



Hello, and welcome to this description of a how to configure the STM32H5 to develop a Trusted Firmware for Cortex-M, also called TFM.

ARM TF-M introduction

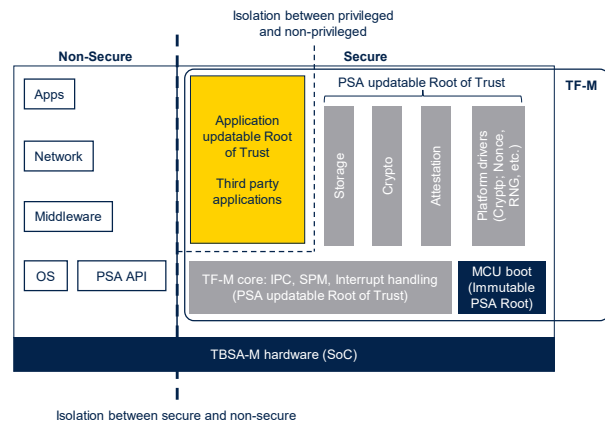
ARM Open-Source reference implementation of PSA standard / Kind of Secure OS

- **TF-M (Trusted Firmware-M):** Arm driven open-source software framework provides a reference implementation of the PSA standard on Cortex-M33 (TrustZone) core

- Secure part
 - PSA immutable RoT (Root of Trust): Secure Boot & Secure Firmware Update
 - PSA Updatable RoT:
 - Secure isolation configuration, secure IT management...
 - Secure cryptographic services based on opaque key APIs
 - Storage: protect data confidentiality/authenticity/integrity in NV Flash storage
 - Internal trusted storage service: NV secure/privilege Flash storage services
 - Attestation: prove product identity via Entity Attestation Token
 - Application Updatable RoT: 3rd party secure services
- Non-Secure part: User Application using PSA APIs to access secure services



TF-M TRUSTED FIRMWARE (<https://www.trustedfirmware.org>)



2

The TFM framework is composed of a Secure Boot and Secure Firmware Update application executed after reset and a set of secure services available at run time.

MCU-boot is a root of Trust and is immutable, it is the first code executed after each reset.

A Non secure application and part of secure application can be updated via the mcu_boot application.

The TFM-core manages the PSA Level 2 isolation inside the secure application and controls access to the secure services from the non-secure application via the PSA APIs.

The following secure services can be requested by the IoT application:

- Crypto services
- Secure Storage
- Attestation services.

TFM is modular:

- Each grey box can be deactivated independently (via compilation switches) so that secure services can be easily reduced to only keeping the MCU boot part
- Secure Crypto services can be configured to only support the crypto algorithms needed by the application

TFM core and TFM secure services are used for STM32H5 PSA Level 3 certification, that includes resistance against physical attack in addition to PSA Level 2 certification requirements.

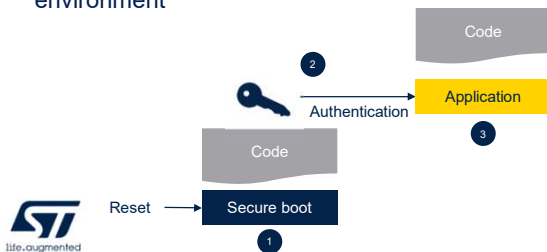
They are based on the hardware protections provided by the STM32H5 Series, referred to as TBSA-M hardware in the figure.

TBSA stands for Trusted Base System Architecture.

SBSFU Services (PSA Immutable RoT)

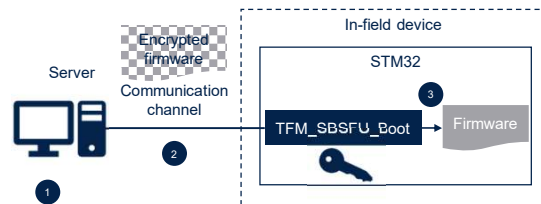
Secure Boot (SB)

- Ensures the integrity and authenticity of the user application image that is executed based on cryptographic checks
- Step1: SB implements a root of trust as a first trusted component
- Step2: every other component is authenticated
- Step3: user application execution in a trusted environment



Secure Firmware Update (SFU)

- Provides a secure implementation of in-field firmware updates
- Downloads a new firmware image to a device in a secure way
- The device authenticates, decrypts and installs the new firmware image and executes it



A device deployed in the field operates in an untrusted environment and it is therefore subject to threats and attacks. To mitigate the risk of attack, the objective is to run only authentic firmware on the MCU.

The Secure Firmware Update relies on a server providing the encrypted firmware and Secure Boot and Secure Firmware Update (SBSFU) service available in the MCU.

