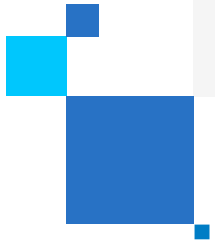
2022 International Cryptographic Module Conference

FIPS 140-Compliant SPDM

Presenter: Xiaoyu Ruan, Principal Engineer, Intel (xiaoyu.ruan[at]intel.com)
Coauthor: Jiewen Yao, Principal Engineer, Intel (jiewen.yao[at]intel.com)
September 15, 2022



intel®

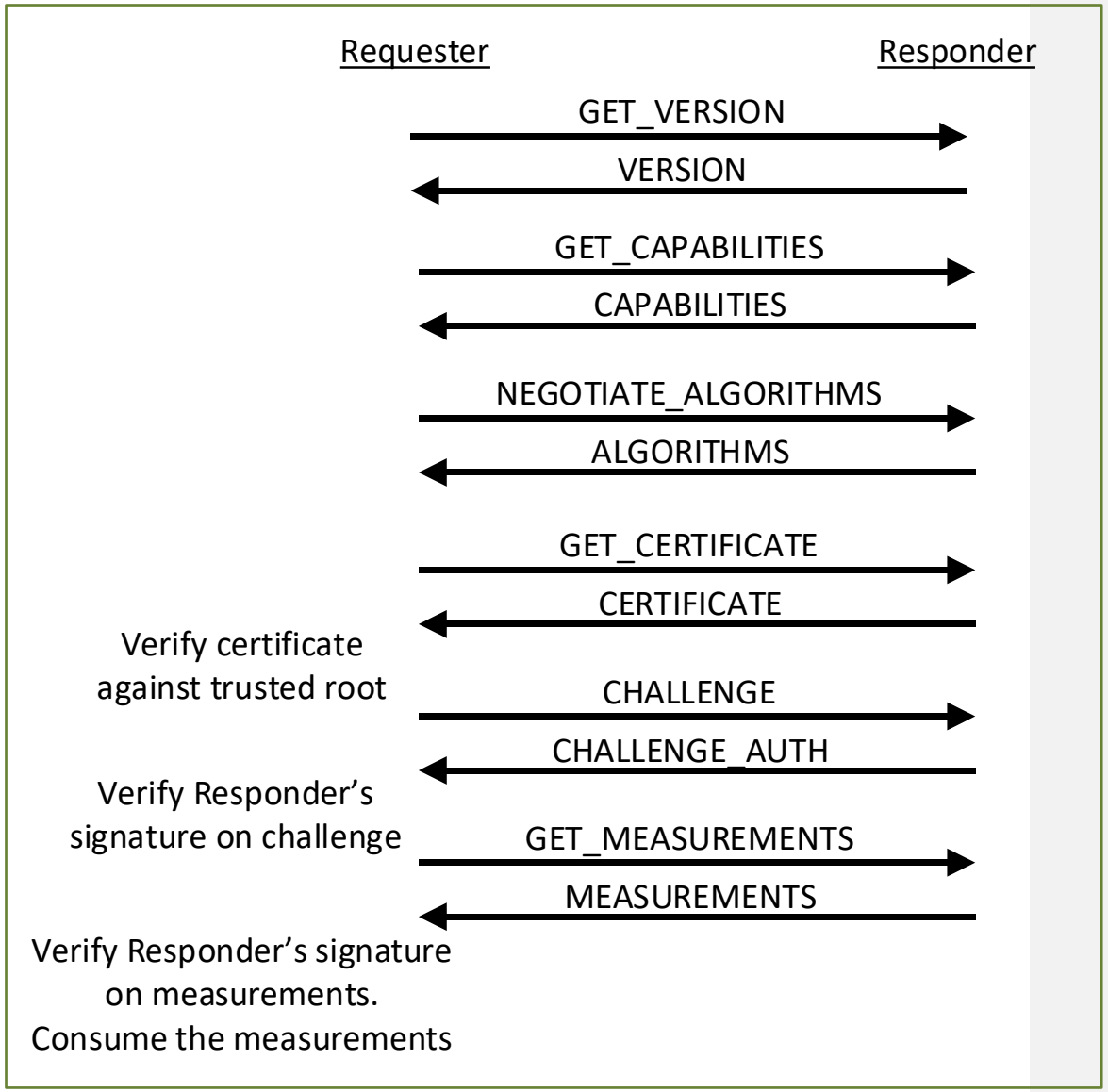
Agenda

- What is SPDM?
- SPDM open-source library
- FIPS Design for SPDM
- Future work

SPDM: Security Protocol and Data Model

https://www.dmtf.org/dsp/DSP0274

- A Distributed Management Task Force (DMTF) standard.
- Defines messages, data objects, and sequences for performing message exchanges over various transports.
- Transport agnostic.
- Leveraged by other standards, such as PCIe IDE.
- Dec. 2019: SPDM 1.0: one-way authentication, attestation
- Aug. 2020: SPDM 1.1: + mutual authentication, session establishment
- Dec. 2021: SPDM 1.2: + bug fixes, enhancements
- SPDM 1.3 under development
- Welcome proposals for new features

