Trusted Firmware-M

Firmware Update Service

Sherry Zhang
Arm

Linaro Connect
VIRTUAL • SPRING 2021

Agenda

- PSA Firmware Update APIs
- Firmware Update(FWU) service in TF-M
- FWU Service Integration with FreeRTOS OTA
- Future Plan

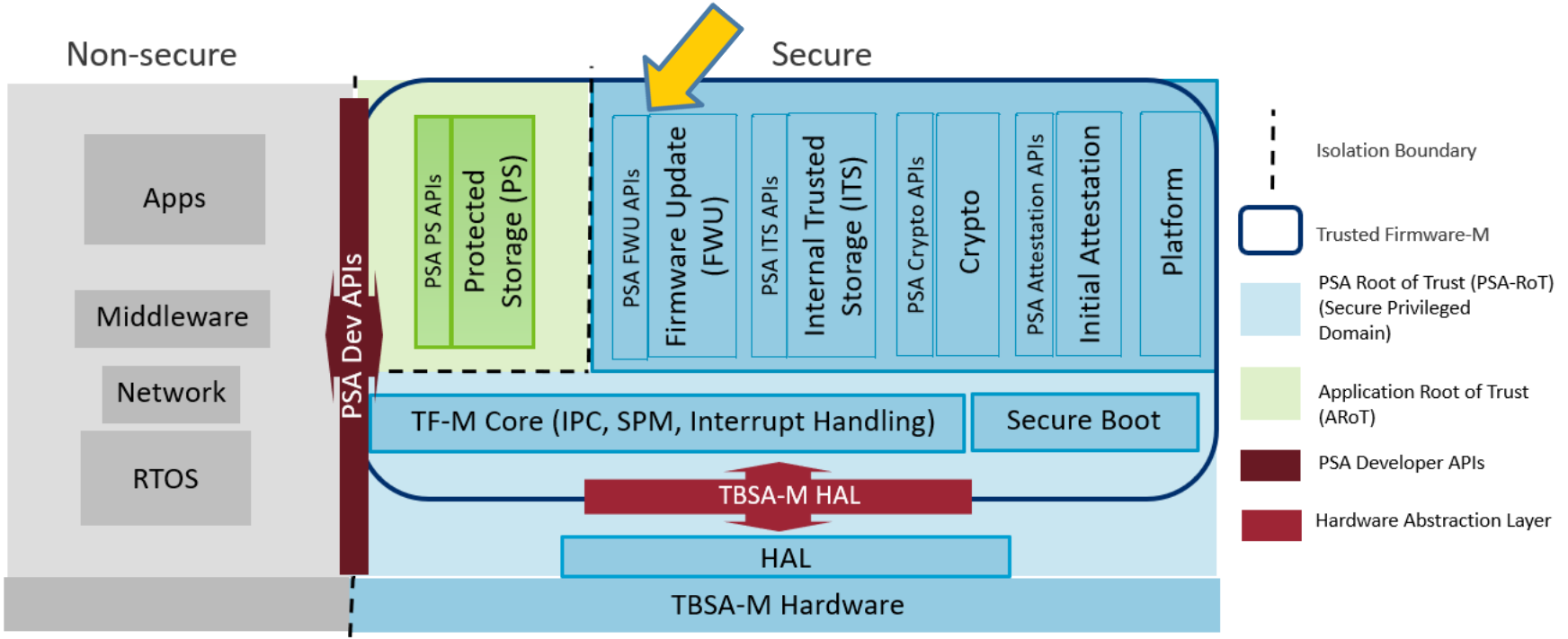
PSA Firmware Update APIs

- Firmware update support is an essential property of a PSA device.
- Arm Published the PSA Firmware Update API Beta 0 version in February 2021.
- It defines a standard firmware interface for firmware updates.