The OEM server and web services are responsible for:

- Storing the new version of the device firmware
- Communicating with the device and sending the new image version in encrypted form.

The STM32H5 is deployed in the field. It embeds a code that runs the firmware update process.

It communicates with the server and receives a new firmware image, authenticates and decrypts it and installs the new firmware image before executing it.

Secure services at run-time

SST: Secure Storage Service

- Implements PSA protected storage APIs
- Relies on HW flash isolation from non-secure area accesses
- Data encryption with AES-GCM based AEAD policy
- High level requirements addressed:
 - Confidentiality: resistance to HW/SW attacks
 - Access Authentication to establish the identity of requester
 - Integrity - Resistance to tampering to detect malicious HW/SW attacks
 - Reliability - Resistance to power failure scenarios and incomplete write cycles
 - Configurability: modular configuration
 - Performance: optimization to suit resource constraints



Internal trusted storage service (ITS)

- Implements PSA internal trusted storage APIs
- Relies on HW flash isolation from non-secure area accesses and application updatable RoT
- No encryption, located in the most secure flash region
- High level requirements addressed:
 - Confidentiality: resistance to HW/SW attacks
 - Access Authentication to establish the identity of the requester
 - Integrity - Resistance to tampering by attackers with physical access by HW isolation mechanism
 - Reliability - Resistance to power failure scenarios and incomplete write cycles
 - Configurability to scale increase/decrease memory footprint

4

The TF-M secure storage (SST) service implements PSA Protected Storage APIs.

The service is supported by hardware isolation of the flash access domain and relies on hardware to isolate the flash area from non-secure accesses.

The current design of the SST service relies on the hardware abstraction level provided by TF-M.

The SST service implements an AEAD encryption policy based on AES-GCM, as a reference, to protect data integrity and authenticity.

The design also meets the following high-level requirements:

- Confidentiality: Resistance to unauthorized accesses by hardware/software attacks
- Access Authentication: Mechanism to establish the identity of the requester (a non-secure entity, a secure entity, or a remote server).

- Integrity: Resistance to tampering by the normal users of a product, package, or system or by others physical access to it. If the content of the secure storage is maliciously modified, the service is able to detect it.
- Reliability: Resistance to power failure scenarios and incomplete write cycles.
- Configurability: High level of configurability to increase or decrease the memory footprint to cater for a variety of devices with varying security requirements.
- Performance: Optimized for use in resource constrained devices with a very small silicon footprint, the PPA (power, performance, area) should be optimal.

The TF-M internal trusted storage (ITS) service implements PSA internal trusted storage APIs that can write data in a microcontroller built in Flash memory region that is isolated from non-secure or unprivileged applications by hardware security protection mechanisms.

The design also meets the following high-level requirements:

- Confidentiality: Resistance to unauthorized accesses by hardware/software attacks, due to hardware isolation of the flash access domain.
- Access authentication: Mechanism to establish the identity of the requester (a non-secure entity, a secure entity, or a remote server).
- Integrity: resistance to tampering by attackers with physical access is provided by the internal flash device itself, while resistance to tampering by non-secure or application updatable RoT attackers is provided by the hardware isolation mechanism.
- Reliability: Resistance to power failure scenarios and incomplete write cycles.
- Configurability: High level of configurability to increase or decrease the memory footprint to cater for a variety of devices with varying requirements.

Secure services at run-time (2)

Secure cryptographic service

- Provides PSA cryptographic APIs in a PSA updatable RoT secure partition in TF-M.
- Based on mbed-crypto*, refer to PSA crypto APIs
- Can be used by other services running in the secure processing environment (SPE)
- Can be used by applications running in the non-secure processing environment (NSPE)

Initial attestation service (IAT)

- TF-M Initial Attestation Service allows the application to prove the device identity during an authentication process to a verification entity
- Can create an Entity Attestation Token (EAT) on request, which contains a fixed set of device specific data

* github.com/ARMmbed/mbed-crypto



5

The TF-M cryptographic service provides an implementation of the PSA cryptographic API in a PSA updatable RoT secure partition in TF-M.

It is based on mbed-crypto, which is a reference implementation of the PSA cryptographic API.

For more details on the PSA cryptographic API or the mbed-crypto implementation, refer to the [MbedCrypto GitHub repository](#) directly.

The service can be used by other services running in the secure processing environment (SPE), or by applications running in the non-secure processing environment (NSPE), to provide cryptographic functionality.

TF-M Initial Attestation Service allows the application to prove to a verification entity the device identity during an authentication process.

The initial attestation service can create an entity attestation

token (EAT) on demand, which contains a fixed set of device specific data.

