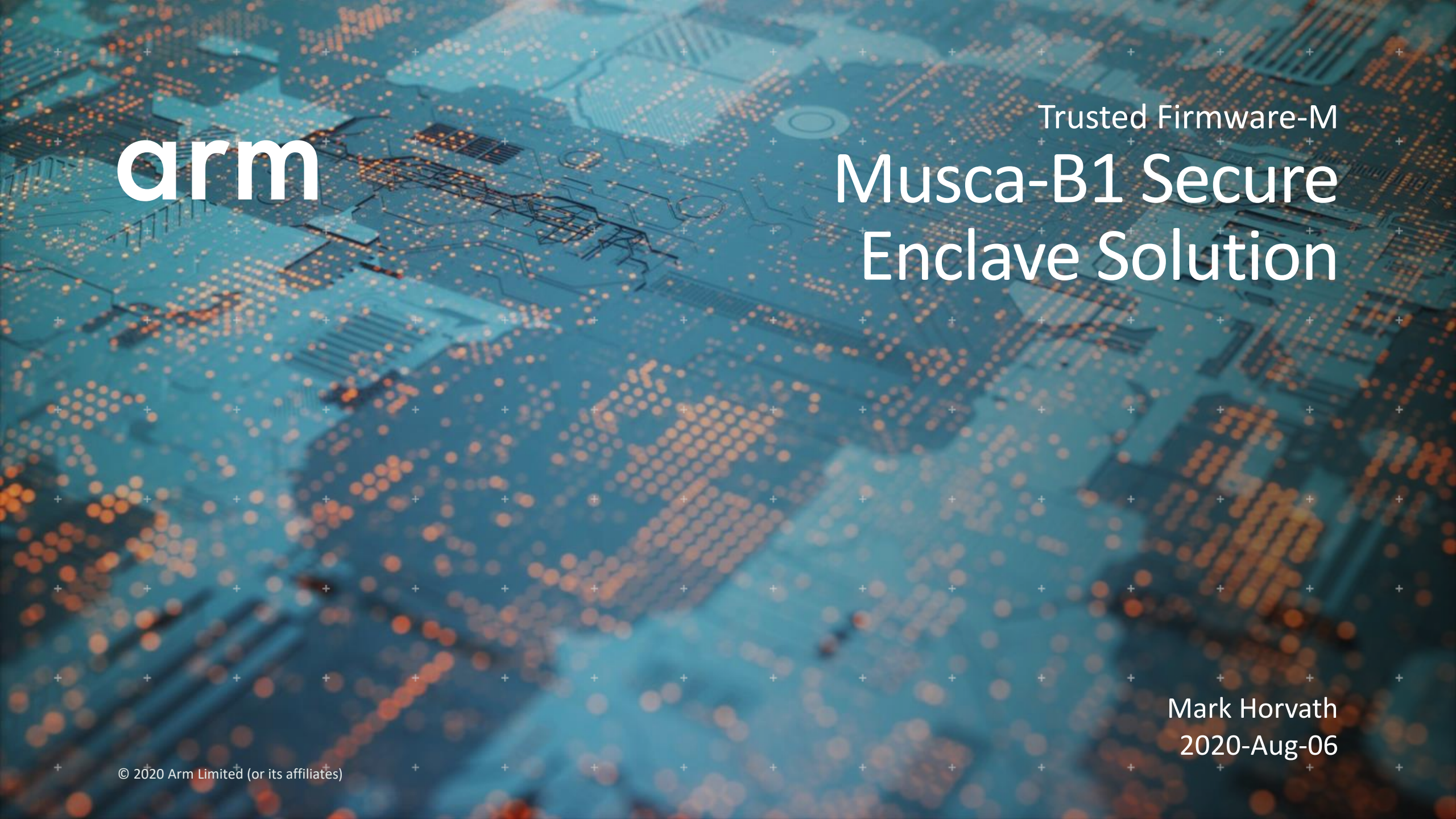


Trusted Firmware-M

Musca-B1 Secure Enclave Solution

Mark Horvath

2020-Aug-06

Agenda

- Goals of the Secure Enclave solution
- Limitations in the Musca-B1 board
- Flash layout and boot-flow
- Details of IPC message forwarding

