Flash Memory Summit

Implementation of IDE in SSD Controllers for Data Centers

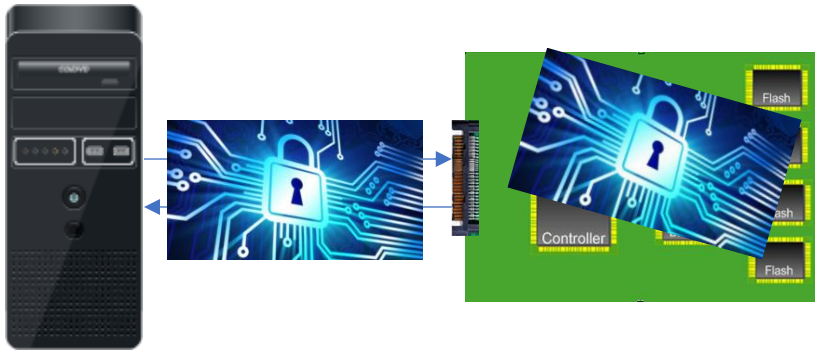
DSEC-301-1: Ensuring Data Security in SSDs (Data Security and Protection Track)
Aug 10, 2023

Presenter: Radjendirane Codandaramane, Sr. Manager, Applications
Microchip Technology Inc.

MICROCHIP

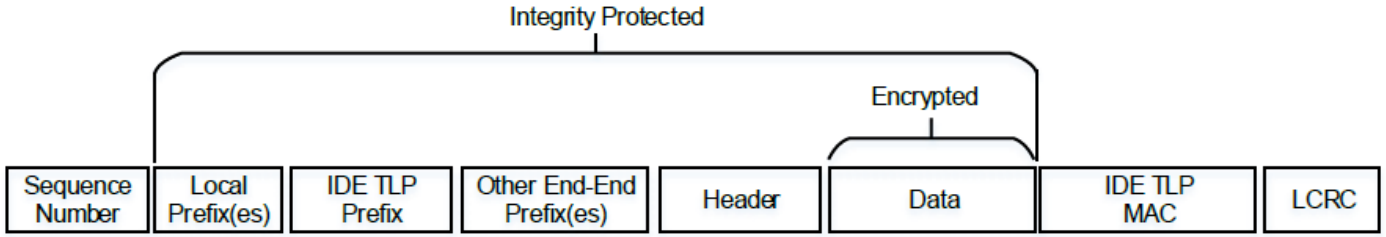
Agenda

- IDE Overview
- SSD Controller Architecture
- IDE in SSD
- Stream State Machine
- Stream Context
- AES-GCM
- Key Management
- Plaintext CRC (PCRC)



Integrity and Data Encryption (IDE)

- Provides confidentiality, integrity, and replay protection for TLPs in transit
- Covers threats from physical attacks on links, to
  - Examine data intended to be confidential
  - Modify, reorder, delete TLP contents
  - Reprogramming switch routing mechanisms or using “malicious” Switches



