ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Formal Analysis of SPDM:
Security Protocol and Data Model 1.2

Cas Cremers

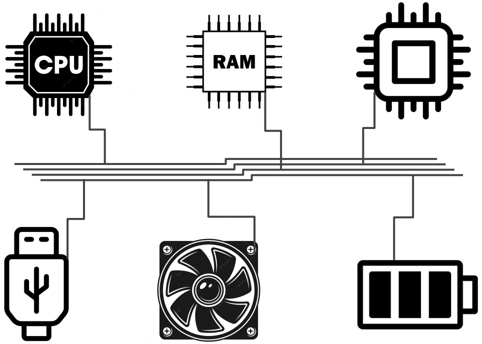
Alexander Dax

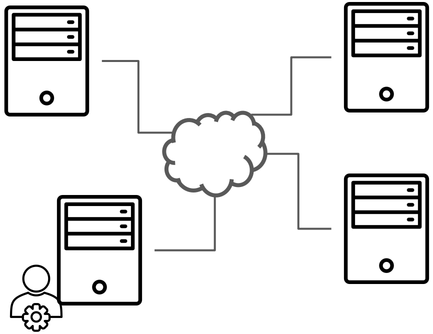
Aurora Naska

Platform Security Risks

Computer platforms comprise of a set of components:

- CPU, GPU, physical wires, external devices, etc
- Mutable components:
  - Firmware version, re-programmable microcode, etc





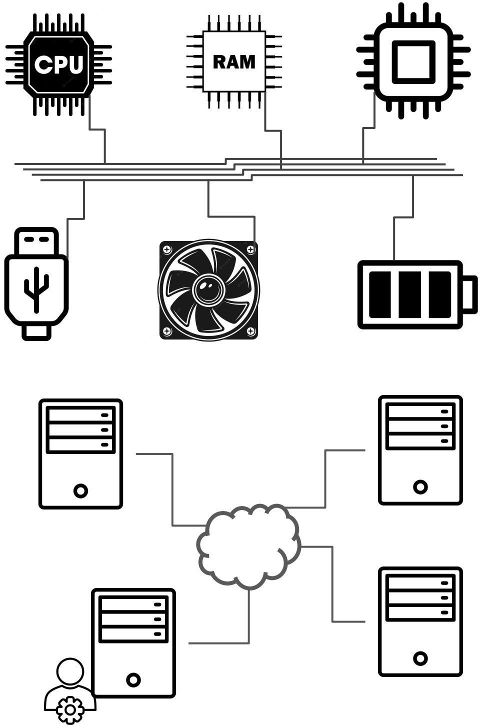
Platform Security Risks

Computer platforms comprise of a set of components:

- CPU, GPU, physical wires, external devices, etc
- Mutable components:
    - Firmware version, re-programmable microcode, etc

Platform components security risks:

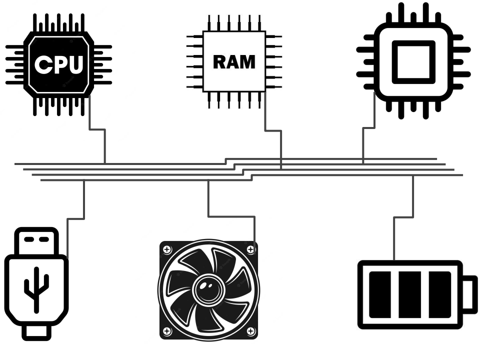
- Compromised firmware
- Fraudulent components
- Un-trusted device(s) snooping via probes



Platform Security Risks

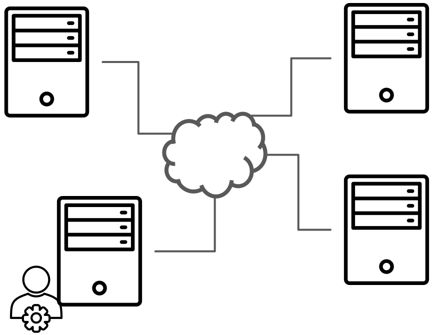
Computer platforms comprise of a set of components:

- CPU, GPU, physical wires, external devices, etc
- Mutable components:
  - Firmware version, re-programmable microcode, etc



Platform components security risks:

- Compromised firmware
- Fraudulent components
- Un-trusted device(s) snooping via probes



Can there be some guarantee over multiple vendors or insecure wire? ?

What is SPDM: **S**ecurity **P**rotocol and **D**ata **M**odel

Industry support behind this protocol:

- DMTF- Distributed Management Task Force
- Supported by other standards groups

MICROCHIP
intel
IBM
CISCO
Lenovo
SAMSUNG
AMD
Microsoft
hp
Google

USB
Enabling Connections™
mipi alliance
CXL Compute Express Link
TRUSTED COMPUTING GROUP

What is SPDM: **S**ecurity **P**rotocol and **D**ata **M**odel

Industry support behind this protocol:

- DMTF- Distributed Management Task Force
- Supported by other standards groups

Two party protocol for secure communication over the wire:

What is SPDM: **S**ecurity **P**rotocol and **D**ata **M**odel

Industry support behind this protocol:

- DMTF- Distributed Management Task Force
- Supported by other standards groups

Two party protocol for secure communication over the wire:

- authentication of hardware identities

What is SPDM: **S**ecurity **P**rotocol and **D**ata **M**odel

DMTF®

Industry support behind this protocol:

- DMTF- Distributed Management Task Force
- Supported by other standards groups

Two party protocol for secure communication over the wire:

- authentication of hardware identities
- measurement for firmware identities

MICROCHIP

intel

IBM

cisco

Lenovo

SAMSUNG

AMD

Microsoft

hp

Google

USB
Enabling Connections™

mipi® alliance

CXL Compute Express Link

TRUSTED® COMPUTING GROUP

What is SPDM: **S**ecurity **P**rotocol and **D**ata **M**odel

DMTF®

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Industry support behind this protocol:

- DMTF- Distributed Management Task Force
- Supported by other standards groups

Two party protocol for secure communication over the wire:

- authentication of hardware identities
- measurement for firmware identities
- session key exchange protocols to enable
  - confidentiality
  - integrity