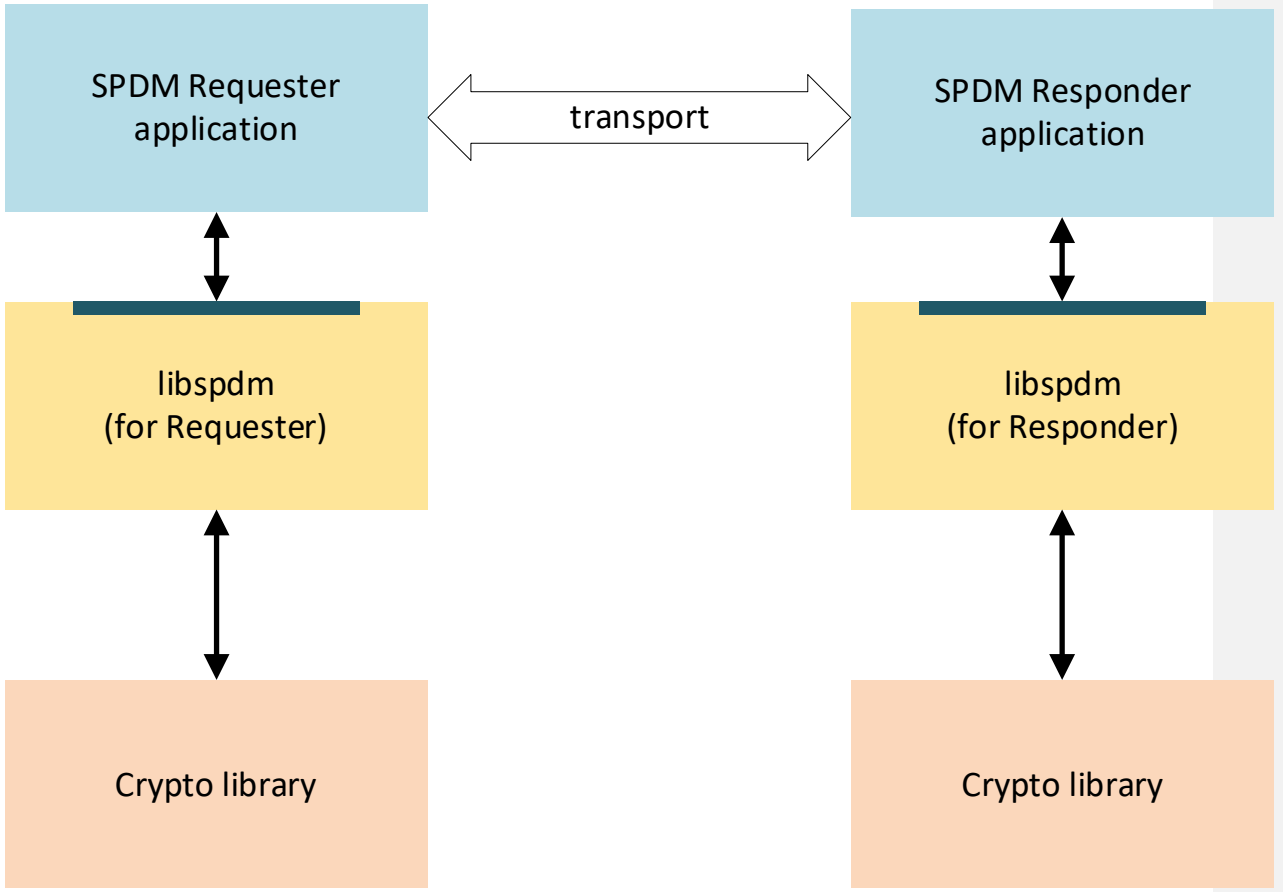


Sample SPDM Flow: Attestation

libspdm: Open-Source SPDM Implementation

https://github.com/DMTF/libspdm

- Reference code for Requester and Responder, and transport binding for MCTP and PCIe.
- Main contributors include Intel, NVIDIA, ARM.
- Written in C.



libspdm block diagram

