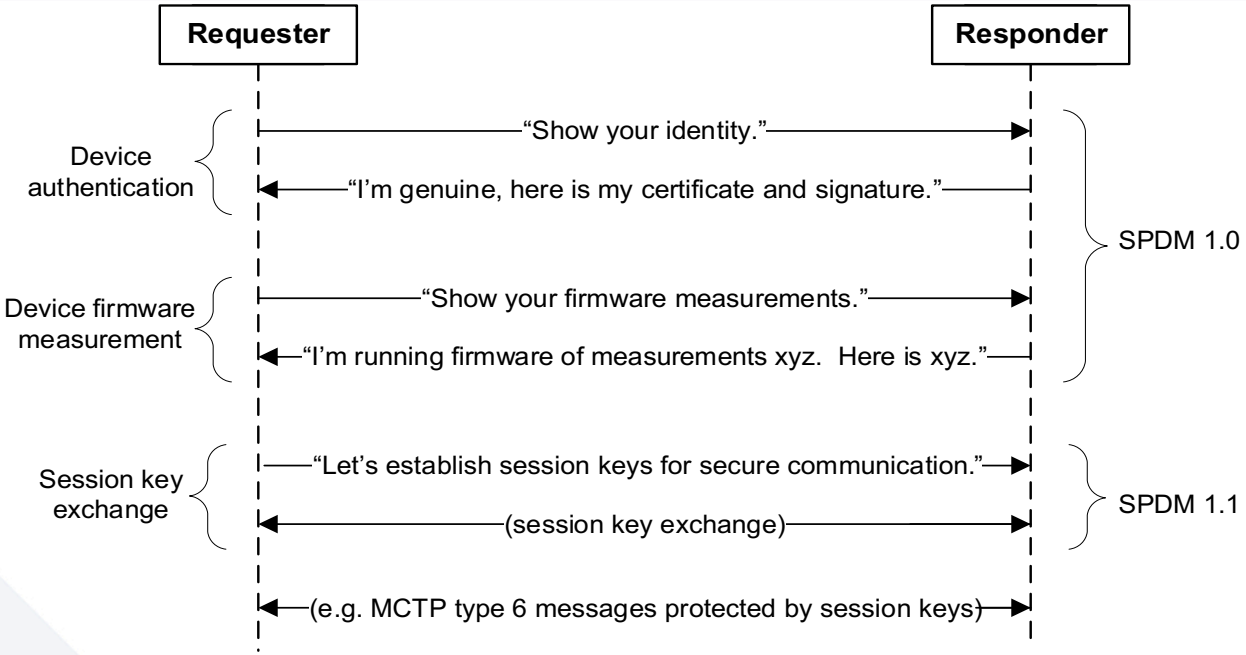
Disclaimer

- 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 DMTF website.
- This information is a summary of the information that will appear in the specifications. See the specifications for further details.

Call for Action

- DMTF welcomes public comment on this Work-in-Progress (WIP) material.
- Please submit your comments via the DMTF Feedback portal https://www.dmtf.org/standards/feedback.
- Please refer to PMCI Upcoming Workgroup Deliverables for timelines of SPDM development: https://www.dmtf.org/standards/pmci.