MICROCHIP

intel

IBM

CISCO

Lenovo

SAMSUNG

AMD

Microsoft

hp

Google

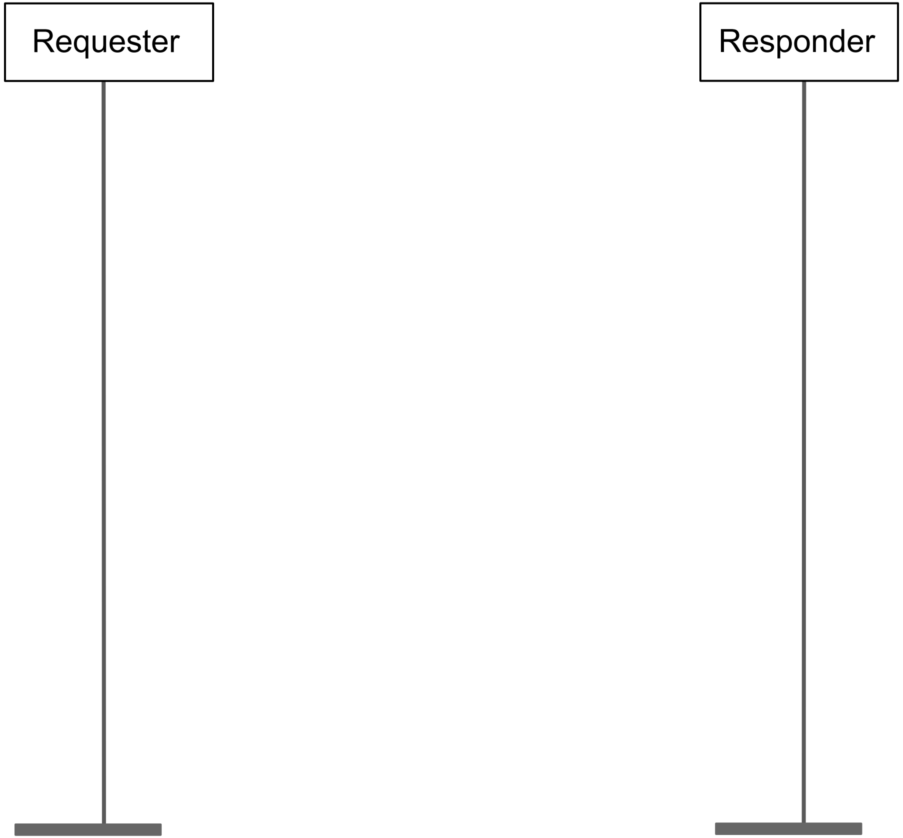
USB
Enabling Connections™

mipi® alliance

CXL Compute Express Link

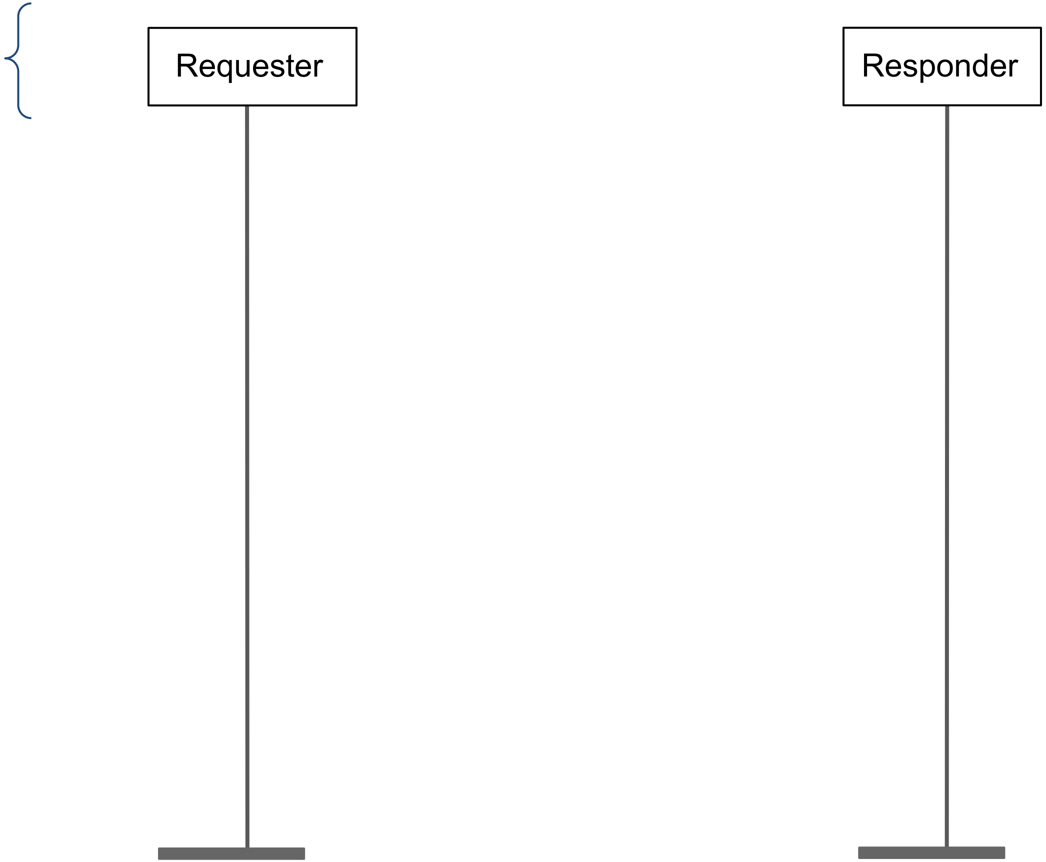
TRUSTED® COMPUTING GROUP

Overview of SPDM



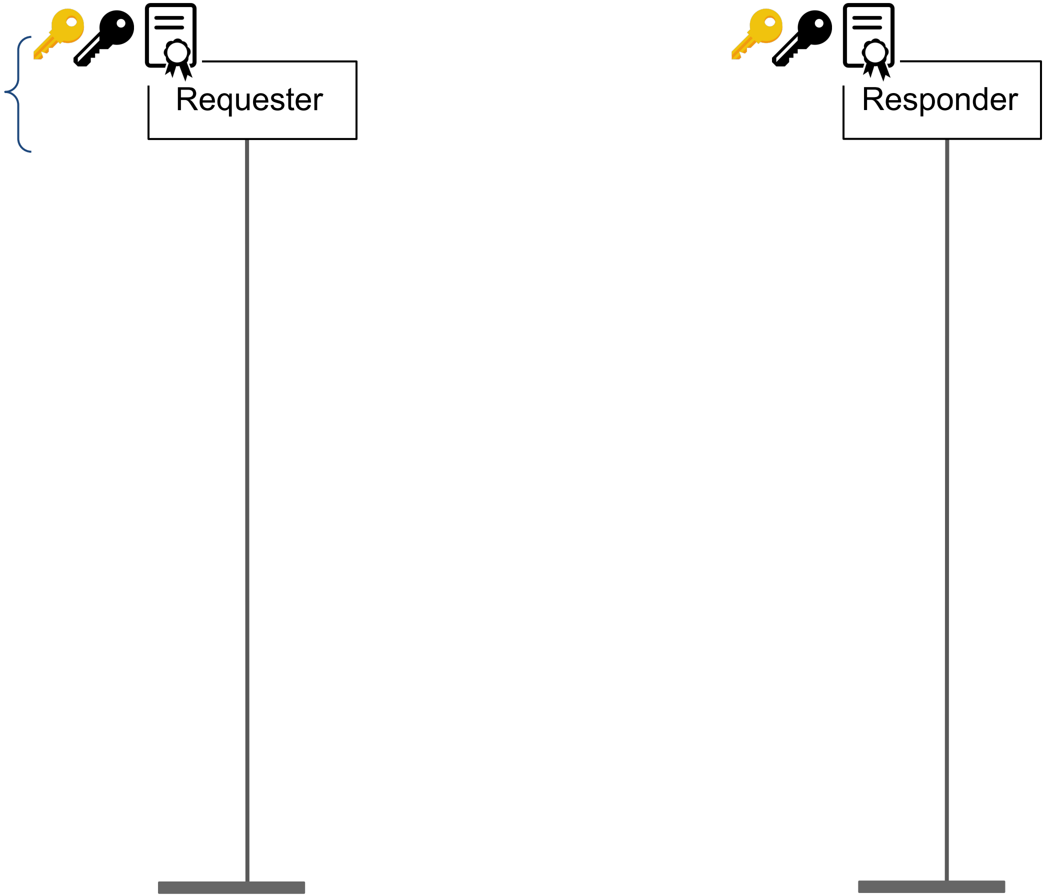
Overview of SPDM

Device Initialization



Overview of SPDM

Device Initialization



Requester

Responder

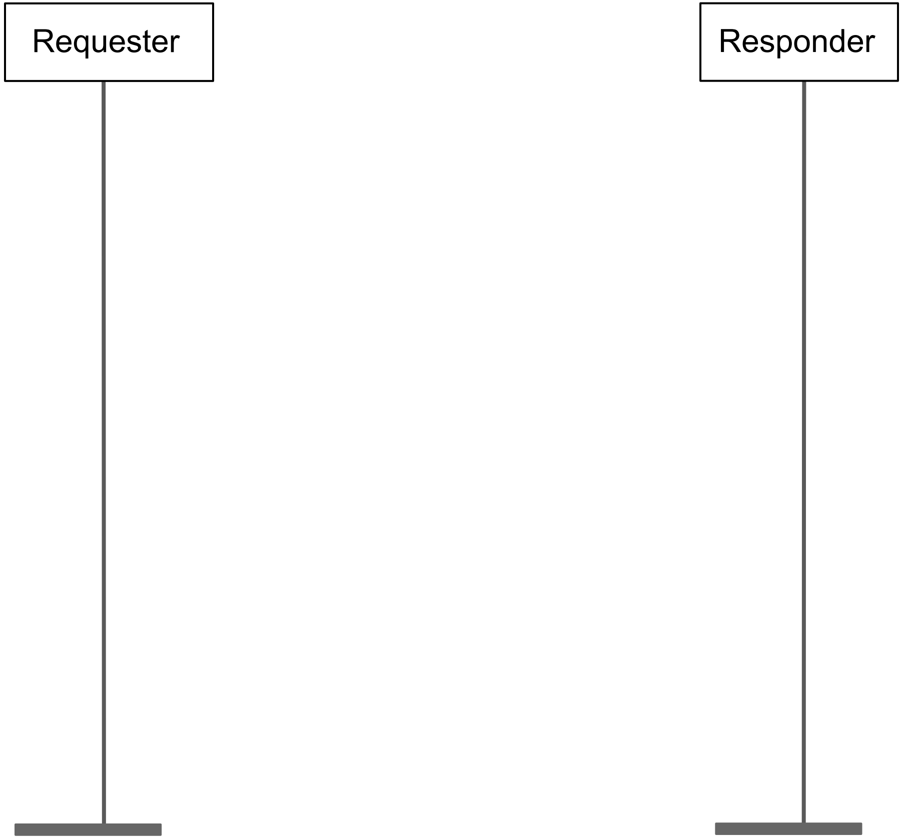
Provisioning of device identities:

- Certificates
- Preshared Symmetric Key
- Preshared Public Key

Overview of SPDM

Device Initialization

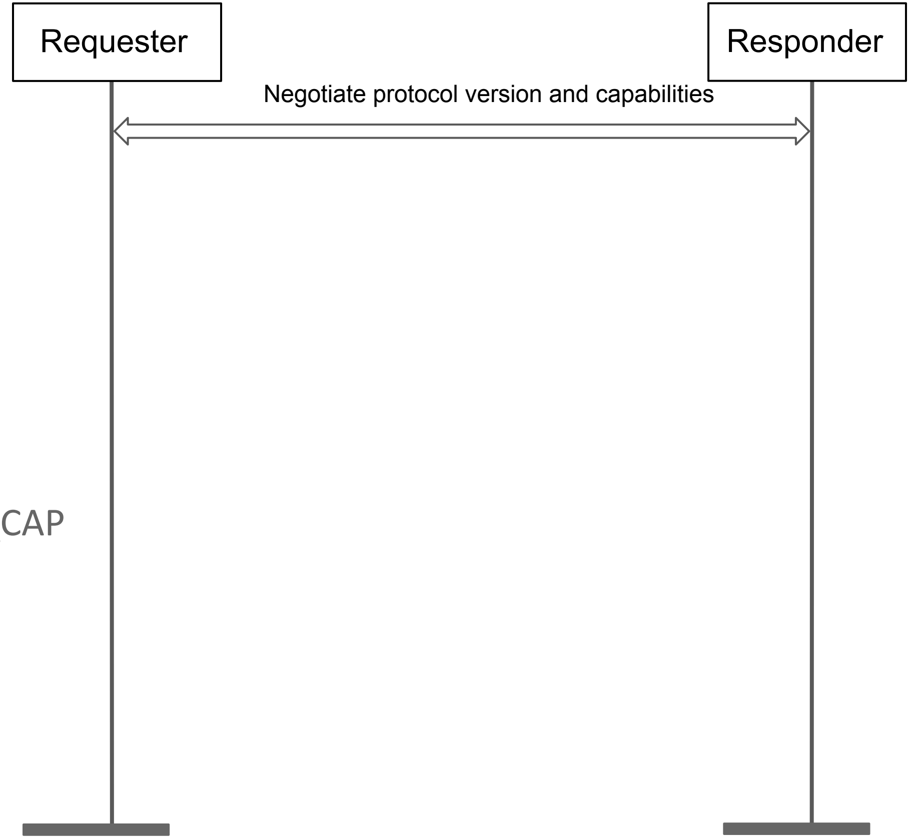
VCA: Version-Capabilities-Algorithms



Overview of SPDM

Device Initialization

VCA: Version-Capabilities-Algorithms



Discovery and Negotiation of:

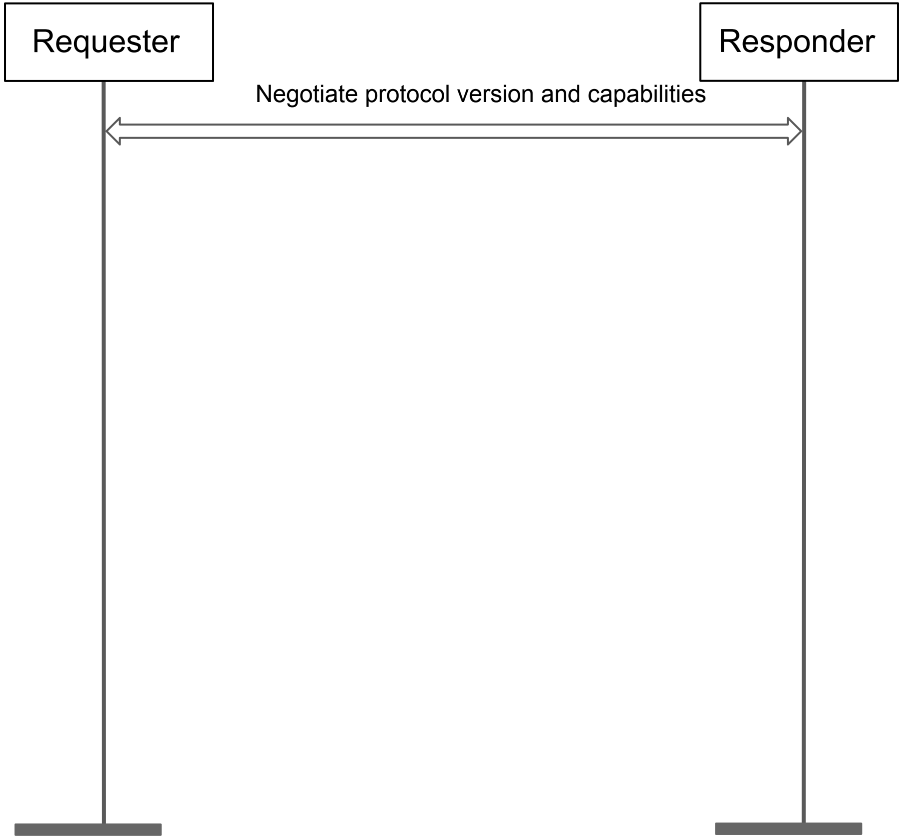
- Protocol **Version**
    - v1.0, v1.1, v1.2
- **Capabilities**
    - ENCRYPT_CAP, MUT_AUTH_CAP
- **Algorithms**
    - SHA_256, SHA3_512

