Integrity and Data Encryption (IDE) ECN Deep Dive

PCI-SIG® Educational Webinar Series

August 25, 2020

Meet the Presenter

David Harriman
PCI-SIG® Protocol Workgroup (PWG) Chair
Senior Principal Engineer, Intel

Disclaimer

- The information in this presentation refers to specifications still in the development process. This presentation reflects the current thinking of various PCI-SIG® workgroups, but all material is subject to change before the specifications are released.

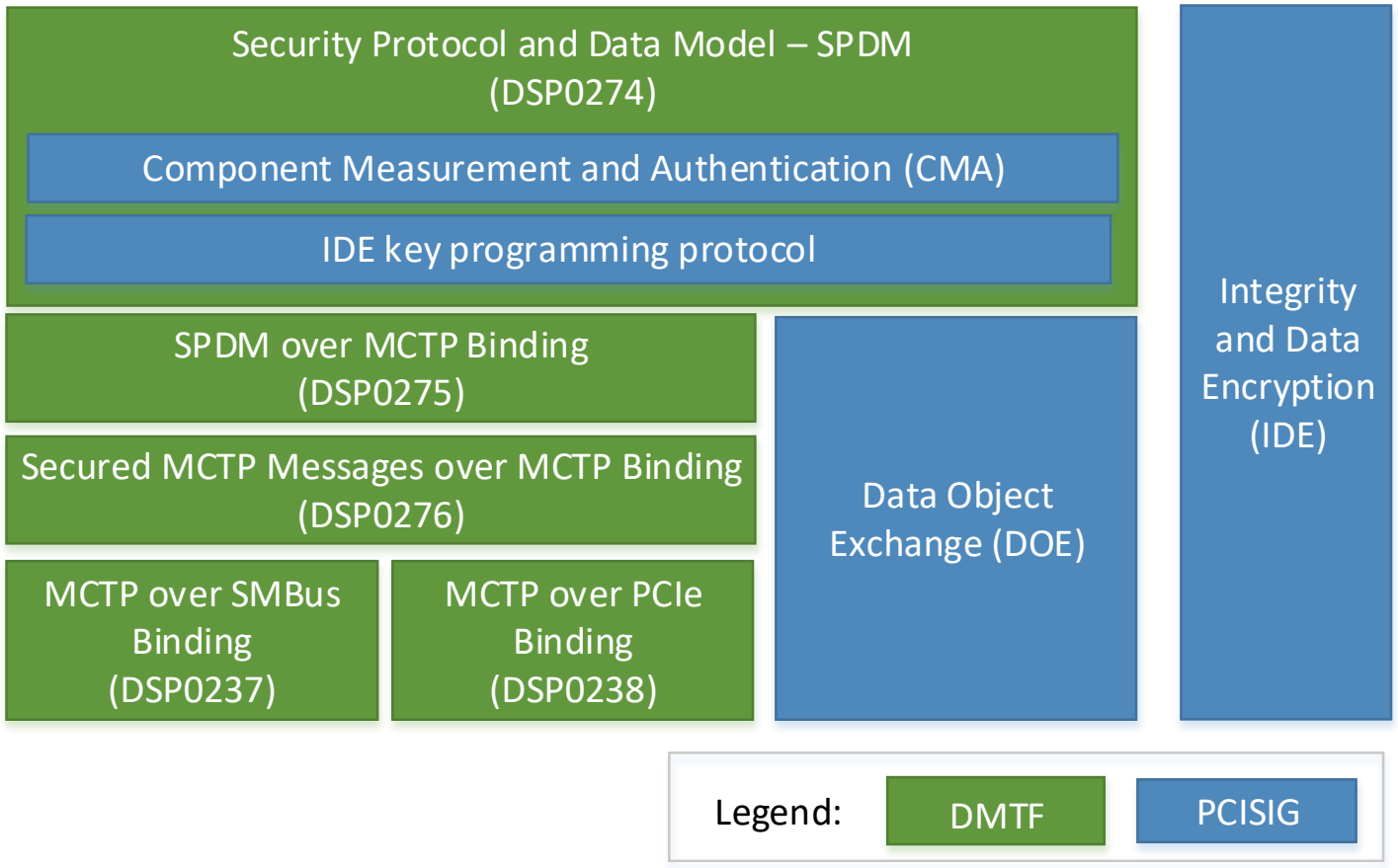
Outline

- Review Context of IDE & Relationship with CMA/DOE & SPDM
- IDE Use Models
- Device's Responsibilities in Maintaining Security
- Next Level of Detail on IDE Draft ECN
- Conclusions and Call to Action

