Embedded Linux Conference
Europe

OpenIoTSummit
Europe

Linaro

MCUboot: Multi-Image

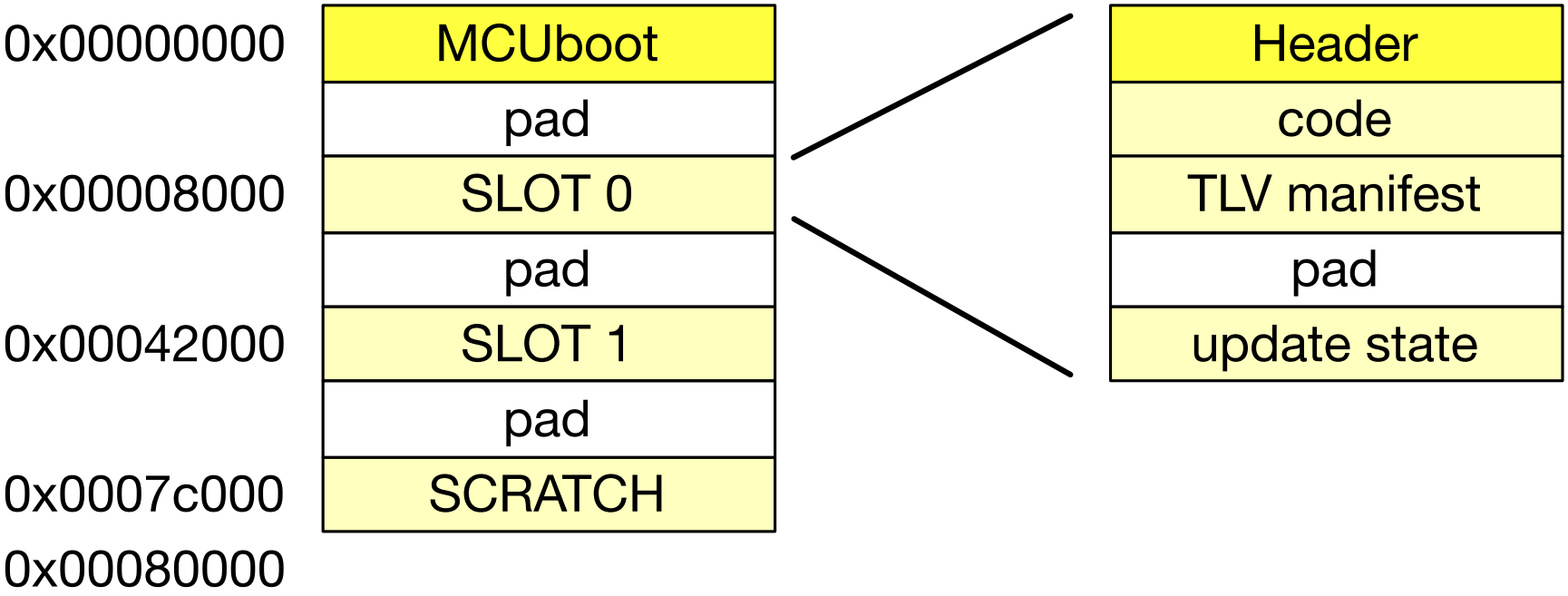
David Brown

THE LINUX FOUNDATION

MCUboot

- MCU: microcontroller
- Boot: bootloader
- Root of trust
- Validates images before booting or upgrading

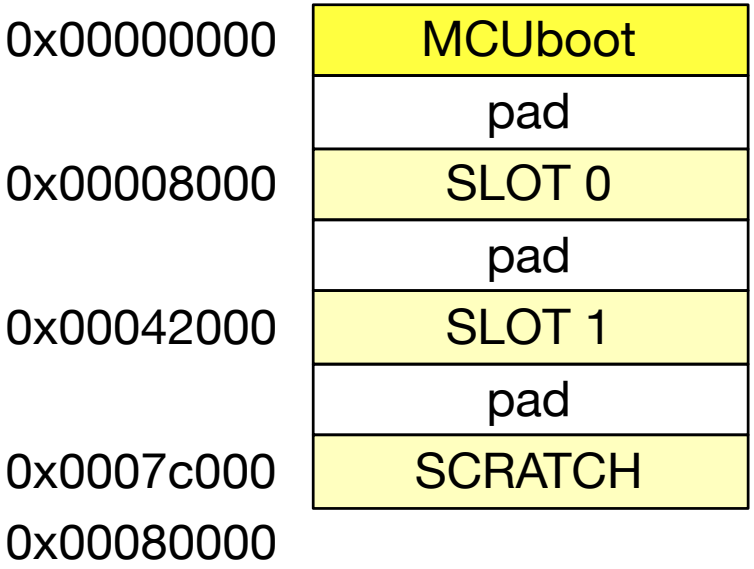
MCUboot memory map



MCUboot Current Features

- Supports XIP MCUs
- Flash is partitioned into two “slots” and a “scratch area”
- It can validate an RSA or ECDSA signature before booting
- If slot1 is newer than slot0, and valid, it can upgrade
- Upgrade is either overwrite, or swap

