Bootloader

BCC Salon Sept. 14, 2022

Presented By: Cramium Labs

Cramium Labs

- Last Silicon Salon we presented as Crossbar Inc.
- Cramium Labs is a division of Crossbar.
- www.cramiumlabs.com
- Mehdi Asnaashari, VP of System Engineering

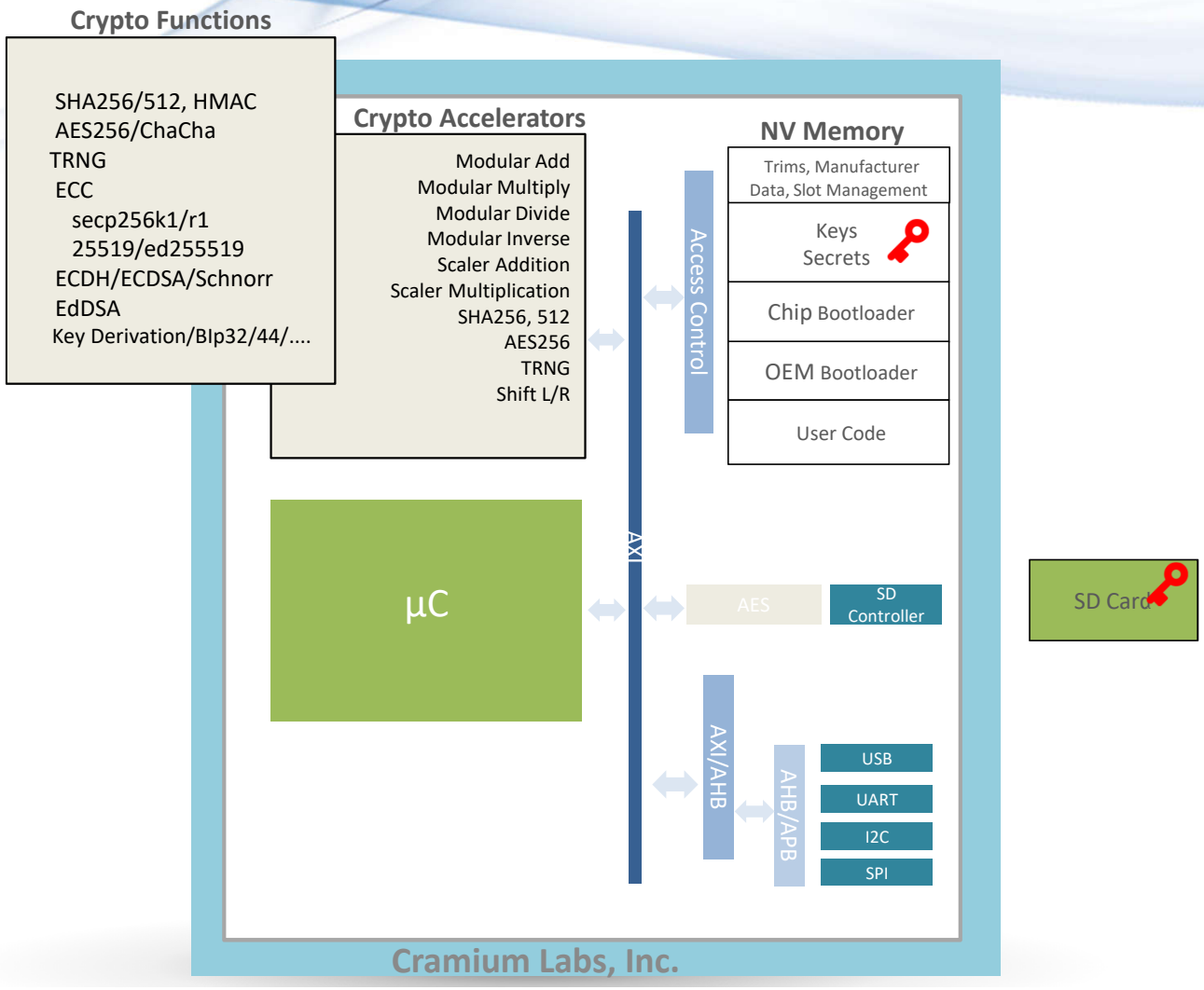
Our mission is to create a breakthrough security platform for the crypto industry that is best-in-class, purpose-built, and tamper-resistant to address the rapidly-evolving security needs of the industry

Bootloader

- What Bootloader should the Chip Manufacturer ship?
  - Only minimum code to open the communication ports for OEM bootloader?
  - Perform all Crypto functions?
  - Or something in between?

