Microsemi
Power Matters.

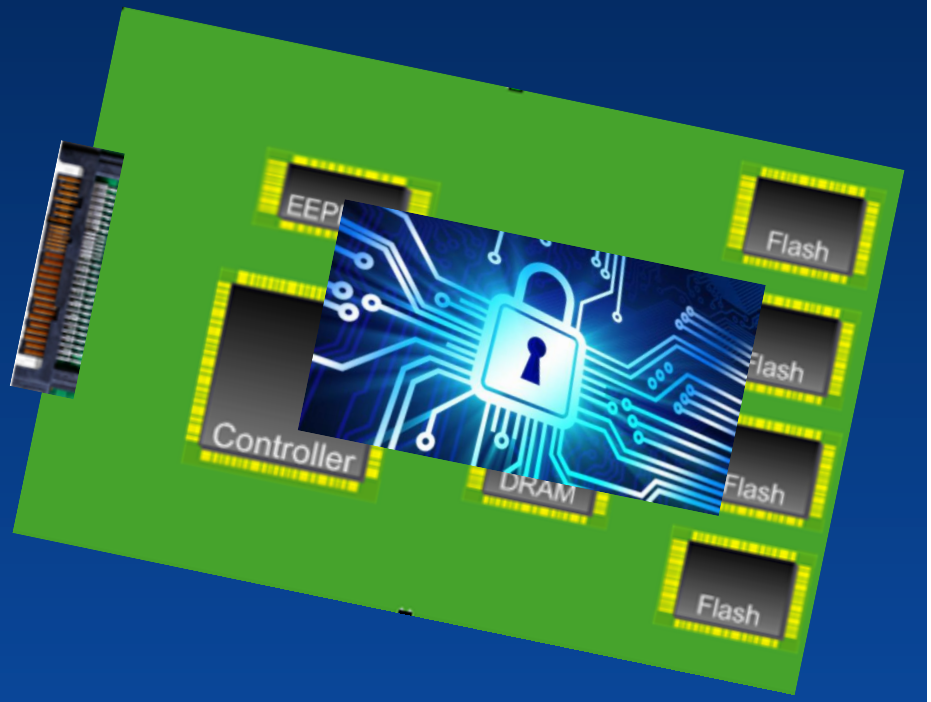
Security in NVMe Enterprise SSDs

Radjendirane Codandaramane,
Sr. Manager, Applications,
Microsemi

Flash Memory Summit

Agenda

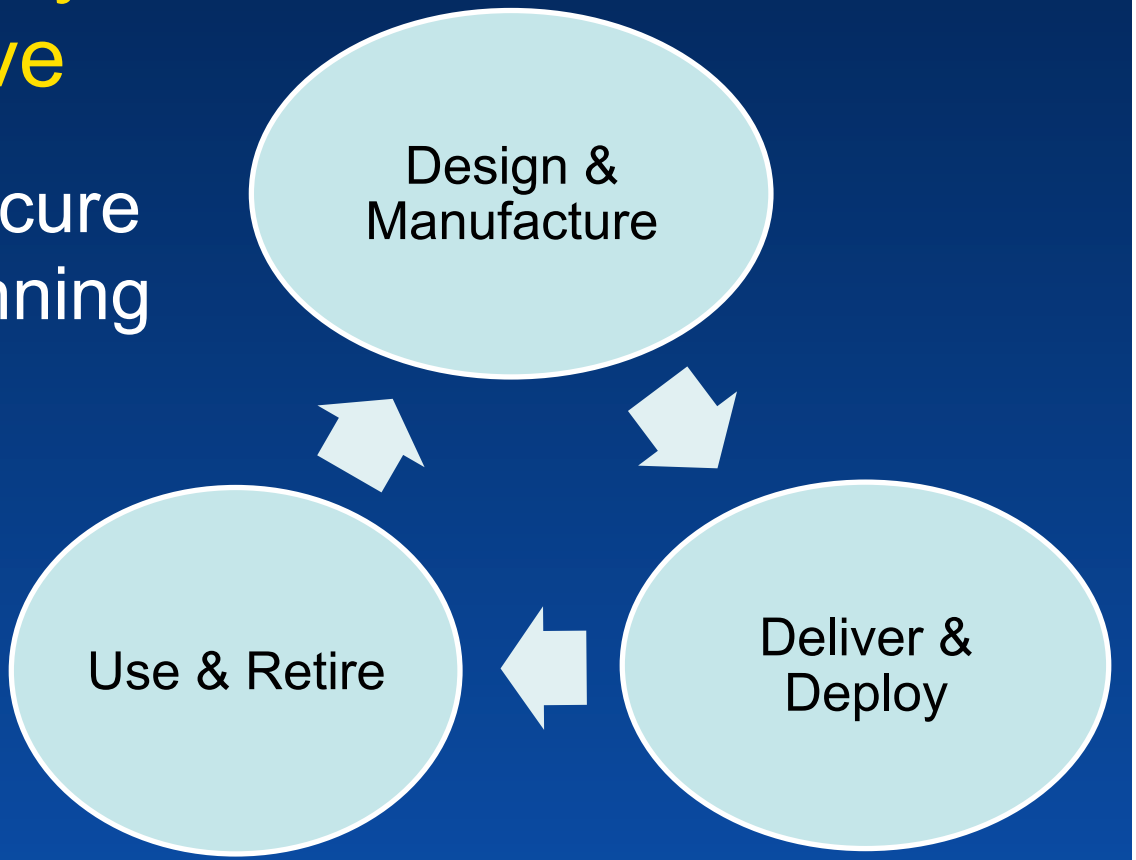
- SSD Lifecycle
- Security threats in SSD
- Security measures for SSD