Key Computational Security Needs

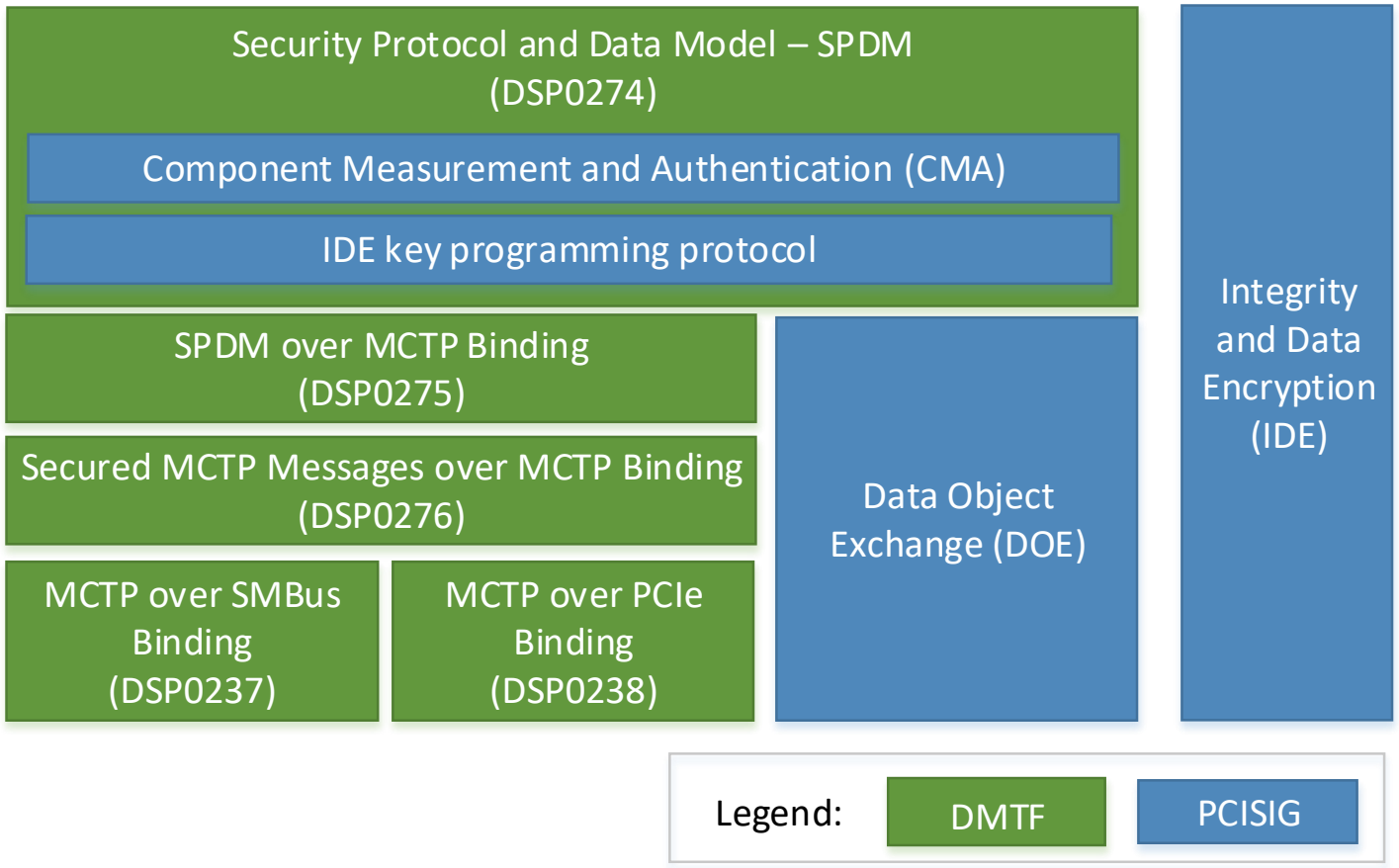
- Protection of key assets
  - Consumers: data integrity, confidentiality
  - Businesses & suppliers: reputation, revenue-stream, intellectual property, business continuity
  - Governments: national security, defense, elections, infrastructure
- Fully secured infrastructure “edge-to-core”
- Must protect against supply chain attacks, physical attacks, persistent attacks, malicious components, etc
- Must secure entire component lifecycle (manufacturing, installation, initialization, operation, addition & replacement)

