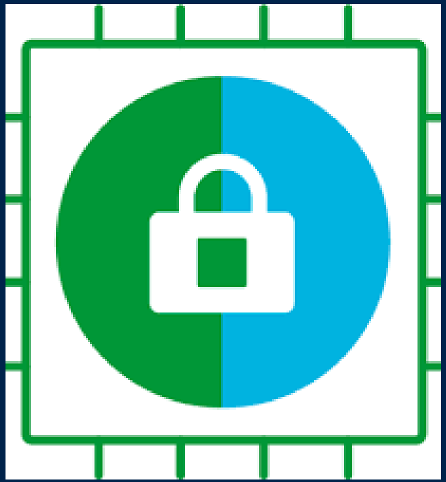


Upstream TF-M Binary

TF.org Technical Steering Committee
December 19th 2024
STMicroelectronics

Agenda

# TF-M Overview

# TF-M GitHub && Cube FW

# ST strategy Overview

# Perspective

life.augmented

Overview of STM32 Platforms upstream approach for TF-M

- TF-M GitHub
  - Current Upstream content of STM32 platforms (STM32L5, STM32U5, STM32H5):
    - Boot stage (bl2)
    - TF-M Secure/Non-Secure applications.
    - HAL drivers, platform security (MPU, SAU, GTZC), flash driver, com driver (Logs), programming scripts, readme
  - New upstream strategy for STM32 next platforms : without BL2
    - TF-M Secure/Non-Secure applications
    - HAL drivers, platform security (MPU, SAU, GTZC), flash driver, com driver (Logs), programming scripts, readme

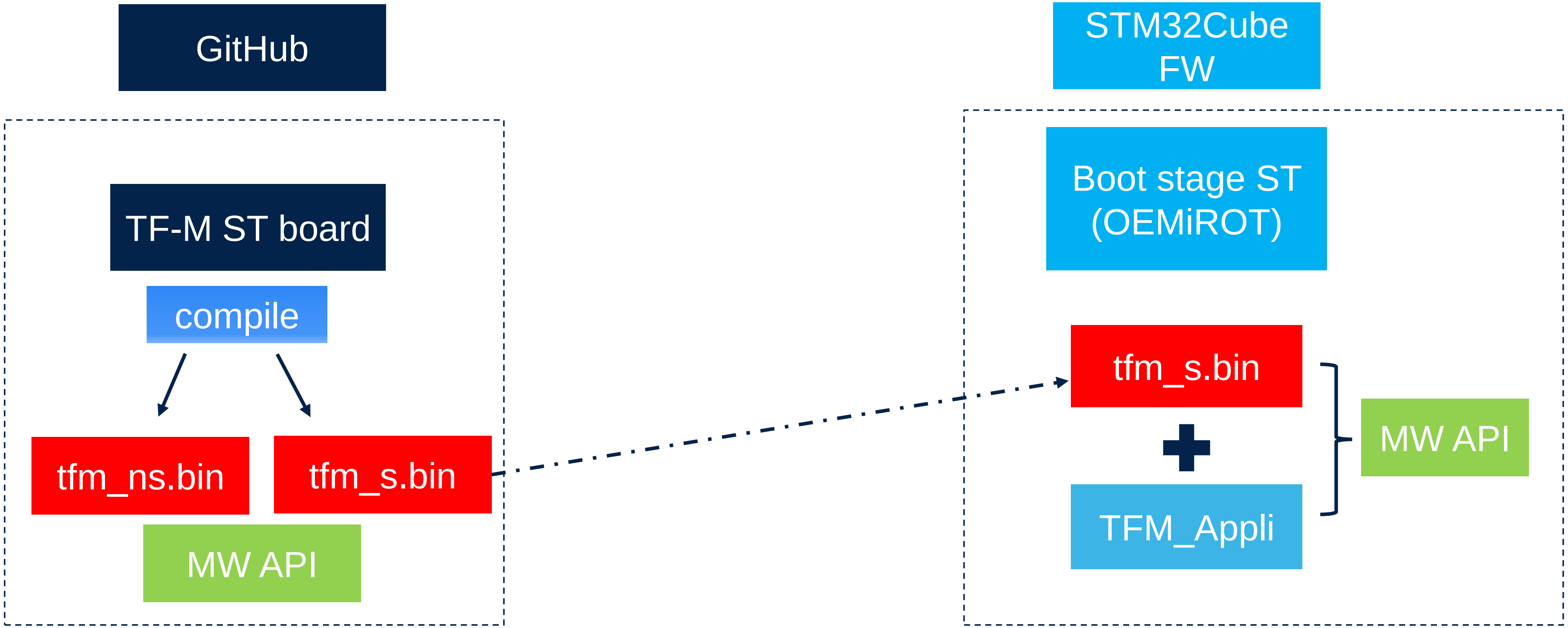
life.augmented

TF-M GitHub && STM32Cube FW

- TF-M GitHub
  - Upstream STM32 platforms strategy :
    - From now: TF-M secure/Non-Secure applications only (next platforms)

- STM32 CubeFW delivery
  - OEMiRoT (Fist stage boot loader in STM32 boot architecture) adaptations for TF-M compatibility.(flash_layout, ..)
  - Deliver MW TFM API (api_ns)
  - Deliver TFM_Appli (demonstrating TF-M features)
  - tfm_s. Binary → (issue for ST Export control rules because it's not ECCN classified).

ST Approach Overview



Adding tfm_s.bin with source code, to ease integration in STM32Cube FW environnement.

life.augmented

Perspective

- Upstream tfm binary with TF-M open source project
  - Why? :
    - Customer benefits : direct reuse

- Binary will be updated every new release.

Our technology starts with You

Find out more at www.st.com

life.augmented