mipi® DEVCON
MIPI ALLIANCE DEVELOPERS CONFERENCE

28-29 SEPTEMBER 2021

Phil Hawkes, Rick Wietfeldt
Qualcomm Inc.
Security Working Group Co-Chairs

MIPI Security for Automotive & IoT – Initial Focus on MASS

Overview

- MIPI Data Security Services
  - Mitigate attacks on image data, control messages, IoT debug messages
- Flexible MIPI Security Framework
  - System Security Mgmt (SSM) Suite establishes Data Security Services
- Security for MIPI Automotive SerDes Solutions (MASS)
  - Overlays MIPI Security Framework on the 1-5 Automotive Model
  - SSM Suite: leverages DMTF security protocols
  - Data Security Services for MIPI CSI-2^{SM}, MIPI DSI-2^{SM}, VESA eDP/DP, MIPI CCI^{SM} and MIPI A-PHY^{SM} control
- Status

DMTF: Distributed Management Task Force

MIPI Automotive SerDes Solution (MASS) in the car

Electronic Control Unit (ECU)

- Advanced driver assistance system (ADAS) based on sensor feeds
- Produces display feeds

Sensors

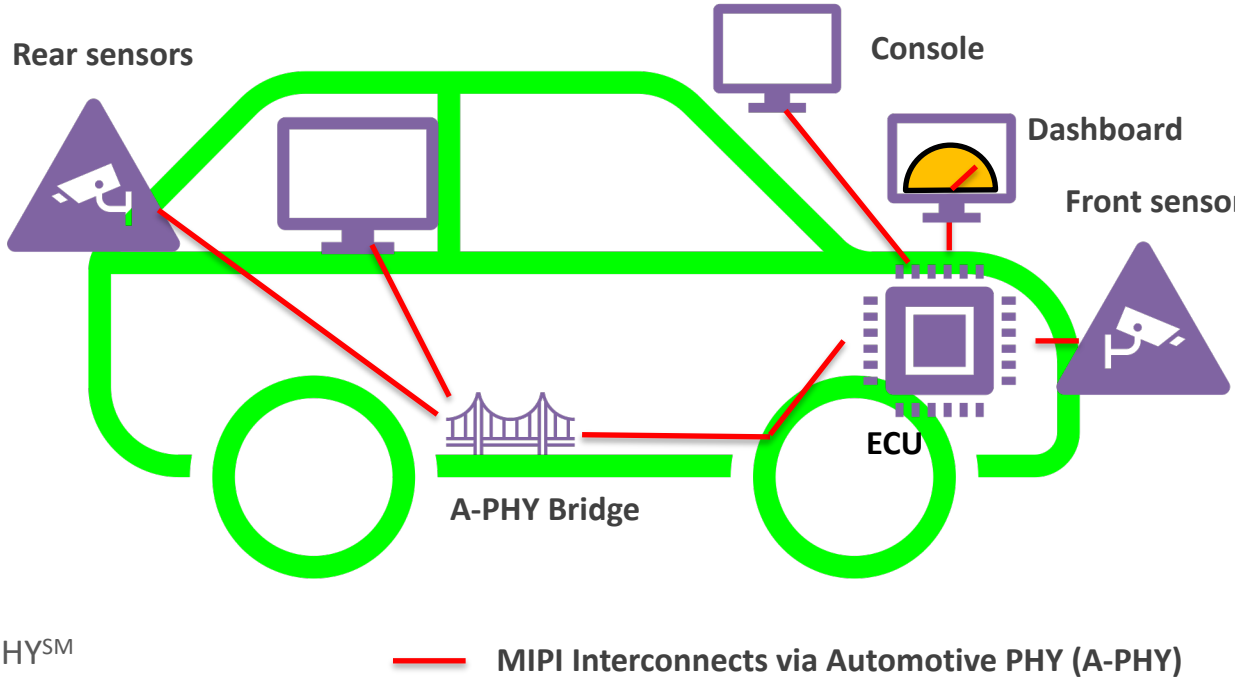
- Camera
- Radar, Lidar

Displays

- Dashboard
- Console
- Side view mirrors
- Entertainment

(Opt) A-PHY Bridges

- Translates between short-range MIPI C-PHY℠/ D-PHY℠ & long-range MIPI A-PHY℠



Security Concepts 101

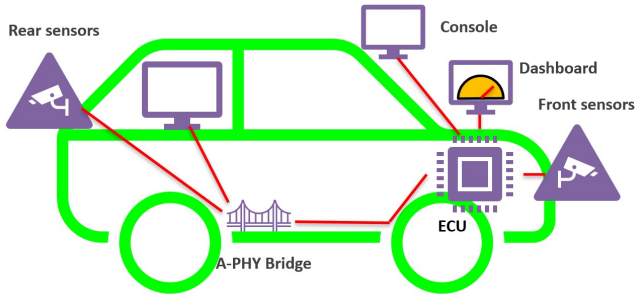
- **Authentication** establishes trust
  - Securely identifying a component
  - Mutual authentication – two components authenticate each other
- Once trust is established, then address
  - **Integrity**
    - Being sure that information came from the expected source and is unaltered
    - Provided by Message Authentication Code (MAC)
  - **Confidentiality**
    - Protecting information against unauthorized access
    - Provided by encrypting messages

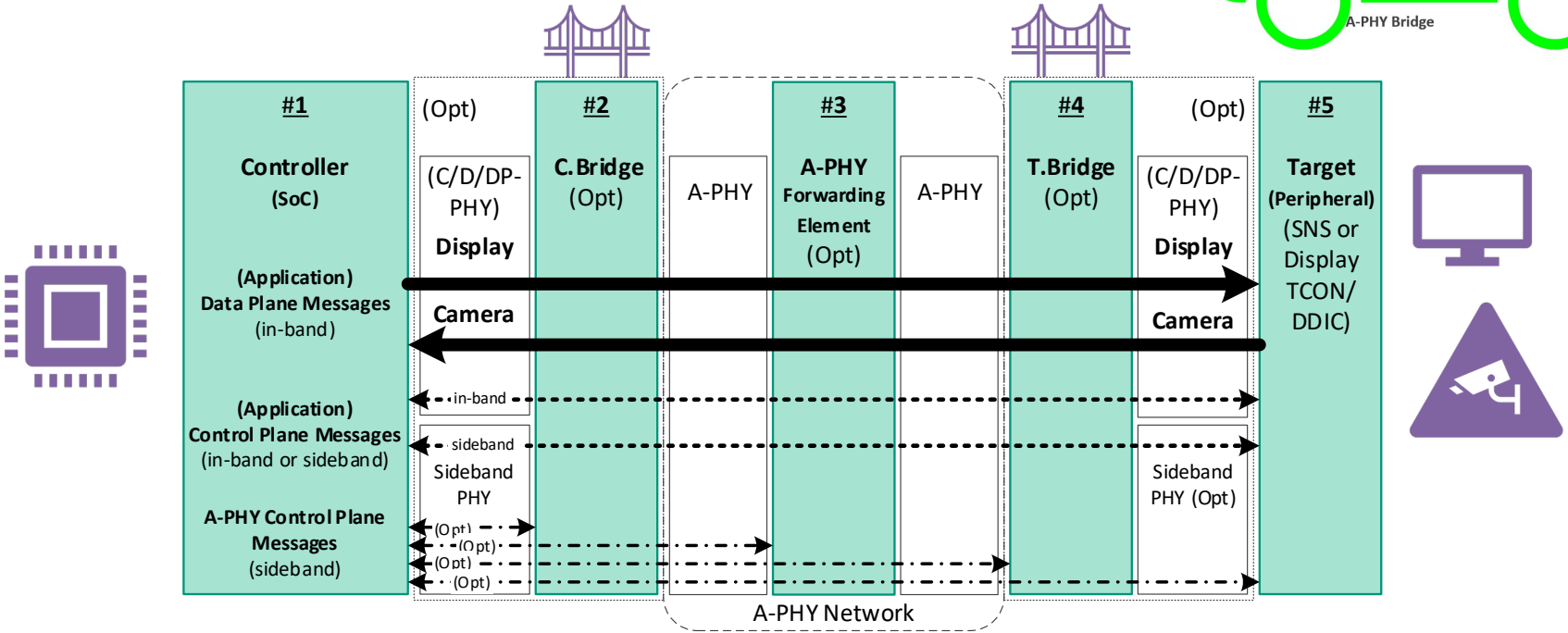
What are the Data Security Services protecting?