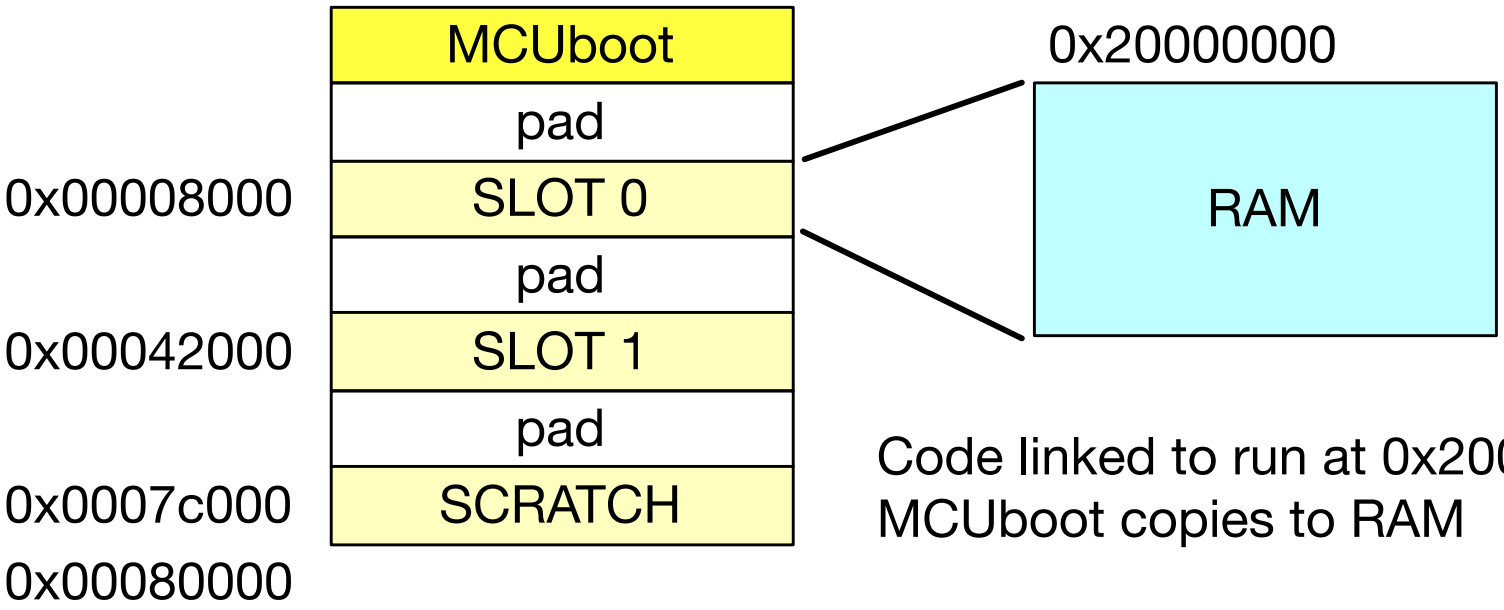
XIP (eXecute In Place)



code linked at 0x8000
and runs out of flash directly

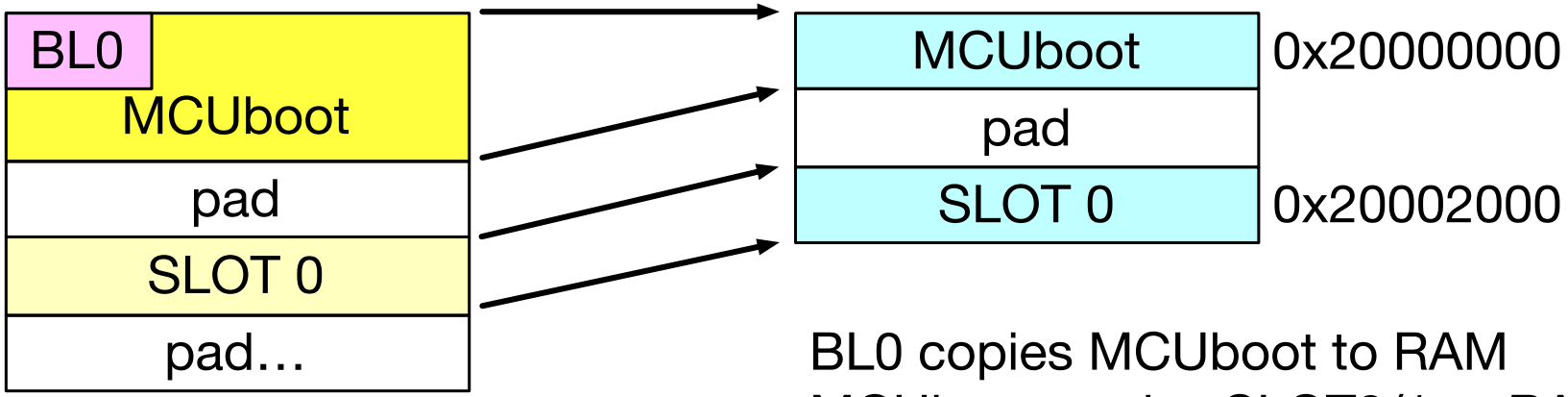
upgrade linked at 0x8000, and
must be moved to SLOT 0 to run

