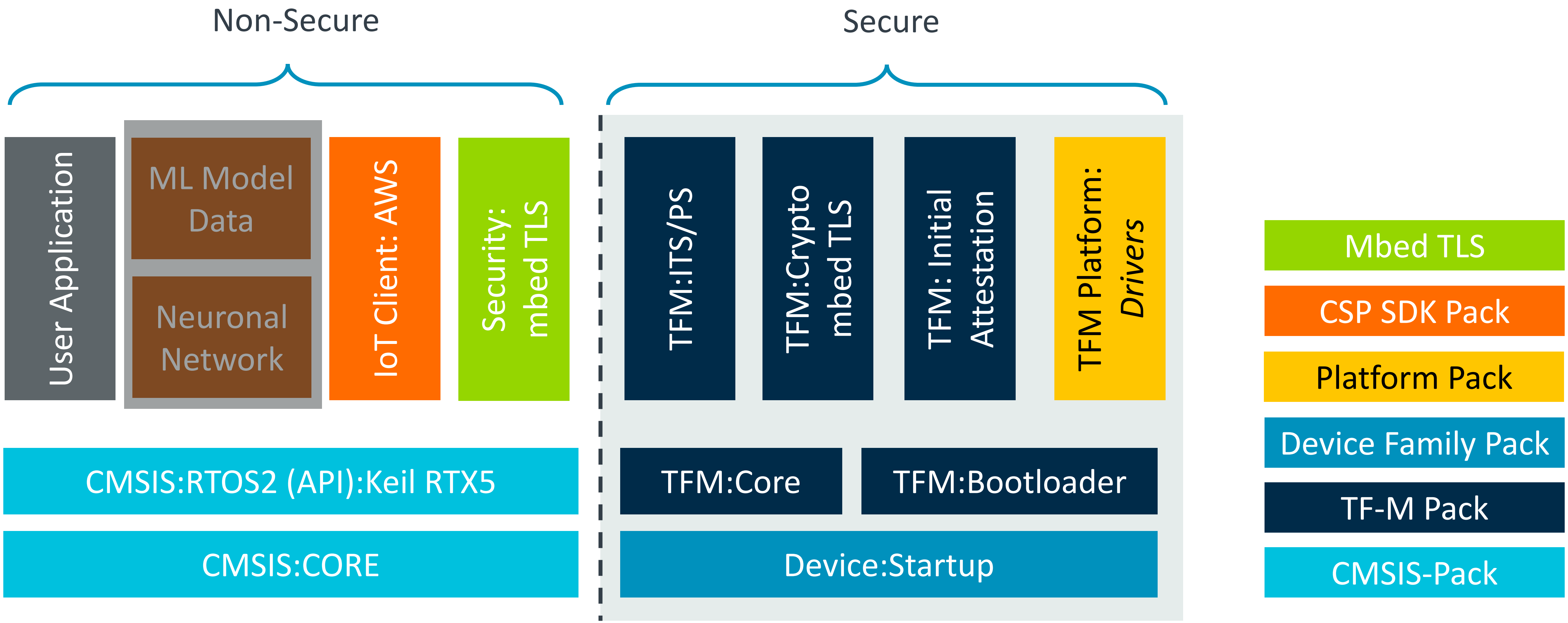
TF-M 1.2 framed in CMSIS-Packs

Reinhard Keil
2021-03-04

© 2021 Arm

IoT Application Example: Pack view



© 2021 Arm

Packs and Examples created for TF-M

- **ARM.TFM.2.1.0.pack**: main TF-M pack, synced to the TF-M repository
- **ARM.TFM-Test.1.0.0.pack**: TF-M integration tests, synced to the TF-M repository
- **ARM.PSA.1.0.0.pack**: should be the PSA API (currently documentation)
- **ARM.mbedTLS.1.7.0.pack**: MbedTLS (upstream 2.24)
- Platform (device) support (memory maps, SAU/MPC/PPC setup):
  - **Keil.LPC55S6x_TFM-PF.1.1.0.pack** (NXP LPC55S6x)
  - **Keil.STM32L5xx_TFM-PF.1.1.0.pack** (STMicroelectronics STM32L5)