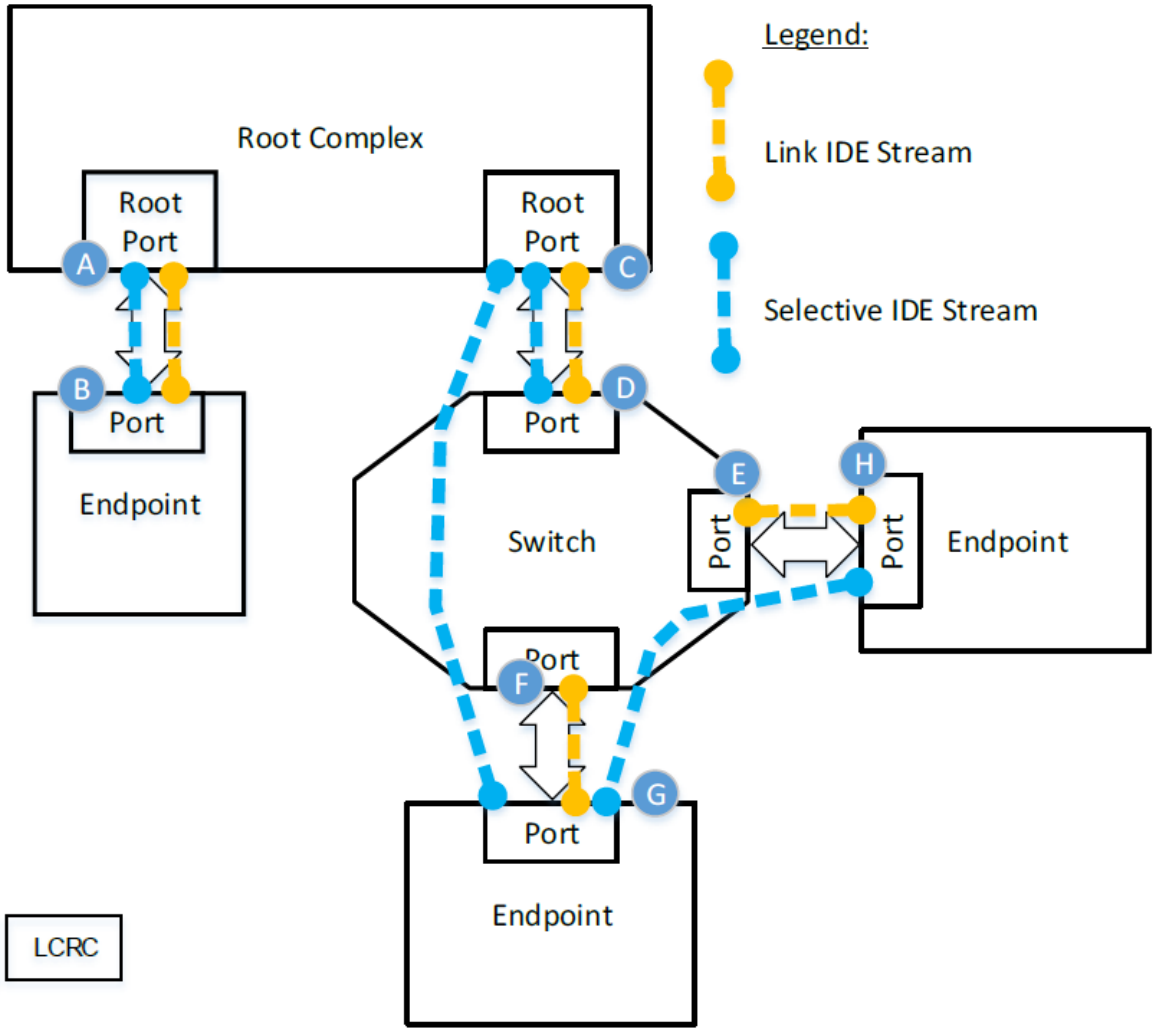
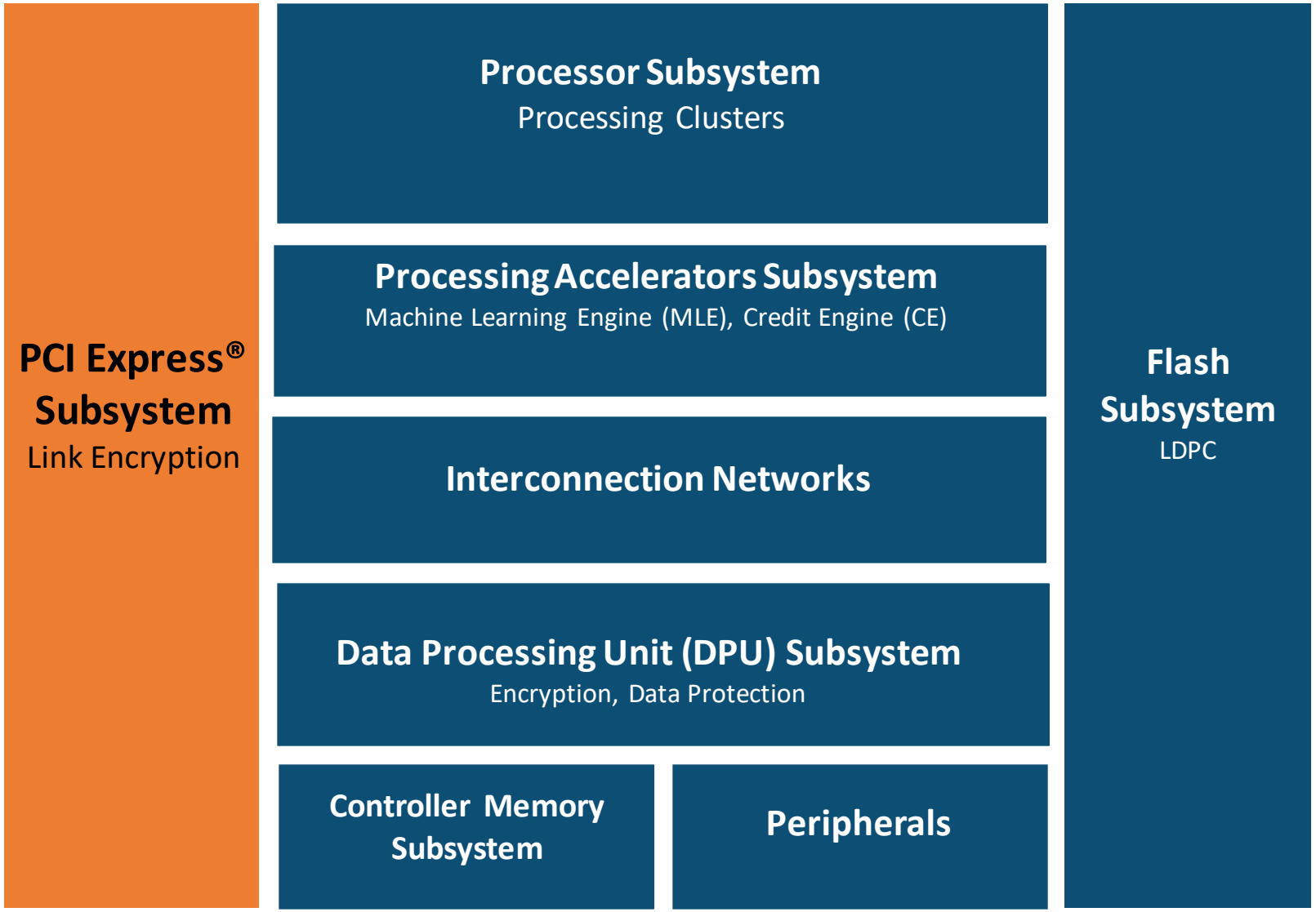