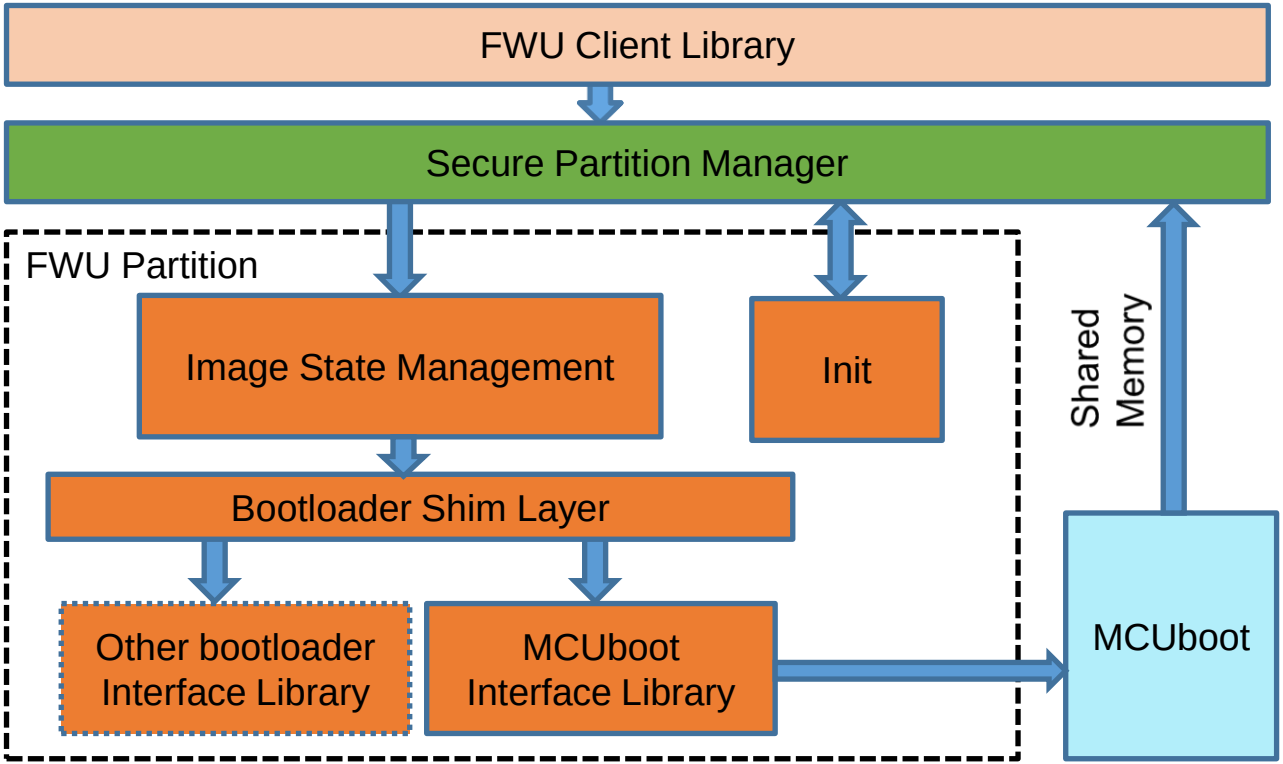
Trusted Firmware M(TF-M)

- Trusted Firmware-M (TF-M) implements a Secure Processing Environment (SPE) for Armv8-M architecture (e.g. the Cortex-M55, Cortex-M33 and Cortex-M23 processors) and dual-core Cortex-M devices.
- It is a PSA reference implementation aligning with PSA Certified guidelines, enabling chips, Real Time Operating Systems, and devices to become PSA Certified.
- An Open Source project hosted in Trusted Firmware Open Governance community project.