Examples currently on www.keil.com/iot

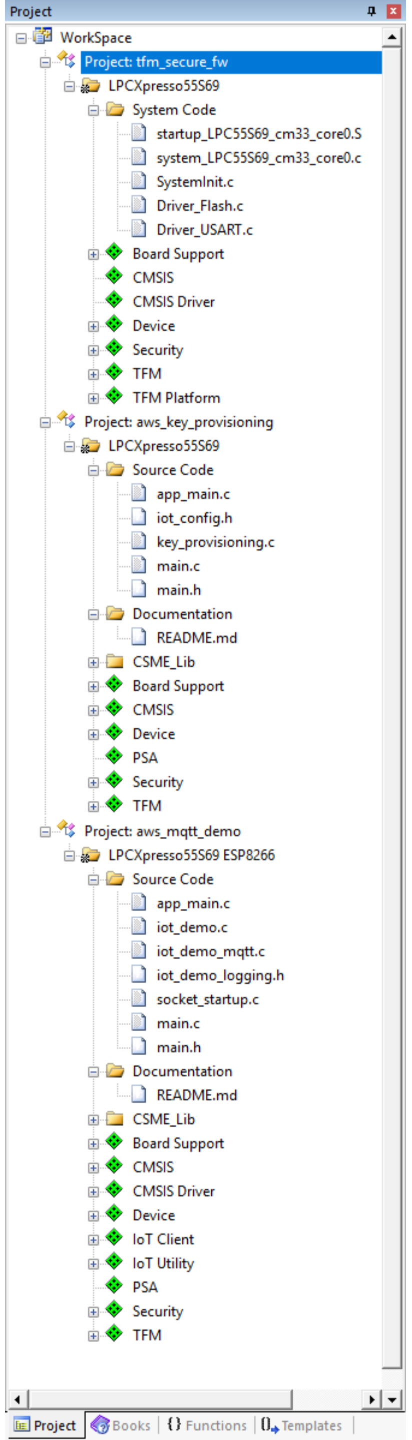
- **LPCXpresso55S69-EVK:** AWS MQTT Example using TrustZone and TF-M
- **STMicroelectronics NUCLEO-STM32L552ZE:** AWS MQTT Example using TrustZone and TF-M
- **STM32L562E-DK**: AWS MQTT Example using TrustZone and TF-M

© 2021 Arm

AWS MQTT example project

- Multi-project workspace
  - **tfm_secure_fw**: Runs the TF_M FW on the secure side
  - **aws_key_provisioning**: stores the keys in internal secure storage
  - **aws_mqtt_demo**: non-secure demo project sending MQTT messages

- Run:
  - Flash tfm_secure_fw to enable the secure side
  - Flash and run once aws_key_provisioning to transfer keys to secure storage
  - Flash and run aws_mqtt_demo; observe output in the Terminal and on the AWS IoT Console