PCI-SIG® & DMTF Specifications for Security



- SPDM defines a “toolkit” for authentication, measurement, and other security capabilities
- CMA defines how SPDM is applied to PCIe devices/systems
- DOE supports Data Object transport between host CPUs & PCIe components over PCIe
- Various MCTP bindings support Data Object transport over different interconnects
- IDE will typically use this toolkit for key exchange, but can use other mechanisms for keys

PCI-SIG® and DMTF Specifications – Status

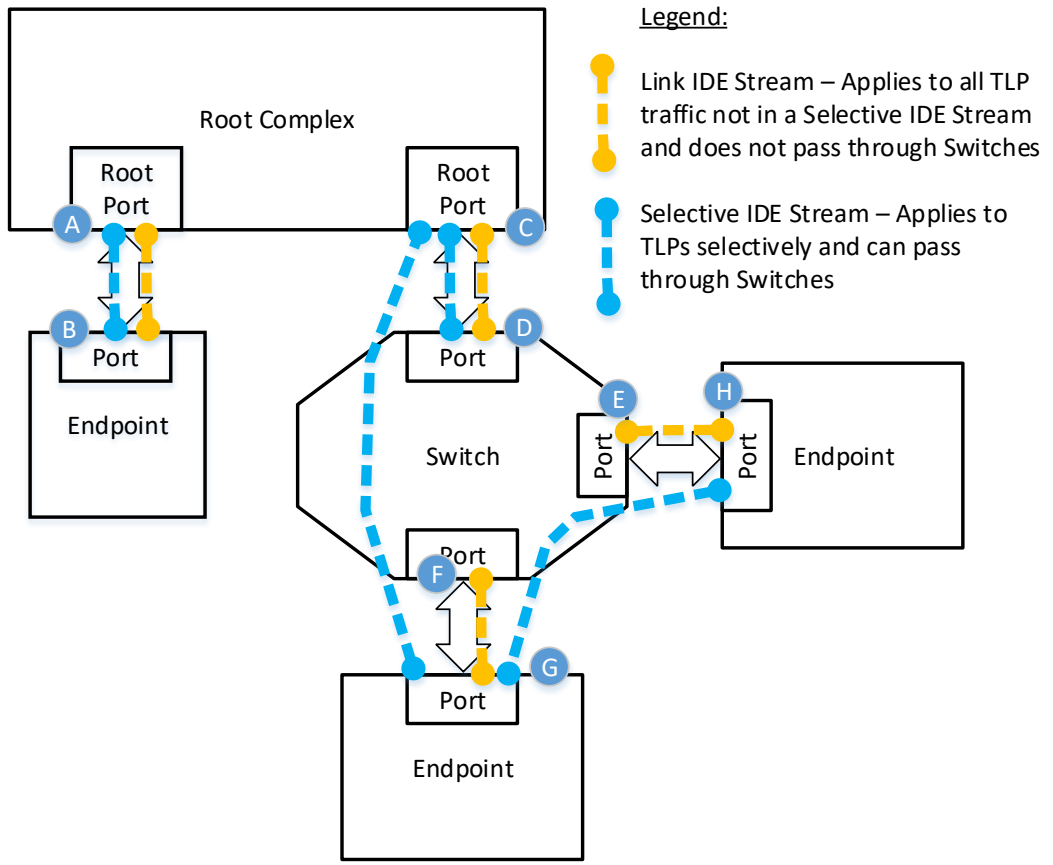


- SPDM: https://www.dmtf.org/dsp/DSP0274
  - Current release (1.0.0) covers Authentication and Measurement
  - 1.1 pending
  - 1.2 (in work queue) will be required for IDE key programming
- CMA published Apr 2020: https://members.pcisig.com/wg/PCI-SIG/document/14236
- DOE published Mar 2020: https://members.pcisig.com/wg/PCI-SIG/document/14143
- IDE in Review
  - Goal: Final Publication End of Q3