Reference open source Secure Enclave solution

Secure Enclave is a separate subsytem next to an application core

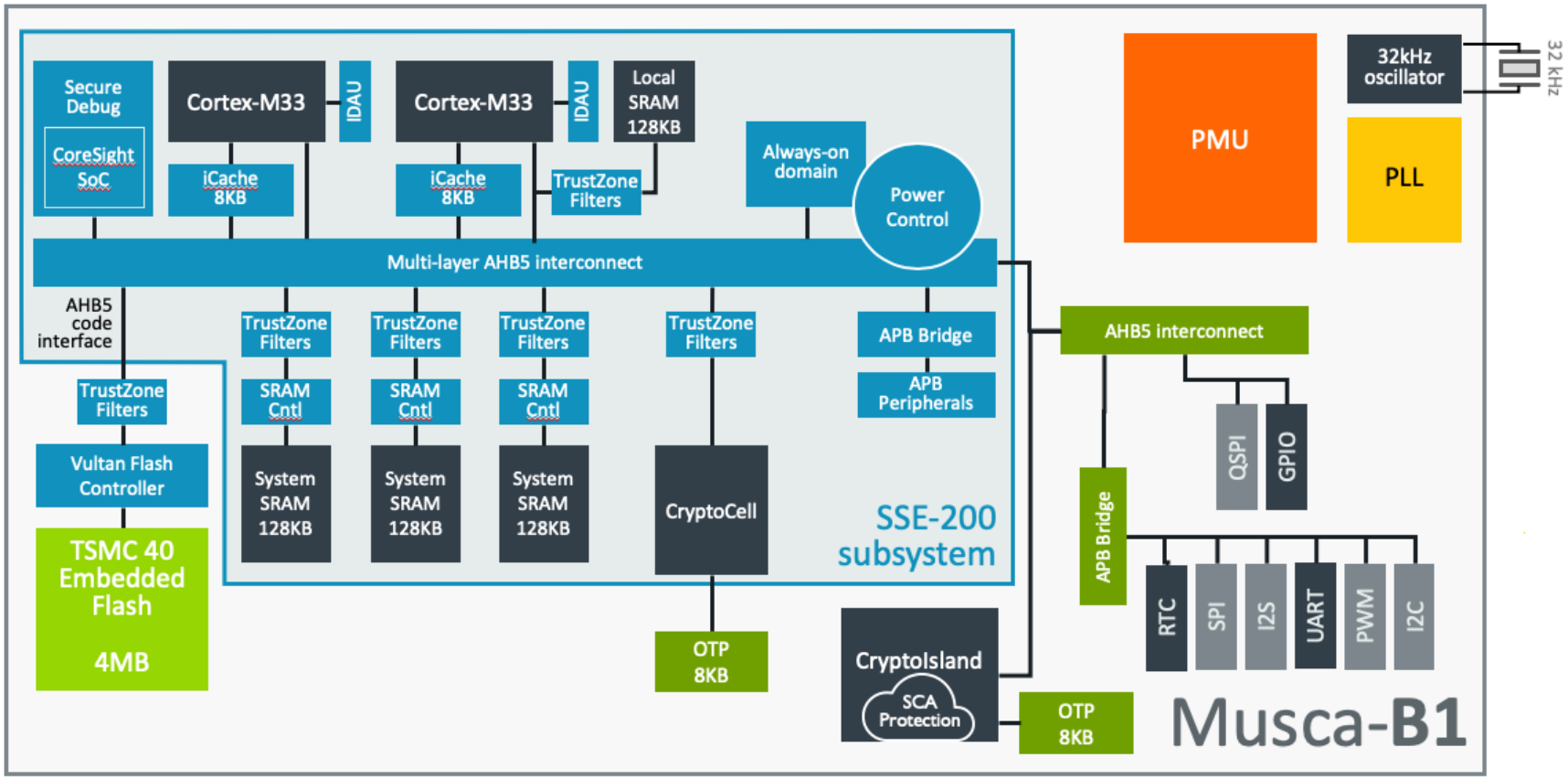
We are running TF-M on it as another platform configuration of TF-M