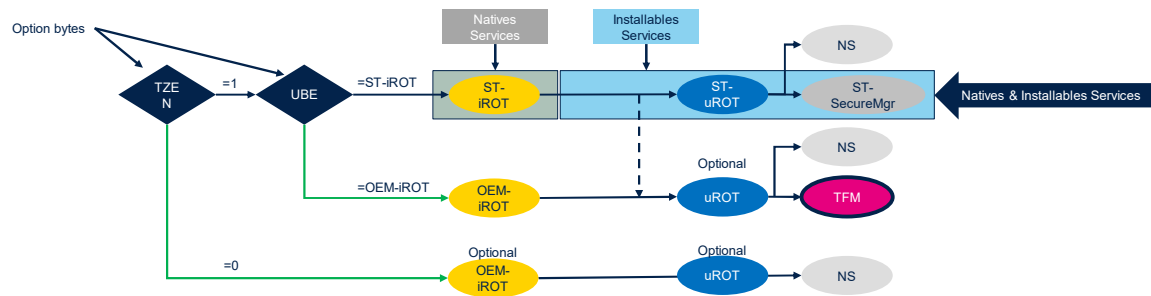
The Device must contain an attestation key pair, which is unique for each device.

The token is signed with the private part of attestation key pair.

The public part of the key pair is known by the verification entity. The public key is used to verify the authenticity of the token.

The data items in the token are used to verify the integrity of the device and assess its trustworthiness. The provision of the Attestation key is beyond the scope of the attestation service and should take place during the manufacture of the product

STM32H5 Paths to TFM Security Configuration



6

Following are the main security configurations available on the STM32H5.

The STM32H57X security implementation supports all the steps of the secure boot: reset, immutable Root Of Trust, updateable Root of Trust, secure and non-secure applications.

The STM32H56X security implementation only supports an OEM iROT, this corresponds to the intermediate part of the figure.

The STM32H503 does not support TrustZone, this case corresponds to be bottom part of the figure, also relevant when Trustzone is disabled on STM32H57X and STM32H56X.

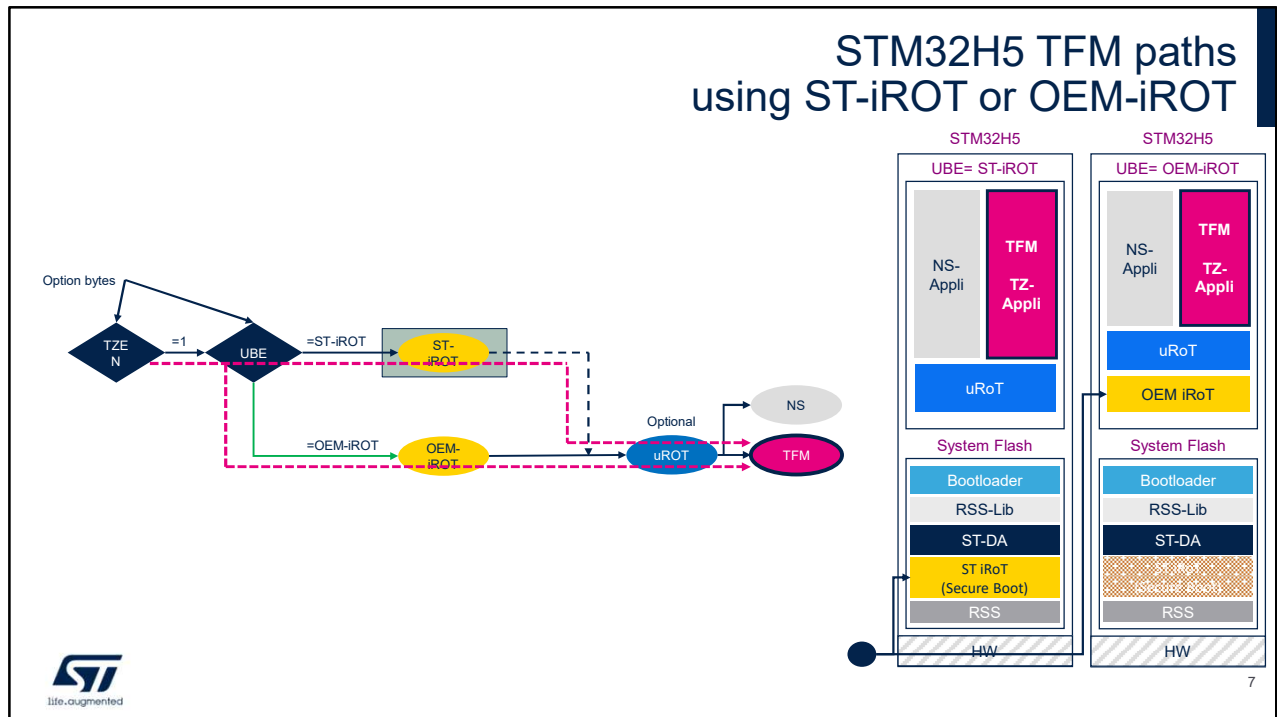
When TrustZone is enabled, either the ST-iROT or OEM-iROT is executed after the reset

In both cases , TF-M can be used as the foundation of the

secure image.