	Security Considerations
• Image Data	
– Integrity of Sensor images	Manipulating ADAS
– Confidentiality of Sensor images	Privacy: location-revealing images
– Integrity of Display images	Incorrect dashboard display
• Control Data	
– Integrity of Sensors Capabilities/config	Disable/manipulate sensor
– Integrity of Display Capabilities/config	Disable/manipulate display
– Integrity of A-PHY Capabilities/config	Disrupt A-PHY network
– Confidentiality of all config	Proprietary/sensitive/privacy
• IoT Debug Data	
– Integrity of read/write config	Disable/manipulate component
– Confidentiality of proprietary data	Proprietary/sensitive/privacy
– *Not discussed further in this presentation. Will leverage some of MIPI security framework*	

MASS 1-5 Model & MIPI Protocols

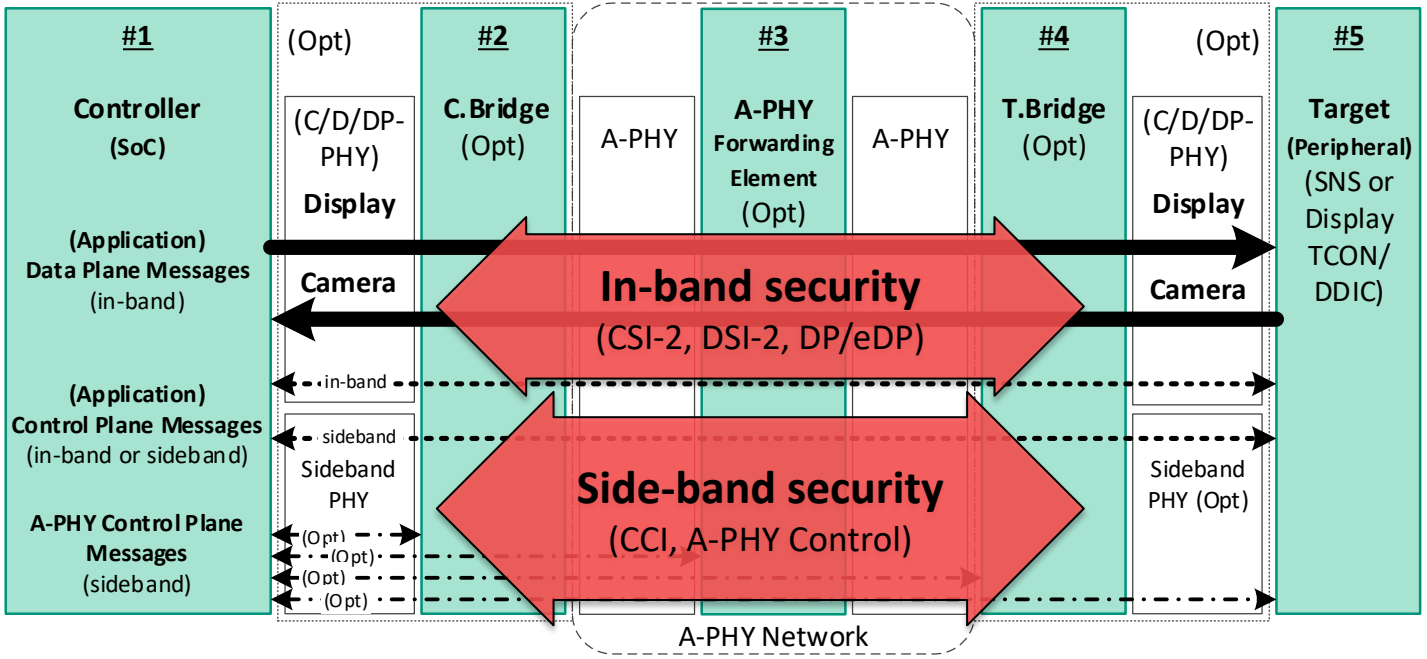
Controller ~ SoC ; Target is either Camera sensor or Display