Responsibilities:

- Provides the RoT in the system
- Secure boot-flow
- Provides PSA RoT services
  - Additional level of isolation for PSA RoT
  - PSA program defines PSA RoT (most trusted security domain) and Application RoT (for additional secure services) domains

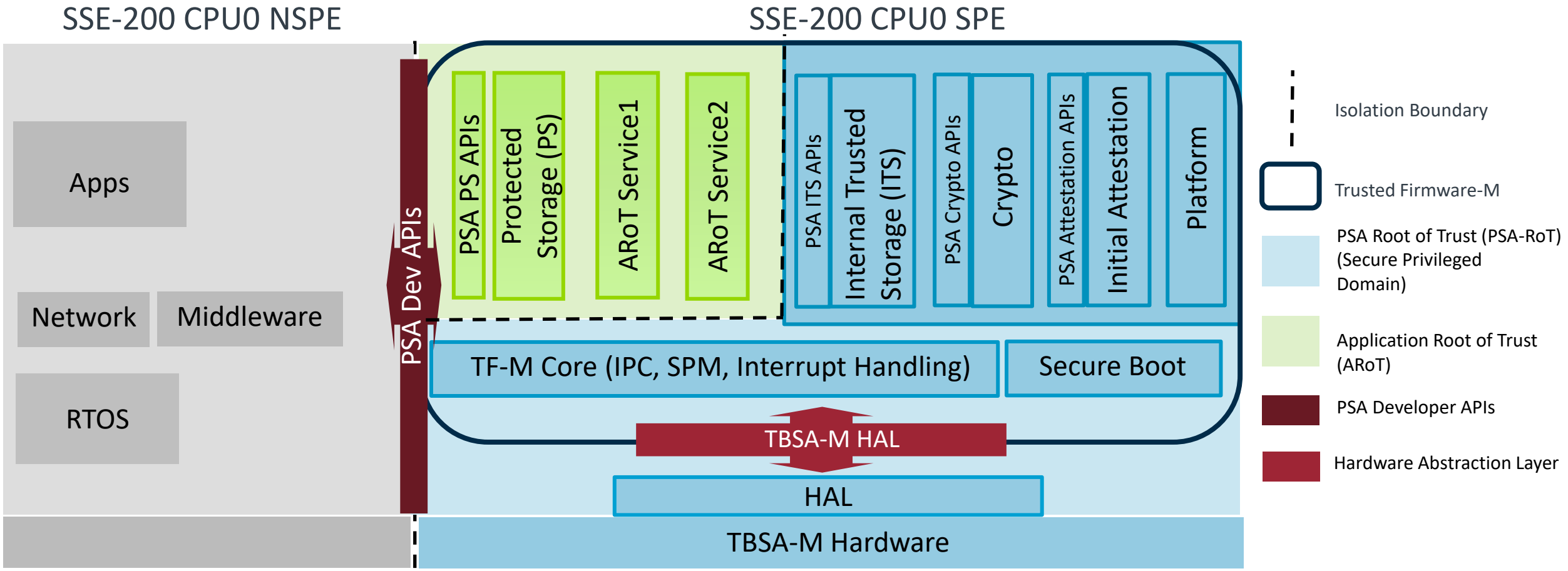
