Flash Memory Summit

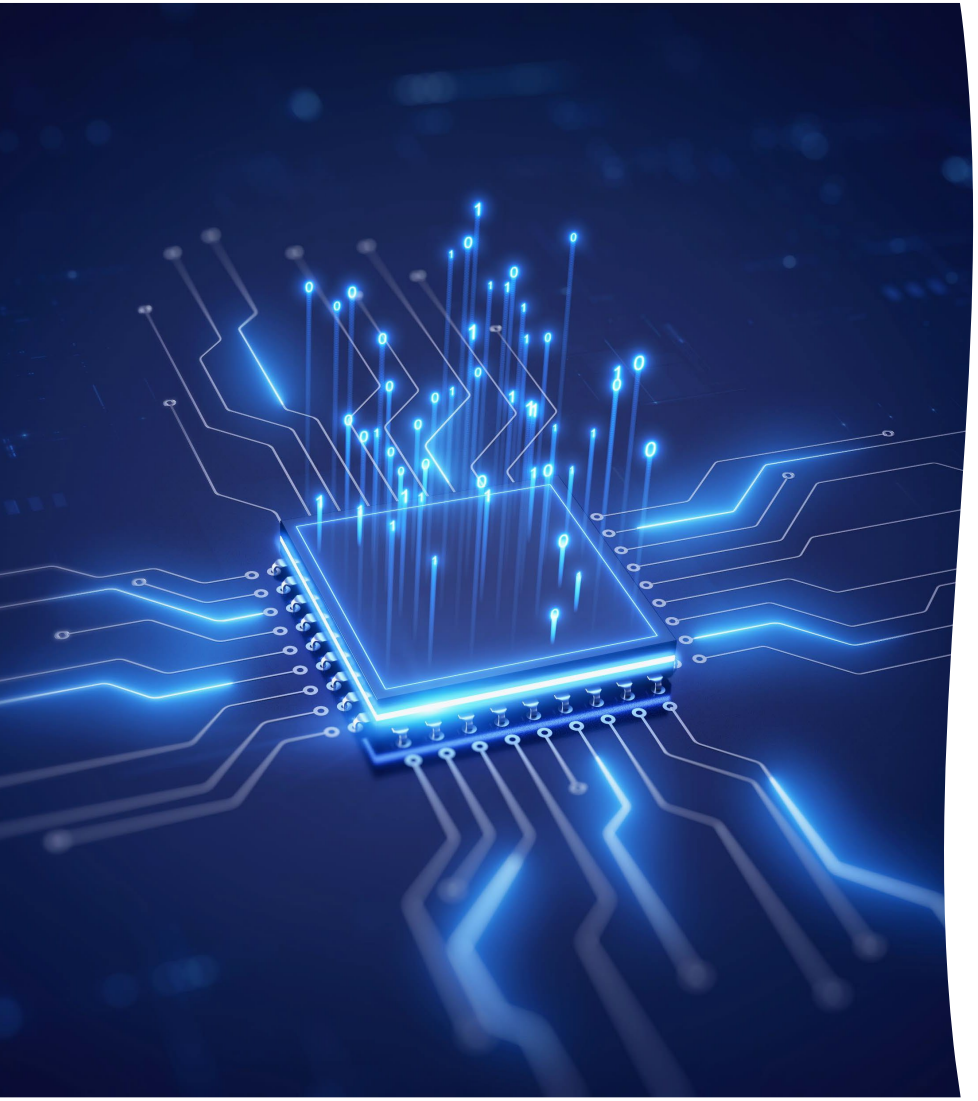
Securing CXL™ Memory

Presenter: Joseph Tinc, Applications Engineer

Microchip Technology Inc.