Why does Intel Care? Why should YOU Care?

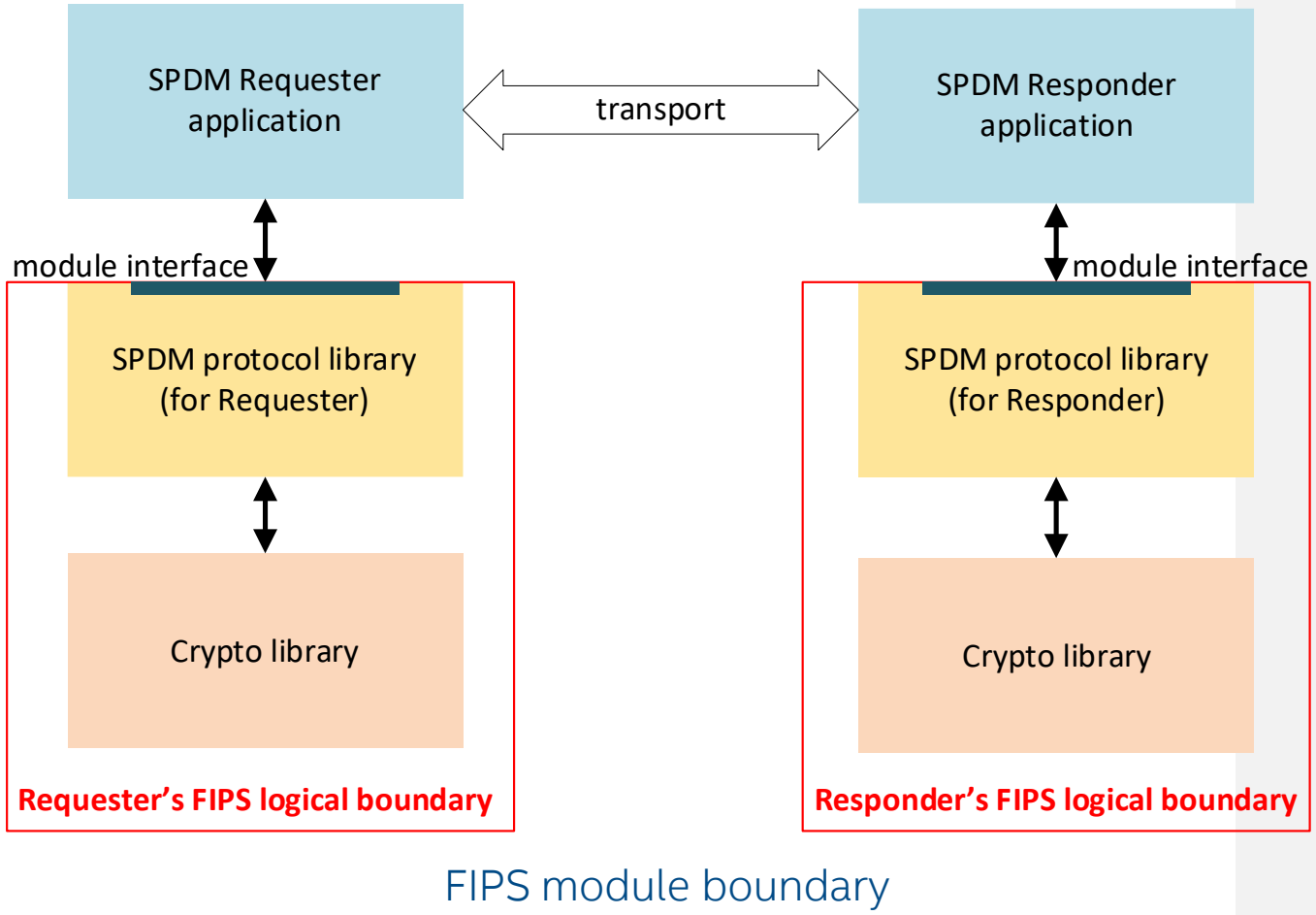
- SPDM is widely deployed in device communication and used by Intel products for PCIe, CXL, Security IPs in Client and Datacenter SoCs, etc.
- Intel takes FIPS 140-3 seriously, striving to meet FIPS 140-3 level 1 for software and level 2+ for hardware.