SSD Life Cycle - Vendor perspective

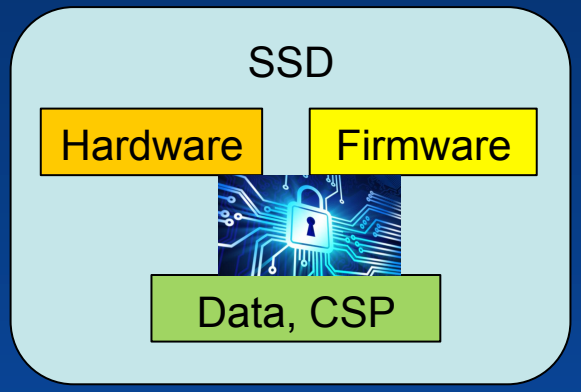
Microsemi
Power Matters.

- Paradigm shift - Secure the SSD from beginning to end of life



SSD Security And Threats

- Secure the Data
  - Protect the user data
- Secure the Product
  - Protect from unauthorized access and the Critical Security Parameters (CSP)
- Secure the Design
  - Protect from Cloning, IP Stealing

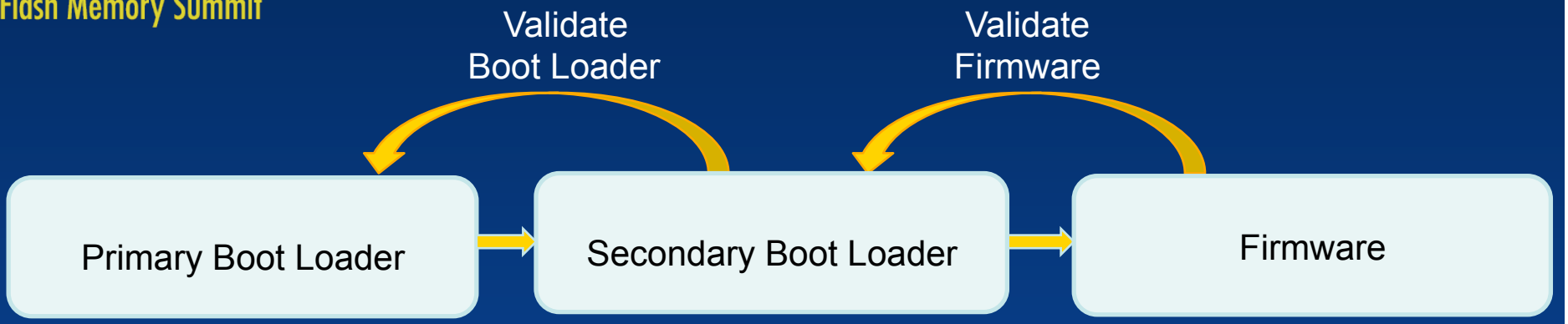


Microsemi
Power Matters.