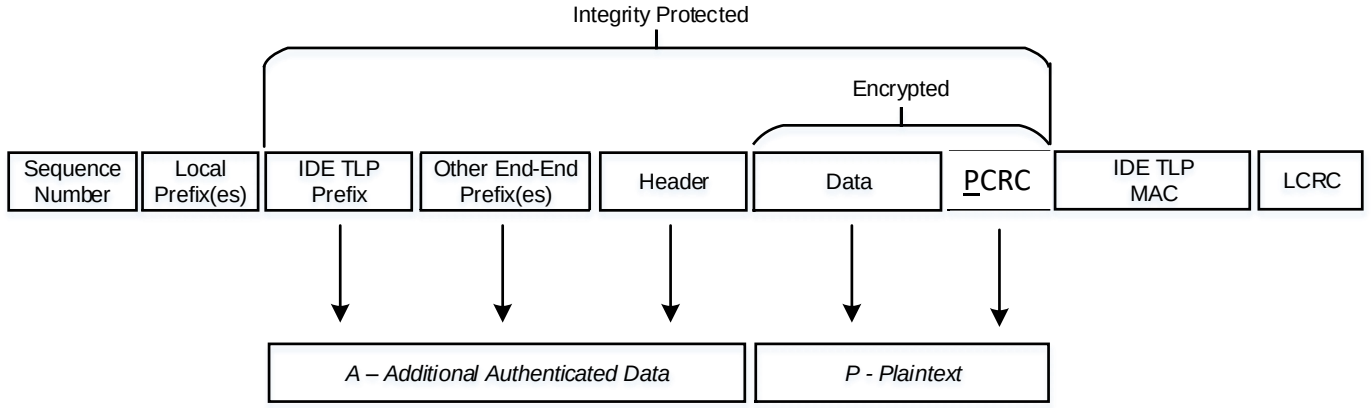
IDE D-ECN to Base 4.0/5.0 is in Review Zone – Member Review ends 7 Sept 2020

Overview: PCIe® Technology Integrity and Data Encryption (IDE)

- Goals: Provide confidentiality, integrity, and replay protection for PCIe Transaction Layer Packets (TLPs)
  - Support wide variety of use models
  - Broad interoperability
  - Aligned to industry best practices & extensible
- Security model - Physical attacks on Links, to read confidential data, modify TLP contents, & reorder and/or delete TLPs, via:
  - lab equipment
  - purpose-built interposers
  - malicious Extension Devices
- TLPs can be protected while transiting Switches
  - Extends security model to address attacks via Switches
- Applies AES-GCM for encryption of TLP Data Payload and authenticated integrity protection of entire TLP