- How Much OEMs trust the Manufacturer?
  - How to improve the perception?

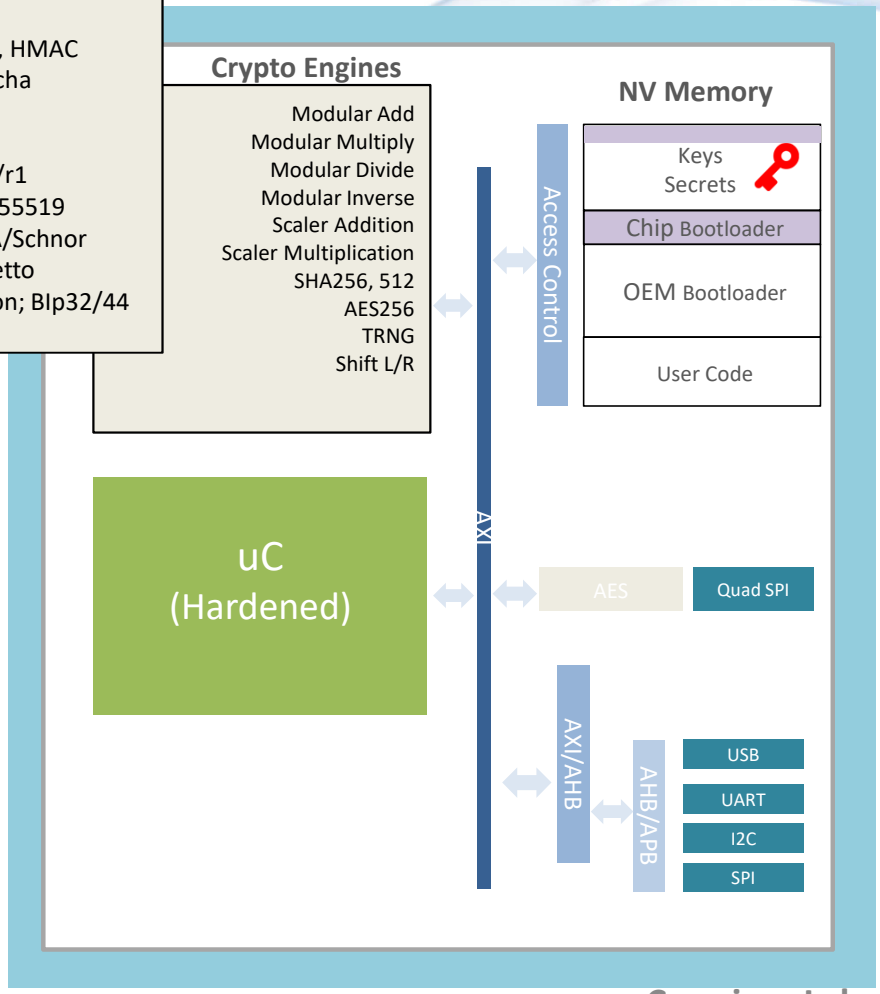
Block Diagram of a Crypto Processor



Minimalistics View

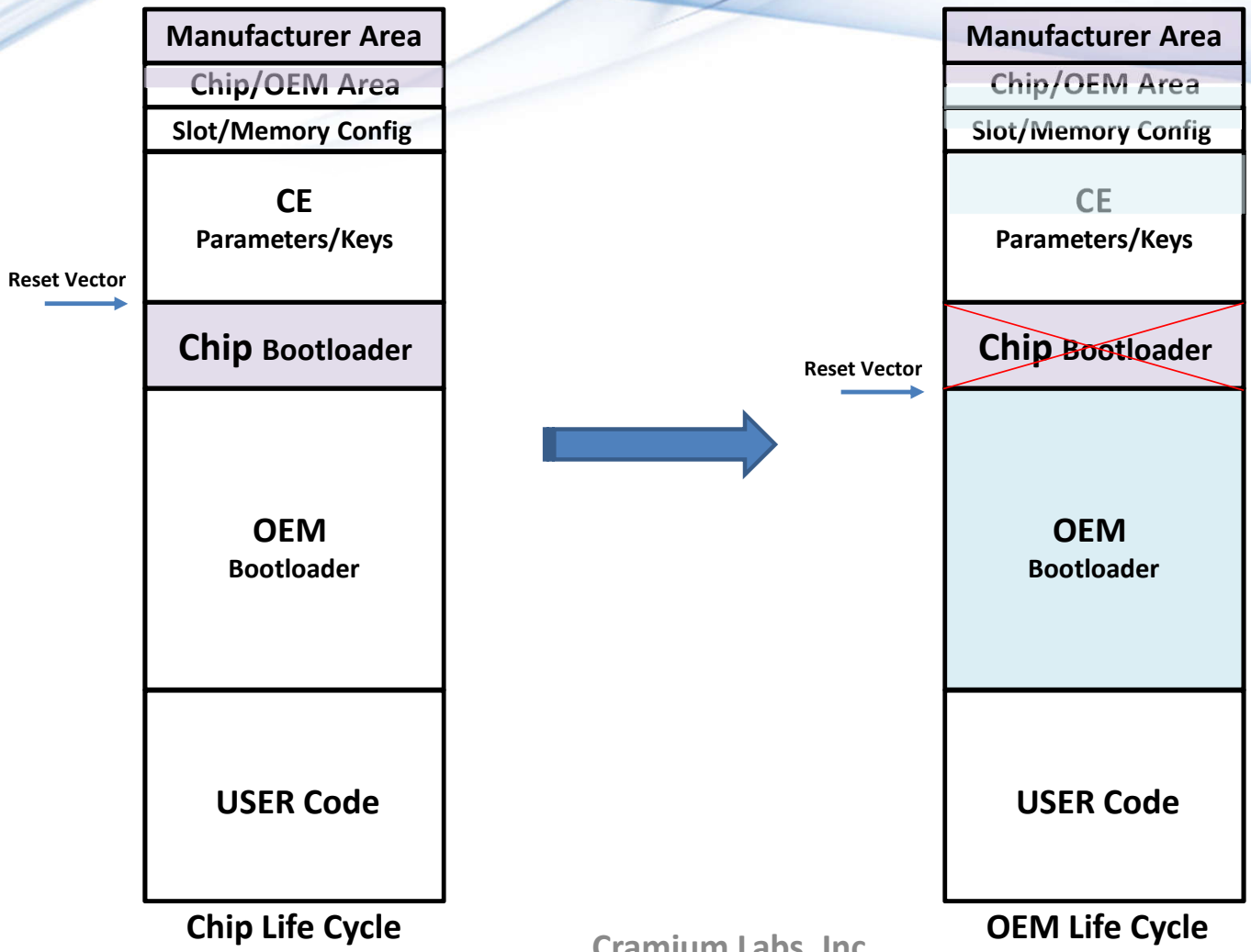
Crypto Functions

SHA256/512, HMAC
AES256/Chacha
TRNG
ECC
secp256k1/r1
25519/ed255519
ECDH/ECDSA/Schnor
EdDSA/Ristretto
Key Derivation; BIp32/44



Manufacturer Area	**Calibration Data, Manufacturer information**
Chip/OEM Area	**Life Cycle, …..**
Slot/Memory Config	**Slot and memory configuration**
CE Parameters/Keys	
Chip Bootloader	**Opens input Ports to Load OEM Bootloader, Execute only, no Read/Write**
OEM Bootloader	
USER Code	

Life Cycle Progression (Chip → OEM)