Overview of SPDM

Device Initialization

VCA: Version-Capabilities-Algorithms

Options

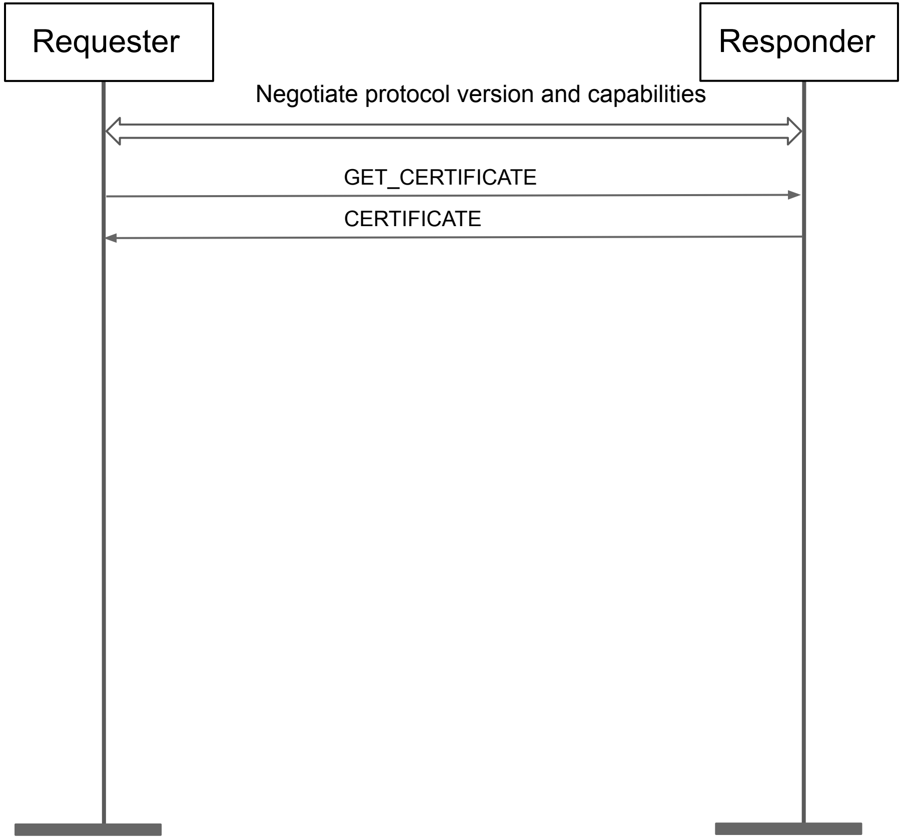


Overview of SPDM

Device Initialization

VCA: Version-Capabilities-Algorithms

Options

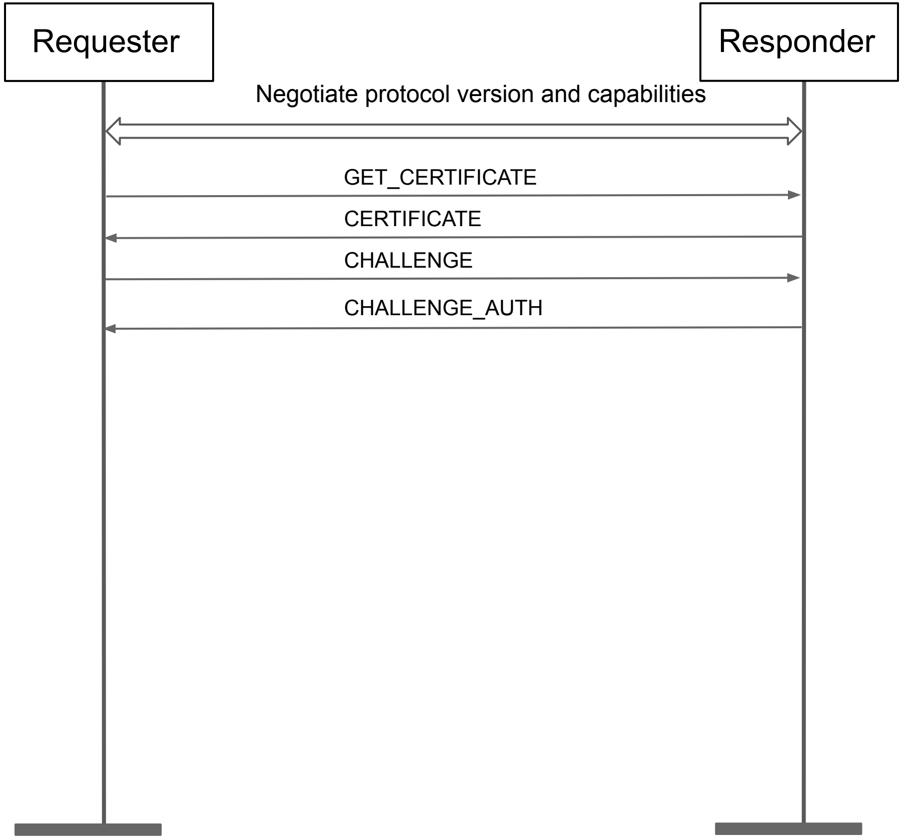


Overview of SPDM

Device Initialization

VCA: Version-Capabilities-Algorithms

Options

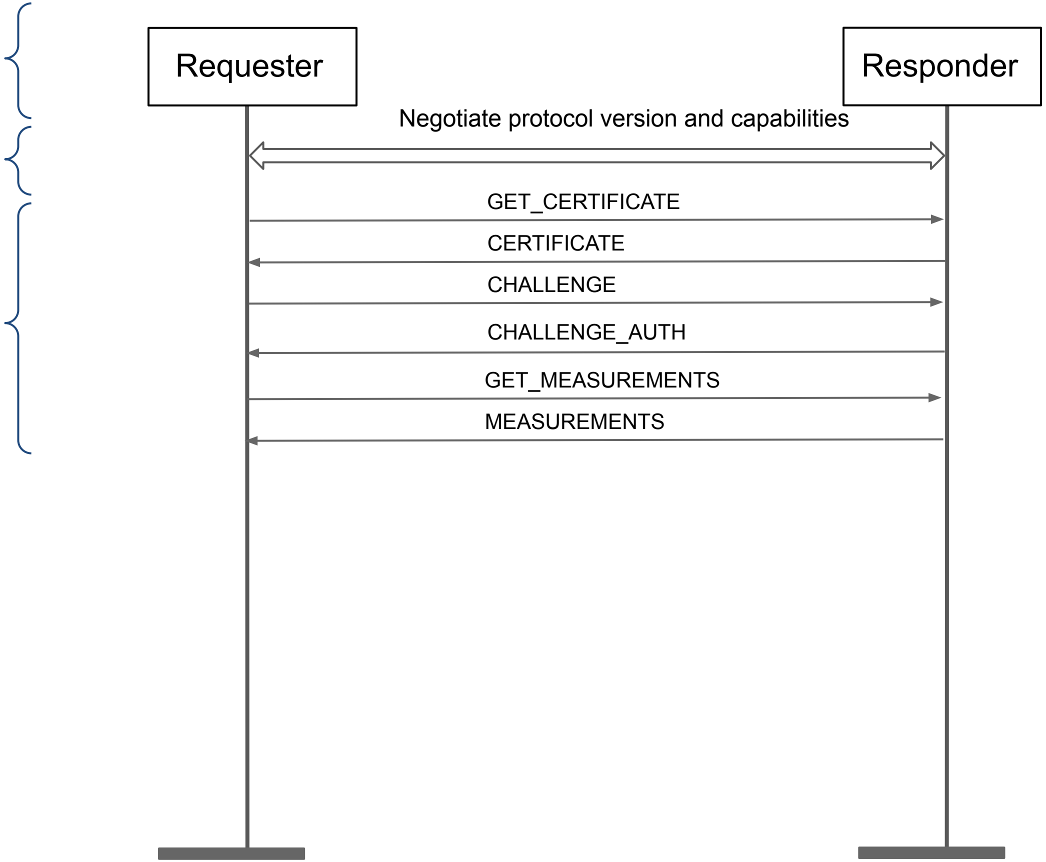


Overview of SPDM

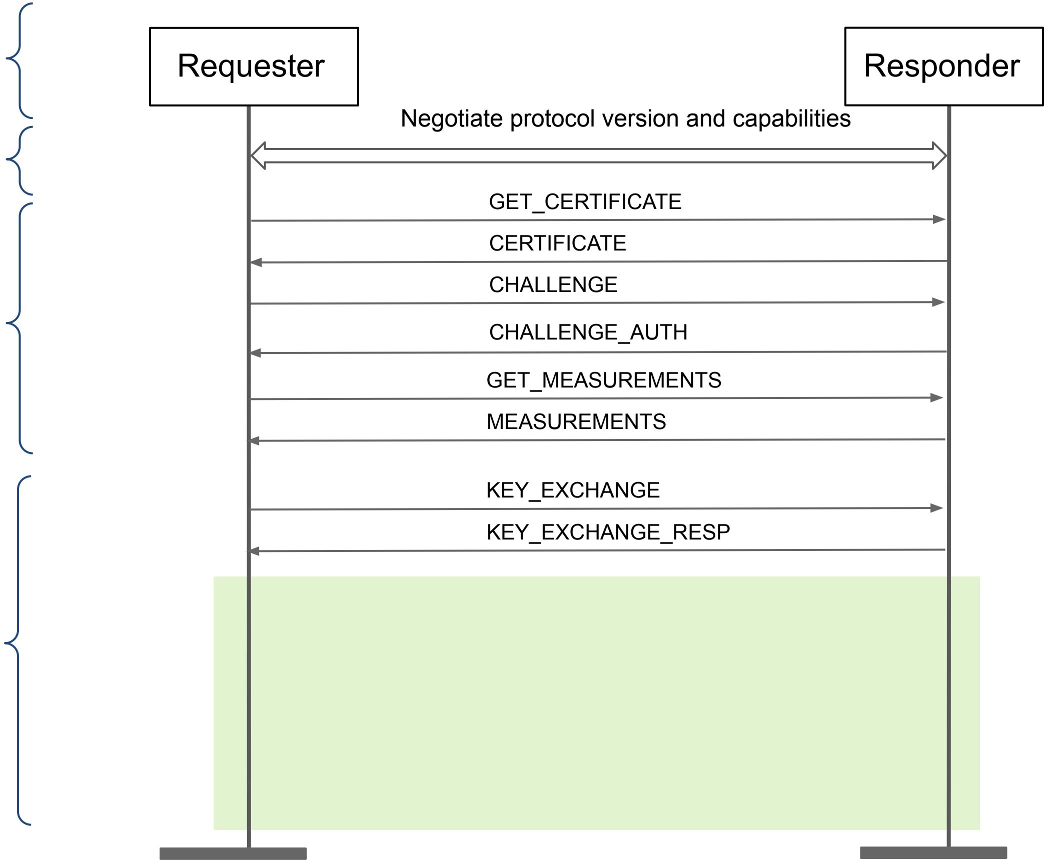
Device Initialization

VCA: Version-Capabilities-Algorithms

Options



Overview of SPDM



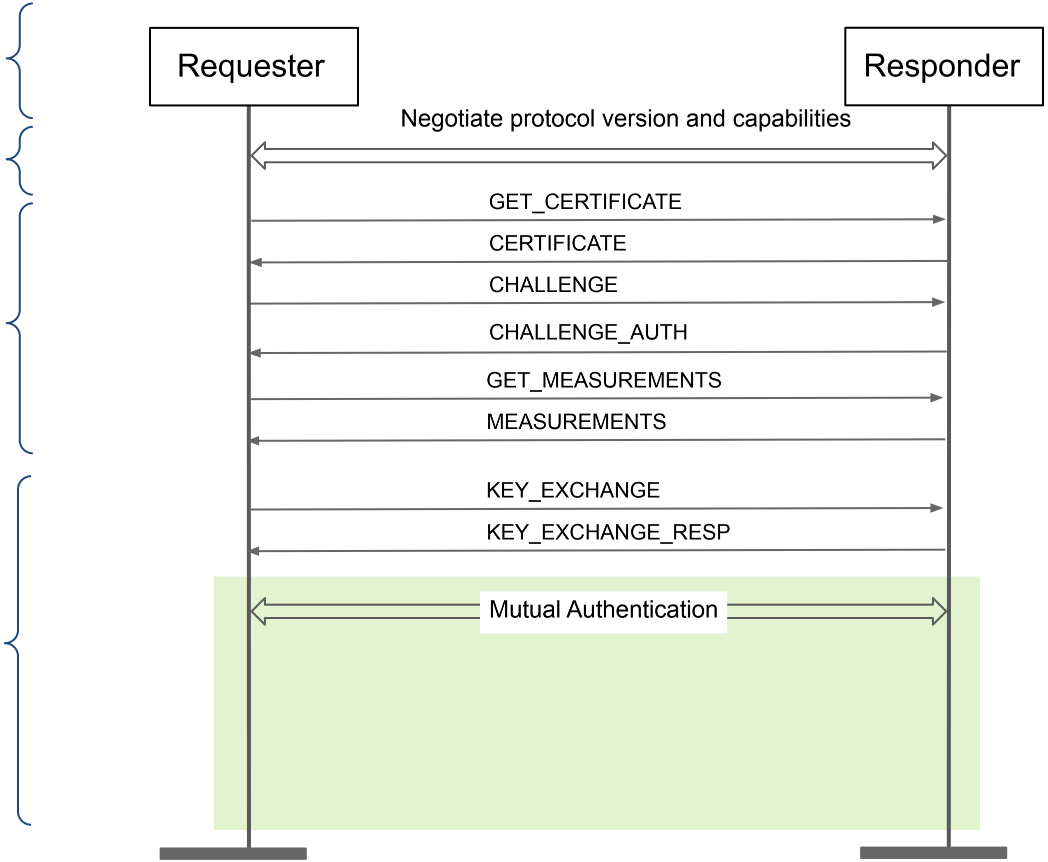
Overview of SPDM

Device Initialization

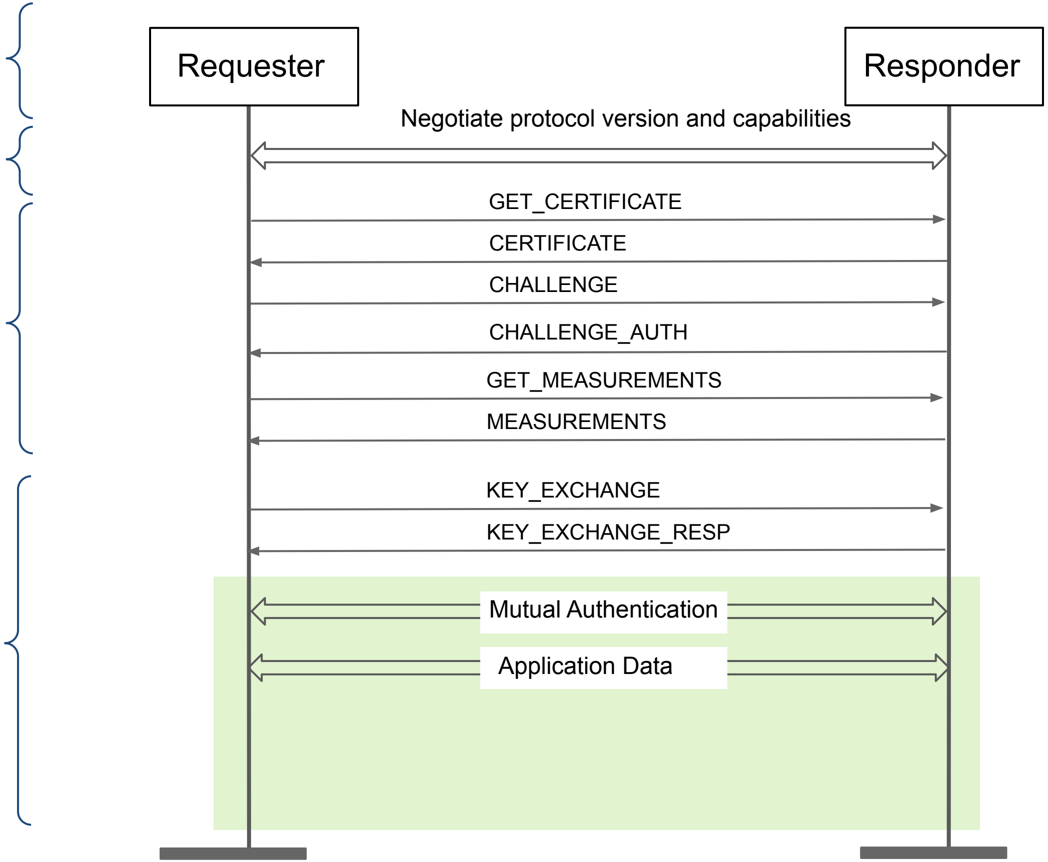
VCA: Version-Capabilities-Algorithms

Options

Sessions



Overview of SPDM



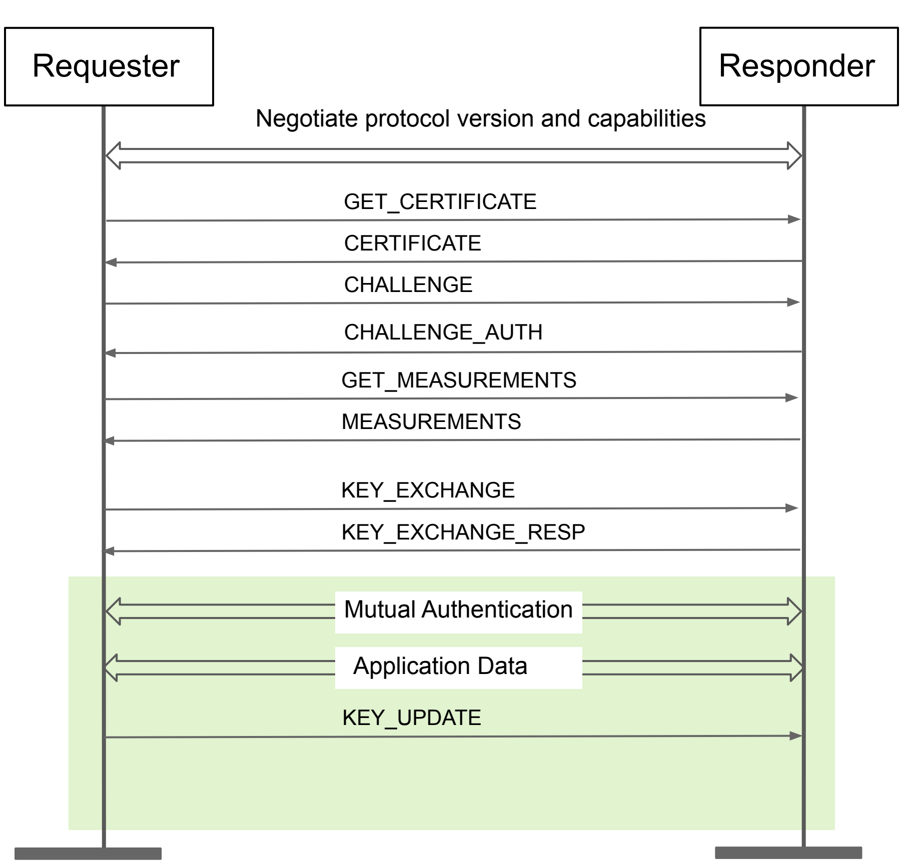
Overview of SPDM

Device Initialization

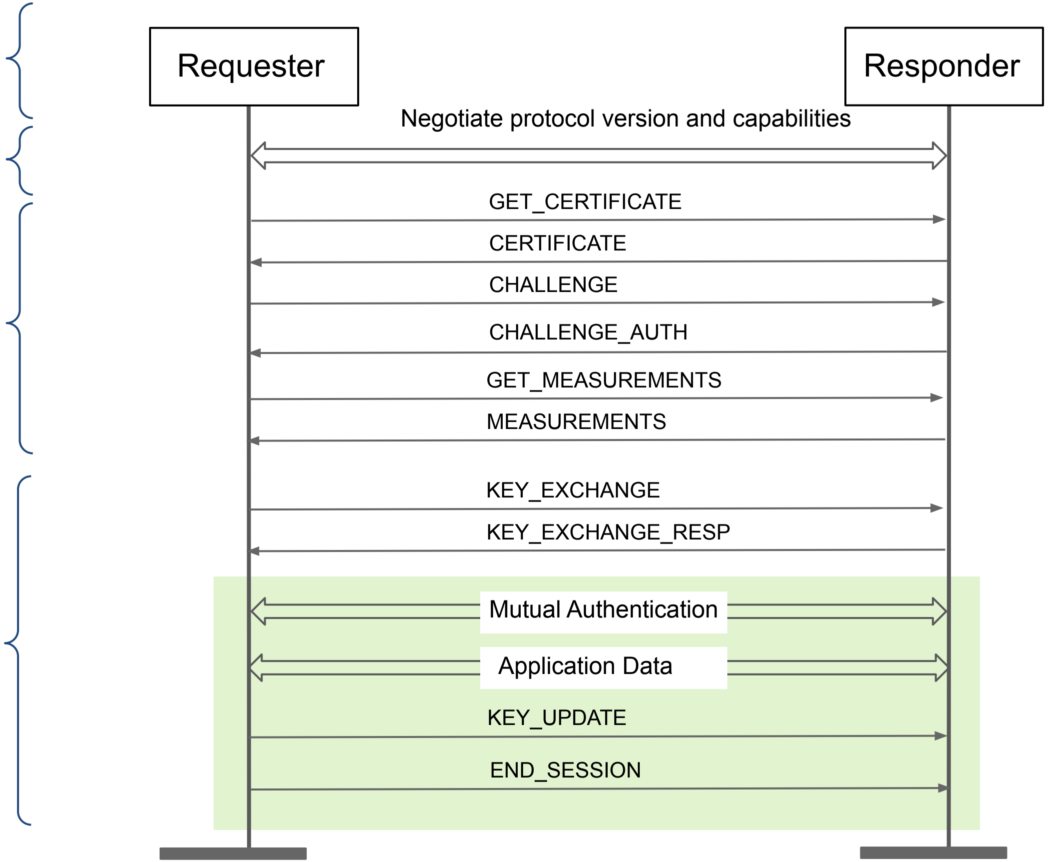
VCA: Version-Capabilities-Algorithms

Options

Sessions



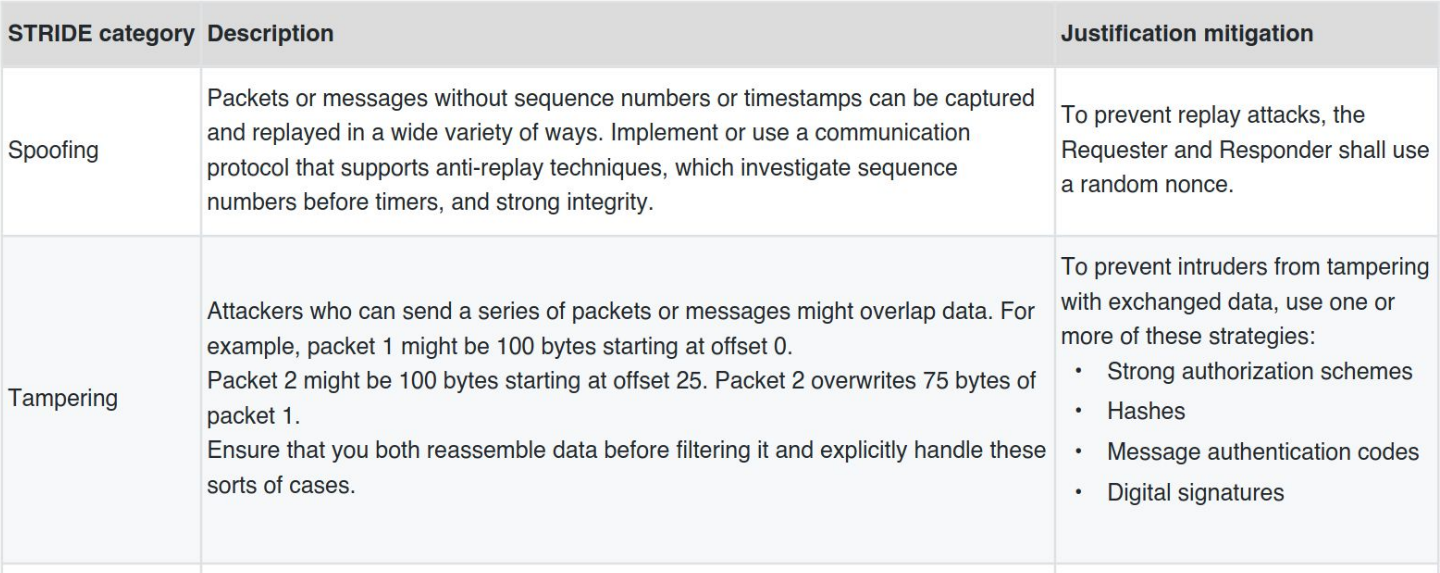
Overview of SPDM



Informal Security Goals for SPDM

SPDM does not have any formal analysis so far

- DMTF provides only a 3-page high-level STRIDE analysis



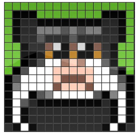
