# 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-inclass, purpose-built, and tamper-resistant to address the rapidly-evolving security needs of the industry

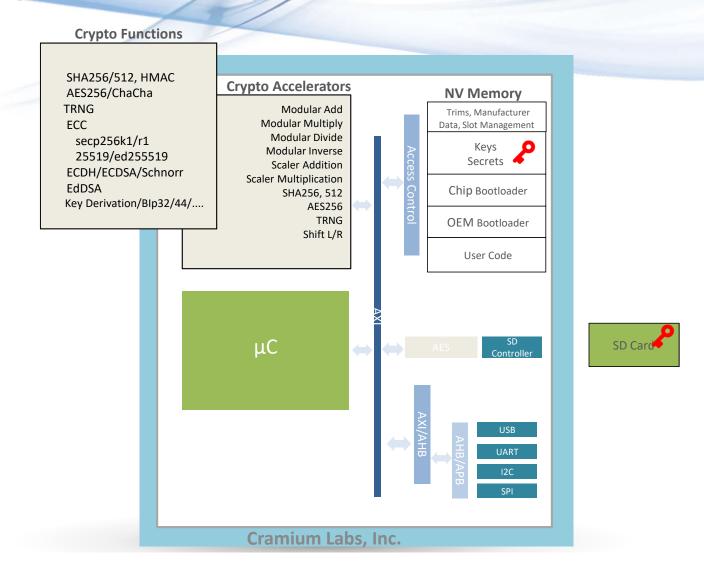
Cramium Labs 2

#### **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?

Cramium Labs, Inc.

### **Block Diagram of a Crypto Processor**



#### **Minimalistics View**

**Crypto Functions** SHA256/512, HMAC **Crypto Engines** AES256/Chacha **NV Memory TRNG** Modular Add **Modular Multiply** ECC Modular Divide secp256k1/r1 Secrets Modular Inverse 25519/ed255519 Scaler Addition Chip Bootloader ECDH/ECDSA/Schnor Scaler Multiplication EdDSA/Ristretto SHA256, 512 **OEM** Bootloader Key Derivation; Blp32/44 AES256 TRNG Shift L/R User Code uC Quad SPI (Hardened) Cramium Labs, Inc.

Manufacturer Area
Chip/OEM Area
Slot/Memory Config

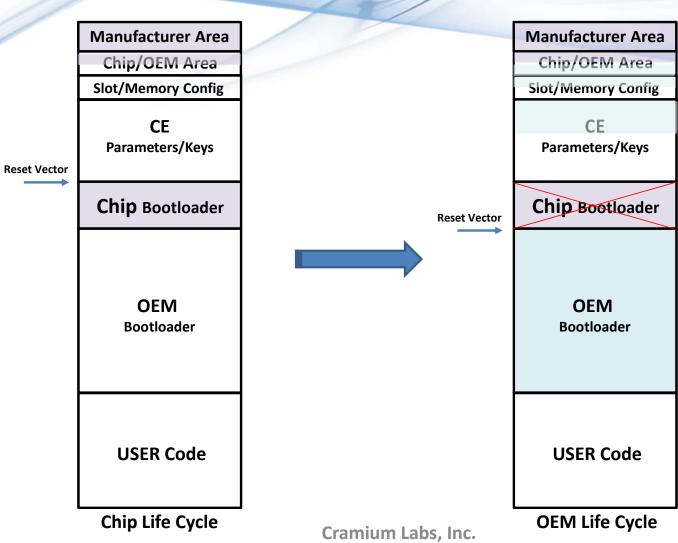
CE
Parameters/Keys

Opens input Ports to Load OEM Bootloader, Execute only, no Read/Write

OEM
Bootloader

**USER Code** 

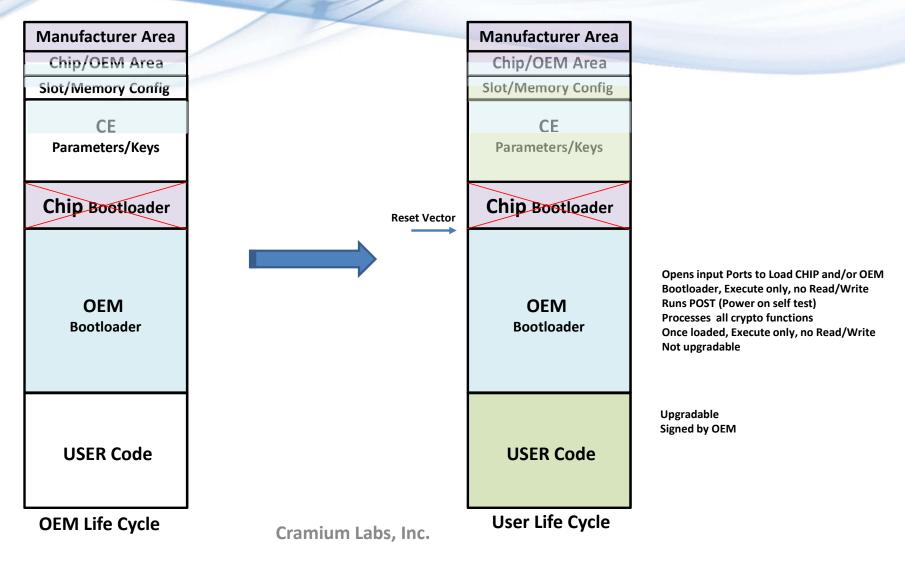
# Life Cycle Progression (Chip → OEM)



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 **Manufacturer Area Calibration Data, Manufacturer information** SHA256/512, HMAC **Crypto Engines** AES256/ChaCha **NV Memory** Chip/OEM Area Life Cycle, ..... **TRNG** Modular Add **Modular Multiply** ECC Slot/Memory Config Slot and memory configuration Modular Divide secp256k1/r1 Secrets Modular Inverse 25519/ed255519 CE Scaler Addition ECDH/ECDSA/Schnorr Keys, Passwords, Seeds Scaler Multiplication Chip Bootloader Parameters/Keys EdDSA/Ristretto SHA256, 512 Reset Vector Key Derivation; Blp32/44 AES256 **OEM** Bootloader TRNG Shift L/R User Code Opens input Ports to Load CHIP and/or OEM Bootloader, Execute only, no Read/Write Runs POST (Power on self test) Chip **Processes all crypto functions Bootloader** Once loaded, Execute only, no Read/Write, not upgradable uC **Quad SPI OEM** Any additional crypto functions/improvements Once loaded, Execute only, no Read/Write, not Bootloader upgradable Non-critical Code/secrets **USER Code** IO HAL, Display, Keypad, Parsing Commands Signed by OEM

Cramium Labs, Inc.

# Life Cycle Progression (OEM → User)



#### **Questions?**

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

Cramium Labs, Inc.

# Thank You