Hello, and welcome to this presentation which provides references to documentation and URLs related to the implementation of TF-M in the STM32U5.

U5 TFM pointers

- Documentation
  - [AN5156]: Introduction to STM32 microcontrollers security - Application note
  - [AN4992]: STM32 MCUs secure firmware install (SFI) overview - Application note
  - [UM2851]: Getting started with STM32CubeU5 TFM Application
  - [UM2852]: STM32U585xx security guidance for PSA Certified™ Level 3 with SESIP Profile
- Application examples available in STM32CubeU5 for the B-U585I-IOT02A discovery board
  - TFM example
  - SBSFU example

life.augmented

2

ST has released several documents that describe the implementation of TF-M in the STM32U5.
The Application Note 5156 presents the basics of security in STM32 microcontrollers.
The Application Note 4995 supports the secure firmware install (SFI) feature available on the STM32U5.
The User Manual number 2851 describes how to get started with the STM32CubeU5 TFM application delivered as part of the STM32CubeU5 MCU Package.
The User Manual number 2852 describes how to prepare STM32U5 microcontrollers to make a secure system solution compliant with the SESIP Profile for PSA Level 3 using the STM32Cube_FW_U585_Security_certification_V1.0.0 software package included in the STM32CubeU5 MCU

Package.
The B-U585I-IOT02A board integrating the STM32U585AI microcontroller is used as the hardware vehicle to implement and test a non-secure application using secure services but it does not bring any additional security mechanism.
STM32CubeU5 TFM application and SBSFU application examples are provided for the B-U585I-IOT02A board.
The TFM based application example consist of four main software components, which can be configured by integrators according to their needs:

- TFM_SBSFU_Boot: Secure Boot and Secure Firmware Update application
- TFM_Loader: application loader application based on Ymodem protocol over USART
- TFM_Appli_Secure: secure application providing secure services to the non-secure user application (at run-time)
- TFM_Appli_NonSecure: non-secure user application.

The SBSFU application is minimal with only the Secure Boot and Secure Firmware Update services of the TF-M.

U5 TFM pointers

- Public documents available online from Trusted Firmware community web site at www.trustedfirmware.org:
  - TF-M User Guide for v1.0:
    - Releases — Trusted Firmware-M 1.4.0+ (gdcfab8ab) documentation
- PSA developer APIs:
  - https://developer.arm.com/architectures/security-architectures/platform-security-architecture#implement

life.augmented

More general documentation can also be useful to gain knowledge on security standards, such as:

- The TF-M user guide for v1.0 and all releases
- The PSA developer APIs.

Thank you

life.augmented

Thank you for attending this presentation!
You can now refer to the other presentations that detail how TFM works

- TFM flash memory footprint
- TFM offer in STM32U5.