Musca-B1 board

PSA development platform for IoT

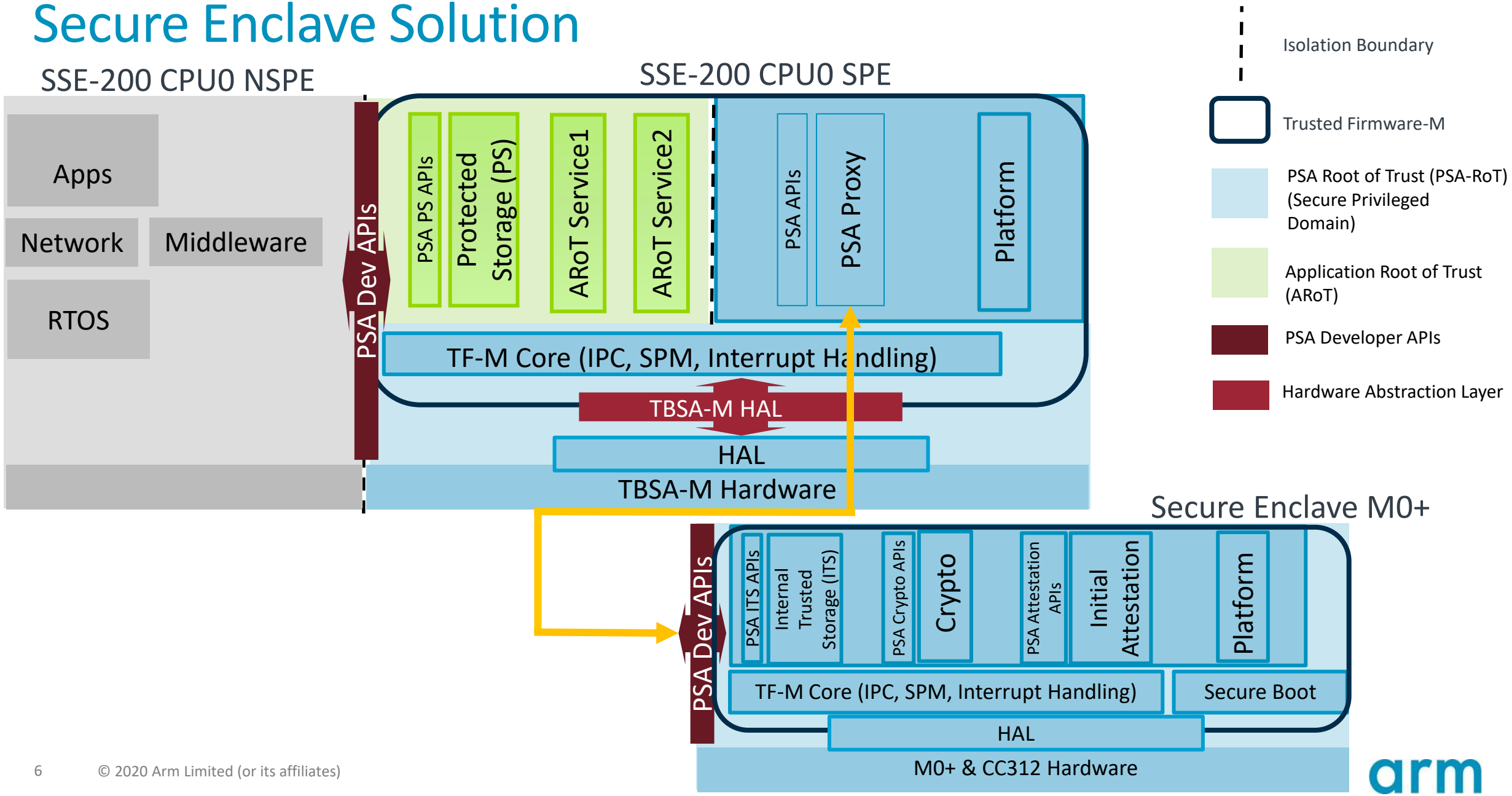


Current TF-M architecture on Musca-B1

In case of PSA Isolation Level 2



Secure Enclave Solution

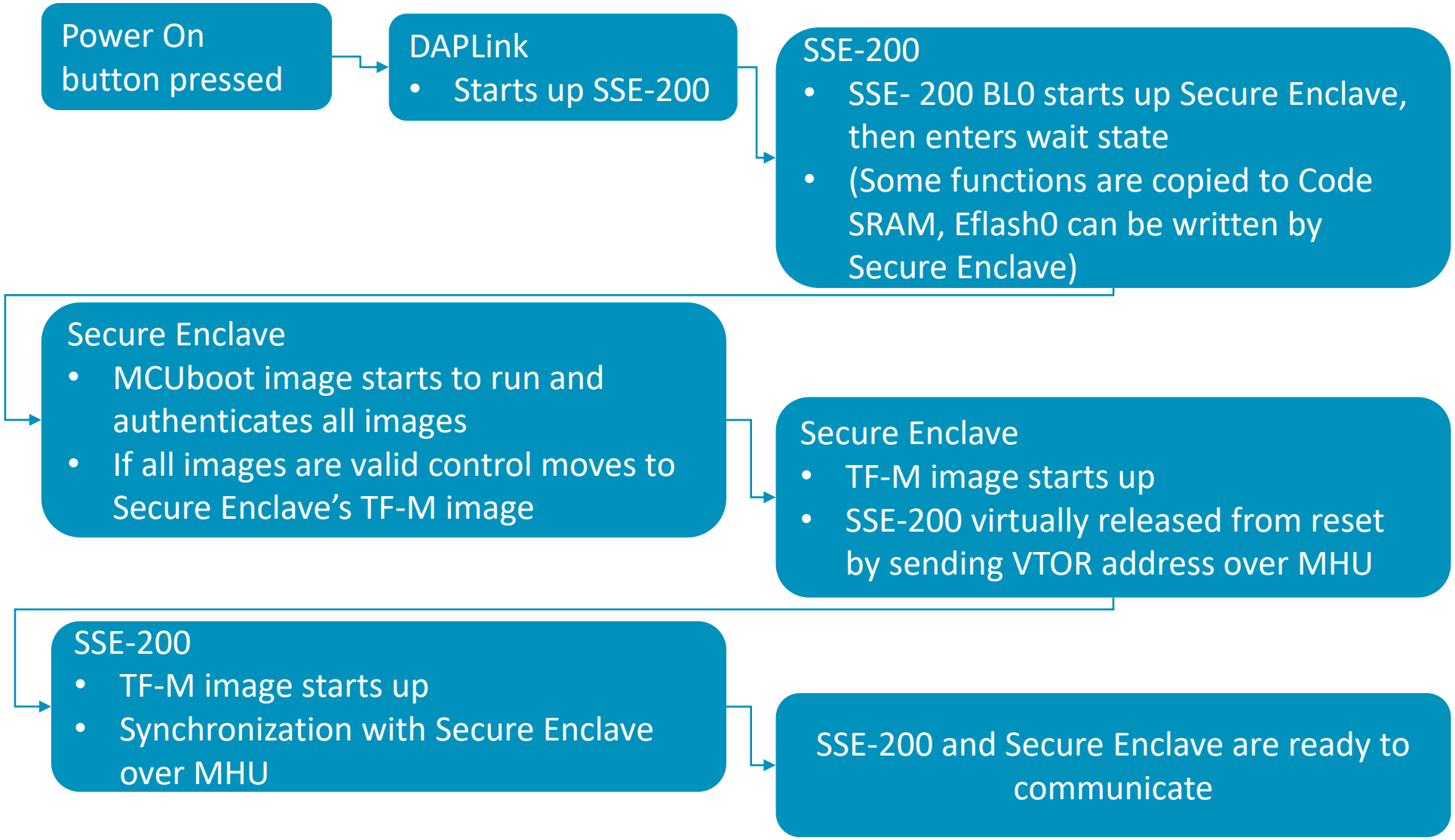


arm

Limitations from Secure Enclave point of view