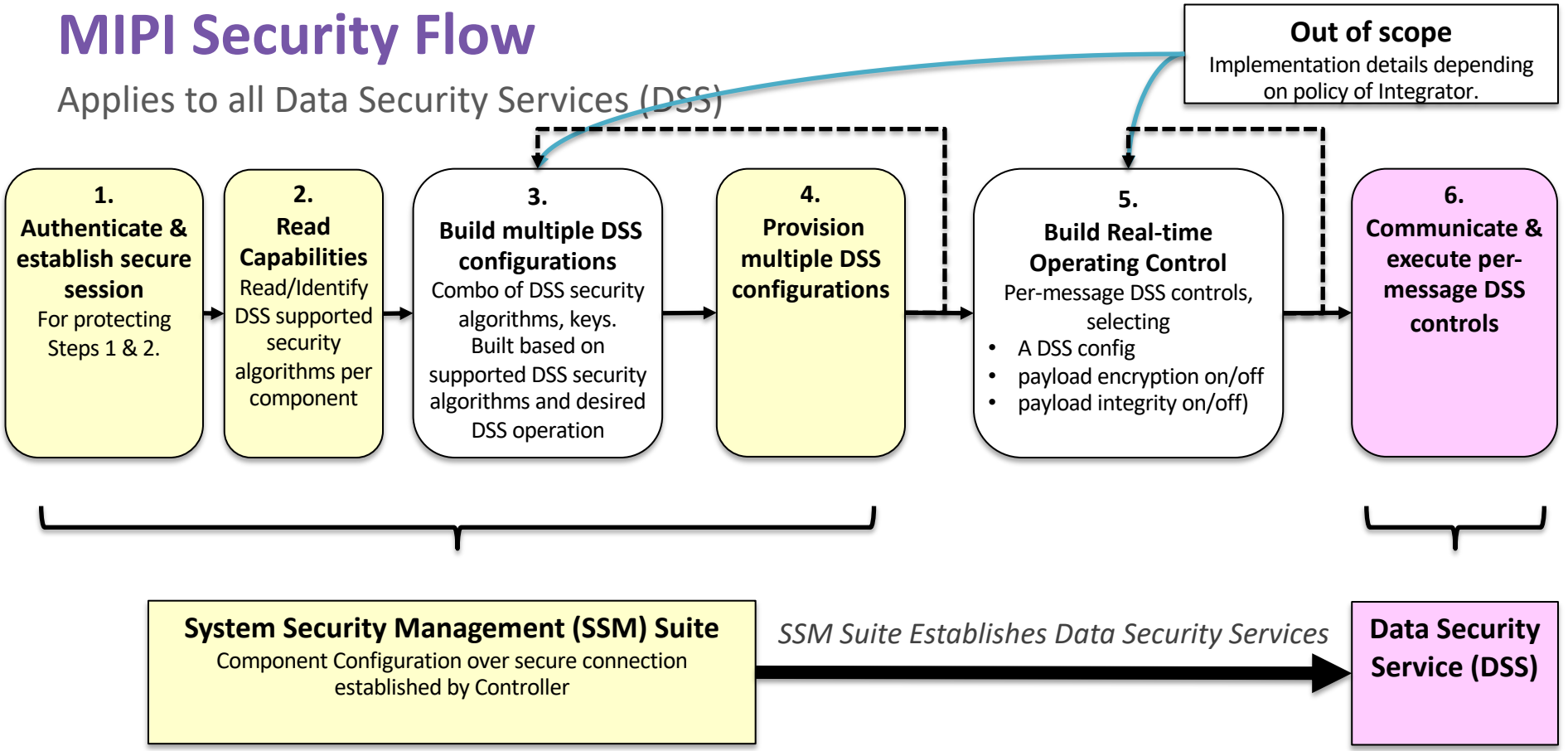
Data Security Services

In-band security and side-band security

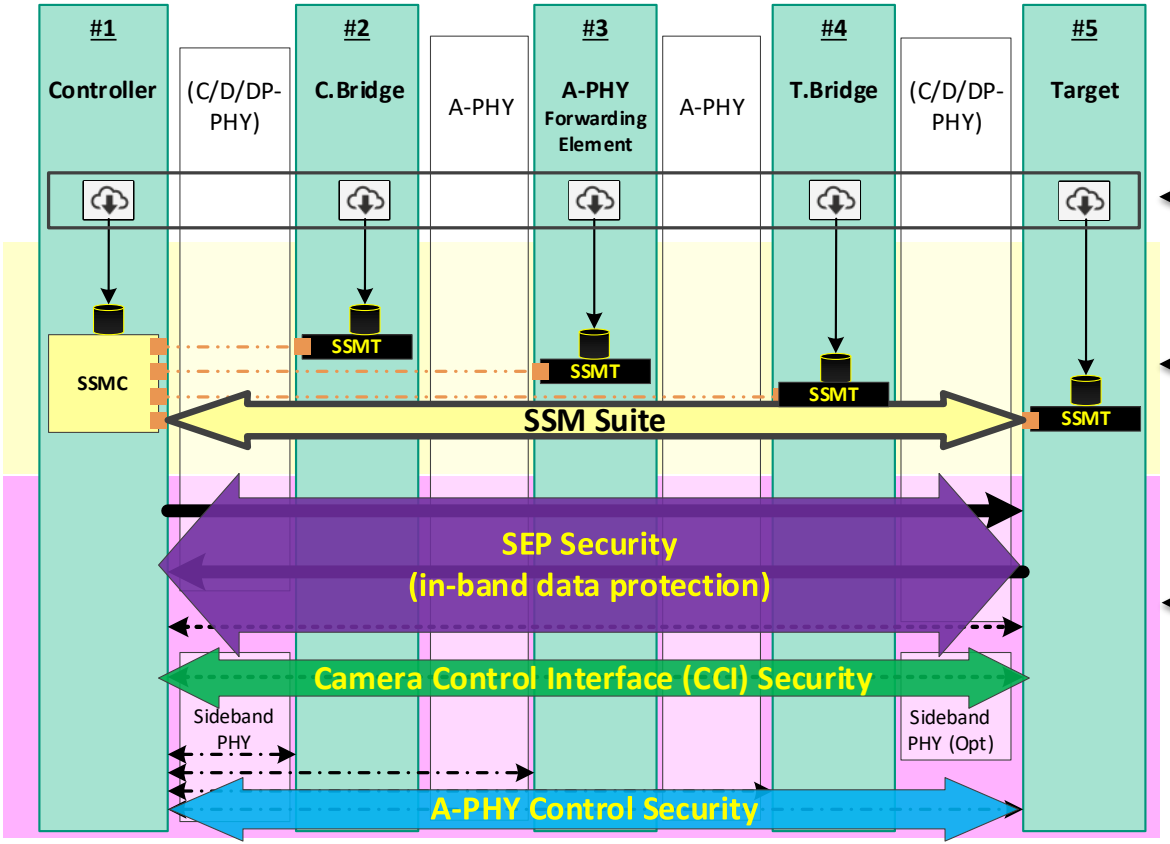


MIPI Security Flow

Applies to all Data Security Services (DSS)



MIPI Security Framework



0. (Out of scope) Integrator provisions authentication credentials

System Security Management (SSM) Suite.
SSMC = SSM Controller (in #1)
SSMT = SSM Target (in #2/3/4/5)