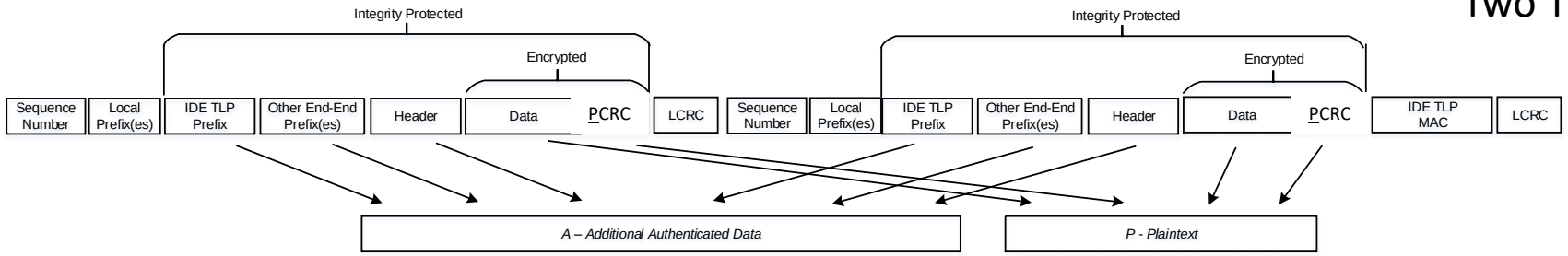


IDE TLPs



Single IDE TLP

Two TLPs Aggregated



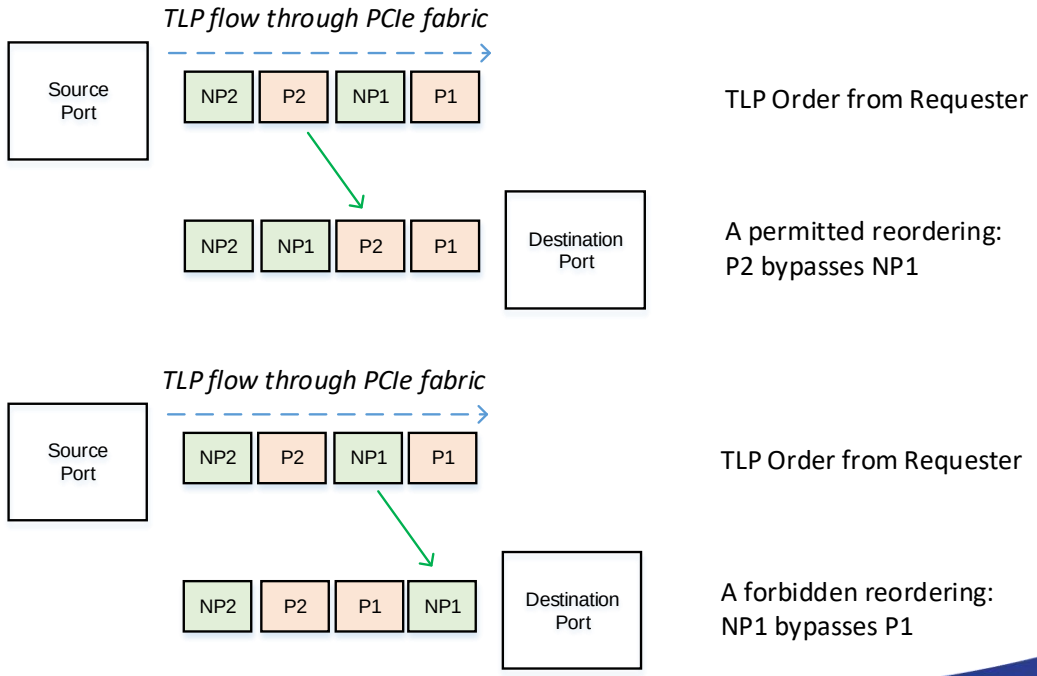
- Examples show TLP format for Selective IDE
- For Link IDE the Local Prefix(es) are also integrity protected
- Aggregation can apply to up to 8 TLPs

Non-FLIT Mode TLPs shown – For Base 6.0 with FLIT Mode the TLP format will be different