Firmware Update(FWU) partition in TF-M



FWU Service Module Design



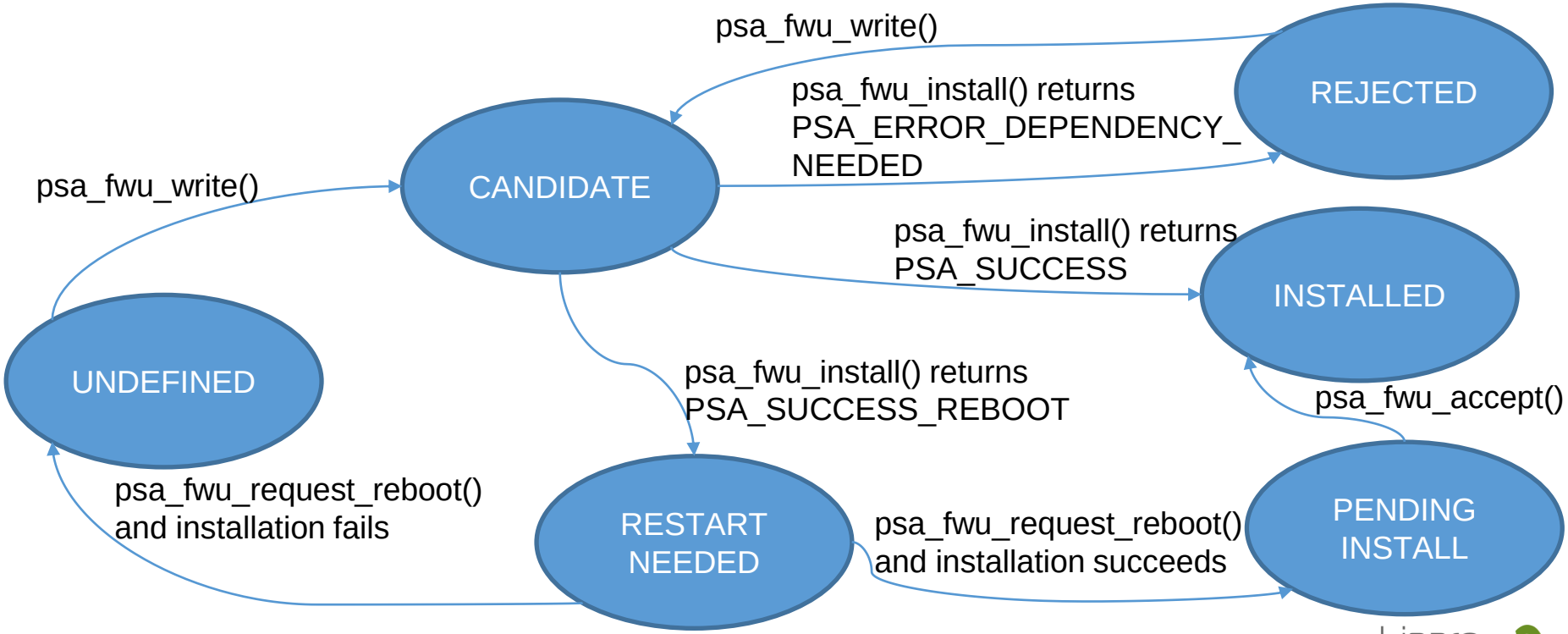
FWU Service APIs

- Query image information
  - psa_fwu_query ---- Returns information for an image of a particular image ID.
- Store image
  - psa_fwu_write ---- Writes an image to its staging area.
- Verify image
  - psa_fwu_install ---- Starts the installation of an image.
  - psa_fwu_accept ---- Indicates that the upgrade is successful.
- Trigger reboot
  - psa_fwu_request_reboot ---- Requests the platform to reboot.

Refer to PSA Firmware Update API for details of all the APIs:

https://developer.arm.com/documentation/ihi0093/0000/

Image State Transition in FWU Partition



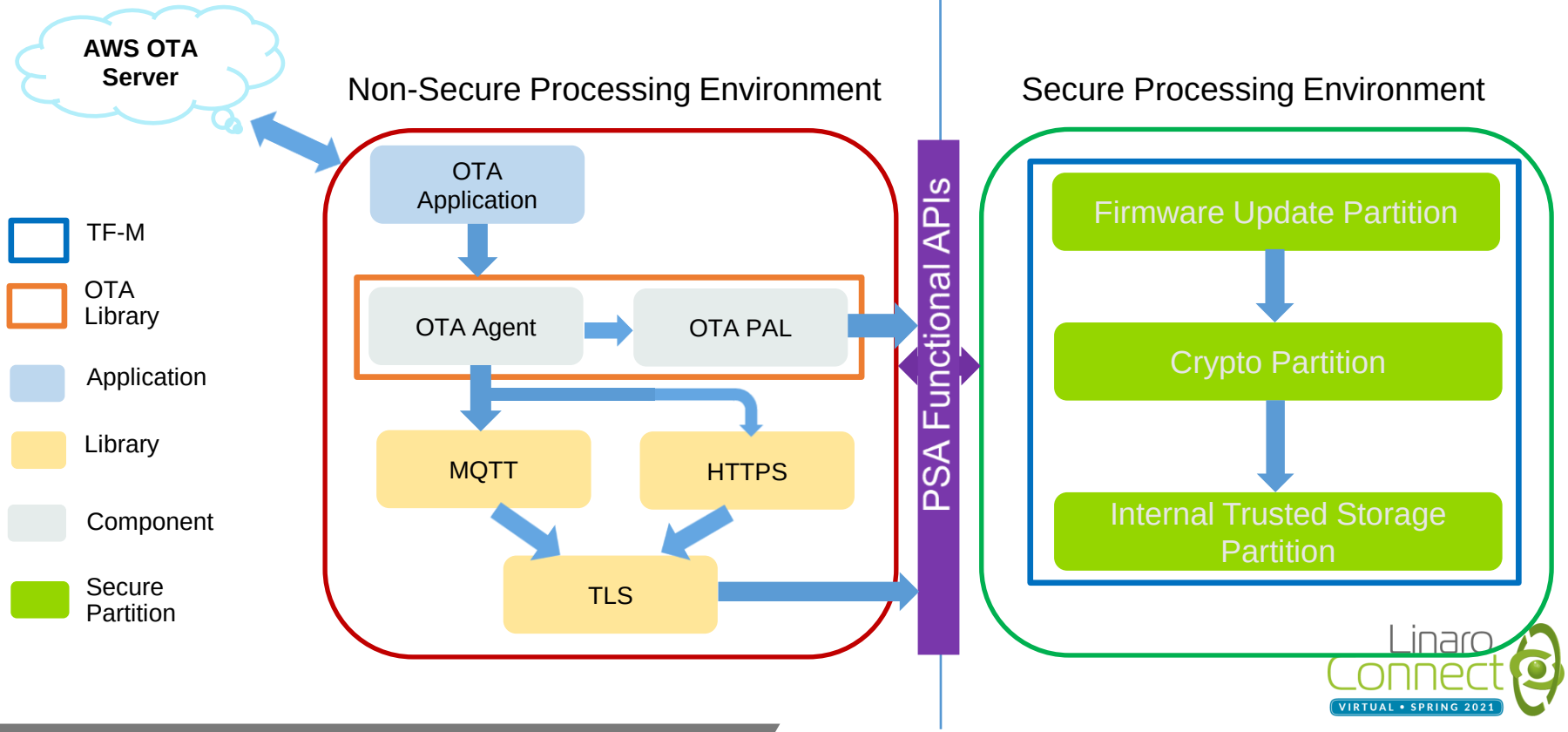
Bootloader Shim Layer APIs

- Initialization
  - fwu_bootloader_init ---- Initialization at FWU partition initialization, such as read necessary data
- Staging area init
  - fwu_bootloader_staging_area_init ---- Prepare the staging area of the image with the given ID for image download.
- Load image to staging area
  - fwu_bootloader_load_image ---- Load a block data to its staging area
- Install image in staging area
  - fwu_bootloader_install_image ---- Starts the installation of an image.
- Accept image
  - fwu_bootloader_mark_image_accepted ---- Mark running image as installed.

TF-M integration with FreeRTOS

- TF-M integration with FreeRTOS kernel based on Armv8-M has been supported in its official repo. https://github.com/FreeRTOS/FreeRTOS-Kernel/tree/main/portable/ThirdParty/GCC/ARM_CM33_TFM
- TF-M integration with PKCS11 library is a standalone repo https://github.com/Linaro/freertos-pkcs11-psa and it is cloned into FreeRTOS by submodule
- TF-M integration with FreeRTOS OTA is in progress https://github.com/Linaro/amazon-freertos/pull/5