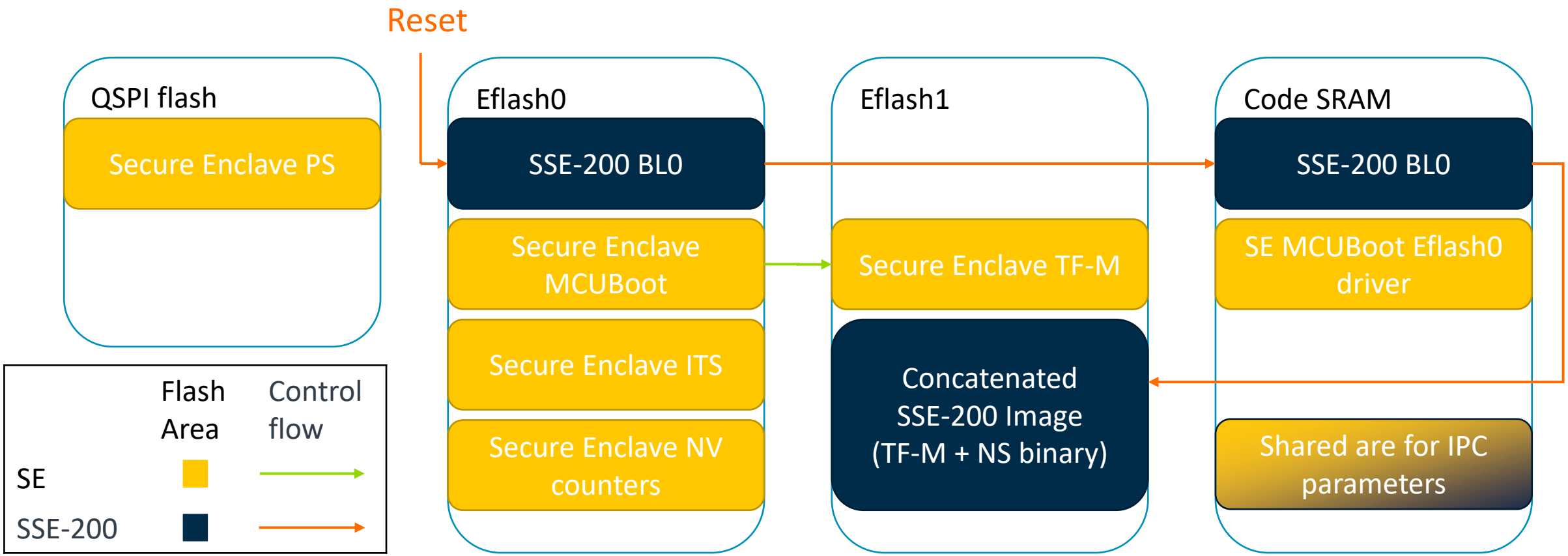
- Secure Enclave does not have serial output
- In the Musca-B1 SoC SSE-200 always has access to important system assets (flash controllers, SCC controller, etc.)
- Desired boot-flow would be to start up Secure Enclave first, and then SSE-200 should be started up by Secure Enclave
  - The DAPLink FW releases the SSE-200 subsystem from reset first, it would require complex changes to modify the boot order
  - SSE-200 BL0 component imitates that Secure Enclave is the first system that starts to run
  - Without SSE-200 BL0 the boot flow can be treated as a valid reference solution