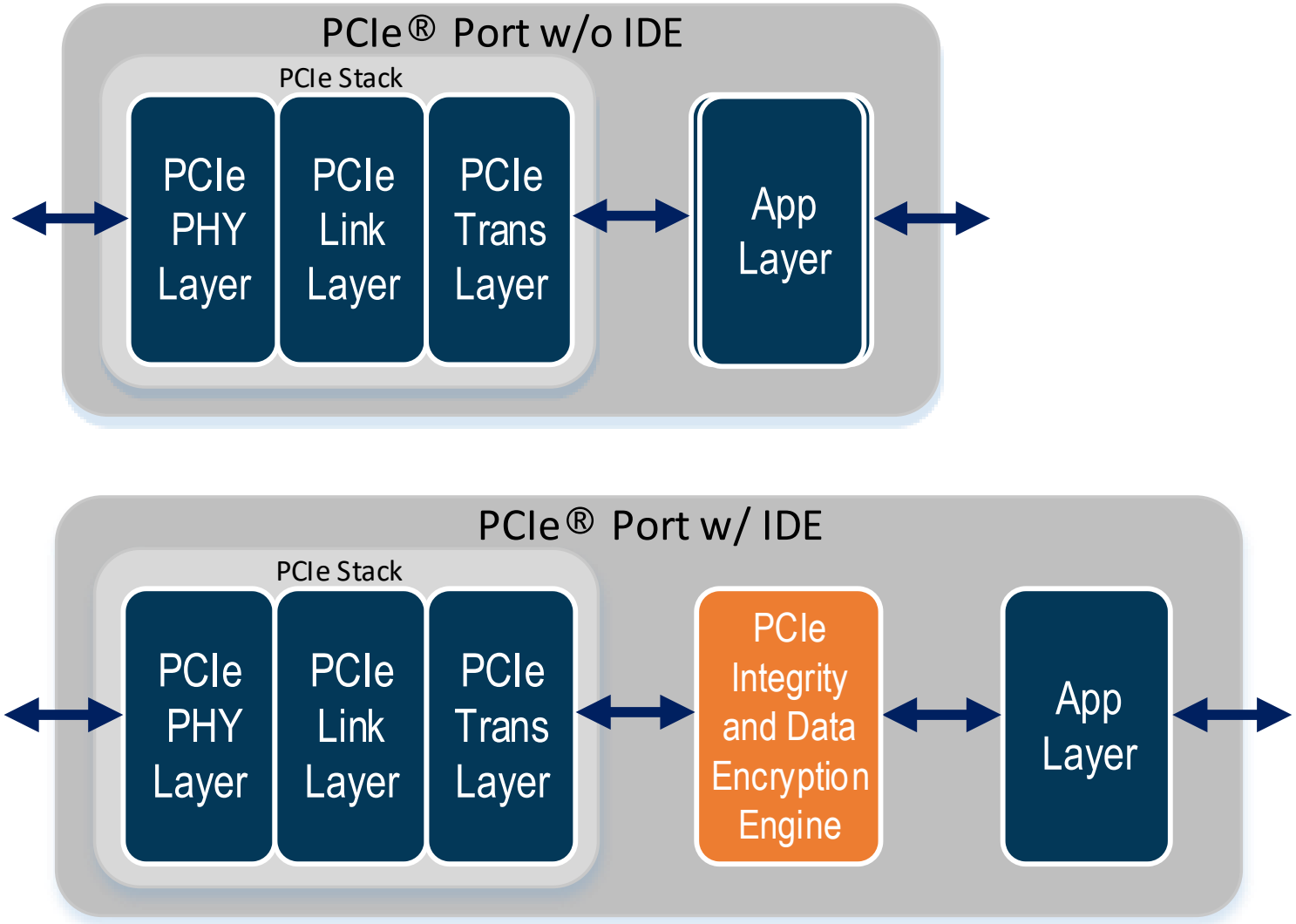
Figure 7-5 IDE Secures TLPs Between Ports