Streams & Sub-Streams

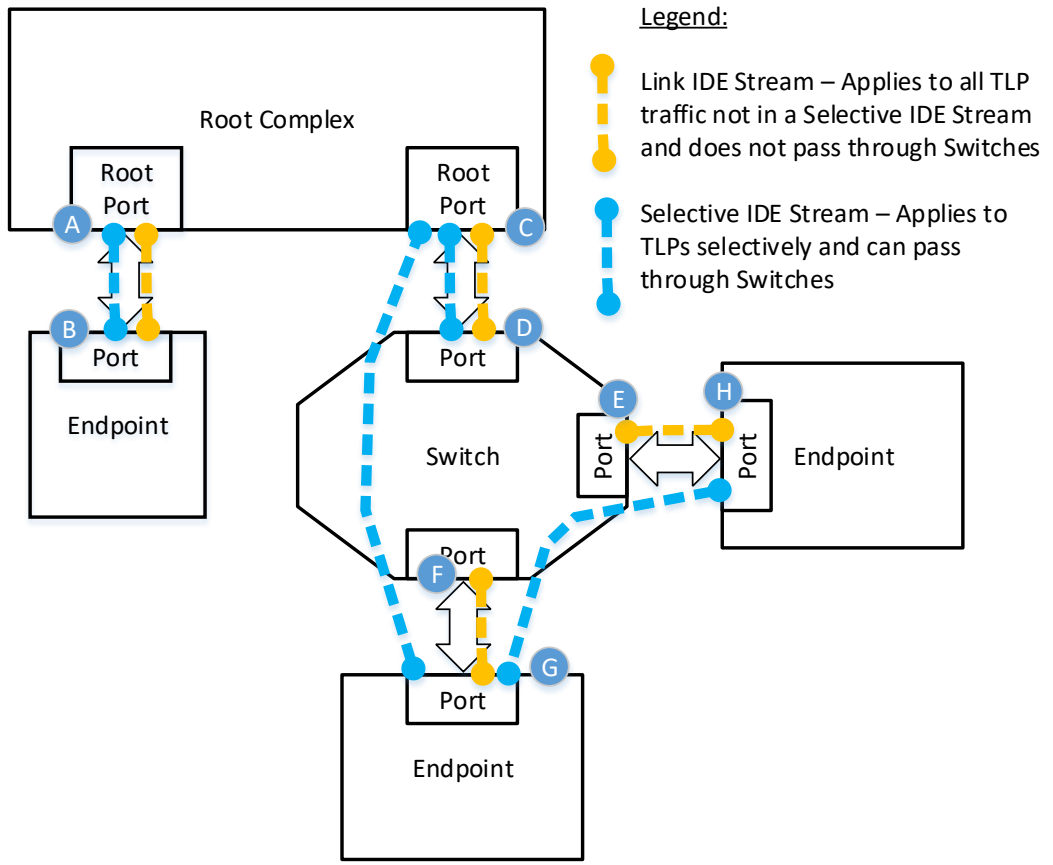
- Each IDE Stream includes Sub-Streams distinguished by TLP type and direction
  - Posted Requests, Non-Posted Requests, & Completions
- Sub-Streams allow the PCIe Producer/Consumer model to be followed in a way that also works well with AES-GCM
  - The TLPs in a Sub-Stream are processed in-order
  - Each Sub-Stream has a unique key and invocation counter
- Within a Stream, Sub-Streams require modification of the Switch ordering rules for flow-through Selective IDE (top right)
  - Between Streams and with non-IDE TLPs, the ordering rules are unchanged
- Examples of permitted and forbidden reordering (right)

Row Pass Column?		Posted Request (Col 2)	Non-Posted Request		Completion (Col 5)
			Read Request (Col 3)	NPR with Data (Col 4)	
Posted Request (Row A)		No	Yes	Yes	a) Y/N b) Yes
Non-Posted Request	Read Request (Row B)	No	No	No	Y/N
	NPR with Data (Row C)	No	No	No	Y/N
Completion (Row D)		No	Yes	Yes	No