MICROCHIP

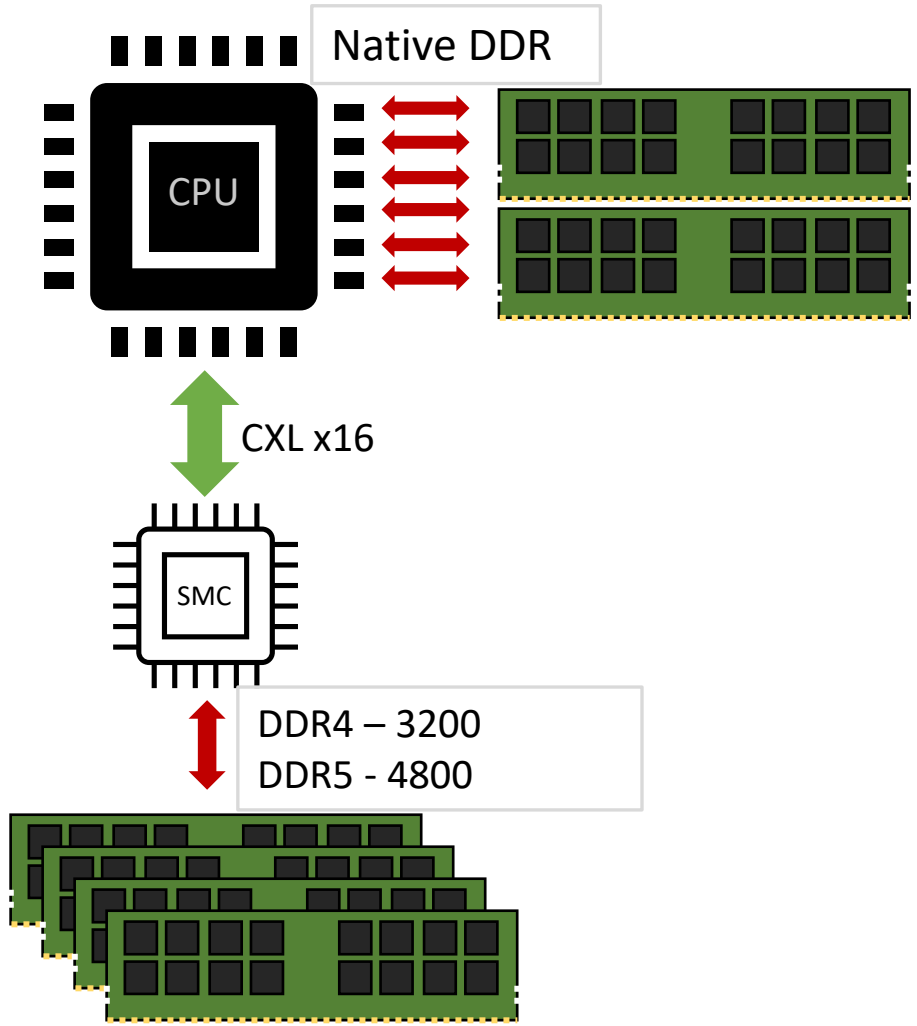
Compute Express Link™ (CXL™)