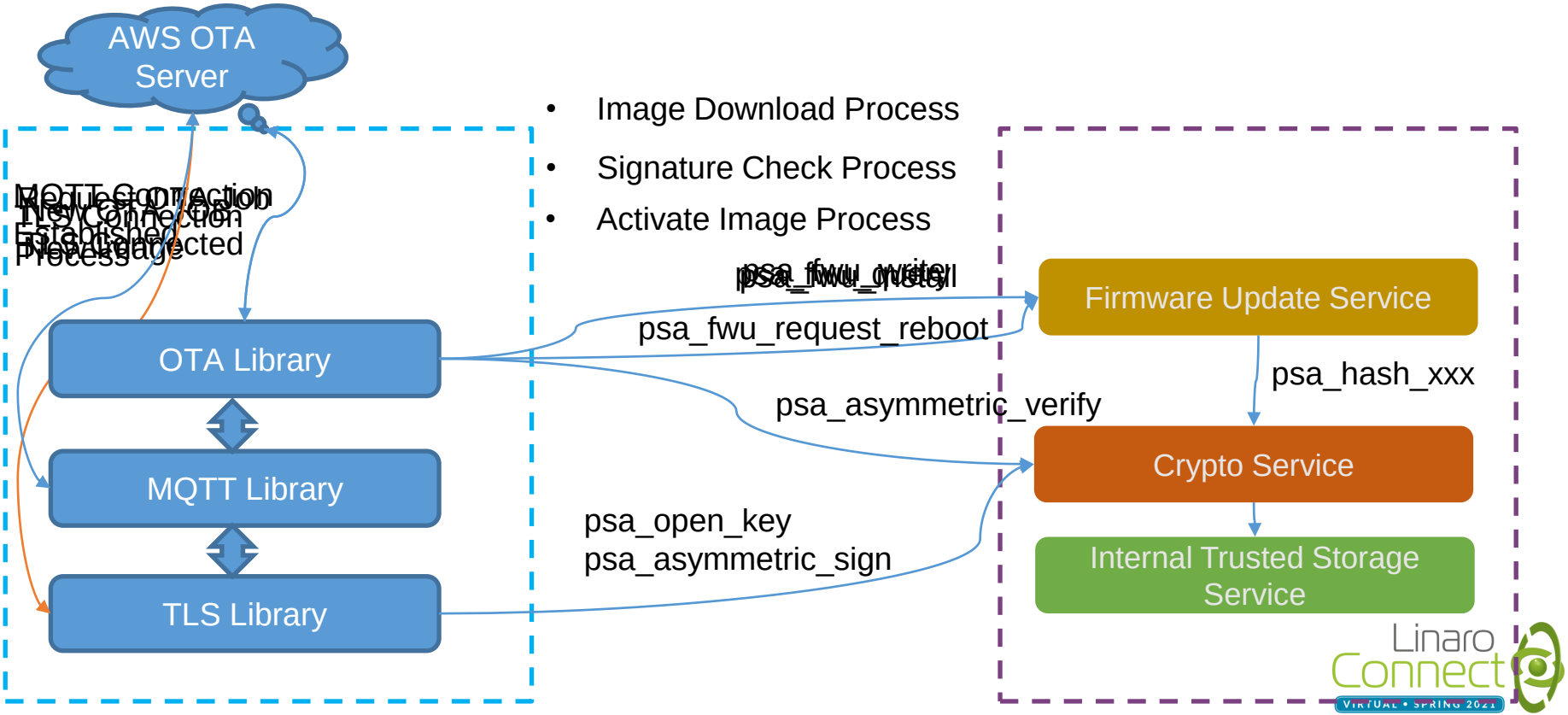
FWU Service Integration with FreeRTOS OTA