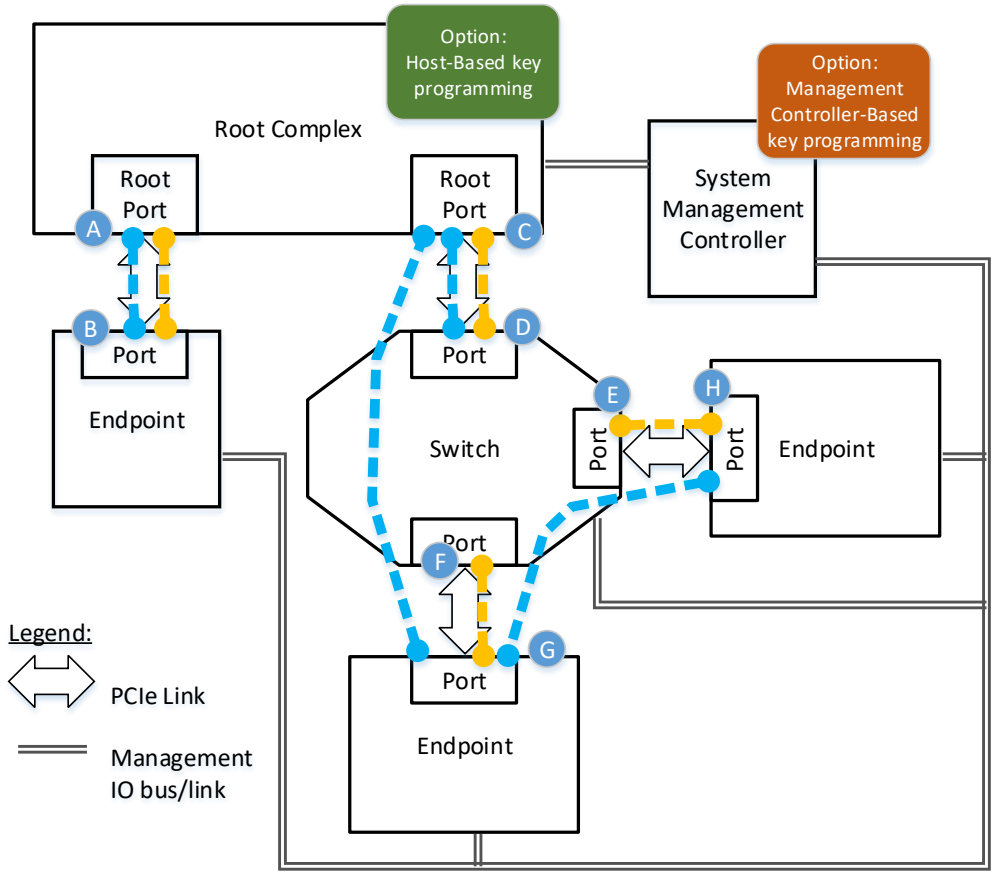
IDE Use Models – Link vs. Selective

- IDE establishes an IDE Stream between two Ports
- Can use Link IDE and/or Selective IDE between two directly connected Ports (e.g. A & B, C & D)
- Desirable if, e.g., different security policies are applied to the Selective IDE TLPs.
- IDE does not establish security beyond the boundary of the two terminal Ports
- Selective IDE Streams between Ports C and G, and between Ports G and H, are secured as they pass through the Switch
- IDE provides security from Port to Port
  - Security must be provided implementation-specific means within the Component past the terminal Port
  - With TLPs flowing “hop-by-hop” through one or more Switches, it is necessary to ensure acceptable security is maintained within the Switch(es)



System Construction

- In-line securing of TLPs –
  a “data plane” capability
- Stream establishment & management –
  a “control plane” capability
- IDE defines key programming from a central trusted entity (e.g., Host Firmware/Software, BMC)
- Supports “Set & Forget” model as well as more active/dynamic approaches



System Level Considerations

- "Verifier" Implementation is key, but outside scope of PCIe® Base specification
  - Build on CMA/SPDM foundation
  - System level policies expected to vary significantly
  - Revisit industry spec requirements as experience base increases
- Securing centralized functions
  - Centralized key programming – single point of failure must be secured!
  - IDE stops at the Port – buffers/memory & processing resources must prevent leaks

Device's Responsibilities in Maintaining Security

- Device requirements parallel those for the Host
- Keys must be secured!
- No paths around encryption eliminated/blocked
- Debug mechanisms must be carefully controlled

IDE Draft ECN – Few Remaining Opens

- Key programming protocol
  - Coordinated with SPDM 1.2
  - Optimizing the layering structure
- Seeking feedback on key size and related requirements
  - See “NOTE TO REVIEWERS”
- Balance between spec / implementation flexibility in “control” plane, e.g.
  - Mechanisms for “locking” configuration
  - Details of set-up and tear-down

Conclusions and Call to Action

- Integrity and Data Encryption (IDE) – In Review
  - Please review and provide feedback
- Consider IDE applies in your applications
- Engage with PCI-SIG®
  - Consider Next Steps for the PCIe® Base Specification

Questions

Thank you for attending the PCI-SIG Q3 2020 Webinar

For more information please go to www.pcisig.com