STRIDE category	Description	Justification mitigation
Spoofing	Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or use a communication protocol that supports anti-replay techniques, which investigate sequence numbers before timers, and strong integrity.	To prevent replay attacks, the Requester and Responder shall use a random nonce.
Tampering	Attackers who can send a series of packets or messages might overlap data. For example, packet 1 might be 100 bytes starting at offset 0. Packet 2 might be 100 bytes starting at offset 25. Packet 2 overwrites 75 bytes of packet 1. Ensure that you both reassemble data before filtering it and explicitly handle these sorts of cases.	To prevent intruders from tampering with exchanged data, use one or more of these strategies: • Strong authorization schemes • Hashes • Message authentication codes • Digital signatures

Formal Analysis using the Tamarin Prover

Created 4 models of the SPDM modes:

- Device Attestation
    - Device Initialization + VCA + Options
- 3 Key Exchange modes
    - Device Initialization + VCA + (single mode) Sessions

Formal Analysis using the Tamarin Prover



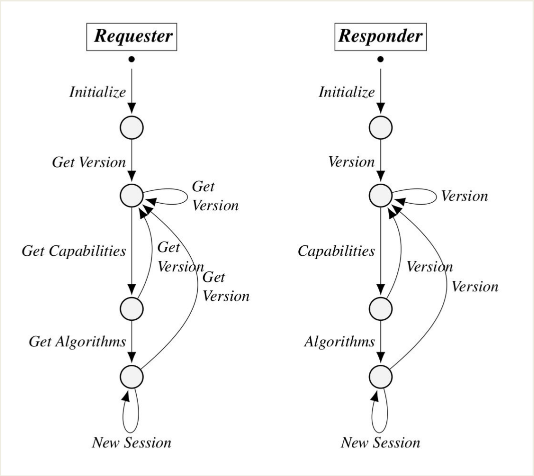
Created 4 models of the SPDM modes:

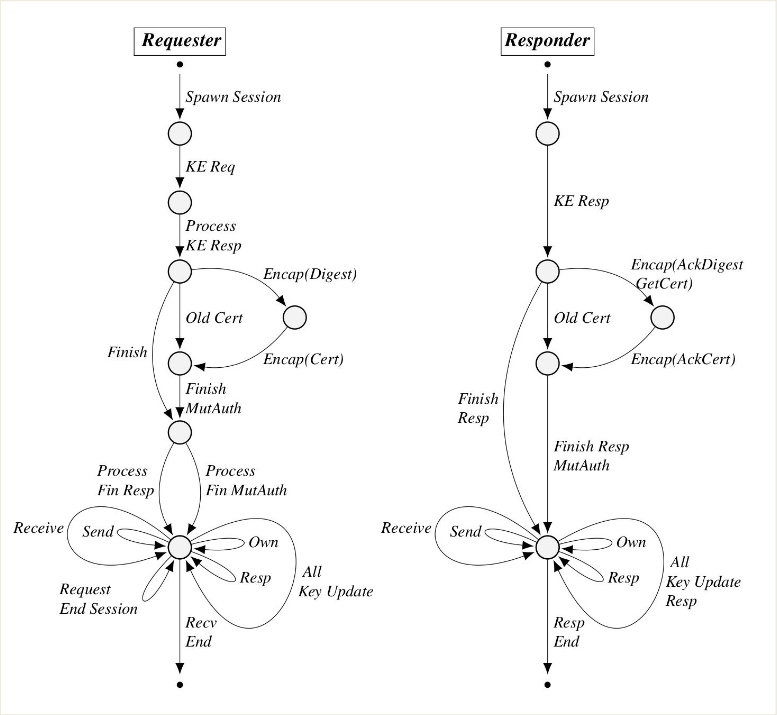
- Device Attestation
  - Device Initialization + VCA + Options
- 3 Key Exchange modes
  - Device Initialization + VCA + (single mode) Sessions

3 Threat Models:

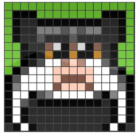
- Attacker-controlled Network
- + Malicious Certificates
- + Compromised Session key

Formal Analysis using the Tamarin Prover



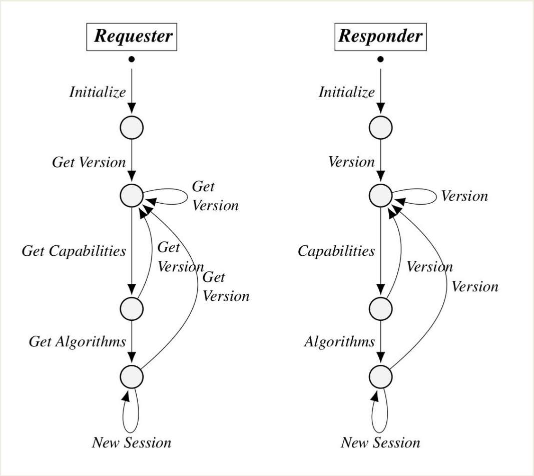


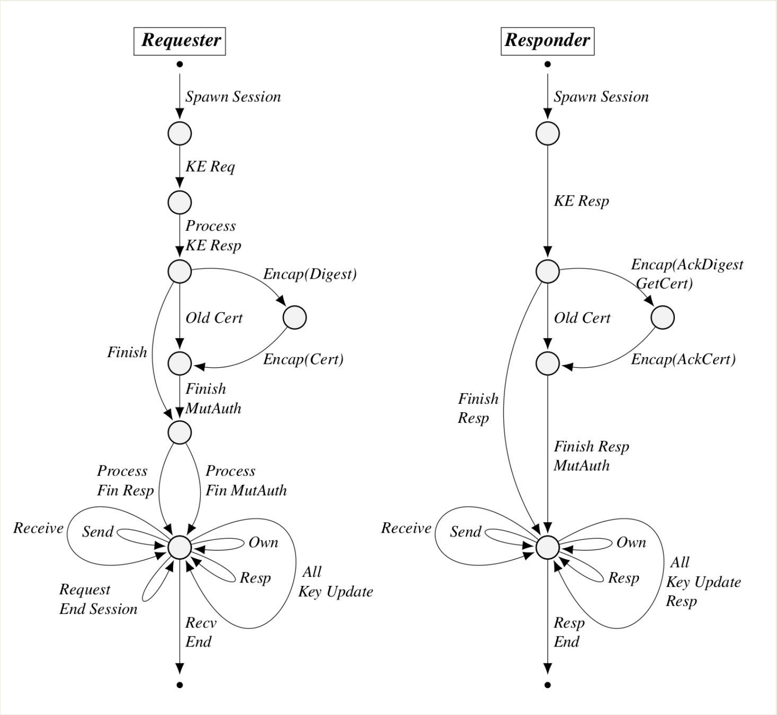
Formal Analysis using the Tamarin Prover



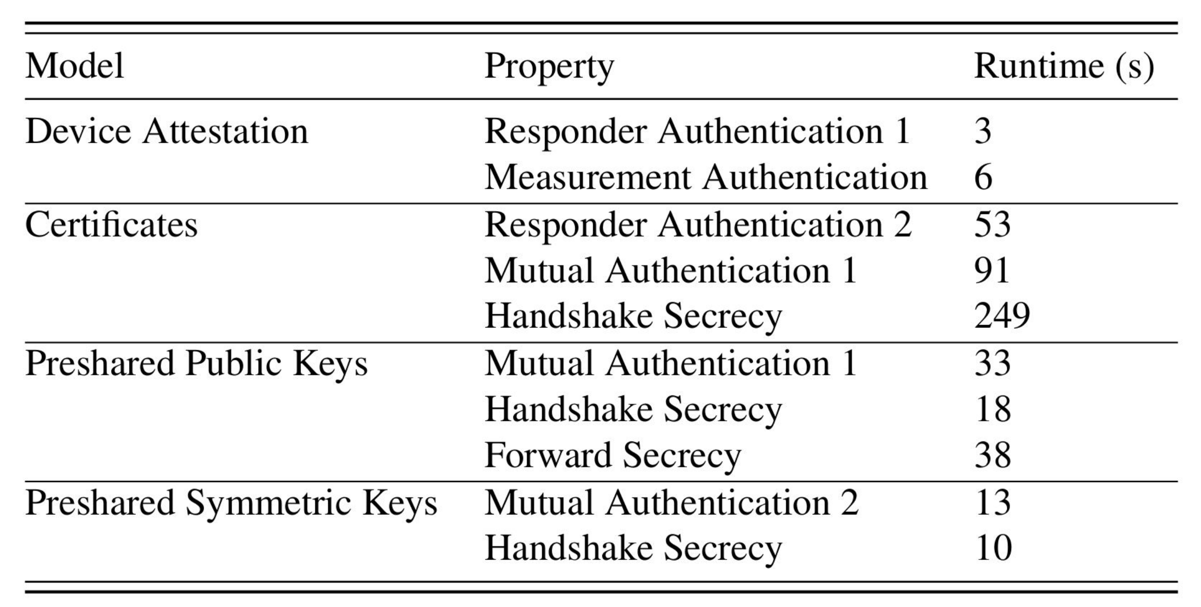
Analysis Effort:

- Models range between ~1000 and ~1800 LoC
- 54 sanity traces & 6 helper lemmas
- 5 core security guarantees
- 6-7 person month of work





Security Properties and Results



Model	Property	Runtime (s)
Device Attestation	Responder Authentication 1	3
	Measurement Authentication	6
Certificates	Responder Authentication 2	53
	Mutual Authentication 1	91
	Handshake Secrecy	249
Preshared Public Keys	Mutual Authentication 1	33
	Handshake Secrecy	18
	Forward Secrecy	38
Preshared Symmetric Keys	Mutual Authentication 2	13
	Handshake Secrecy	10

Potential Design Pitfalls

Identified several potential design pitfalls:

- Session ID size and optional responder nonce

Potential Design Pitfalls

Identified several potential design pitfalls:

- Session ID size and optional responder nonce
- No restrictions on vendor-defined request/response

Potential Design Pitfalls

Identified several potential design pitfalls:

- Session ID size and optional responder nonce
- No restrictions on vendor-defined request/response
- No policy for remotely setting certificates

Potential Design Pitfalls

Identified several potential design pitfalls:

- Session ID size and optional responder nonce
- No restrictions on vendor-defined request/response
- No policy for remotely setting certificates
- Device reset may lead to counter reuse
- Authentication of keys versus device authentication
- Setting certificates

Formal Analysis of SPDM:
Security Protocol and Data Model 1.2

Standard under development and supported by major IT industry players

- First formal analysis of the standard’s modes
- Proved main security properties for individual modes

Identified potential design pitfalls

Future work

- Analysis on the full composition needed
- Not included underspecified functionalities

Aurora Naska: aurora.naska@cispa.de

Artifact: https://github.com/AnalysisSPDM/FormalModel

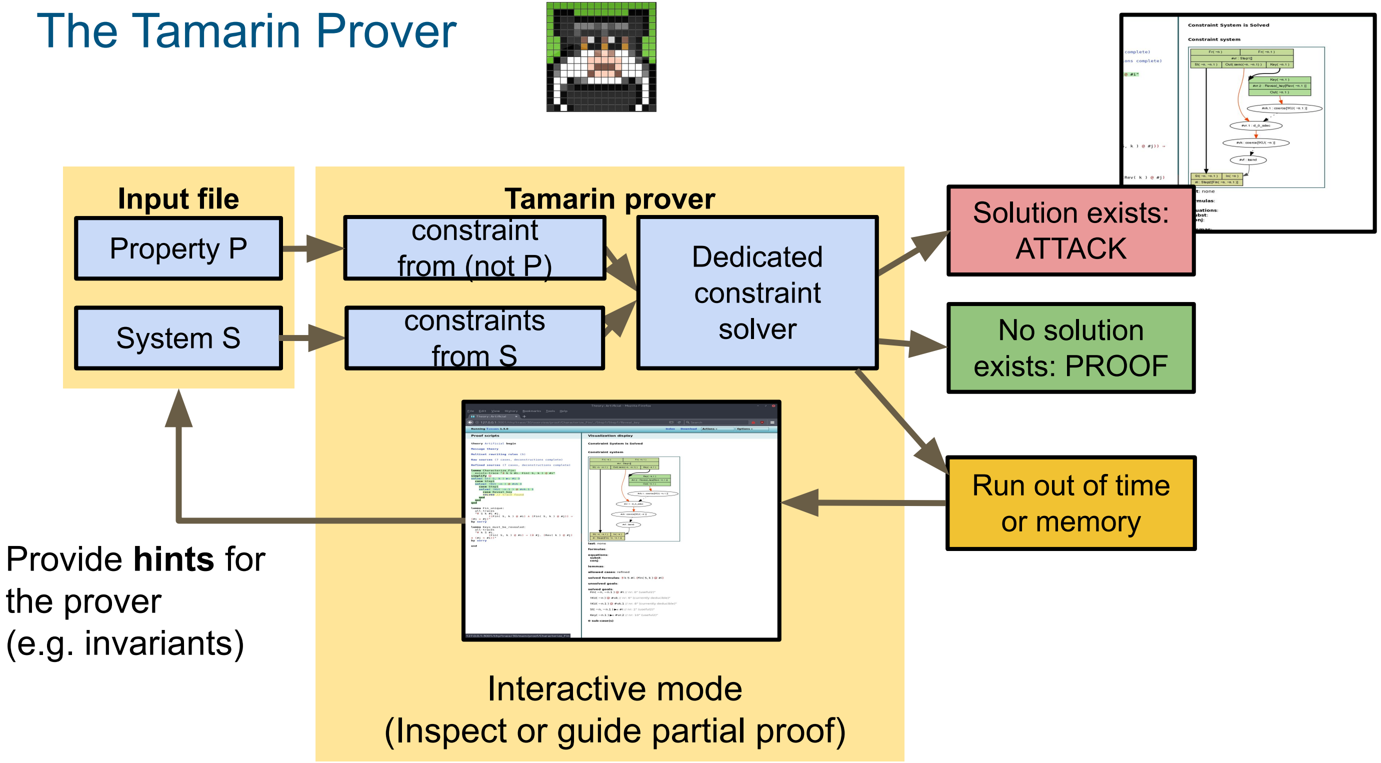
ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Additional Slides