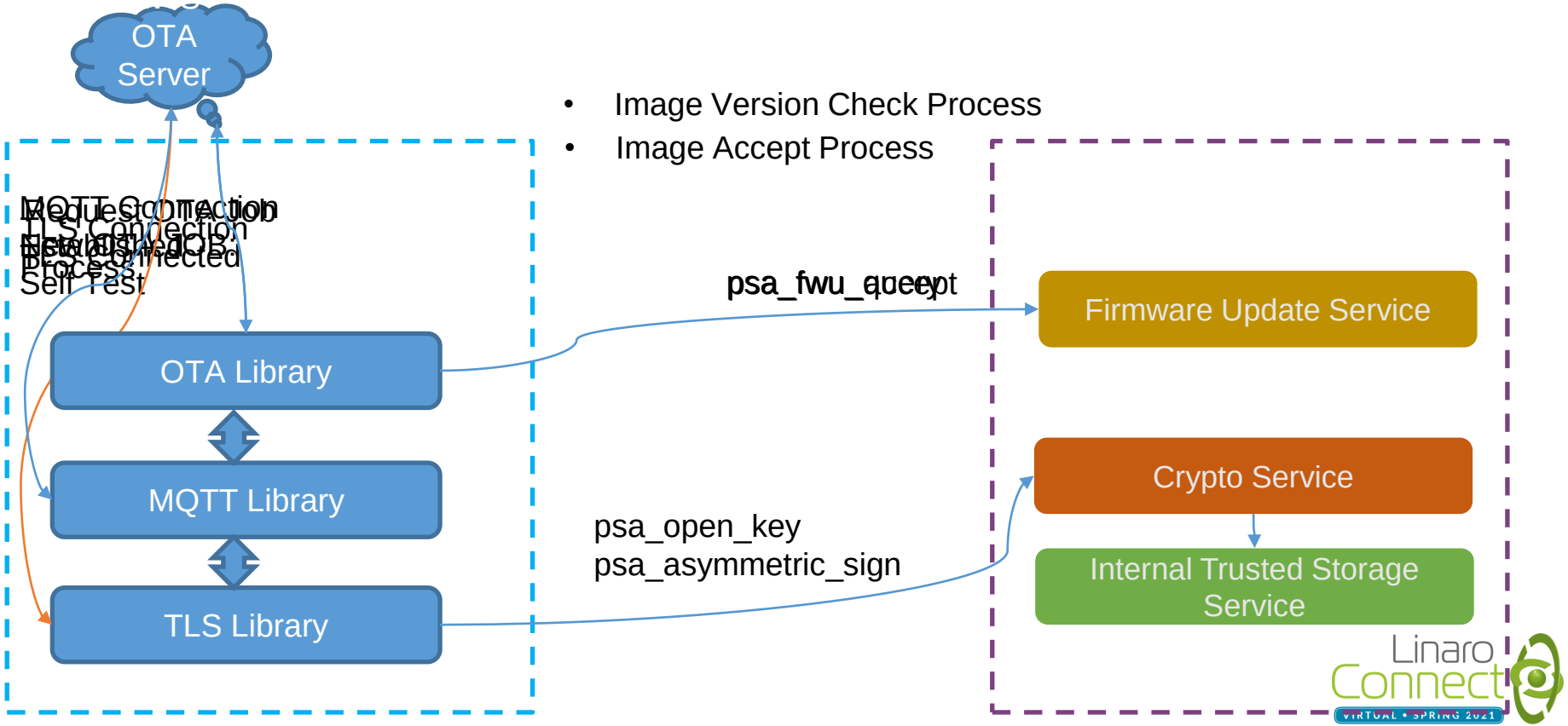
Mapping of the TF-M FWU Service APIs and FreeRTOS OTA PAL APIs

OTA PAL API	PSA Functional APIs
prvPAL_Abort	psa_fwu_abort
prvPAL_CreateFileForRx	None
prvPAL_CloseFile	psa_fwu_query psa_asymmetric_verify
prvPAL_WriteBlock	psa_fwu_write
prvPAL_ActivateNewImage	psa_fwu_install psa_fwu_request_reboot
prvPAL_ResetDevice	psa_fwu_request_reboot
prvPAL_SetPlatformImageState	psa_fwu_accept
prvPAL_GetPlatformImageState	None