1. Authenticate & establish secure session
   DMTF protocols (DSP0274, DSP0277)
2. Read support security algorithms
3. *(Out of scope) Build DSS config*
4. Write DSS config
5. *(Out of scope) Build real time operating control*

6. Apply Data Security Services

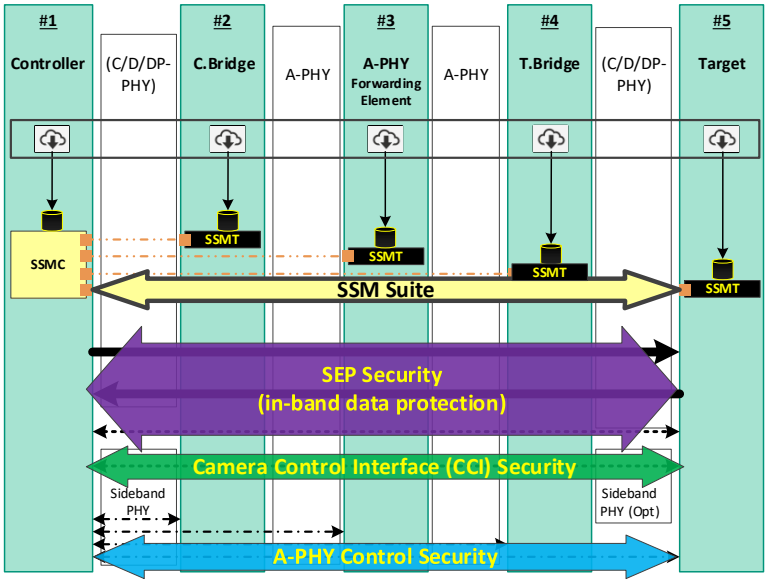
This can be applied directly from Controller #1 to Target #5 over any MIPI PHY – does not require presence of A-PHY