The Tamarin Prover



Input file

Property P

System S

Tamarin prover

constraint from (not P)

constraints from S

Dedicated constraint solver

Constraint System is Solved

Constraint system

Solution exists: ATTACK

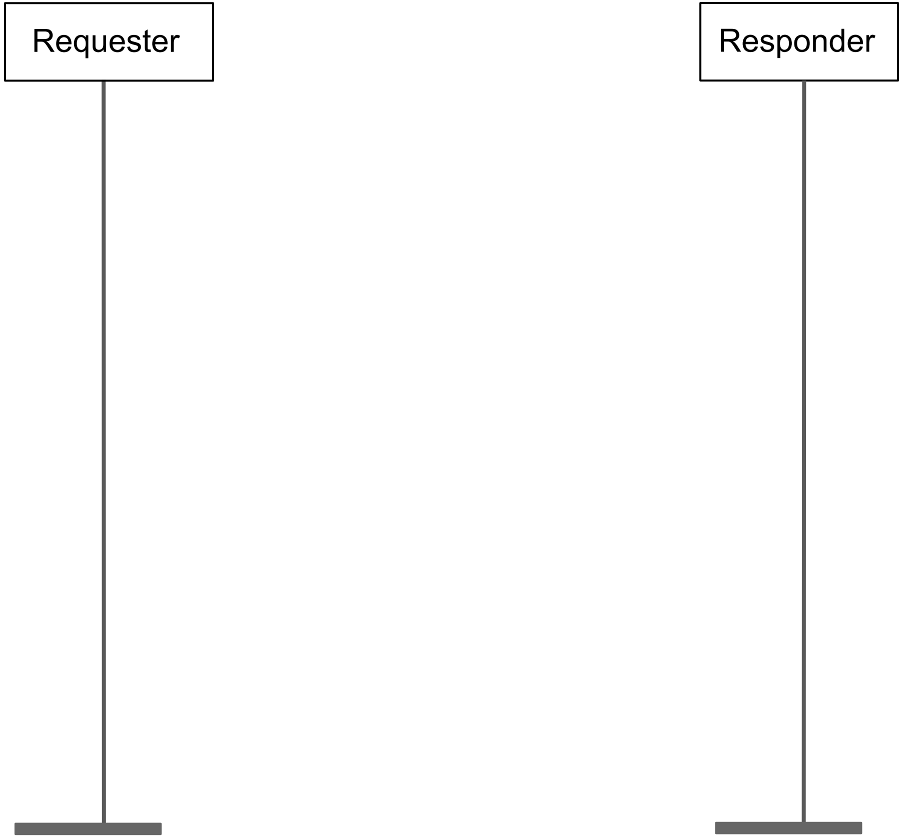
No solution exists: PROOF

Run out of time or memory

Provide **hints** for the prover (e.g. invariants)

Interactive mode (Inspect or guide partial proof)

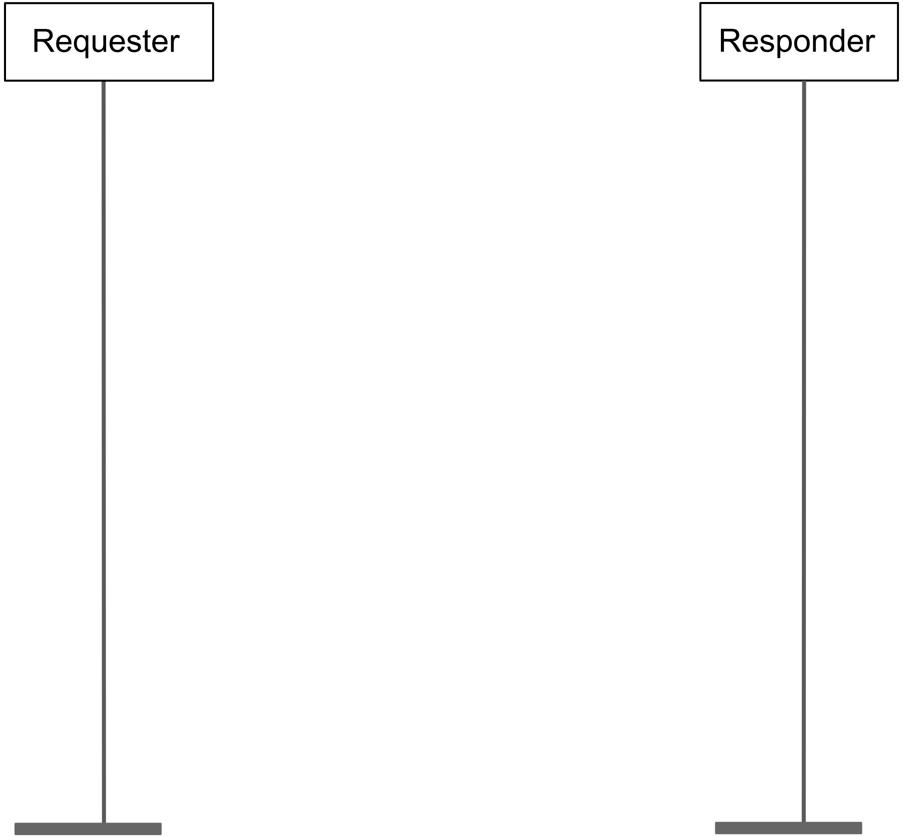
Overview of SPDM



Overview of SPDM

SPDM protocol is divided in 4 phases:

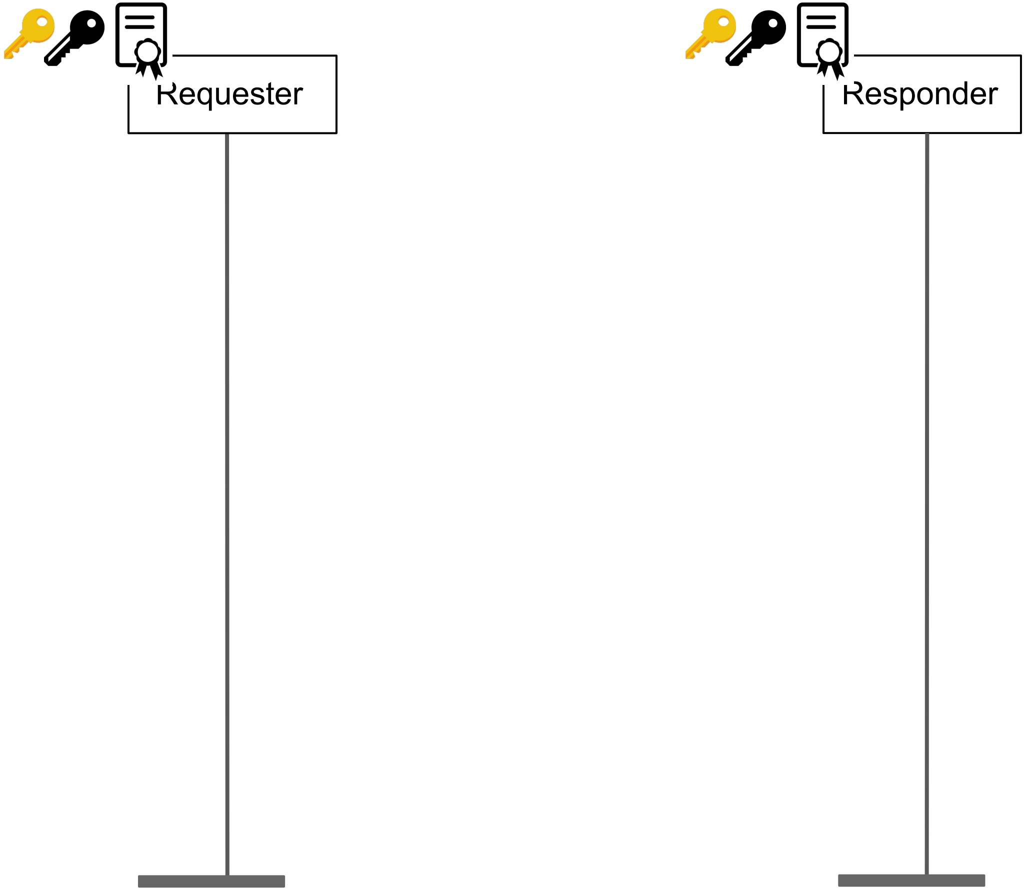
- Device Initialization



Overview of SPDM

SPDM protocol is divided in 4 phases:

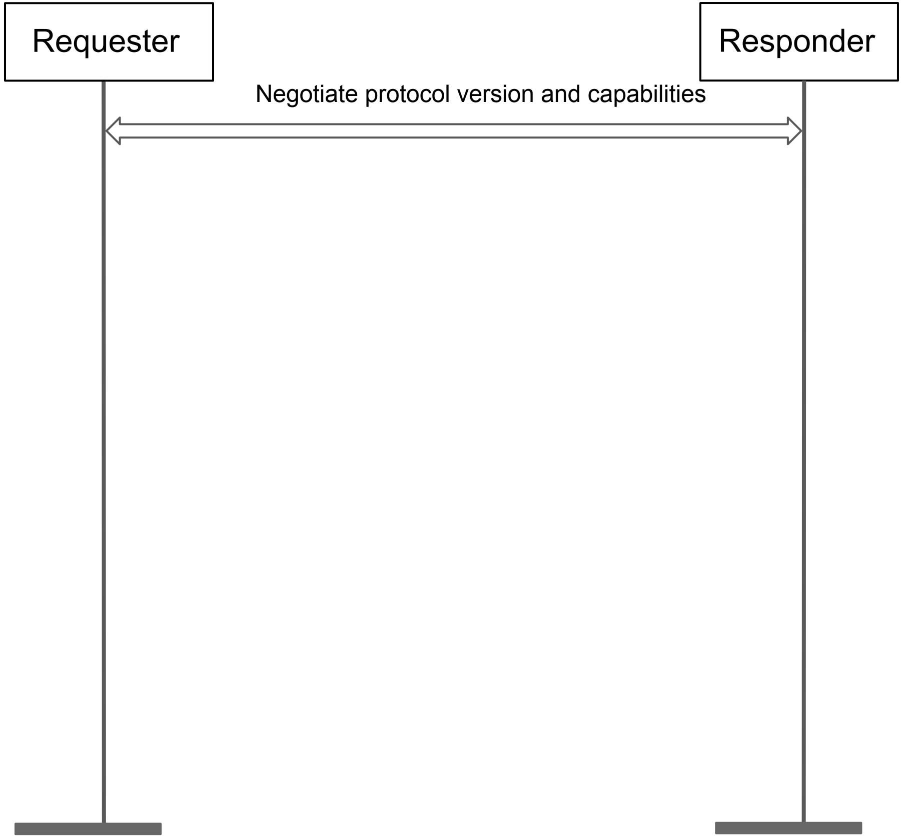
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys



Overview of SPDM

SPDM protocol is divided in 4 phases:

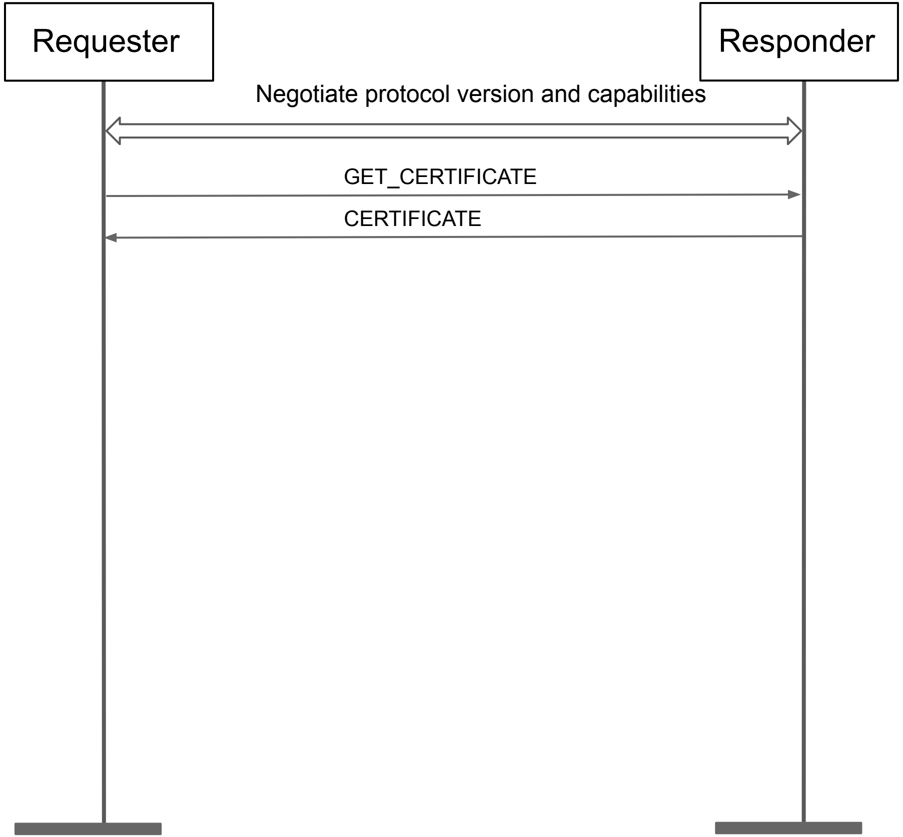
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms



Overview of SPDM

SPDM protocol is divided in 4 phases:

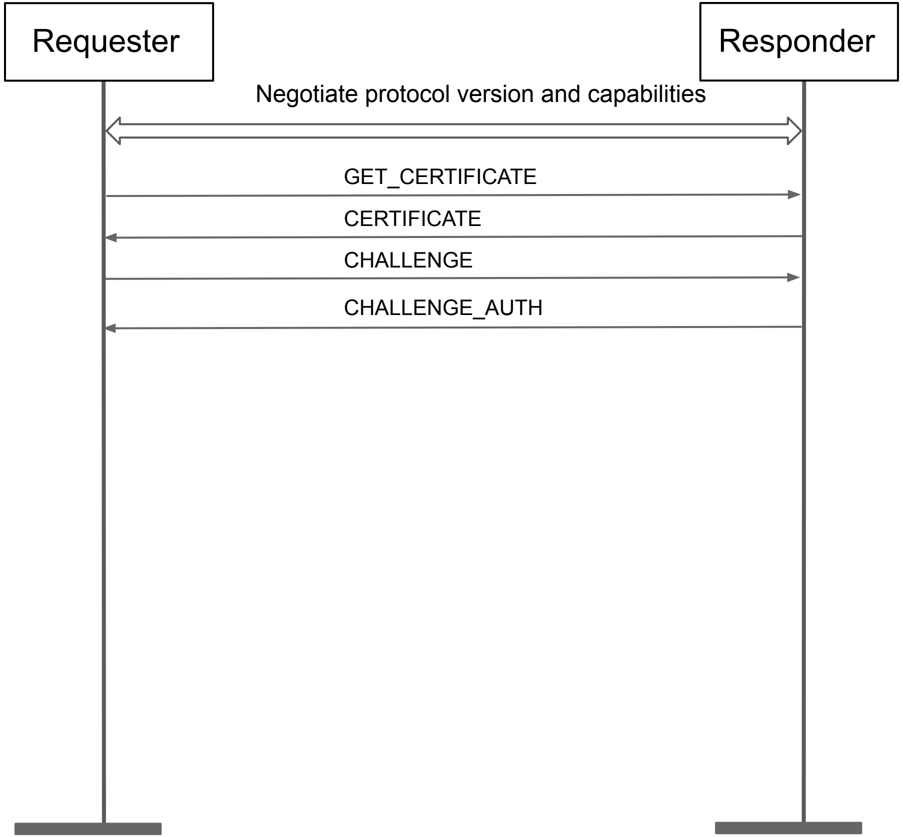
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options



Overview of SPDM

SPDM protocol is divided in 4 phases:

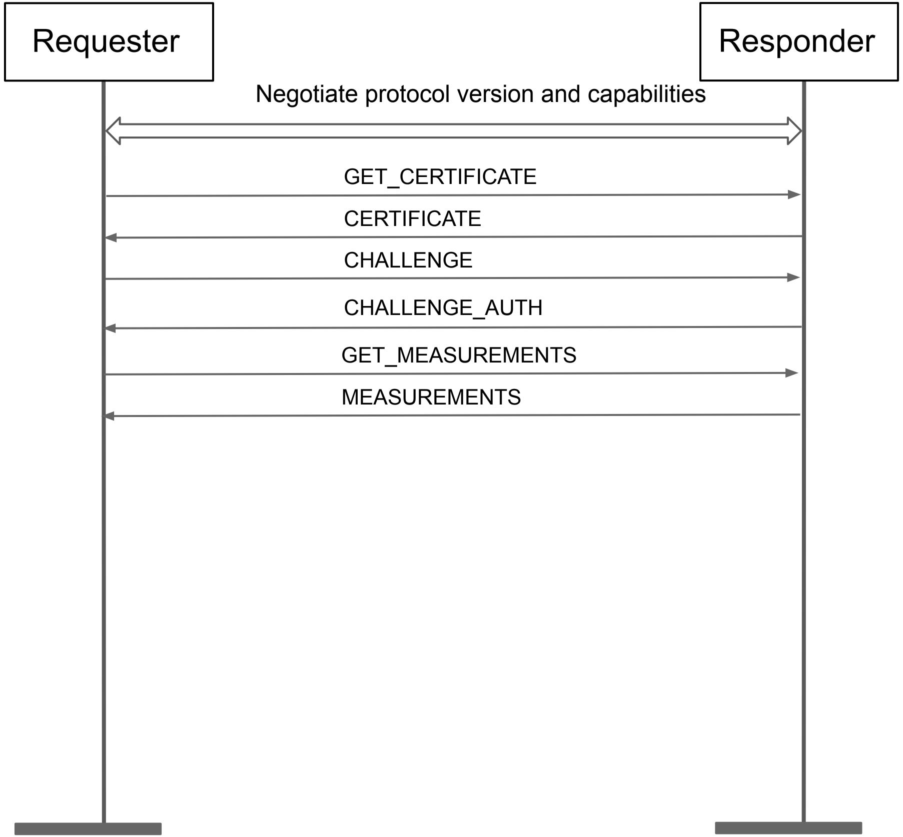
- Device Initialization
    - Certificates
    - Preshared Symmetric Keys
    - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options



Overview of SPDM

SPDM protocol is divided in 4 phases:

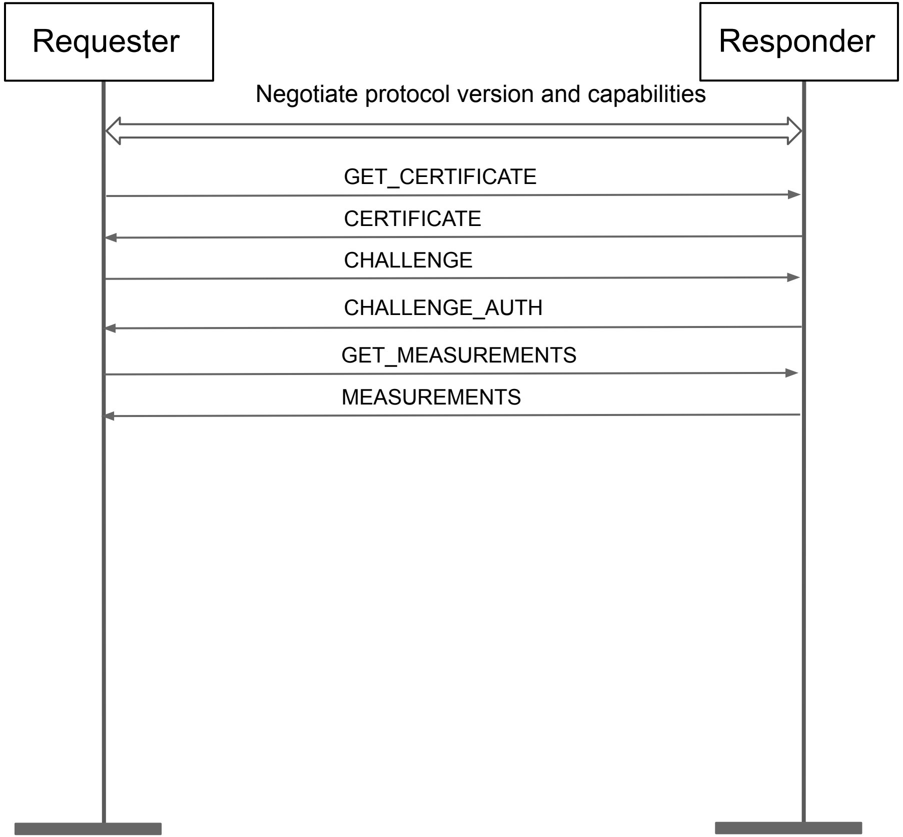
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options



Overview of SPDM

SPDM protocol is divided in 4 phases:

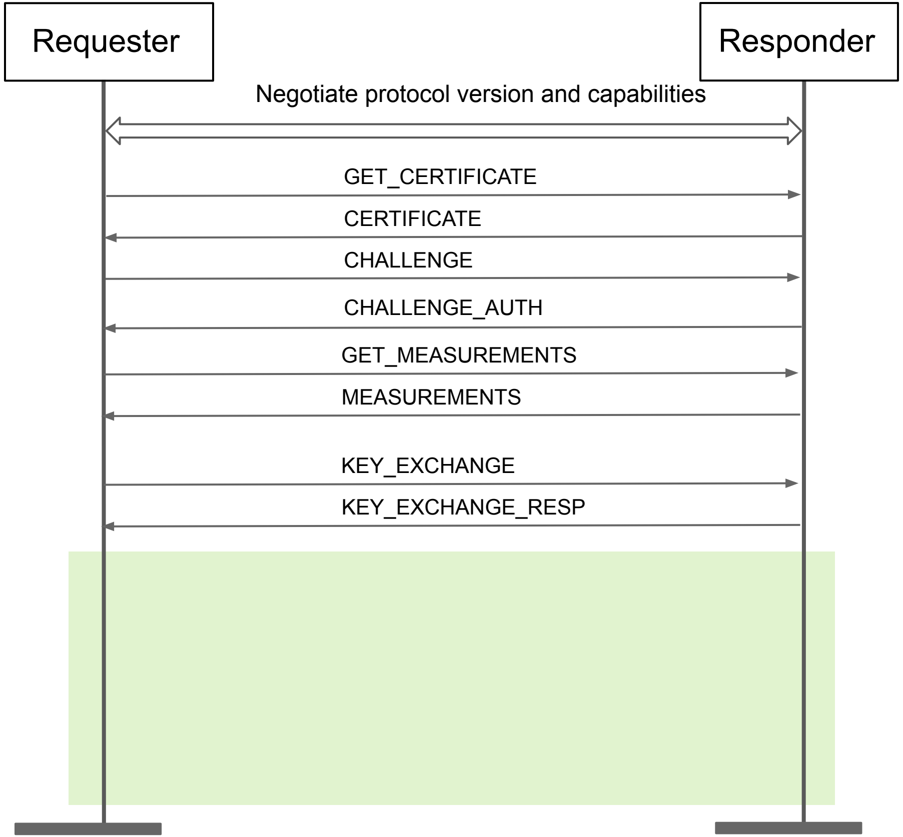
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions



Overview of SPDM

SPDM protocol is divided in 4 phases:

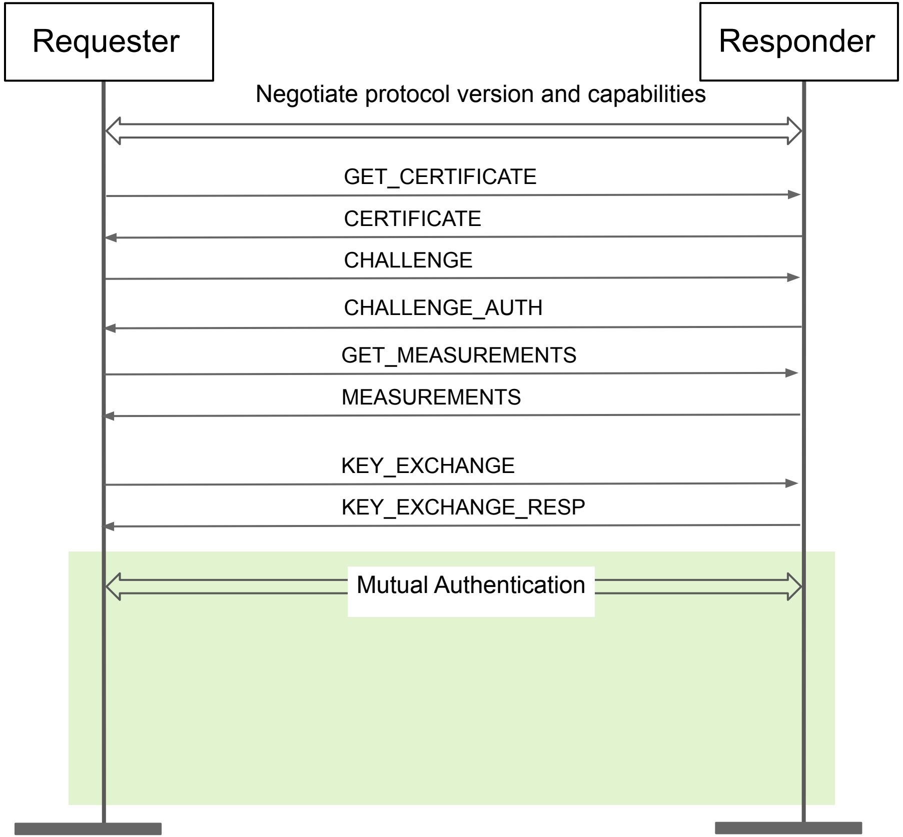
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
  - Key Exchange in three modes