TF-M protected FreeRTOS OTA Process

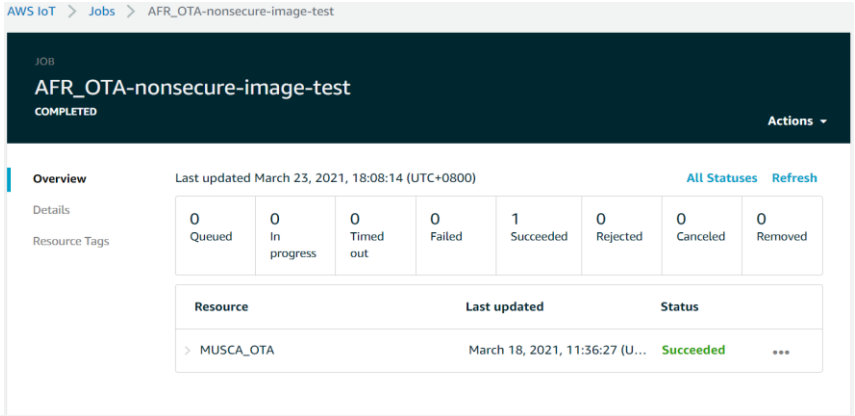


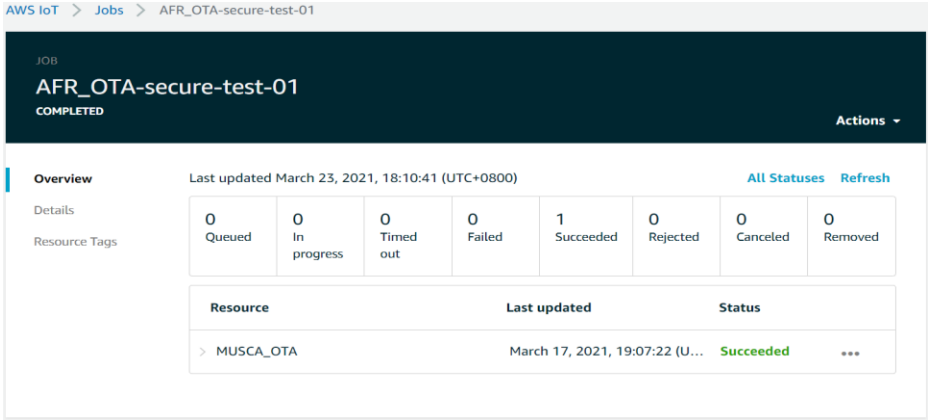
TF-M protected FreeRTOS OTA Process

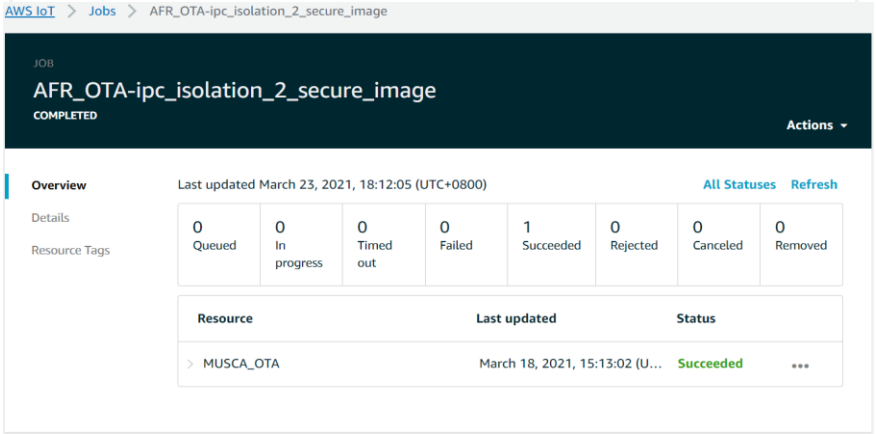


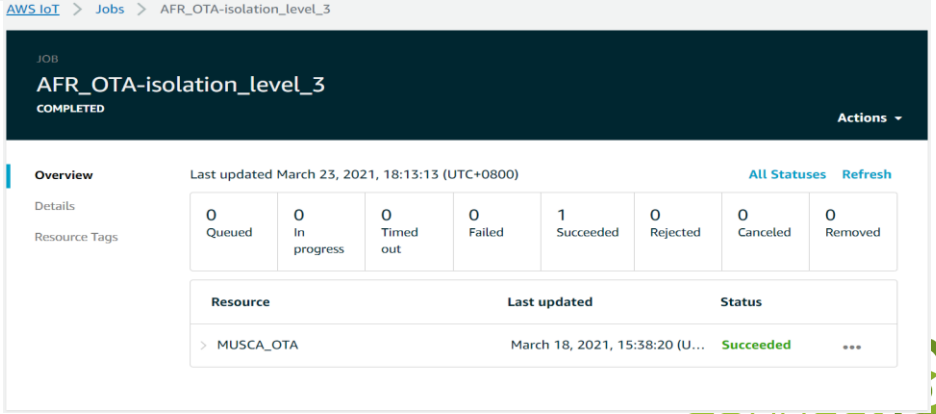
- Image Version Check Process
- Image Accept Process