Security Measures for SSDs

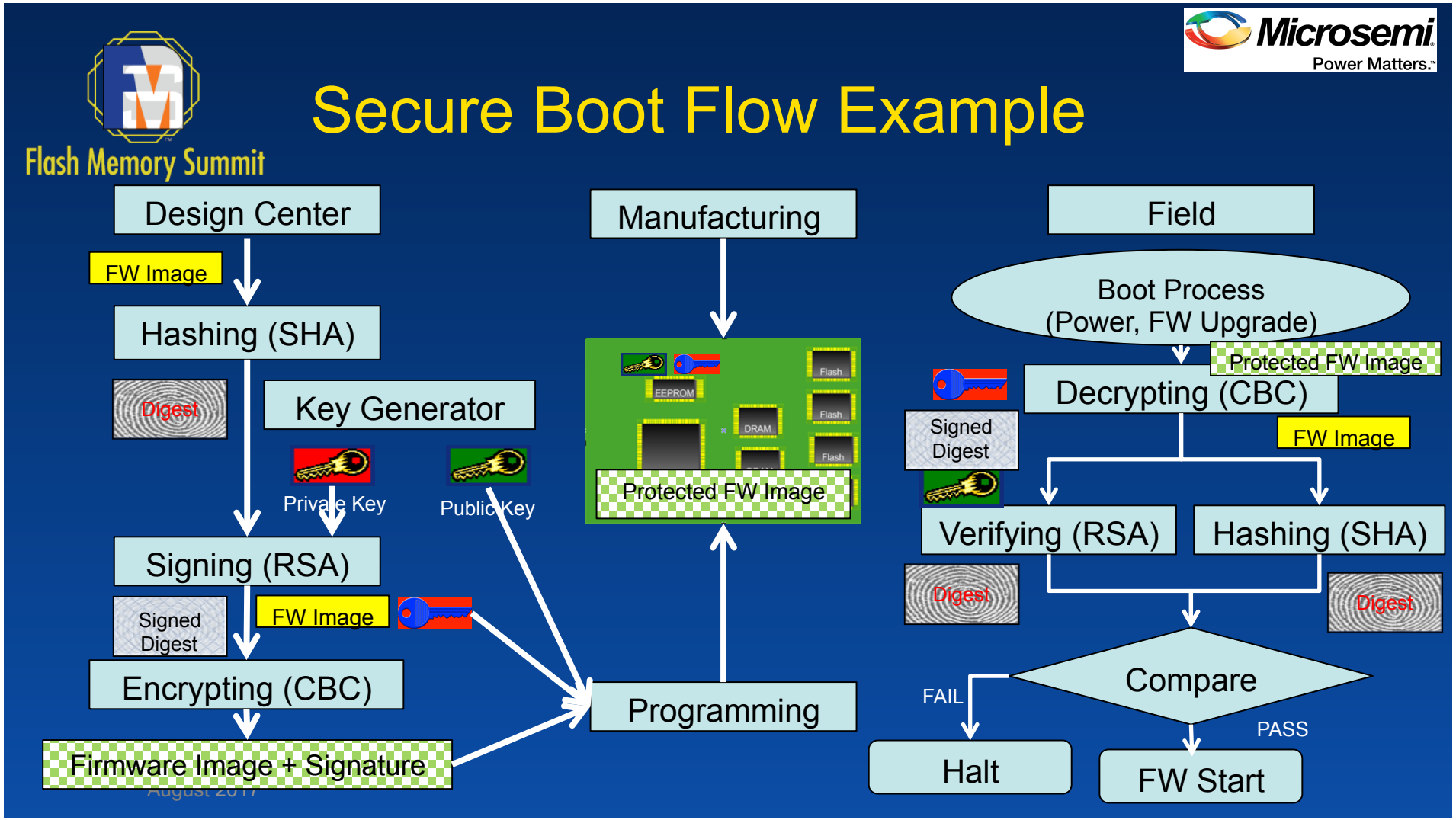
1. Secure Boot
2. Authentication
3. Key Management
4. Data Encryption
5. Physical Security

1. Secure Boot



- Verify the Boot Image and Firmware came from trusted source and has not been tampered with
- Establish a root of trust at the time of design & manufacturing
- Signature Verification (e.g. CRC, SHA, RSA), Encrypted Image (e.g. CBC)

Secure Boot Flow Example



2. Authentication

- Verify the authorized system / users are accessing the service
- Establish a Authentication Key at the time of Manufacturing or deployment
- Authentication using HMAC, SHA-2, Key Unwrapping etc.
- Authentication key may be used for wrapping Data Encryption Keys (DEK)