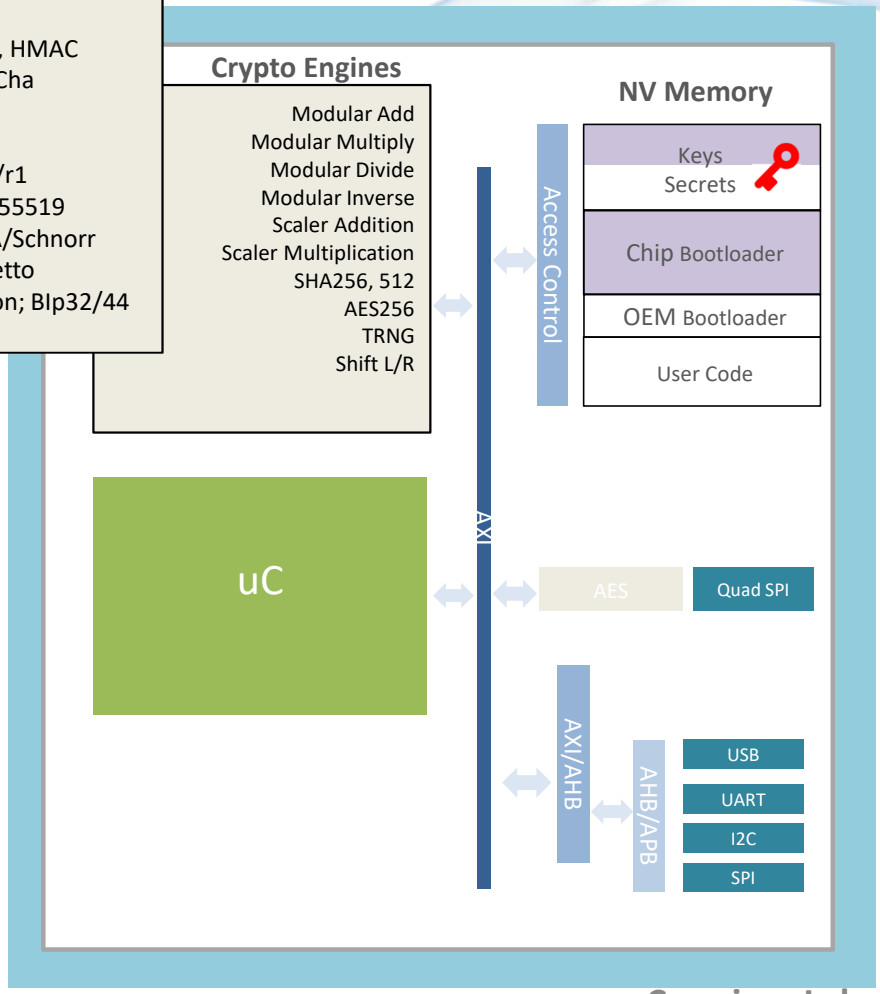


Opens input Ports to Load CHIP and/or OEM Bootloader, Execute only, no Read/Write
Runs POST (Power on self test)
Processes all crypto functions
Once loaded, Execute only, no Read/Write
Not upgradable