Non-XIP



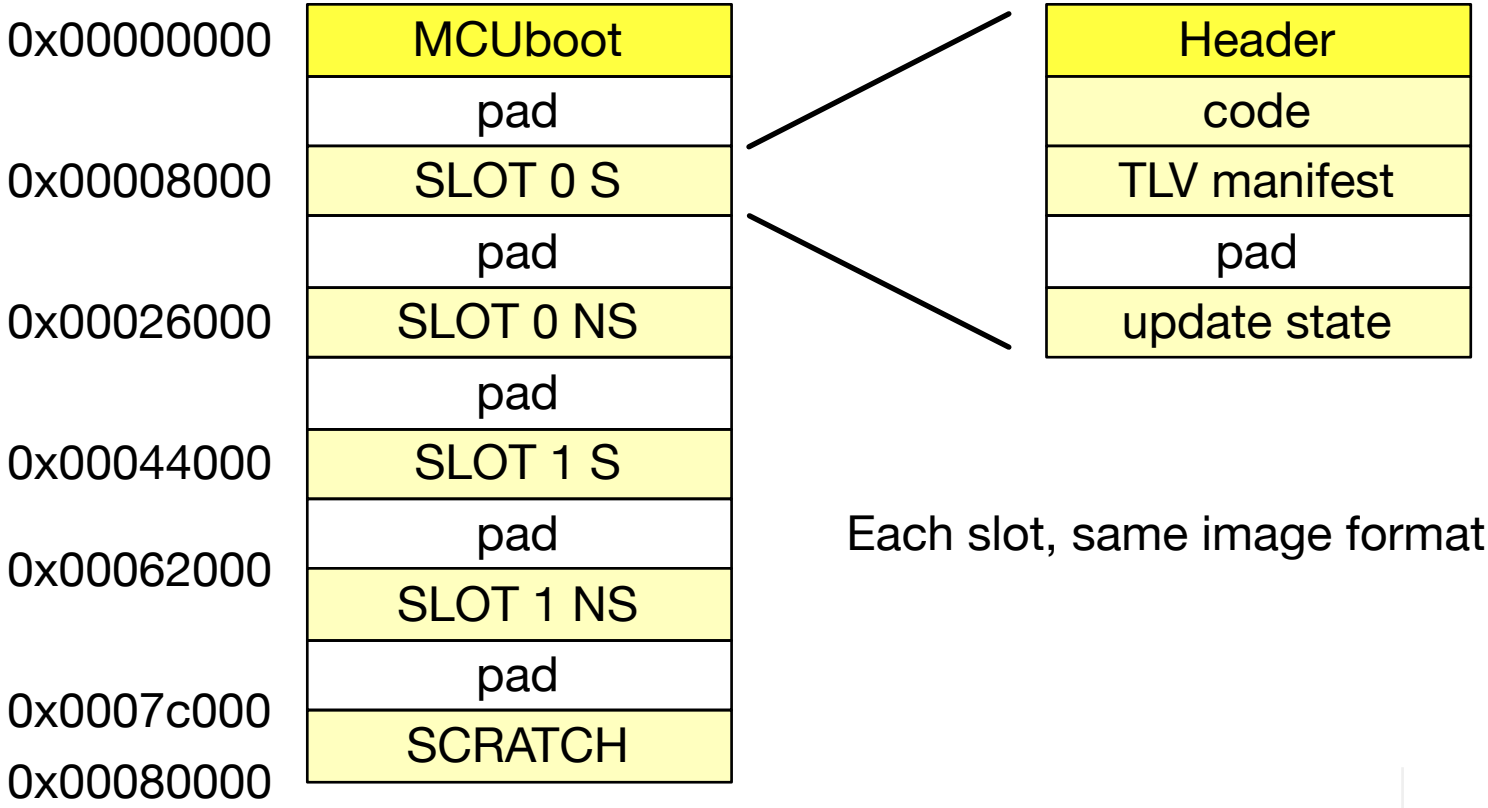
Code linked to run at 0x2000000
MCUboot copies to RAM