Overview of SPDM

SPDM protocol is divided in 4 phases:

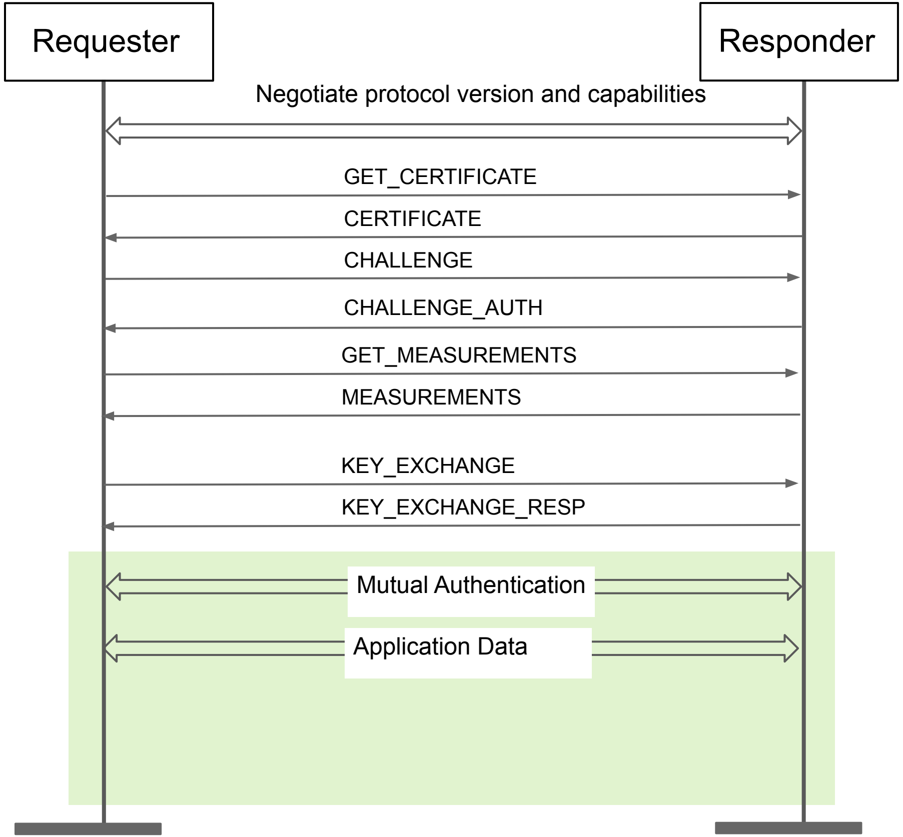
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
  - Key Exchange in three modes



Overview of SPDM

SPDM protocol is divided in 4 phases:

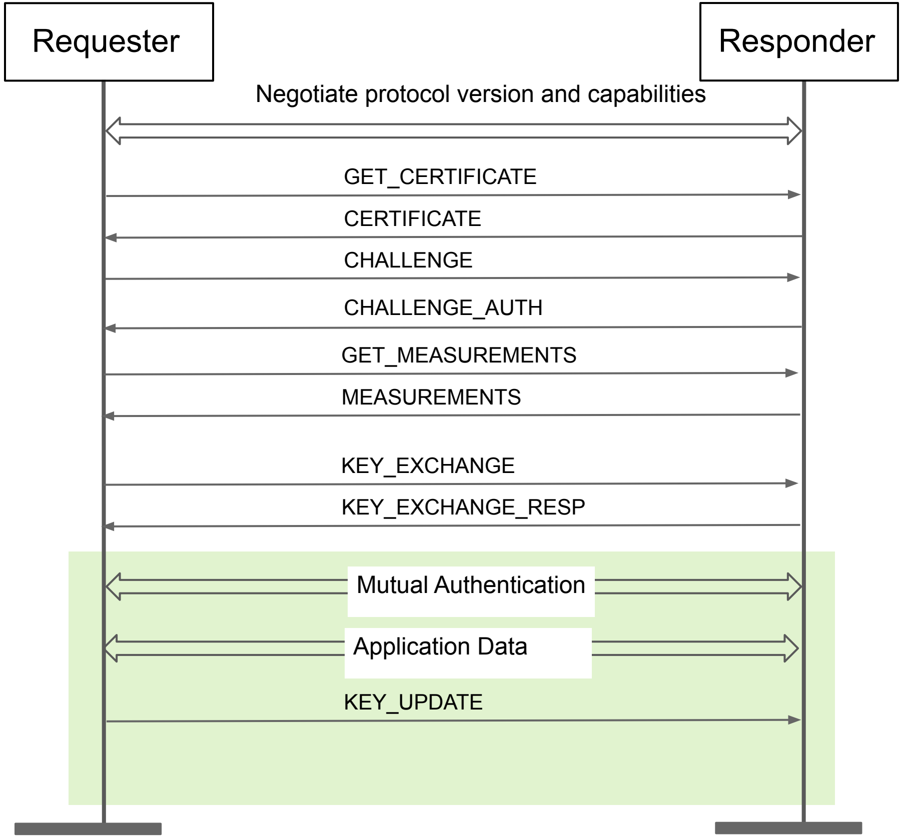
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
  - Key Exchange in three modes
  - App Data Messages



Overview of SPDM

SPDM protocol is divided in 4 phases:

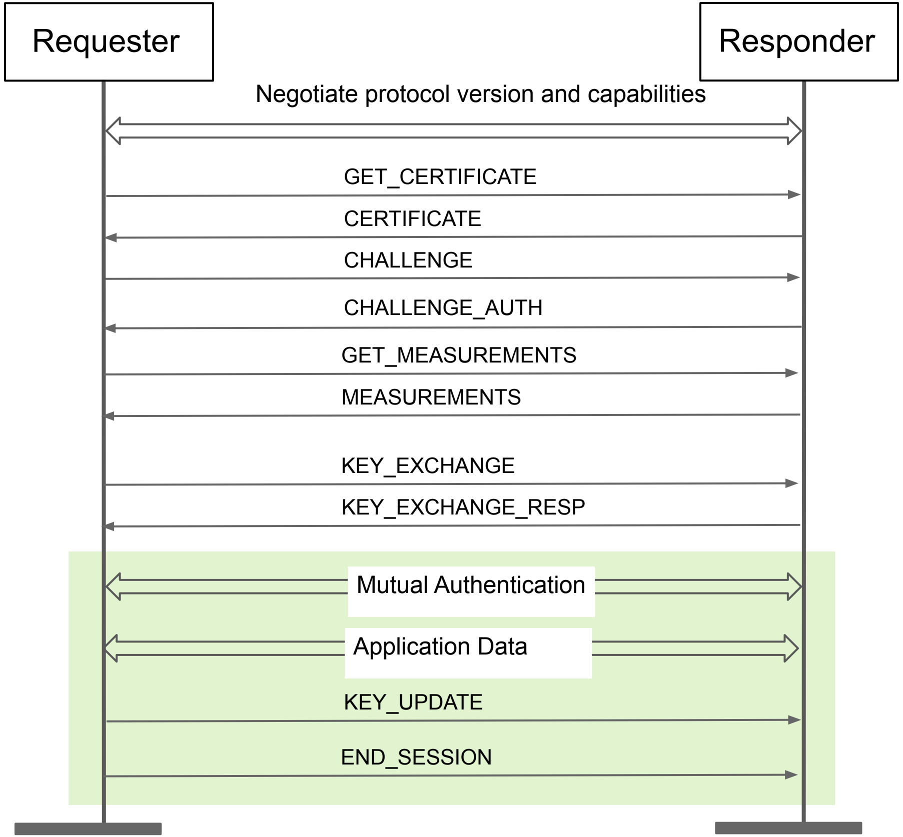
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
  - Key Exchange in three modes
  - App Data Messages
  - Key Update



Overview of SPDM

SPDM protocol is divided in 4 phases:

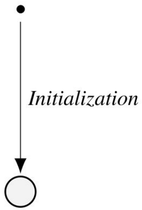
- Device Initialization
  - Certificates
  - Preshared Symmetric Keys
  - Preshared Public Keys
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
  - Key Exchange in three modes
  - App Data Messages
  - Key Update
  - Terminate Session



Overview of SPDM

SPDM protocol is divided in 4 phases:

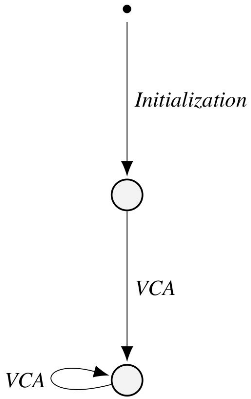
- Device Initialization



Overview of SPDM

Protocol divided in 4 phases:

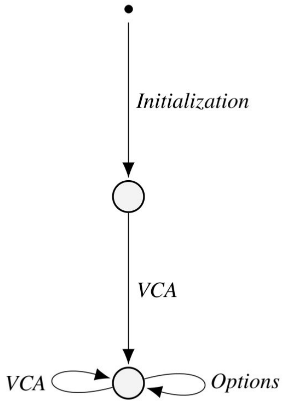
- Device Initialization
- VCA Version-Capabilities-Algorithms



Overview of SPDM

Protocol divided in 4 phases:

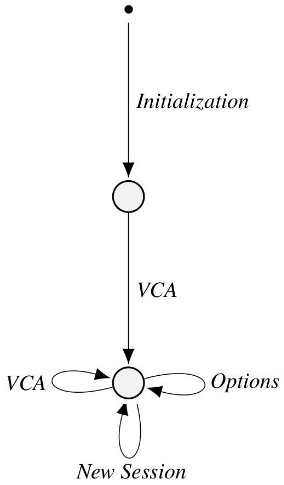
- Device Initialization
- VCA Version-Capabilities-Algorithms
- Options



Overview of SPDM

Protocol divided in 4 phases:

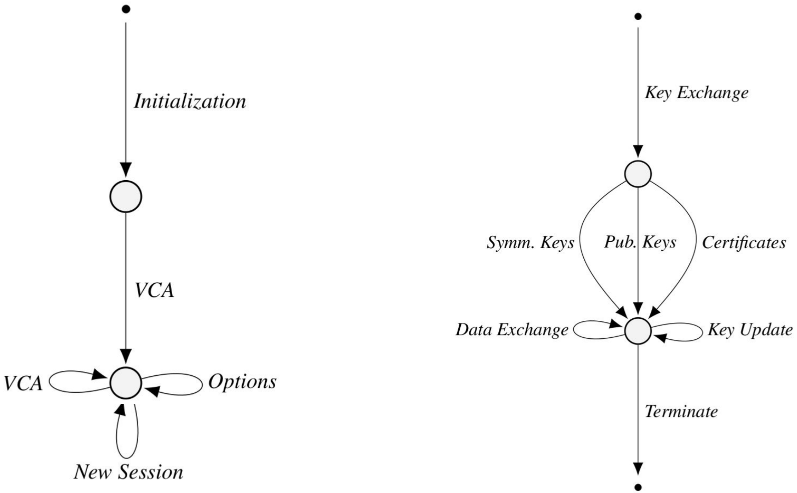
- Device Initialization
- VCA Version-Capabilities-Algorithms
- Options
- Sessions



Overview of SPDM

Protocol divided in 4 phases:

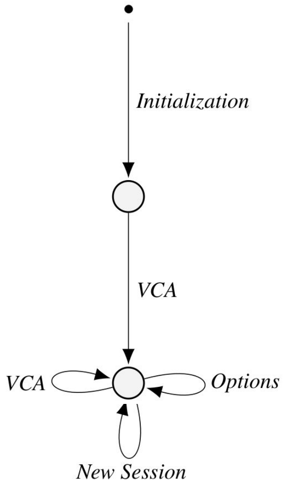
- Device Initialization
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
    - Key Exchange in three modes
    - App Data Messages
    - Key Update
    - Terminate Session

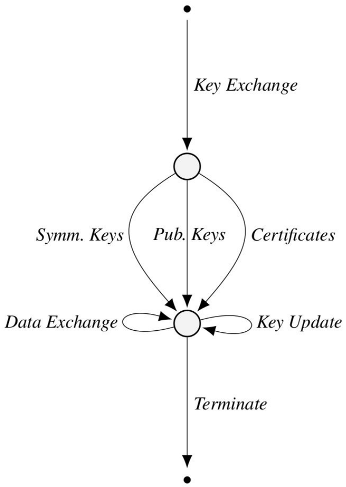


Overview of SPDM

Protocol divided in 4 phases:

- Device Initialization
- VCA Version-Capabilities-Algorithms
- Options
- Sessions
    - Key Exchange in three modes
    - App Data Messages
    - Key Update
    - Terminate Session





No security analysis of the protocol !