TF-M 1.2 framed in CMSIS-Packs
IoT Application Example: Pack view

Non-Secure

User Application
ML Model Data
Neuronal Network

IoT Client: AWS
Security: mbed TLS

CMSIS:RTOS2 (API): Keil RTX5
CMSIS: CORE

Secure

TFM: ITS/PS
TFM: Crypto mbed TLS
TFM: Initial Attestation

TFM Platform: Drivers

TFM: Core
TFM: Bootloader

Device: Startup

Mbed TLS
CSP SDK Pack
Platform Pack
Device Family Pack
TF-M Pack
CMSIS-Pack
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](http://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
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
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
- Neuronal Network
- ML Model Data
- Cloud Connector
- Secure Network Interface

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