Non-XIP reality



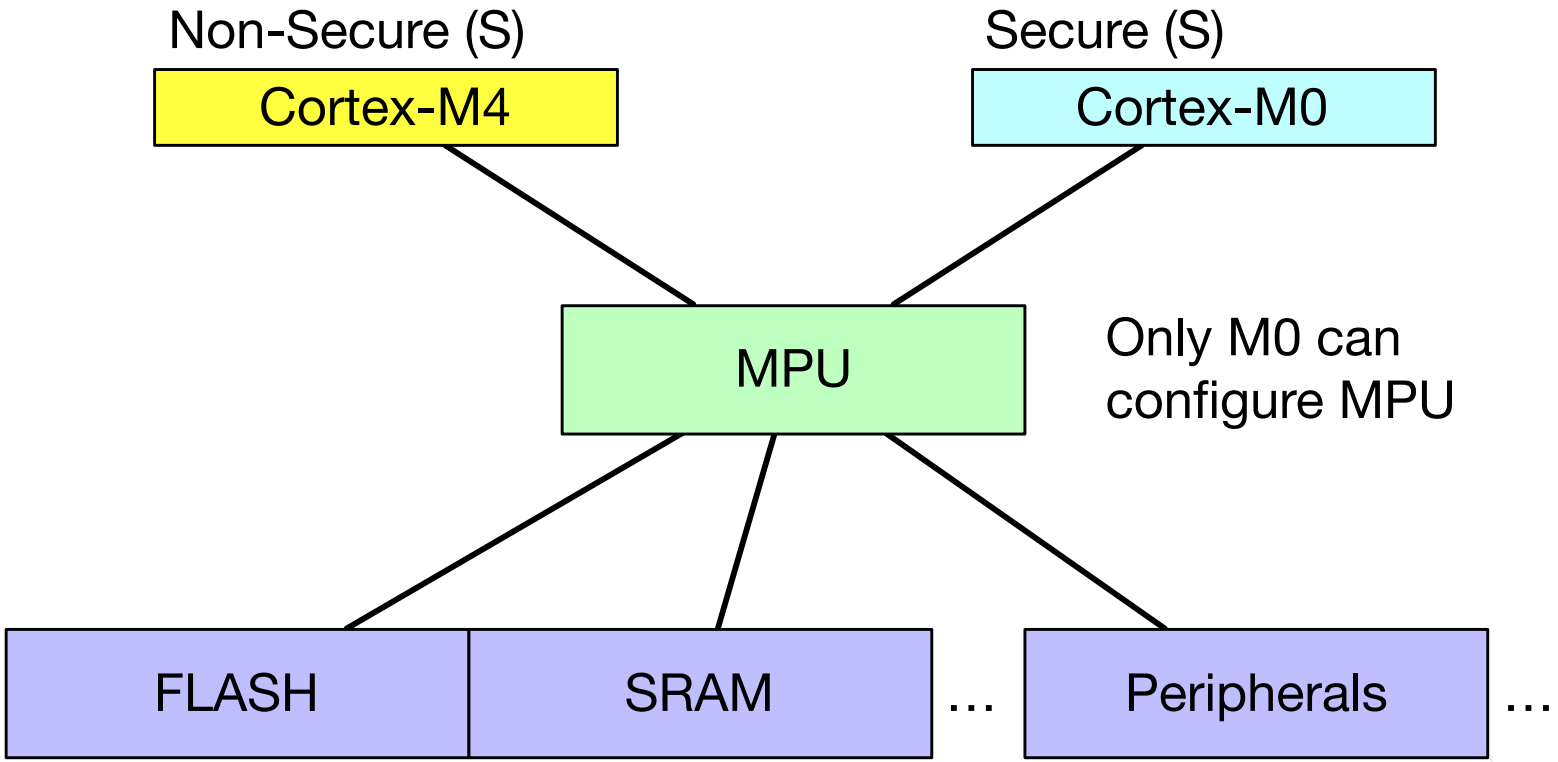
BL0 copies MCUboot to RAM
MCUboot copies SLOT0/1 to RAM