System Security Management (SSM) Suite

Set of protocols between Controller #1 and other Components (#2-#5)

- DMTF's SPDM (DSP0274) performs symmetric or asymmetric mutual authentication to establish secure session
- DMTF's Secured Messages (DSP0277) protects MIPI SACP
  - Encryption and integrity protection
- MIPI's Service Association Configuration Protocol (SACP)
  - Read Security Capability Registers for Data Security Services
  - Write Security SA Registers for Data Security Services

MIPI's SSM Suite is defined in MIPI Security Specification



DMTF: Distributed Management Task Force

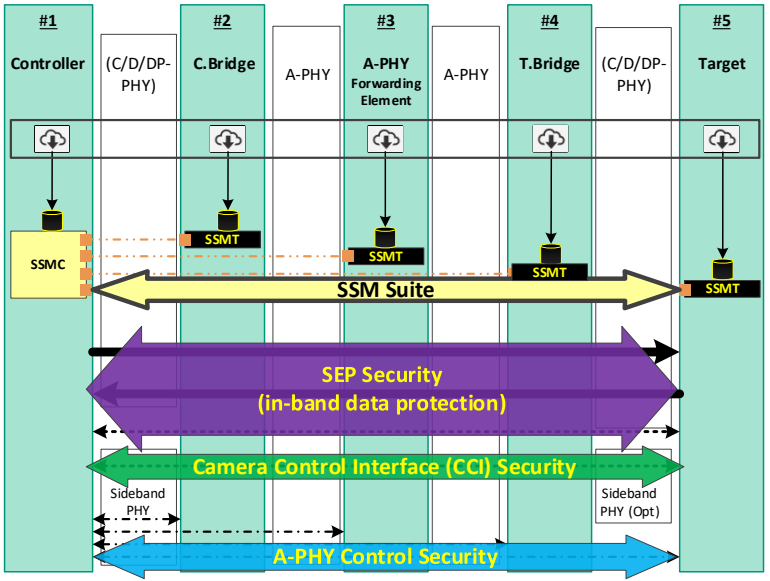
SPDM: Security Protocol and Data Model

Data Security Services

- SEP Security
  - MIPI CSI-2SM, MIPI DSI-2SM, VESA eDP/DP
  - To be defined in Camera/Display Service Extensions (MIPI CSESM/MIPI DSESM) specifications
- ESS CCI2 Security for CCI (Camera Control Interface)
  - I2C-based register access
  - To be defined in MIPI CSESM specification
- ACMP2 Security for MIPI A-PHYSM Control
  - I2C-based register access
  - Reuse ESS CCI2 protocol
  - To be defined in MIPI A-PHYSM specification

Integrity protection via Message Authentication Code (MAC) adds communication and computation overhead

- Sending MAC Per-frame vs per-message reduces communication overhead
- Protecting a fraction of image payloads reduces computation overhead with security trade-off



SEP: Service Extension Packet	ESS CCI2: Extended Safety & Security CCI	ACMP2: A-PHY Configuration & Management Protocol

Conclusion

- MIPI Security Framework
  - Supports various topologies, with and without A-PHY integration
  - System Security Management (SSM) Suite managing Data Security Services
- System Security Management (SSM) Suite
  - Provides mutual authentication & configuration of Data Security Services
  - *Defined in* MIPI Security Specification
- Data Security Services (DSS)
  - Protects image data (MIPI CSI-2℠, MIPI DSI-2℠, VESA eDP/DP) and control data
  - Provides end-to-end security
  - *Defined in* MIPI **CSE℠**, MIPI **DSE℠**, MIPI **A-PHY℠** Specifications
- Set of security specifications expected mid 2022

mipi®
DEVCON
MIPI ALLIANCE DEVELOPERS CONFERENCE

28-29
SEPTEMBER
2021

THANK YOU!