Source: PCI®-SIG IDE ECN

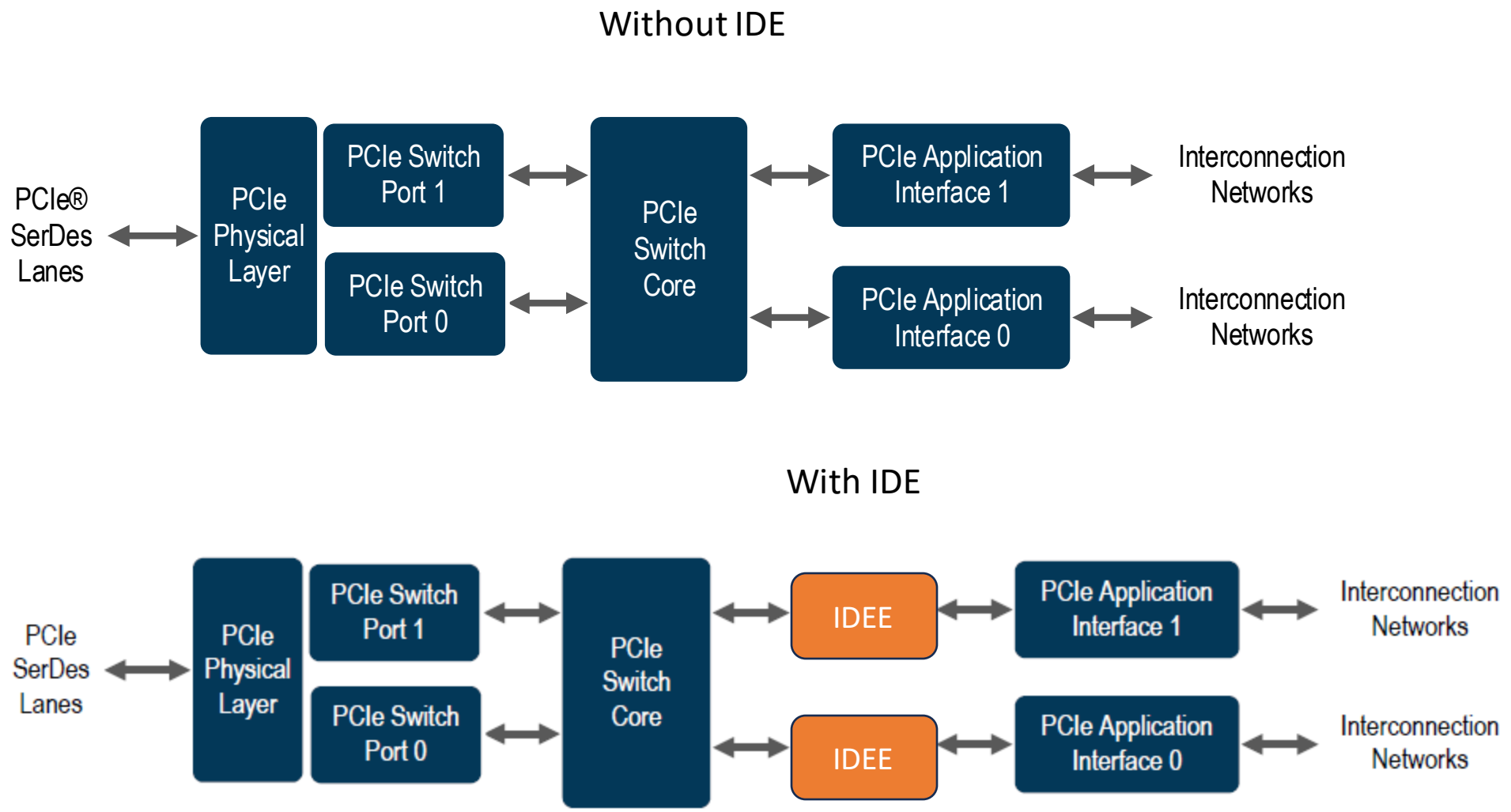
IDE in SSD Controller



IDE in SSD Controller – Example

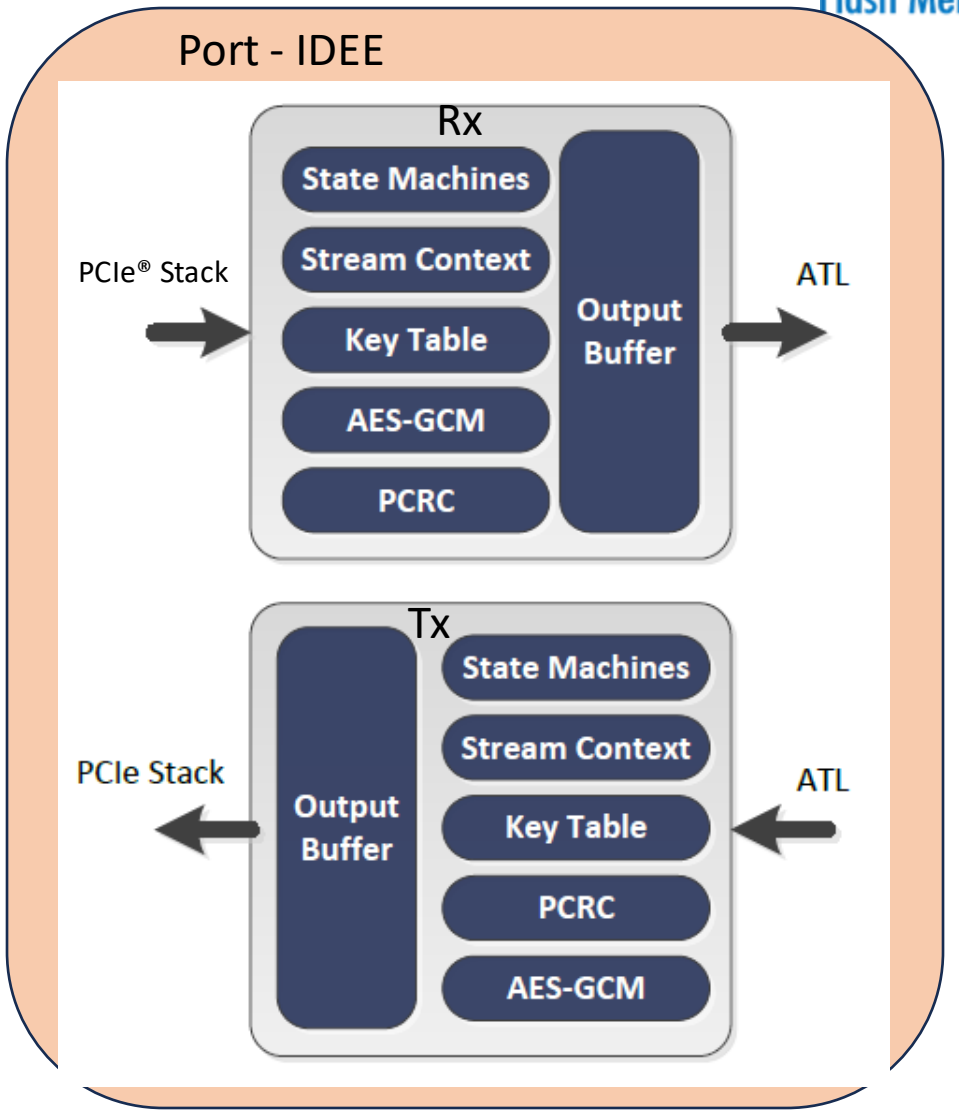


IDE in SSD Controller – Dual Port Example



IDE Engine

- Receive direction
  - Decrypts received data and checks the Message Authentication Code (MAC) for authentication using AES-GCM
  - Checks PCRC if the P bit is set
  - Generates IDE fail messages in firmware, when detecting a mismatched MAC
- Transmit direction
  - Generates PCRC if it is enabled for the stream
  - Encrypts transmit data and generates the MAC for authentication using AES-GCM
  - Generates IDE sync messages in hardware



Stream State Machine

- Insecure State
  - Power-on reset state; Defa state – All Rx & Tx data are discarded
  - Enter through any error fa conditions or by firmware
  - Exit to secure state by Firmware initiation
- Secure State
  - Operation state
  - Enter through firmware configuration
  - Exit to insecure state when error or fail condition or through firmware