Multi-image

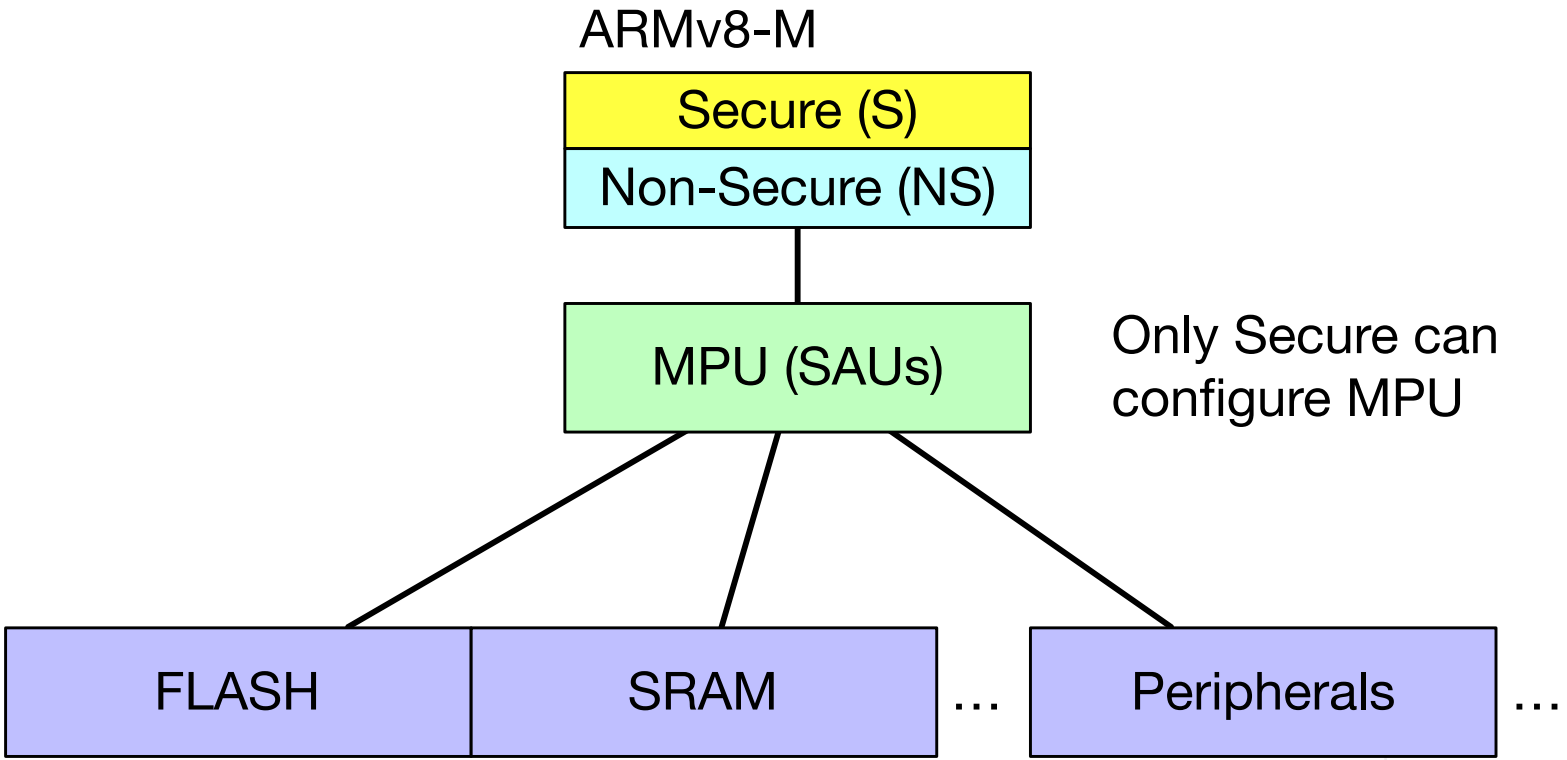


Each slot, same image format

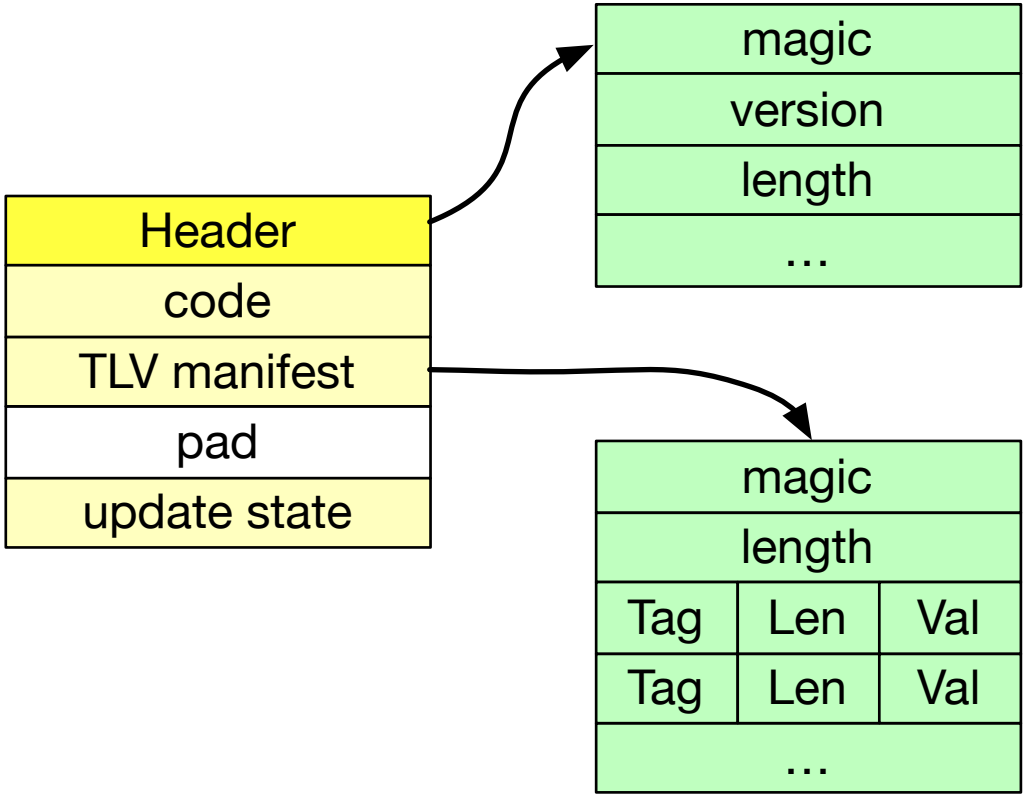
Multiple CPUs



Trusted Execution



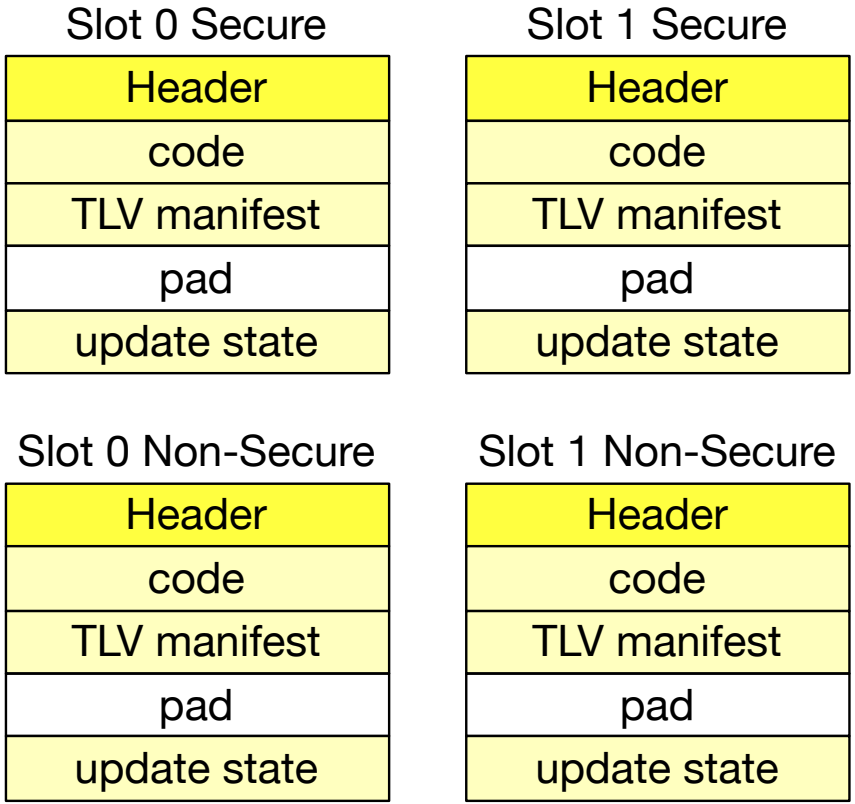
The manifest



Example tags

SHA256
Key hash
RSA2048 PSS
Key hash 2
ECDSA256

Multi-manifest