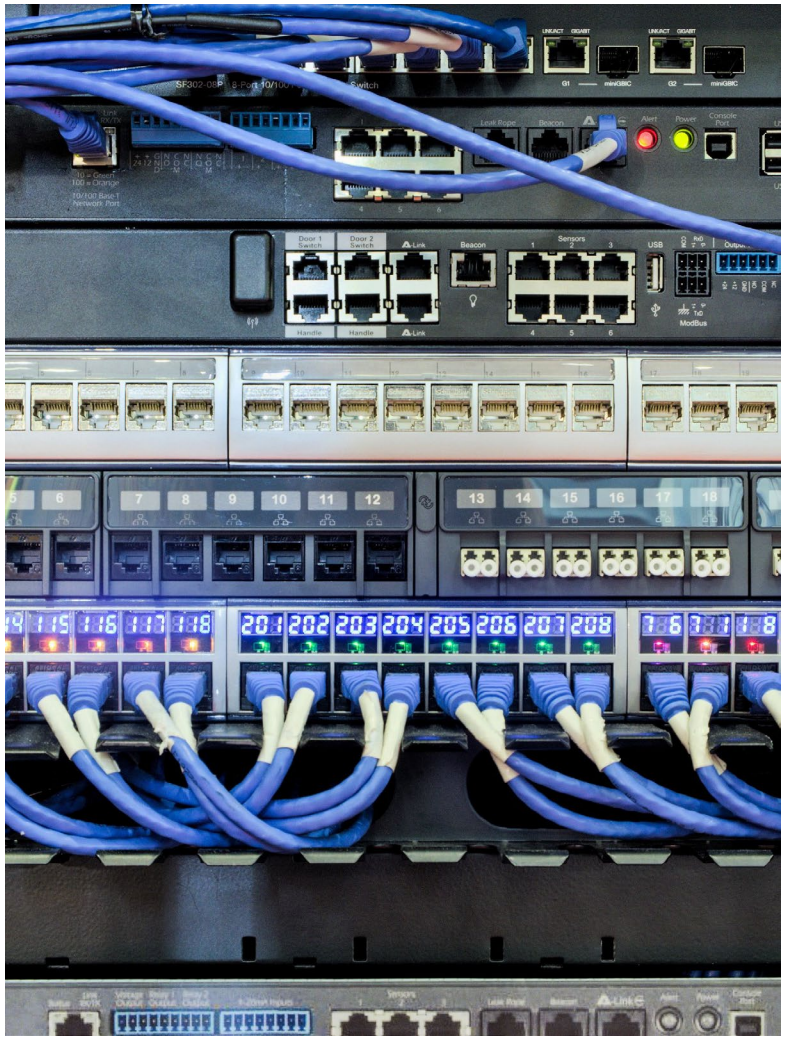
- CXL is on its way to becoming the ubiquitous interconnect in data centers
- The speed and semantics CXL offers have potential for many devices in many industries
- Security is imperative for CXL memory devices

Context on Memory

- CXL™ memory controllers are a perfect solution to the memory wall problem
- Need to consider vulnerabilities of the CXL link