Therefore TF-M can still be implemented on STM32H5 devices.

STM32H5 TFM paths using ST-iRoT or OEM-iRoT

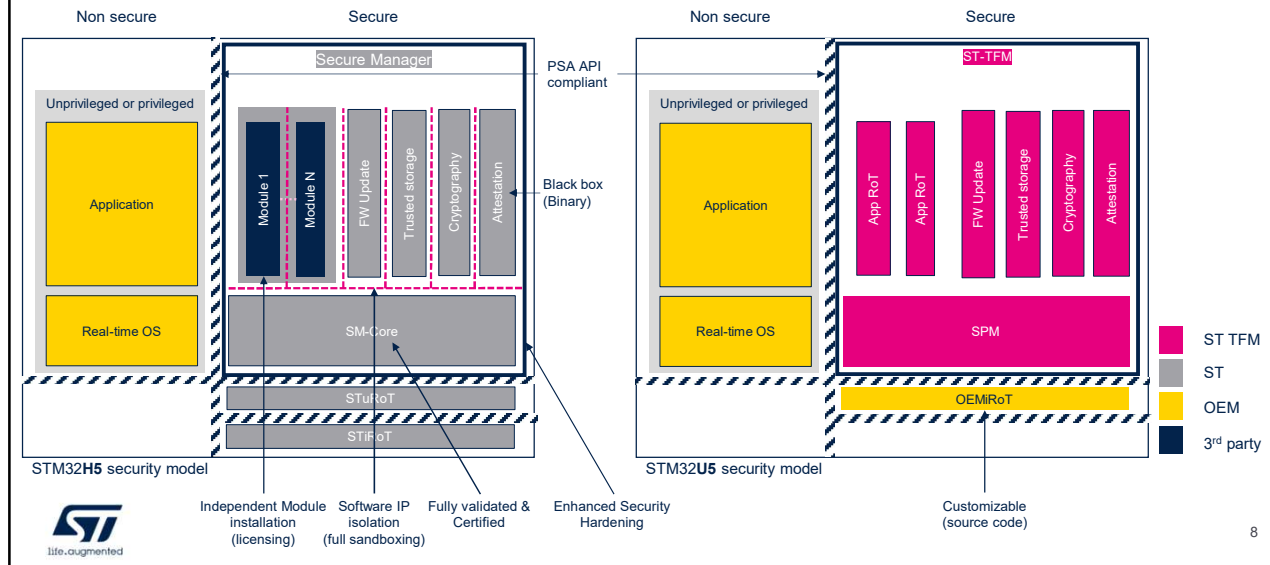


The possible paths to TFM implementation are colored in pink in the figure.

Either executing the ST iRoT and then an OEM uRoT that launches TF-M on the secure side.

The OEM uRoT can also be executed after the OEM iRoT.

STM32H5 Secure Manager vs. STM32U5 TFM



Secure Manager is the new strategy of the STM32H5, the TFM approach is changed versus the STM32U5 solution. The STM32H5 security model is represented on the left, the STM32U5 security model is represented on the right.

The main benefits offered by the secure manager are:

- Easing security integration (security seen as a **configurable black box**)
- Enhancing ST security offer (added value security services: Software IP protection...)
- Delivering **validated** and **certified** security solution

Due to the Secure Manager new offer, we are changing the TF-M approach.

The TF-M delivery management will be done in a different way on STM32H5 compared to STM32L5 and STM32U5.

- For STM32L5/U5, the TF-M source code is delivered in Cube Package STM32Cube TFM

- For STM32H5, the TF-M source code will be up streamed directly through the external TFM GitHub.
- Then STM32CubeH5 TFM, will embed ONLY a binary corresponding to the up streamed version.

The STM32Trust TEE secure manager encompasses two types of package: the STM32Trust TEE secure manager access kit (SMAK) and the STM32Trust TEE secure module development kit (SMDK).

Easy to be installed into STM32 products by the customers on their production lines, the STM32Trust TEE secure manager access kit (SMAK) offers a ready to use, high performance, and certified solution to support the Secure Boot, root of trust, cryptographic, internal trusted storage, initial attestation, and firmware update functions as defined by the Arm® PSA specifications.

Thank you

© STMicroelectronics - All rights reserved.
The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.



Thank you for attending this presentation!