Multi-manifest + dependencies

Slot 0 Secure

Header
code
TLV manifest
pad
update state

Slot 1 Secure

Header
code
TLV manifest
pad
update state

Slot 0 Non-Secure

Header
code
TLV manifest
pad
update state

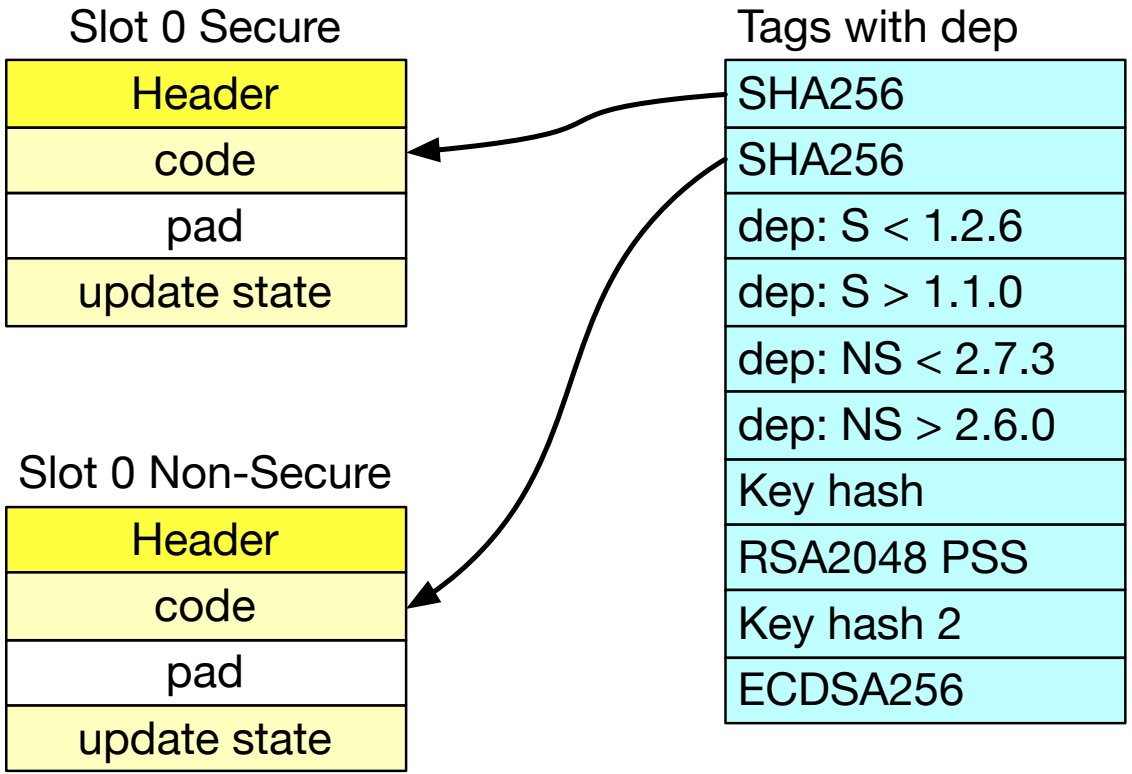
Slot 1 Non-Secure

Header
code
TLV manifest
pad
update state