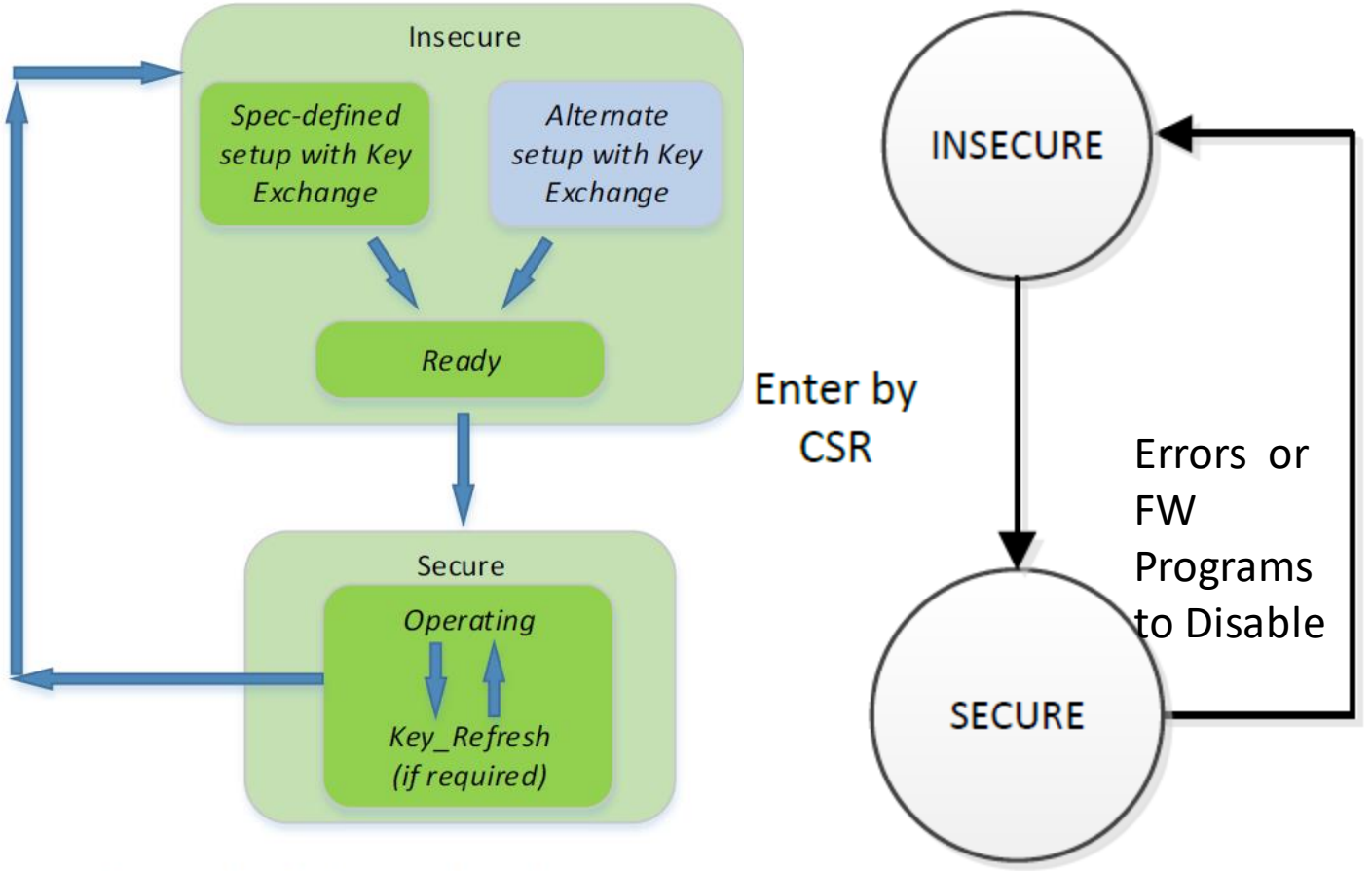


Figure 7-6 IDE Stream State Machine

Source: PCI®-SIG IDE ECN

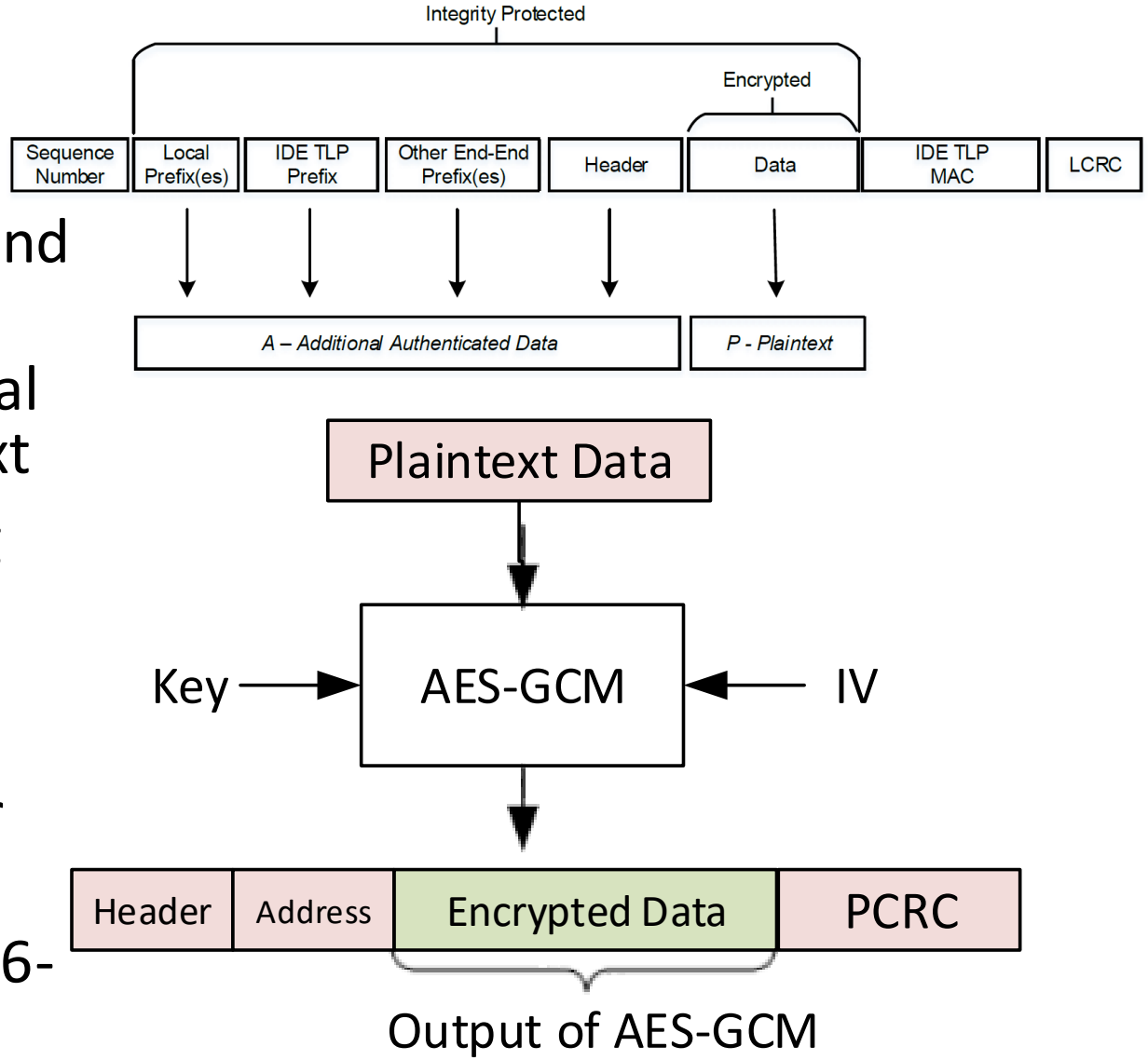
Stream Context

- The Stream Context identifies whether a TLP belongs to a Link or Selective stream based on the Stream ID
- It stores and retrieves the context of each sub-stream such as the Initialization Vector (IV) and the receive/transmit counters
  - The AES-GCM requires an Initialization Vector (IV) input for each computation. The PCIe® IDE defines the IV as 96 bits
- Transmit Counters: 2x 8-bit counters are maintained
- Receive Counters: 2x 64-bit counters are maintained