Full Feature Software

Crypto Functions

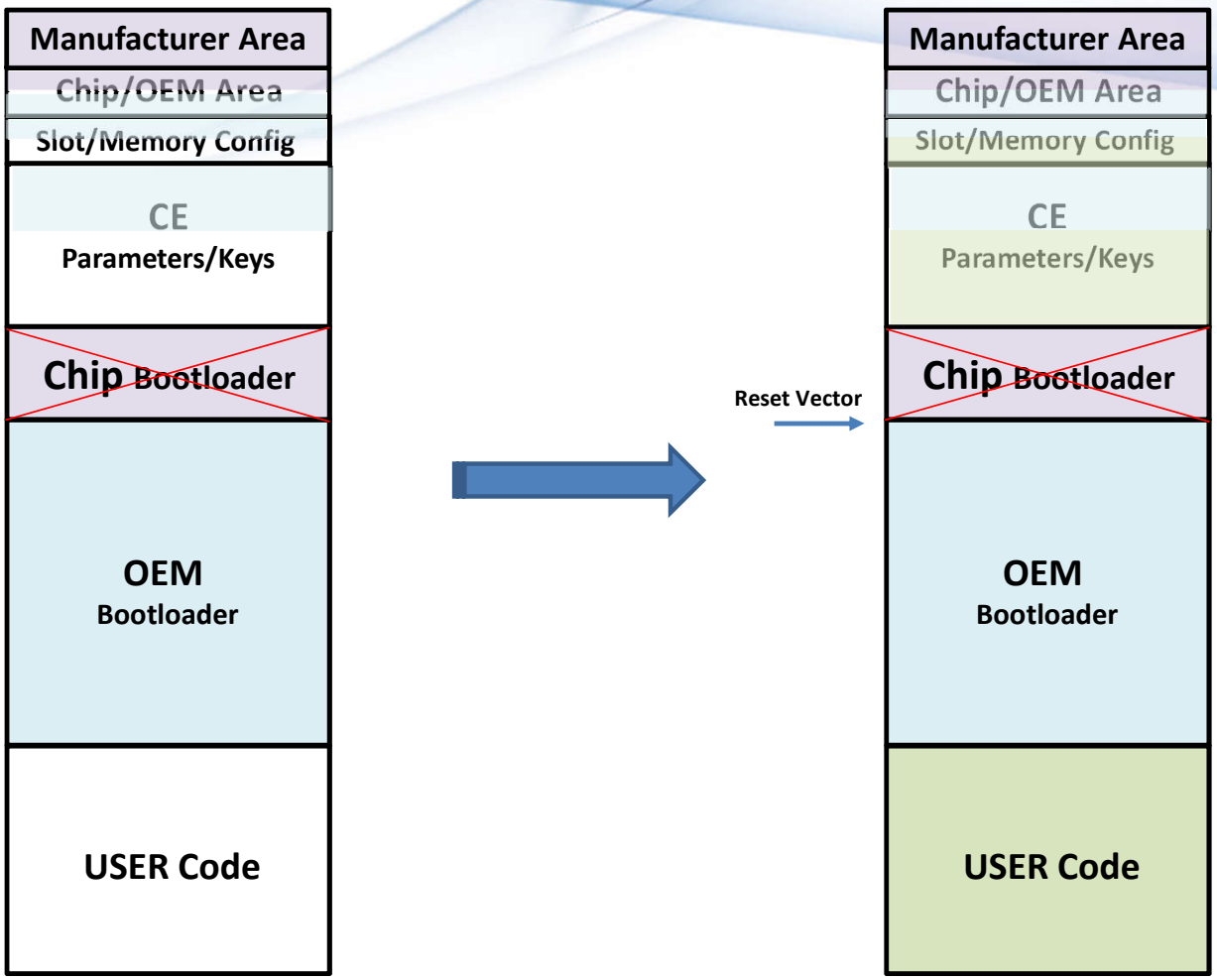
SHA256/512, HMAC
AES256/ChaCha
TRNG
ECC
secp256k1/r1
25519/ed255519
ECDH/ECDSA/Schnorr
EdDSA/Ristretto
Key Derivation; BIp32/44



Reset Vector

Manufacturer Area	Calibration Data, Manufacturer information
Chip/OEM Area	Life Cycle, …..
Slot/Memory Config	Slot and memory configuration
CE Parameters/Keys	Keys, Passwords, Seeds
Chip Bootloader	Opens input Ports to Load CHIP and/or OEM Bootloader, Execute only, no Read/Write Runs POST (Power on self test) Processes all crypto functions Once loaded, Execute only, no Read/Write, not upgradable
OEM Bootloader	Any additional crypto functions/improvements Once loaded, Execute only, no Read/Write, not upgradable
USER Code	Non-critical Code/secrets IO HAL, Display, Keypad, Parsing Commands Signed by OEM

Life Cycle Progression (OEM → User)



Opens input Ports to Load CHIP and/or OEM Bootloader, Execute only, no Read/Write
Runs POST (Power on self test)
Processes all crypto functions
Once loaded, Execute only, no Read/Write
Not upgradable

Upgradable
Signed by OEM

Questions?

- What should Chip manufacturer further improve ?
  - Supply Chain authentication at Chip level?
  - Support Reverse Life Cycle Progression
    - Destroy all Secrets?

Thank You