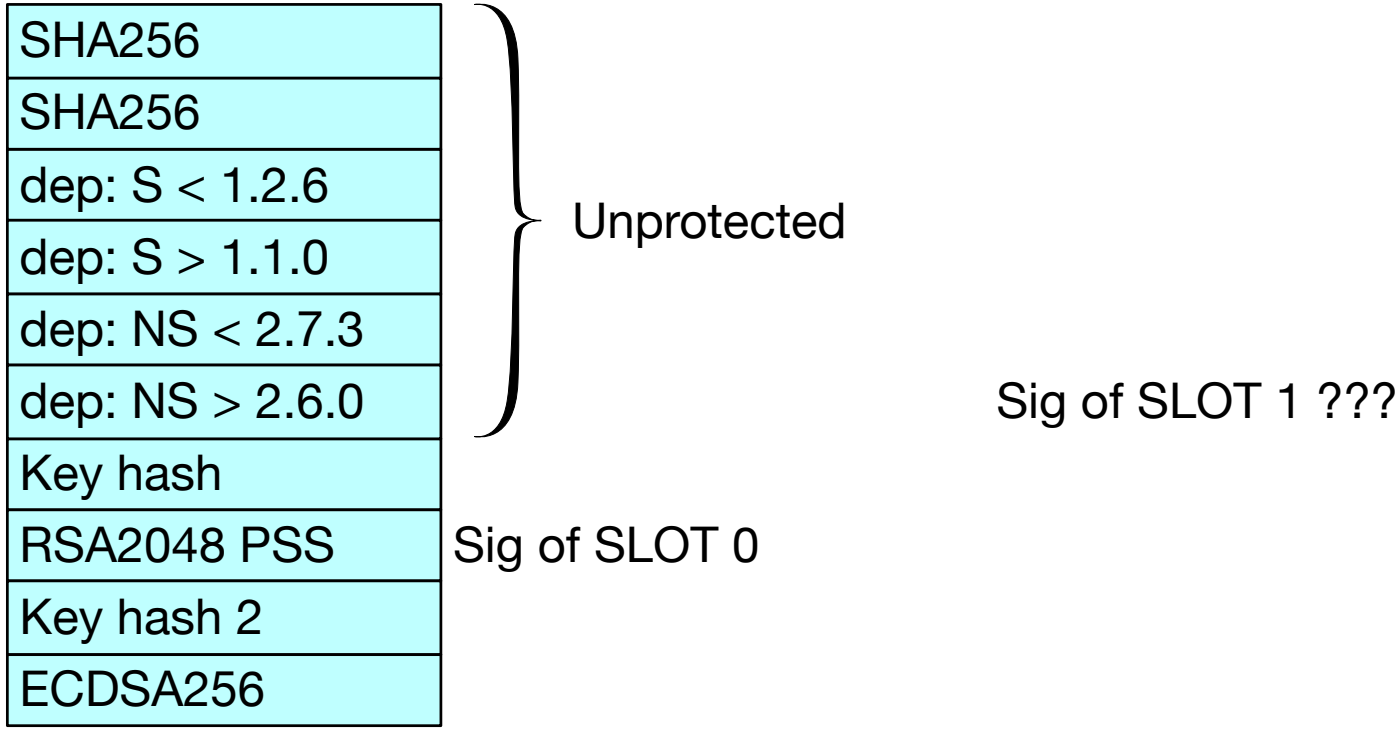
Tags with dep

SHA256
dep: S < 1.2.6
dep: S > 1.1.0
Key hash
RSA2048 PSS
Key hash 2
ECDSA256

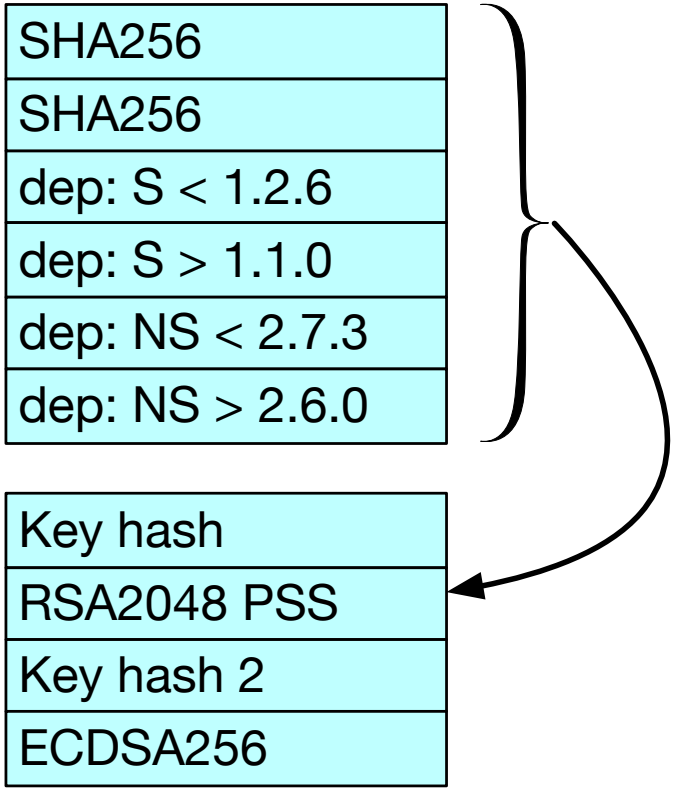
Detached manifest



What is signed?



Sign the manifest

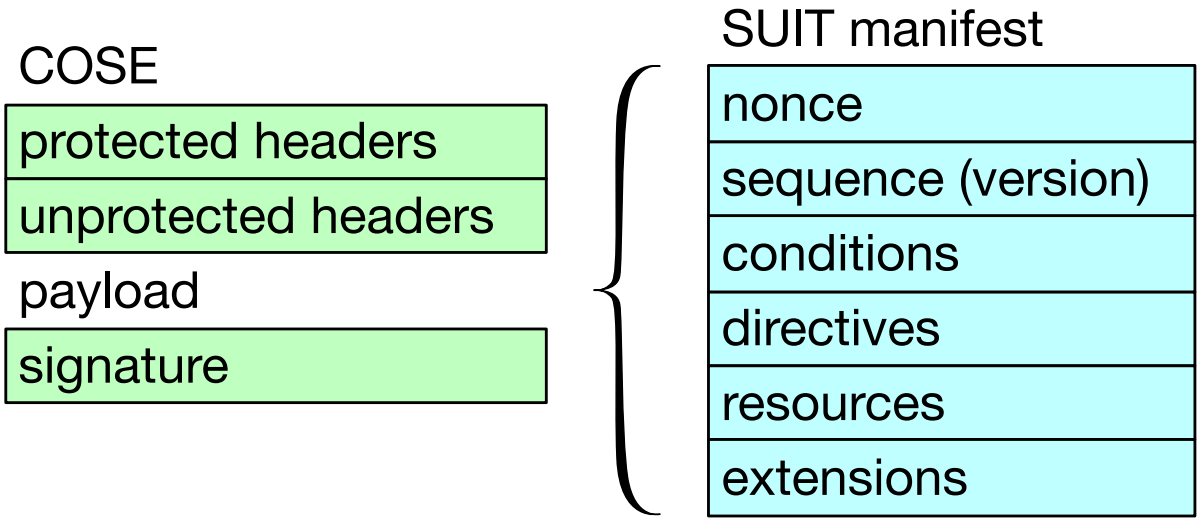


- Sign the first part of manifest
- Protects everything in manifest
- Allows multiple images

SUIT

https://datatracker.ietf.org/wg/suit/about/

COSE SUIT



all encoded in CBOR

“resources” contains hash of each image

MCUboot plans

- SUIT: wait
- Non-XIP: now
- Multiple images
  - Each with manifest: now
  - Detached manifest: do we need it?