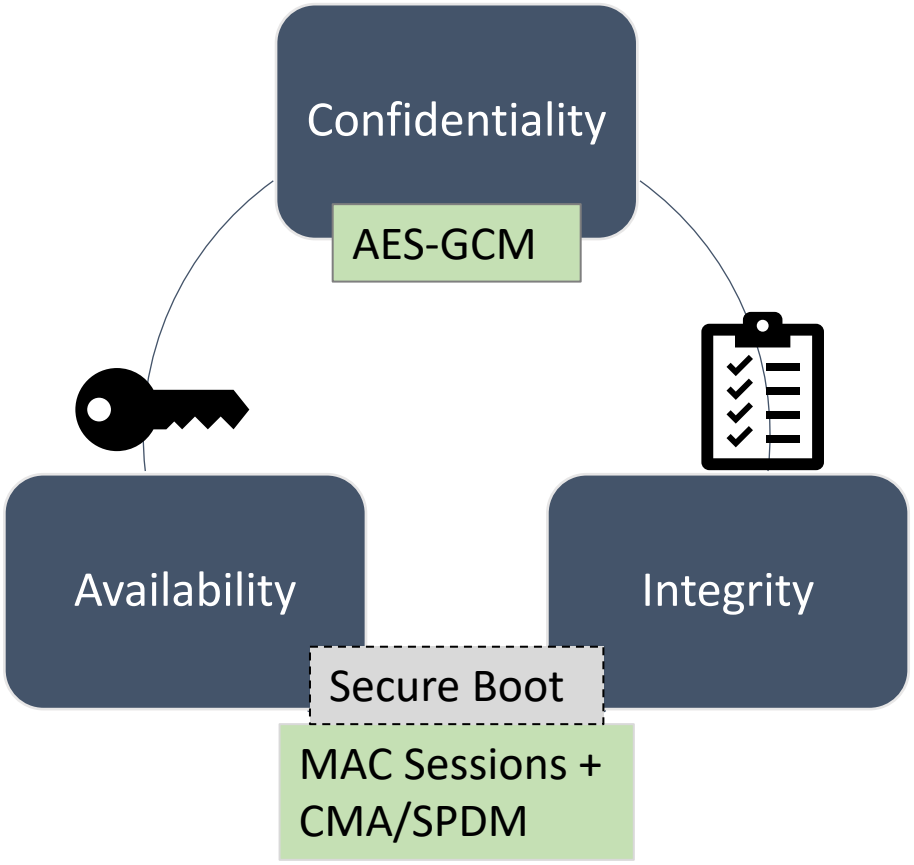
“Edge-to-Core” Protection



- Encryption protocols exist for the internet
- Evolving threats need to be considered:
  - In the server chassis
  - Intra and inter rack links not previously exposed
  - Middleman attacks between CPU and endpoint over PCIe®/CXL™

Why IDE, Why Now?

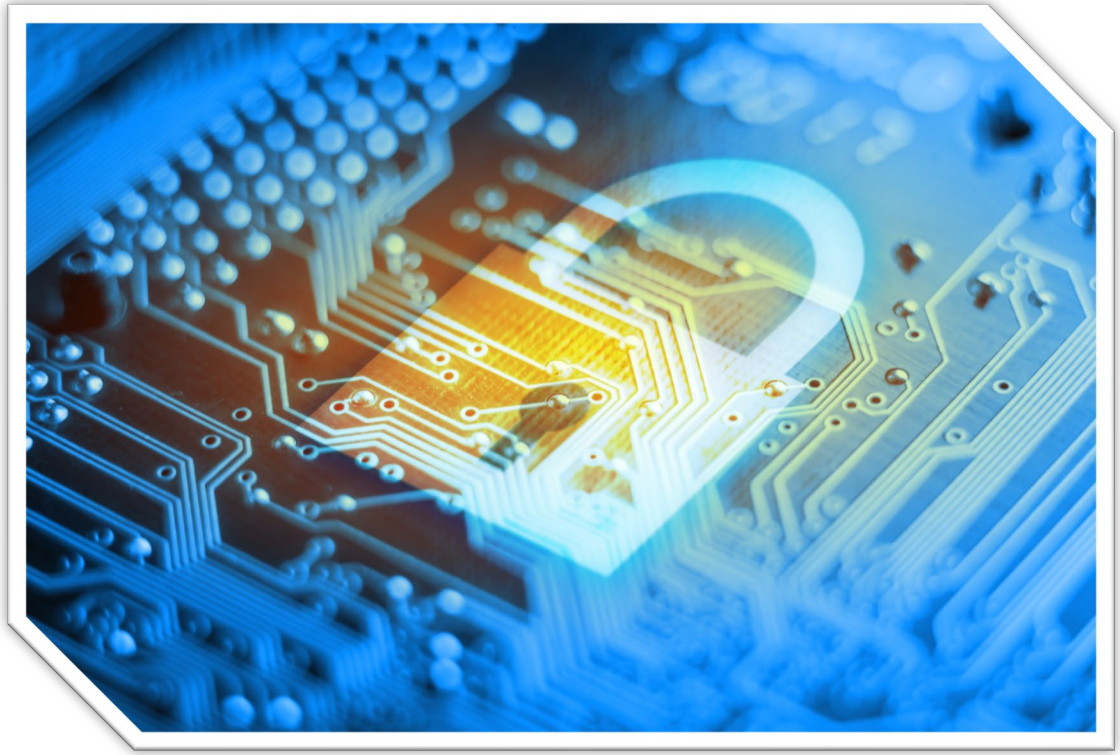
- Integrity and Data Encryption (IDE) offers solutions to C&I
  - AES-GCM addresses confidentiality
  - CMA/SPDM addresses integrity
- Secure Boot: implementation-specific but necessary



AES-GCM

- IDE encryption is performed by an algorithm called AES-GCM (Advanced Encryption Standard using Galois/Counter Mode of operation)

- Competition winner:
  - Insurmountable security
  - Computationally efficient
  - Can detect data tamper