Stream Context
Stream ID
Initialization Vector [95:0]
Transmit Counter
PR_Sent_Counter-NPR [7:0]
PR_Sent_Counter-CPL [7:0]
Receive Counters
PR_Received_Counter-NPR [63:0]
PR_Received_Counter-CPL [63:0]

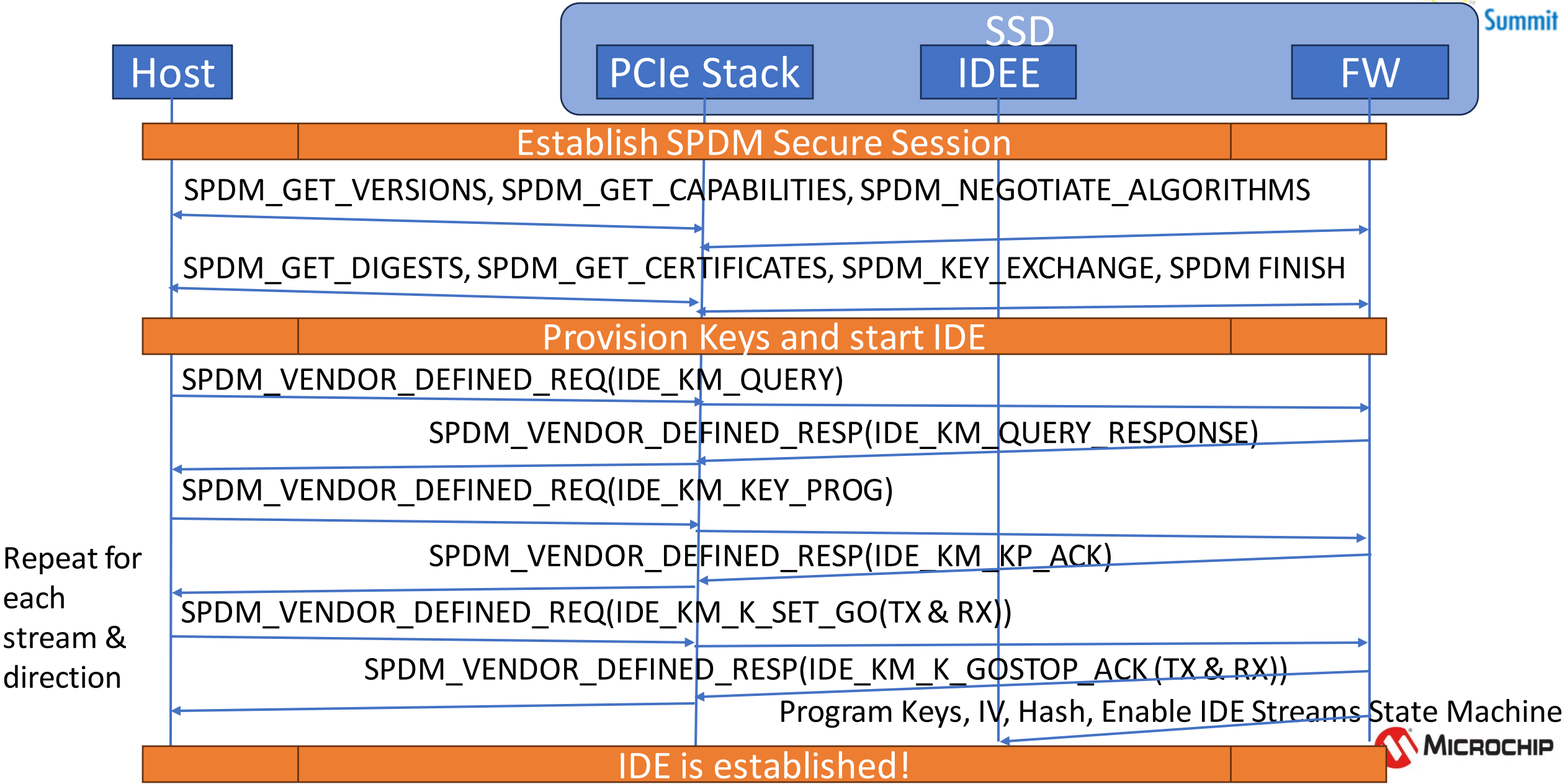
AES-GCM

- The PCIe® IDE utilizes the AES-GCM (Advanced Encryption Standard-Galois Counter Mode) protocol for encryption and authentication
- The AES-GCM inputs require an Additional Authentication Data (AAD) and a plaintext
- The AAD consists of all the prefixes along with the TLP header, and the plaintext is composed of the TLP payload and PCRC
- The encryption and authentication functions are always performed together when a stream is enabled
- Message Authentication Code (MAC) is 96-bit value