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date
4158	Intel Corporation	Cryptographic Module for Intel® Converged Security and Manageability Engine (CSME)	Hybrid	02/17/2022
4150	Intel Corporation	Intel® Converged Security and Manageability Engine (CSME) Crypto Module for Tiger Point PCH, Mule Creek Canyon PCH, and Rocket Lake PCH	Firmware-Hybrid	02/10/2022
4025	Intel Corporation	Intel® Offload and Crypto Subsystem (OCS)	Hardware	09/09/2021
3838	Intel Corporation	Cryptographic Module for Intel® Platforms' Security Engine Chipset	Firmware-Hybrid	03/04/2021
3662	Intel Corporation	Intel® DC SSD D7-D4512	Hardware	05/29/2020 06/22/2020 07/24/2021
3511	Intel Corporation	Optane™ SSD DC D4800X	Hardware	08/12/2019 08/28/2019 12/06/2019 12/23/2019 03/20/2020 08/31/2020

Intel's FIPS certificates

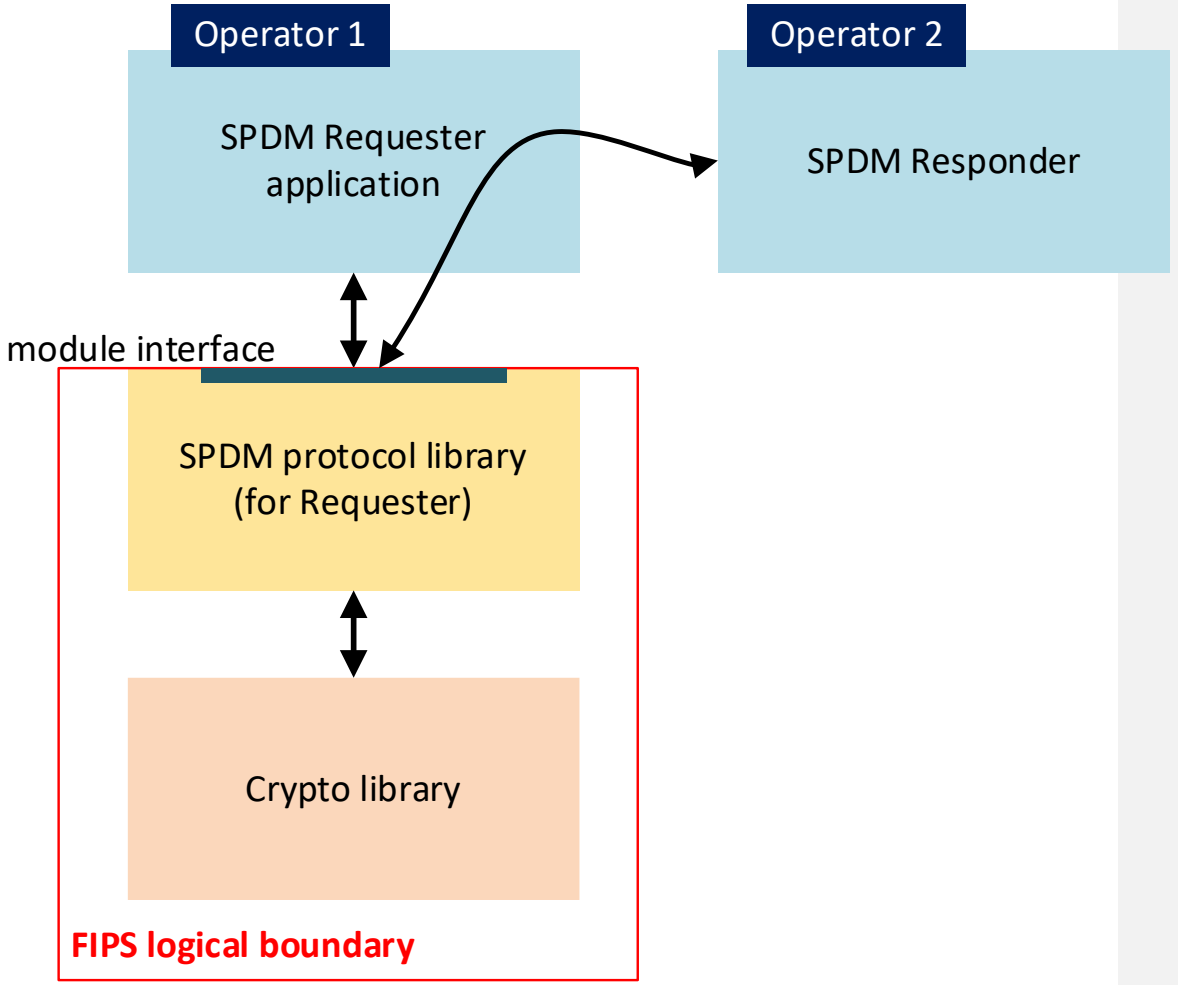
SPDM's FIPS Considerations

- FIPS boundary = SPDM library + crypto library
- Integrity selftest
- Pre-operational CASTs
- APIs for module ID & status.
- Services: SPDM library APIs for processing SPDM messages from the peer
- SPDM "negotiate_algorithms" must select only Approved algorithms



Operator Authentication for Level 2+

- SPDM 1.1+ supports one-way or mutual authentication
- To meet level 2+, the SPDM library shall
  - Authenticate the peer (Operator 2) during secure session establishment with the peer.
  - Then provide Approved services (i.e., handle messages from the peer) within the secure session.



Level 2+ Consideration for Requester FIPS

Missing Pieces & Future Work

- Uniqueness of session key and IV
  - SPDM 1.2 uses Diffie-Hellman-based SIGMA for key establishment, like TLS 1.3.
  - If CMVP reviews SPDM and approves it in IG C.H, then FIPS labs do not need to repeat the review of every SPDM module by different vendors.
- FIPS compliance for libspdm
  - Create a FIPS configuration for libspdm
  - Integrity self-test for libspdm and crypto library
  - CASTs for crypto library
  - Only Approved algorithms