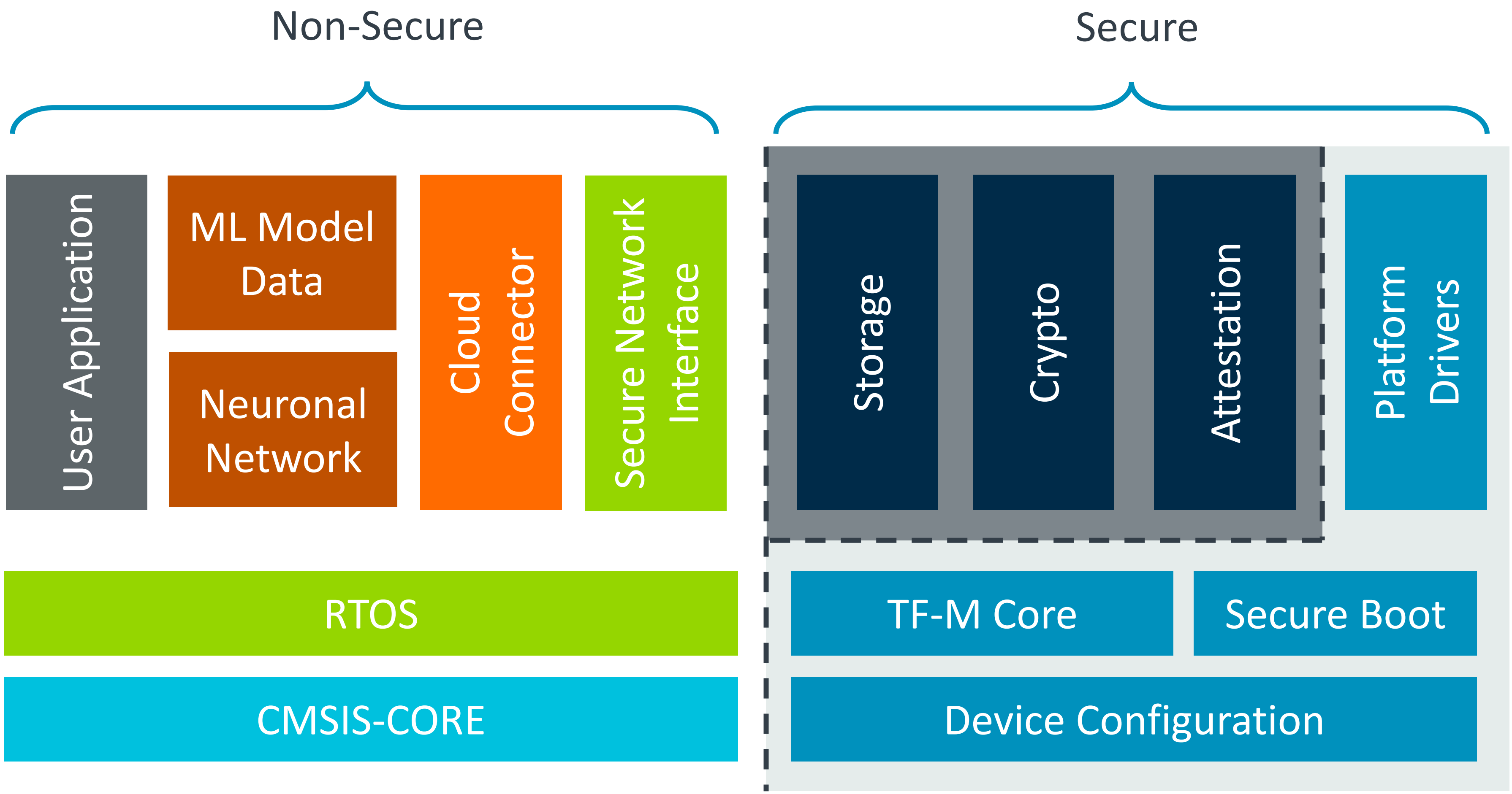


```
WorkSpace
  Project: tfm_secure_fw
    LPCXpresso55S69
      System Code
        startup_LPC55S69_cm33_core0.S
        system_LPC55S69_cm33_core0.c
        SystemInit.c
        Driver_Flash.c
        Driver_USART.c
      Board Support
      CMSIS
      CMSIS Driver
      Device
      Security
      TFM
      TFM Platform
  Project: aws_key_provisioning
    LPCXpresso55S69
      Source Code
        app_main.c
        iot_config.h
        key_provisioning.c
        main.c
        main.h
      Documentation
        README.md
      CSME_Lib
      Board Support
      CMSIS
      Device
      PSA
      Security
      TFM
  Project: aws_mqtt_demo
    LPCXpresso55S69 ESP8266
      Source Code
        app_main.c
        iot_demo.c
        iot_demo_mqtt.c
        iot_demo_logging.h
        socket_startup.c
        main.c
        main.h
      Documentation
        README.md
      CSME_Lib
      Board Support
      CMSIS
      CMSIS Driver
      Device
      IoT Client
      IoT Utility
      PSA
      Security
      TFM
```

© 2021 Arm

IoT Application on Cortex-M with ML and TF-M

Simplified view to the software components of an IoT endpoint with ML



Non-Secure

User Application

ML Model Data

Neuronal Network

Cloud Connector

Secure Network Interface

RTOS

CMSIS-CORE

Secure

Storage

Crypto

Attestation

Platform Drivers

TF-M Core

Secure Boot

Device Configuration

FIRMWARE UPDATE

Images are downloaded by the **Cloud Connector** and temporarily stored. **Secure Boot** verifies the digital signature and updates Flash memory.

Multiple Images

Secure Firmware

Non-Secure Firmware

ML Model Data

© 2021 Arm

Thank You

Danke

Gracias

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

© 2021 Arm

The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks

© 2021 Arm