MICROCHIP

Key Management Flow



Key Management Support in Controller

Stream	Type	Key Table Address
Link Stream	Posted	0
	Non-Posted	1
	Completion	2
Selective Stream 0	Posted	3
	Non-Posted	4
	Completion	5
Selective Stream 1	Posted	6
	Non-Posted	7
	Completion	8

Key Set 0
Valid
Tx AES Key[255:0] IV[63:0]
Tx Hash Key[127:0]
Rx AES Key[255:0] IV[63:0]
Rx Hash Key[127:0]
Key Set 1
Valid
Tx AES Key[255:0] IV[63:0]
Tx Hash Key[127:0]
Rx AES Key[255:0] IV[63:0]
Rx Hash Key[127:0]

- Keys (256 bits) are independent for the Rx and Tx directions
- Key table entry holds two sets per sub-stream: Key Set 0 and 1
- Key set consists of the Valid bit, AES Key and the Hash Key

MICROCHIP

Key Management Support in Controller

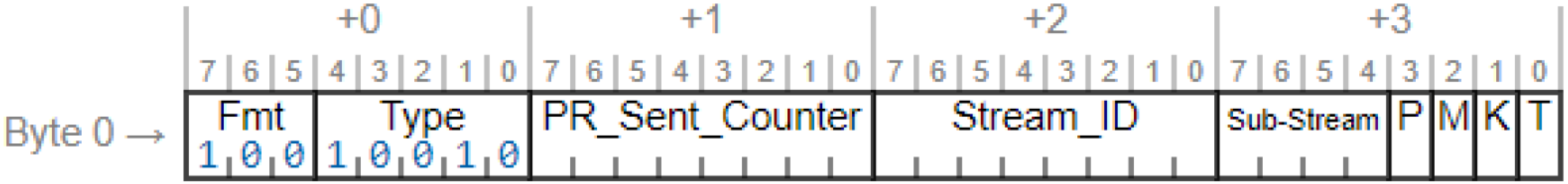


Figure 7-17 IDE TLP Prefix

Source: PCI®-SIG IDE ECN

- Transmit: Key set bits is set by firmware and indicates which key set the hardware uses to encrypt the transmit TLP
- Receive: K bit in the IDE TLP prefix of the receiving TLP and it indicates which key set the hardware uses to decrypt the receiving TLP
- After reset and successful authentication complete, firmware loads keys, IV and hash into AES-GCM
- Any error will cause Insecure mode and TLPs will be discarded

PCRC

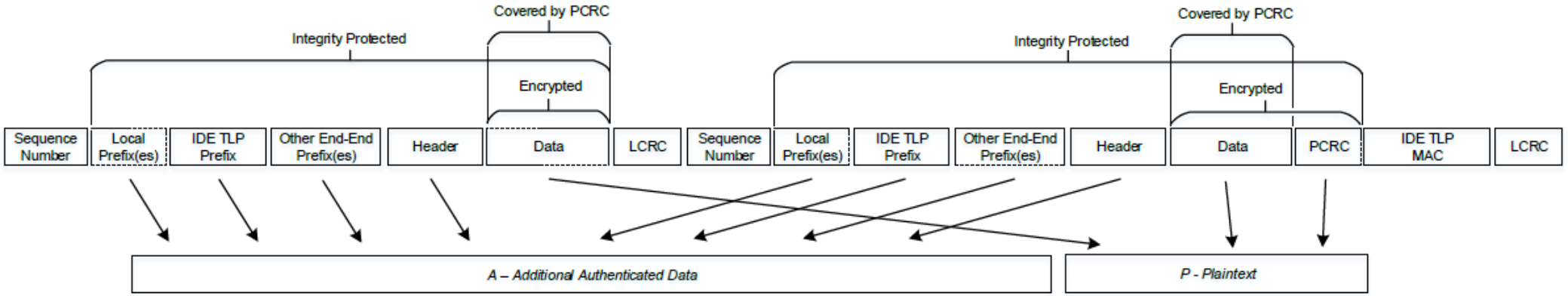


Figure 7-23 Example Illustrating PCRC Application to Two Aggregated IDE TLPs for a Link IDE Stream

Source: PCI®-SIG IDE ECN

- Optional Plaintext CRC (PCRC) is used to detect faults in the encryption/decryption logic
- The P bit is detected in the IDE prefix, used to indicate if the TLP has PCRC (enabled only if both ports support)
- PCRC uses same algorithm as ECRC
- PCRC is generated before encryption on Tx and checked after decryption on Rx
- TLPs can be aggregated to reduce the IDE overhead

Summary

- Integrity and Data Encryption provides data-in-transit protection of TLPs
- Dual port example implementation of IDE in SSD Controller Architecture
- Key Management flow
- Division of labor between Firmware and Hardware
- Performance and Error handling considerations

MICROCHIP

Thank you!

Visit Microchip Booth# 419