Boot chain



arm

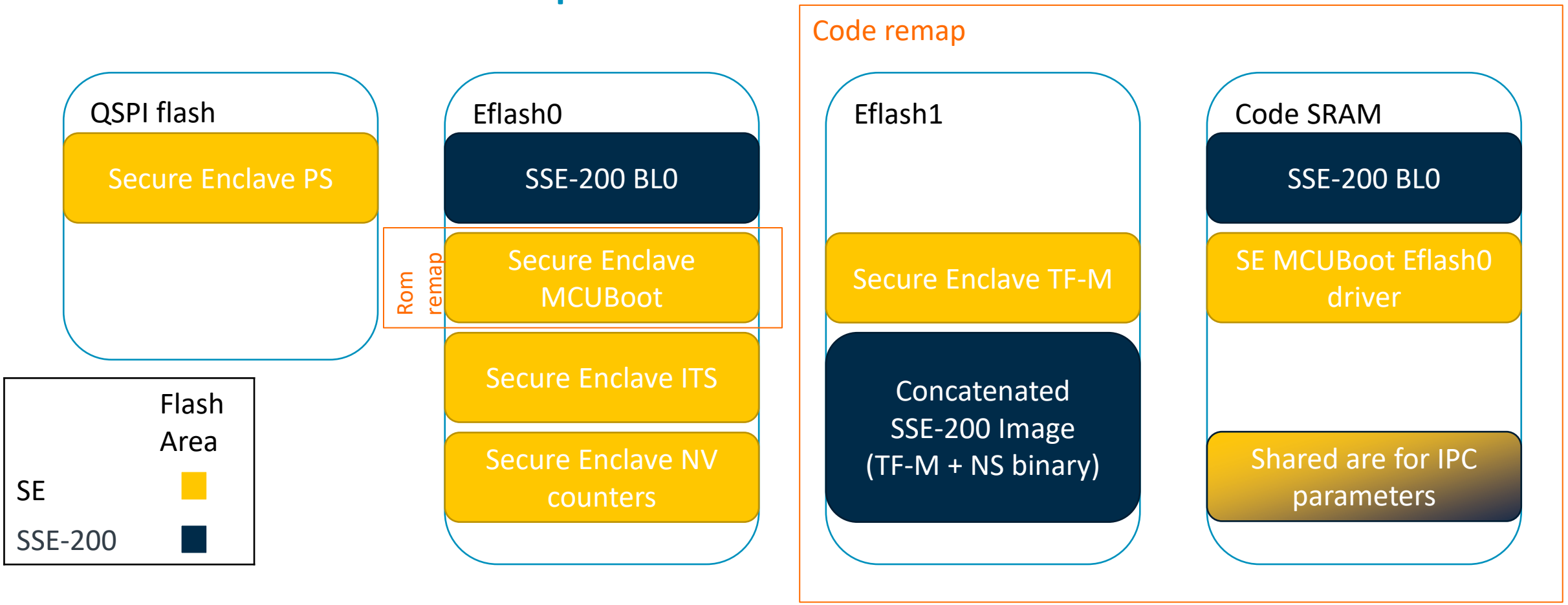
Musca-B1 flash layout with Secure Enclave



- SSE-200 BL0 just starts up SE by writing SCC registers, then waits for MHU message
- If SE finds all images intact it virtually starts up SSE-200 by sending an MHU message

arm

Secure Enclave remaps



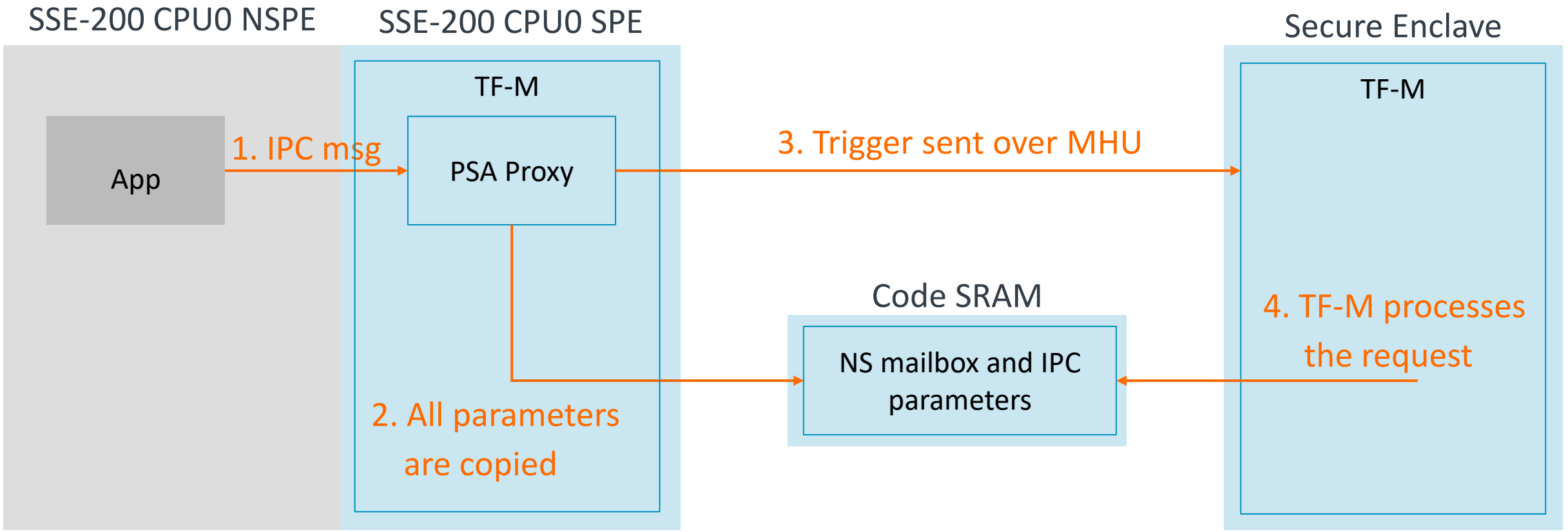
- Sys remap is used to access flash controllers from Secure Enclave
- Secure Enclave has its internal RAM