Session Key Exchange



Objective: Establish session keys that are known to only Requester and Responder

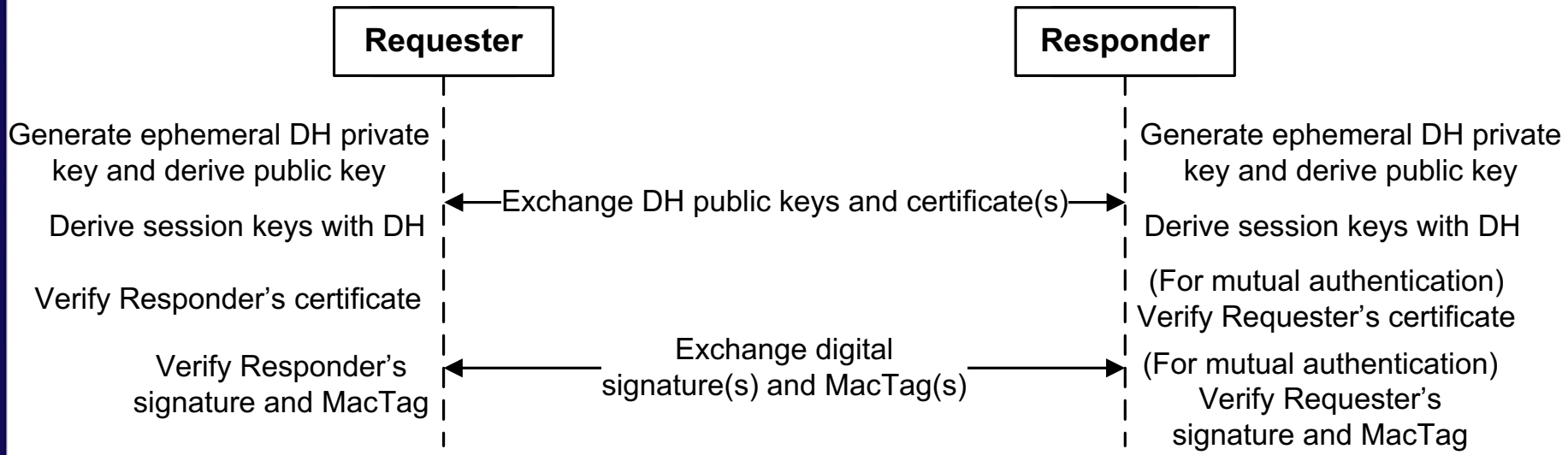
- Either endpoint may abort a session at any time.
- Authentication happens with session key exchange – no need to run "Device authentication" of SPDM 1.0 if session key exchange is run.

SPDM 1.1 plans to specify the following session key exchange schemes:

1. **SIGMA** option: based on ephemeral Diffie-Hellman and digital signatures.
2. **Pre-shared secret** option: based on a pre-shared secret known to both endpoints.

*SPDM 1.0 draft: https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_0.9.0a.pdf
*SIGMA: http://webee.technion.ac.il/~hugo/sigma-pdf.pdf

SIGMA Option for Session Key Exchange



- Diagram above illustrates high-level sequence; arrows do not map to actual commands.
- Based on SIGMA and TLS 1.3 handshake protocols.
- Session key agreement uses Diffie-Hellman scheme (ECDHE or FFDHE).
- Features mutual or one-way (Responder to Requester) authentication.
- Features forward secrecy.
- Requester capabilities: RSA and/or ECC, HMAC, RNG
- Responder capabilities: RSA or ECC, HMAC, RNG (if mutual authentication or forward secrecy is required)
- Responder examples: graphics card, SSD, FPGA

Pre-Shared Secret Option: Introduction

- Pre-shared secret (pss) is a secret known to both the Requester and the Responder, before the session key exchange flow is executed.
- Provisioning of pss is out of scope of SPDM 1.1. Implementer's policy is also out of scope of SPDM 1.1.
- Responder benefits: low cost (HMAC + unique device secret or secure storage for pss)
- Responder examples: integrated webcam, integrated fingerprint scanner, devices soldered on board, CPU, GPU, NIC
- Requester capabilities: HMAC, RNG, secure storage

Pre-Shared Secret Option for Session Key Exchange

- Diagram below illustrates high-level sequence; arrows do not map to actual commands.
- Some provisioning schemes require Requester to send opaque_pss_data to Responder during session key exchange flow, so the Responder can derive pss. Content of opaque_pss_data depends on the underlying pss provisioning scheme and both are out of scope of SPDM.
- Requester context and Responder context are described in diagram below.
- Session keys are derived from pss and contexts.