  - Operator authentication for level 2+

The FIPS 140-3 IG Section C.H enumerates several options for a module to meet 800-38D's GCM key/IV pair uniqueness requirements. The first option reads

"Construct the IV in compliance with the provisions of a peer-to-peer industry standard protocol whose mechanism for generating the IVs for AES-GCM has been reviewed and deemed acceptable by the appropriate validation authorities and subject to the additional requirements established in this guidance."

More Thoughts on Attestation and FIPS

- A secure attestation mechanism requires a protocol like SPDM, not a single command.
- An implementation that returns signed attestation record would meet the clause in the working draft below, but would be vulnerable (e.g., replay attacks)
- Is protocol in the scope of FIPS 140? For example, FIPS 140 does not cover secure session protocol.

ISO IEC 19790 4th working draft (July 2022)

1302 **7.4.5 Device attestation**

1303 This subclause is not applicable if the cryptographic module vendor does not claim device attestation.

1304 NOTE If no vendor claims are made, the vendor's public documentation should reflect that no claims have been made regarding
1305 device attestation

1306 In order to counter substitution attacks on a given cryptographic module, a cryptographic module may support device
1307 attestation suitable for both uniquely identifying a target module alongside allowing reporting of the integrity of the module
1308 and its configuration.

1309 If the cryptographic module supports device attestation:

1310 — The module **shall [04.58]** provide an attestation record, Following module configuration by the Crypto Officer,
1311 exporting the attestation record **shall [04.59]** only be available to authorised users; and

1312 — The module security policy **shall [04.60]** provide guidance to the user on device attestation including how to verify
1313 records returned by the module.


intel

Q & A