arm

IPC message forwarding

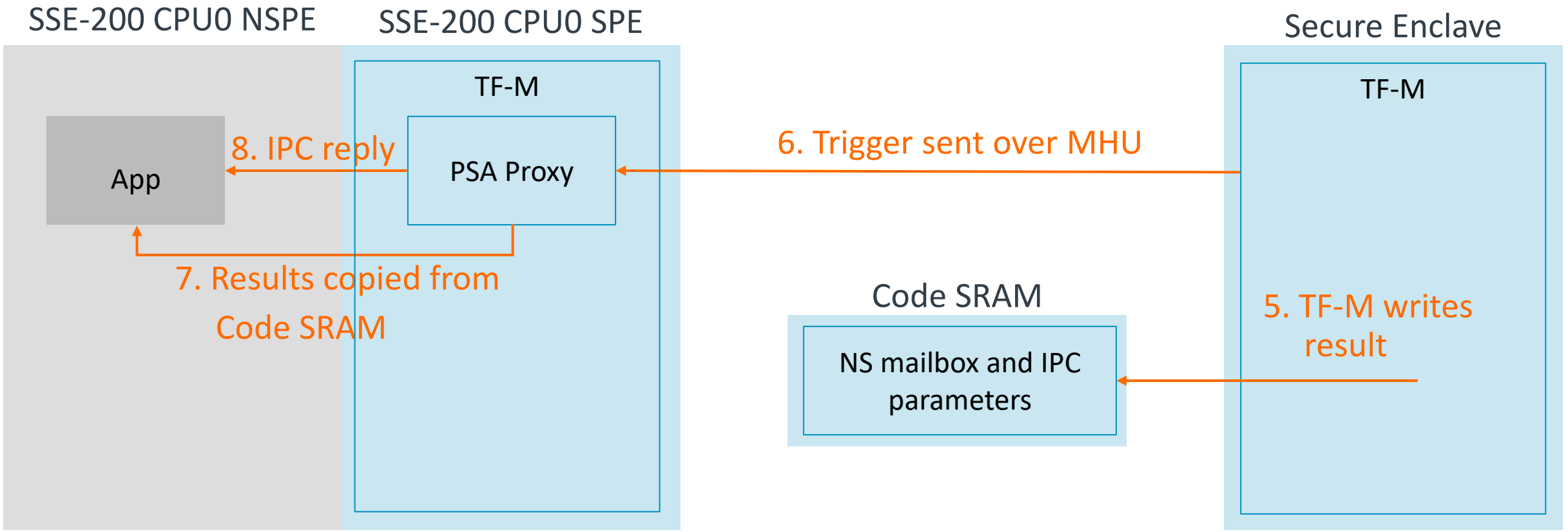
- Reuses mailbox solution already available in Cypress port
- In the SSE-200 subsystem PSA Proxy Partition provides virtually all PSA RoT services
- PSA parameters are copied into the Code SRAM to be accessible by Secure Enclave (This copy can be eliminated if Secure Enclave can access all memory regions)

IPC message forwarding II



arm

IPC message forwarding III



arm

IPC message forwarding IV

- If a request is sent by PSA Proxy control is given back to SPM while waiting for answer from Secure Enclave
- More PSA messages can be forwarded simultanously
- Secure Enclave cannot process messages parallelly, but that can change in the future

Planned schedule

- Start review by early September
- Merge solution at end of September

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה