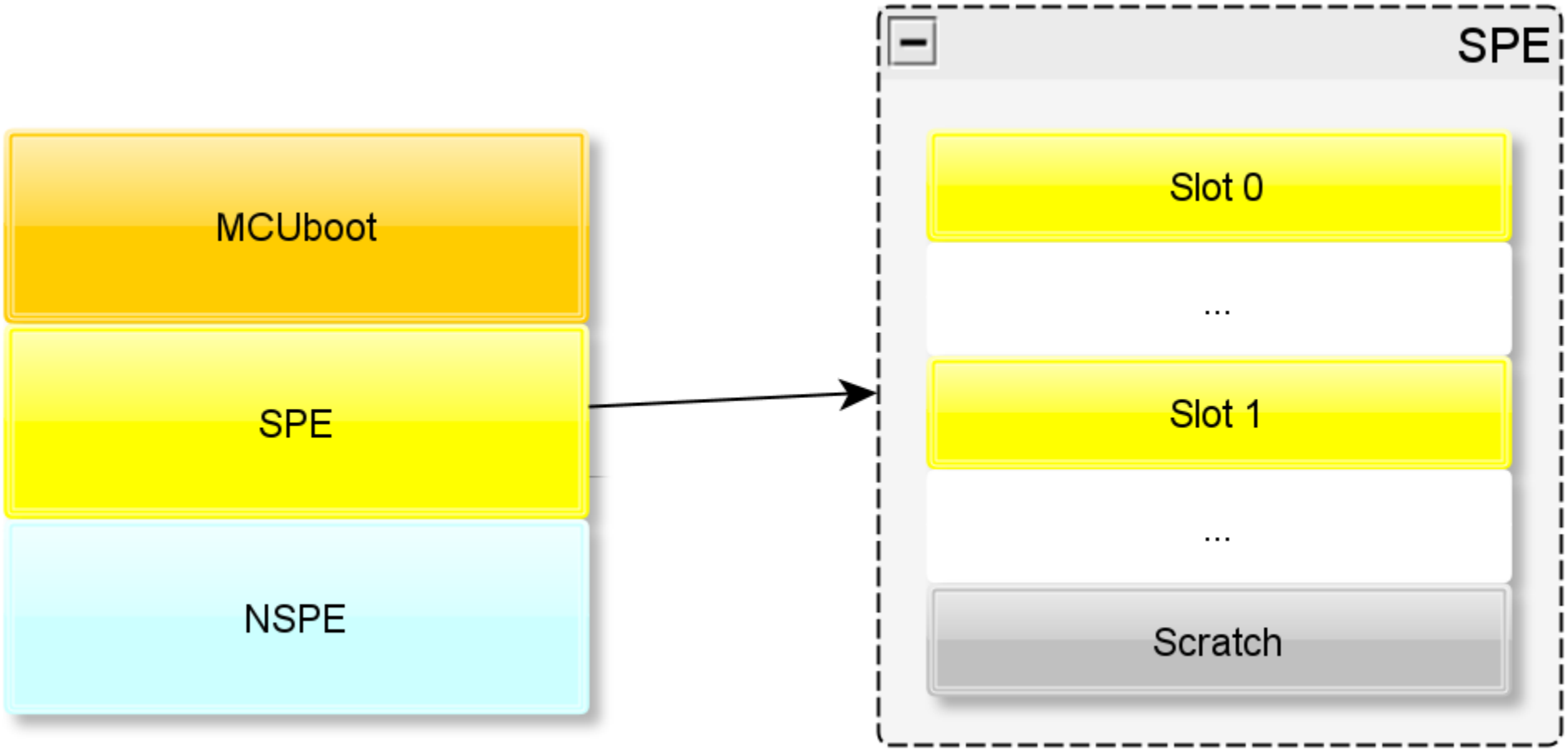
MCUBoot Attestation

David Brown

What is MCUboot



MCUboot

- Secure bootloader
- Its History
- Manages signed images
- Handles updates, maintaining security
- Currently, custom manifest (SUIT maybe some day)

What is TF-M

- Reference implementation of PSA
- Implements secure and non-secure environments
- Does many things

Upstream & TF-M MCUboot

- TF-M started with a fork of MCUboot
- Convergence is underway
- Goal is for MCUboot to be a submodule

Claims from MCUboot

- Handful of claims come from MCUboot
  - Versions of images
  - Hashes and keys involved in these images
  - State of boot
- More are described in the TF-M code than implemented
- More may be useful (e.g. how MCUboot itself is configured)

Keys and provisioning

- Different keys for different purposes
- MCUboot has one or more public keys
  - Currently compiled into the code, and immutable
  - Other images are signed with these keys
- Attestation needs private keys to sign token
- Device probably needs other keys
  - Root certs for secure communication
  - Private keys to authenticate with services

Provisioning keys

- MCUboot public key currently hardcoded
- Private keys: something has to be done at the factory
- Key management
- For private key, how to manage public key?
- Talking with industry, people seem to normally use X.509 certs to demonstrate device identity