3. Key Management

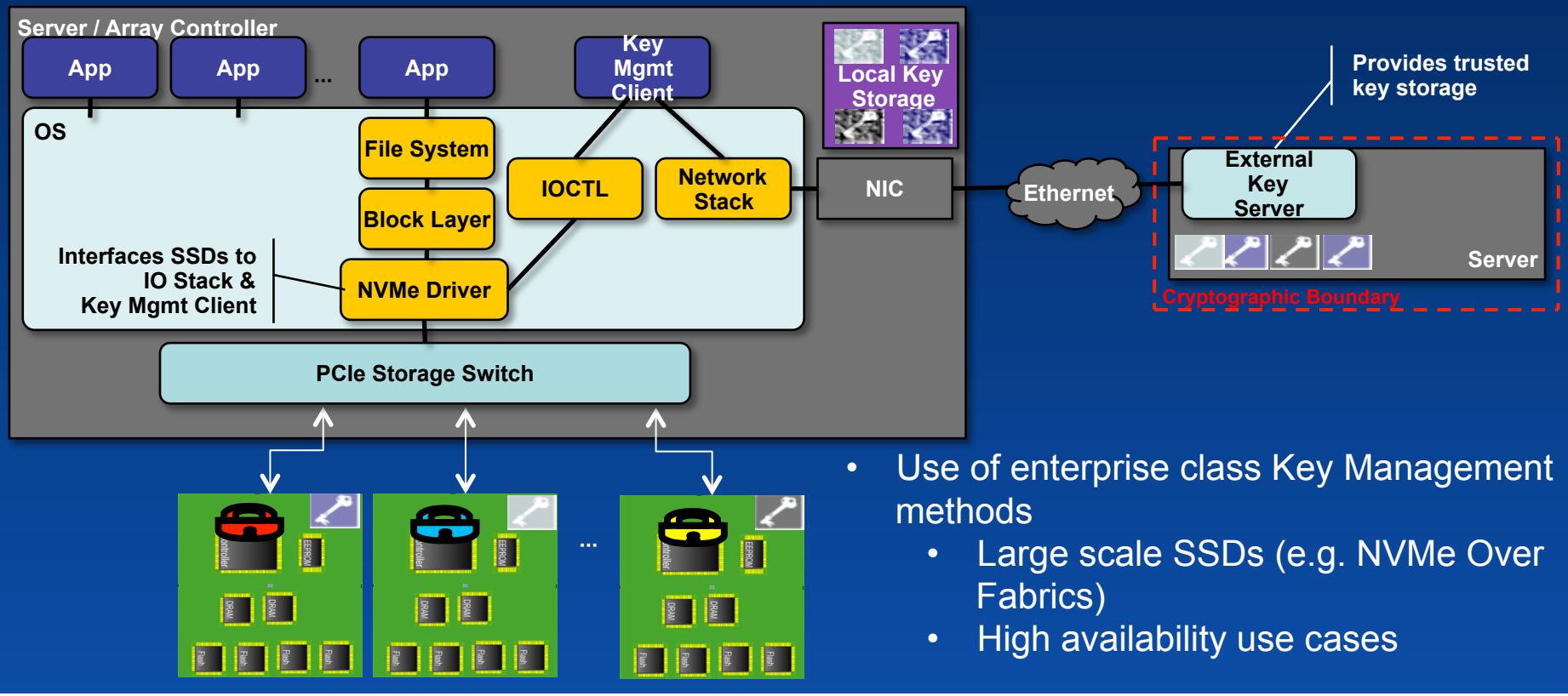
Keys maybe generated and stored locally, or provisioned from the host

- Key is the “Key to overall security” – determines the security strength, instant secure erase, different keys for different user data
- Flexibility - Keys either locally generated using TRNG (True Random Number Generator) or provisioned and managed through an external Key Server
- Scalability is an important factor for enterprise applications
- Securely store and manage the keys - Key Wrapping and Unwrapping functions, establish root of trust from manufacturing or deployment time

Flash Memory Summit

Microsemi
Power Matters.

Flash Array Key Management



- Use of enterprise class Key Management methods
  - Large scale SSDs (e.g. NVMe Over Fabrics)
  - High availability use cases

4. Data Encryption

- Protect the user data-at-rest
- Encryption / Decryption using standard algorithm (XTS-AES) with 256 bit keys
- No performance degradation
- Power on and On-demand Self-test

5. Physical Protection

- Protect from snooping, tampering, backdoor access etc.
- Cross check any exposure of CSP, loopholes due to error conditions during design itself
- Establish a secure supply chain
- FIPS compliant design

Microsemi
Power Matters.

Summary

- Secure the SSD in all phases of life
- Protect the Design, Product and User Data
- Secure Boot, Authentication, Key Management, Data Encryption and Physical protection are the key security features of an enterprise SSD

Thanks!!

Flash Memory Summit

- Microsemi offers range of products for Flash Security (Come and visit us at booth #213)
- www.microsemi.com