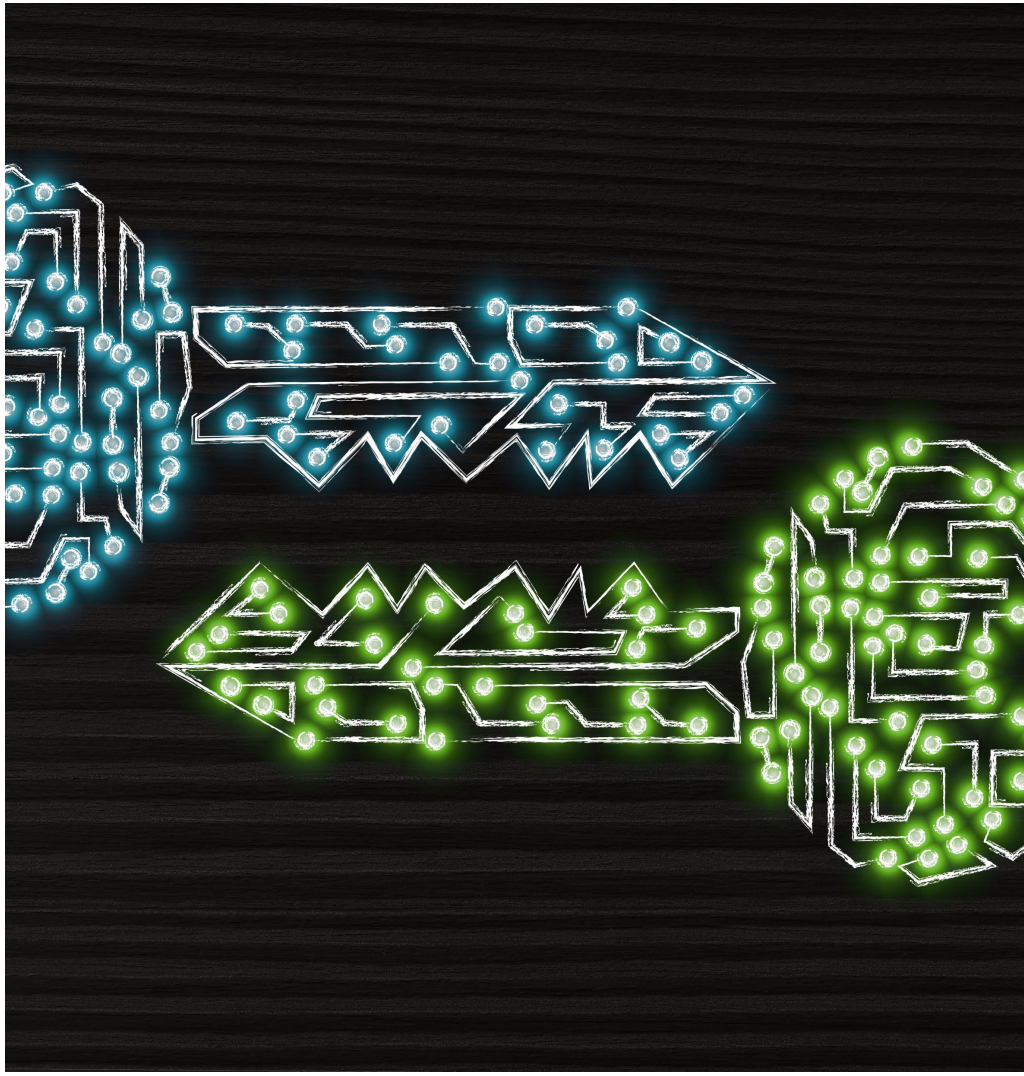


Considerations for Memory Controllers

- Which device should hold the encryption engine? Host or controller?
- What are the tradeoffs?

CMA/SPDM

- DMTF-defined protocol used to do attestation and authentication
  - CMA (Component Measurement and Authentication)
  - SPDM (Security Protocol and Data Model)



Thank you!
Visit Microchip at Booth 419.

MICROCHIP