Test with AWS cloud







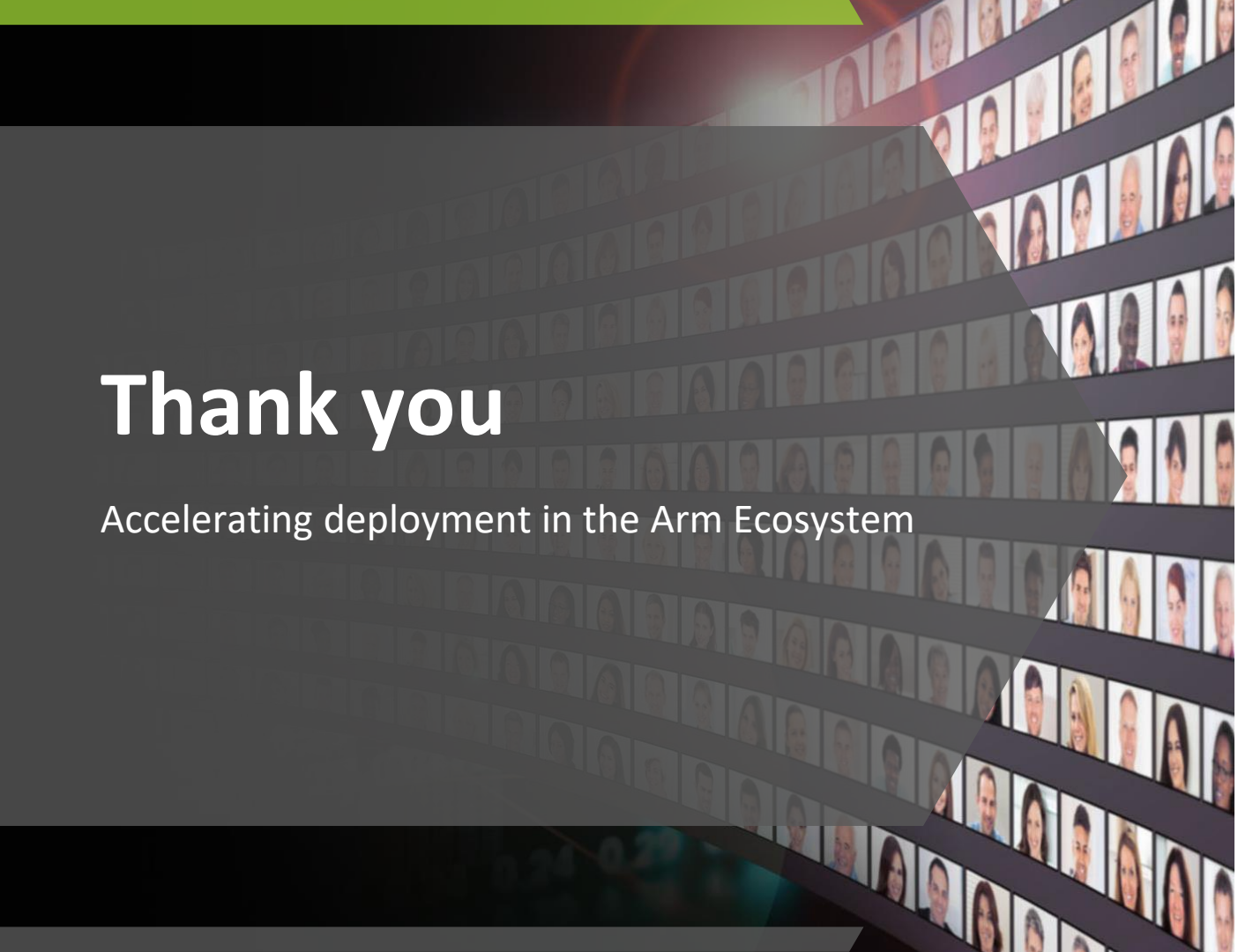


What’s Protected in whole OTA Process?

- TLS connection process
  - The private key is protected by PSA Crypto Service and PSA Internal Trusted Storage Service.
- OTA process
  - protects the image in the passive or staging area from being tampered with by the NSPE
  - protects the active image from being manipulated by NSPE

Future Plan

- Add FWU secure partition to TF-M v1.3.0 release
- Complete upstreaming the integration of TF-M Firmware Update service with the OTA PAL of FreeRTOS
- Align the implementation with PSA FWU specification future update



Thank you

Accelerating deployment in the Arm Ecosystem

Linaro Connect
VIRTUAL • SPRING 2021