



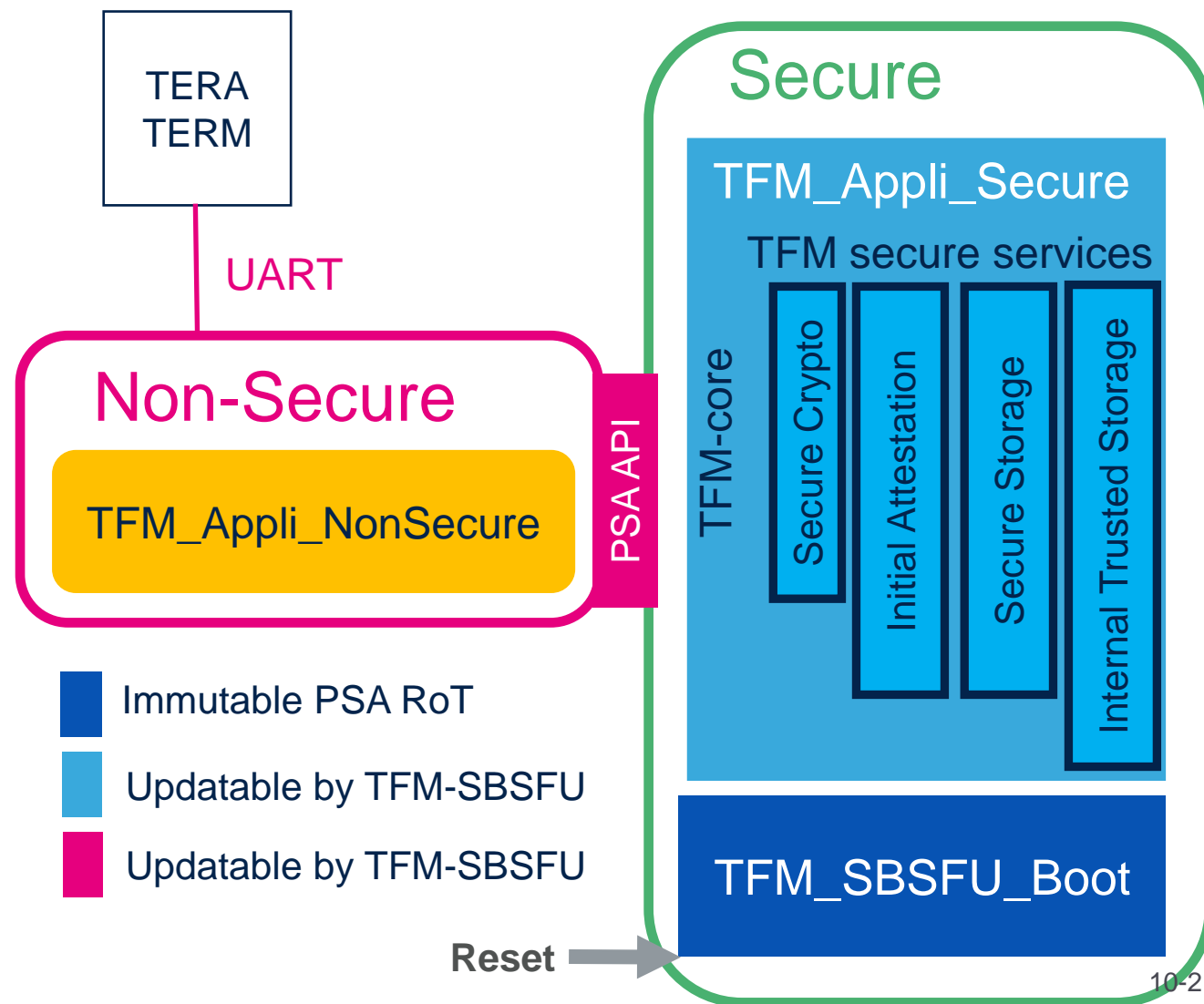
life.augmented

# STM32 Security Workshop

## PSA-TFM Homework

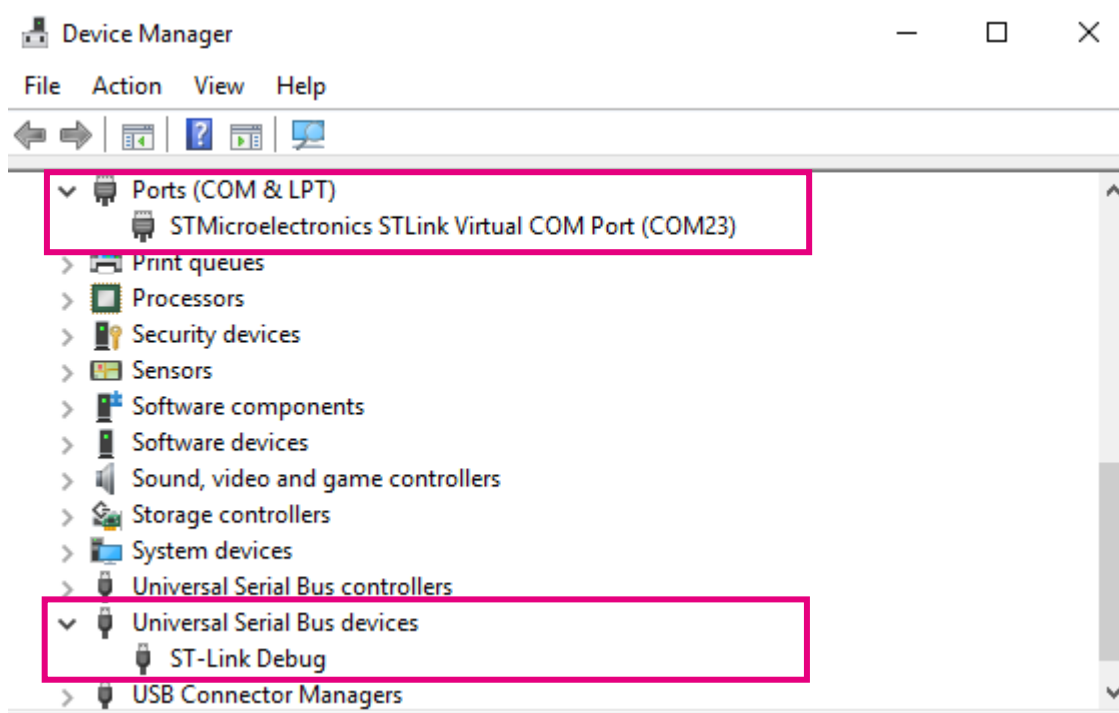
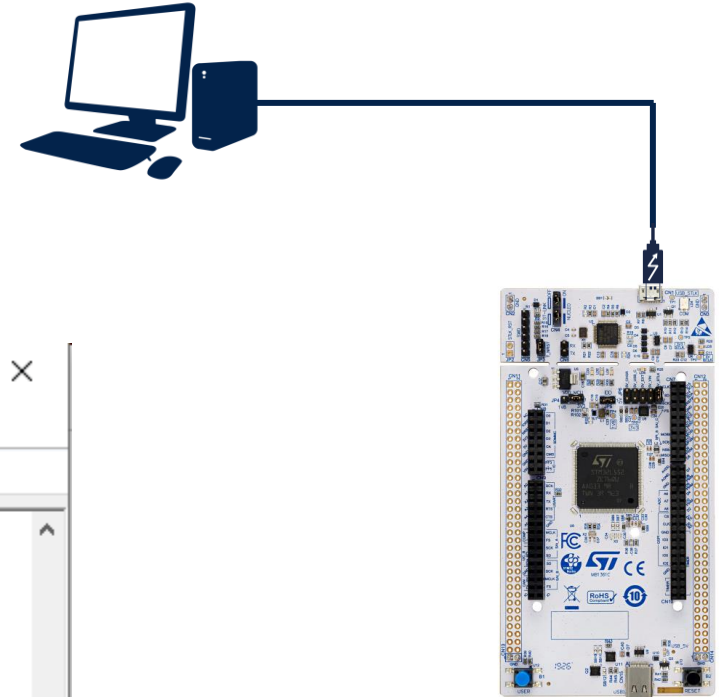
# L5-TFM homework

- Purpose :
  - Check the workshop environment ( HW and SW) is ready for TFM Hands-on
- Scenario ;
  - configure STM32L5 board and flash a precompiled TFM thanks windows script 3 steps :
    - STEP1\_Prepair\_L5\_for\_TFM.bat
    - STEP2\_flash\_precompiled\_TFM.bat
    - StartTeraTermL5



# Connect the Nucleo-L552ZE

- Connect the Nucleo-L552ZE ( CN1-USB-Link) to your PC
- You can check the windows device manager :



# Update the ST-Link firmware

- Launch CubeIDE 

 STM32SecuWS - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window

Help

1

STLinkUpgrade 3.3.4

ST-LINK/V2

Refresh device list

4

Open in update mode

3

ST-Link ID: 066FFF505352716587230728

Current Firmware:

Type: STM32 Debug+Mass storage+VCP

☐ Change Type (Require last USB driver from ST website, else do not use!)

Version: V2137M26

Update to Firmware: V2137M26 STM32 Debug+Mass storage+VCP

Upgrade

4



Information Center

Help Contents

Search

Show Contextual Help

Show Active Keybindings... Ctrl+Shift+L

Tips and Tricks...

Cheat Sheets...

Eclipse User Storage >

Check for Updates

Install New Software...

Eclipse Marketplace...

MX Data Refresh

MX Check for Updates

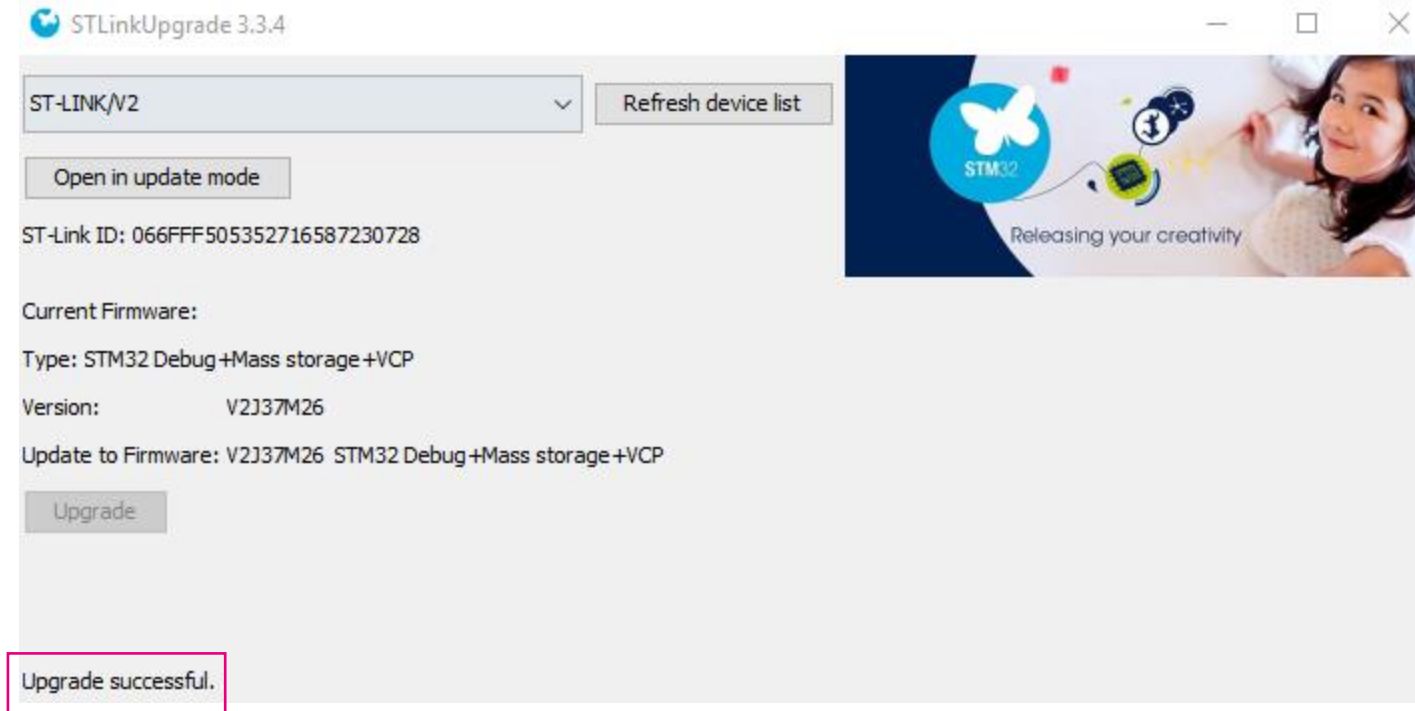
MX Manage embedded software packages

ST-LINK Upgrade

2

IDE About STM32CubeIDE

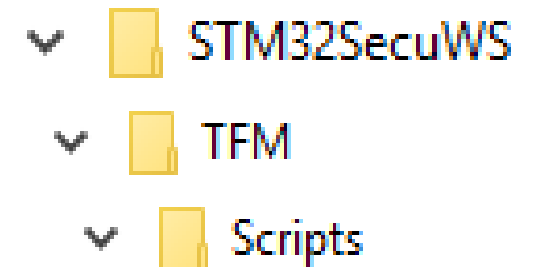
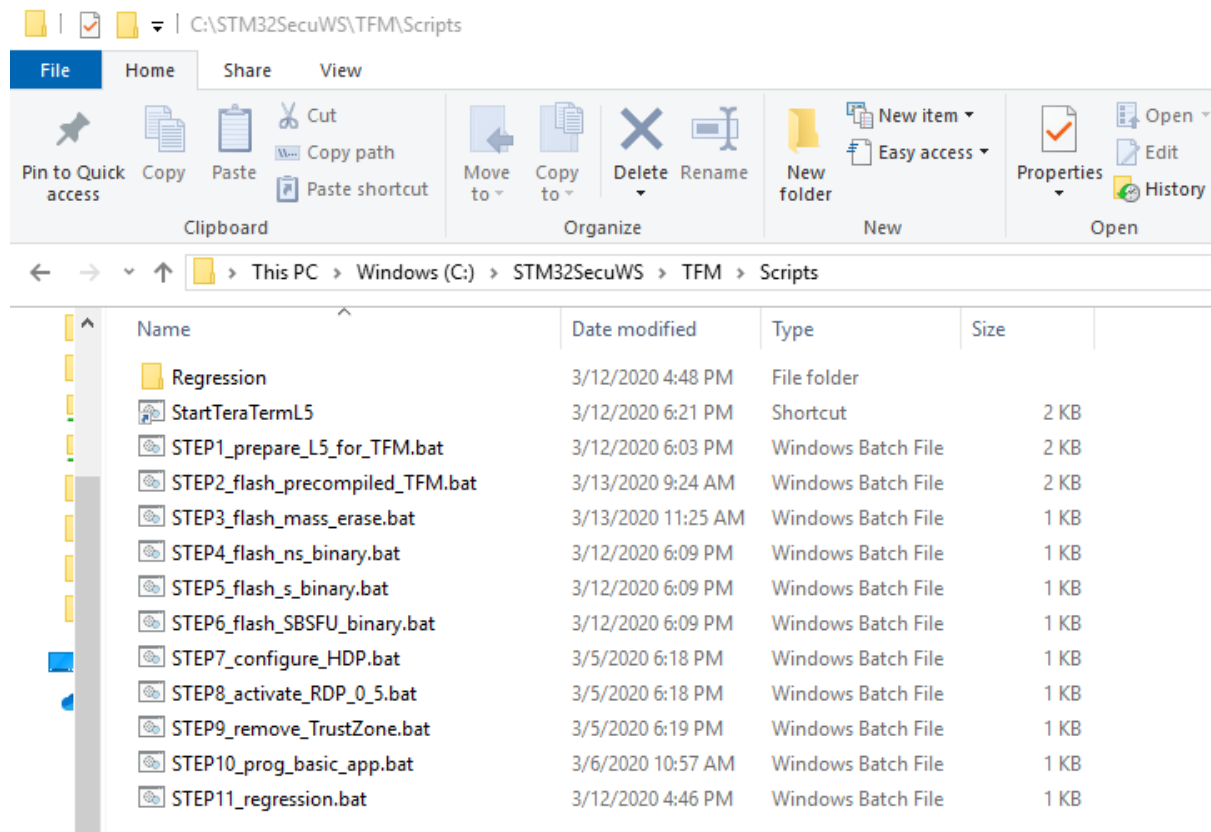
# Update the ST-Link firmware



- Quit Cube IDE

# Open an explorer dedicated to scripts

- During this homework, you will use scripts
- Please keep an explorer window open to access rapidly to these scripts:



# STM32L5 option byte settings

- Activate TrustZone and configure the flash split between secure and non-secure.
- Please launch and check the traces :  
**C:\STM32SecuWS\TFM\Scripts\  
STEP1\_Prepere\_L5\_for\_TFM.bat**

Please check the log...

Some warning as DBank and TZEN already set by previous config. But you should seen no error !

```
C:\windows\system32\cmd.exe

Bank      : 0x00
Address   : 0x50022040
Size      : 32 Bytes

100%

Bank      : 0x01
Address   : 0x50022060
Size      : 16 Bytes

100%

OPTION BYTE PROGRAMMING VERIFICATION:

Option Bytes successfully programmed

*****
"Option setting"
*****
"TZ      : enabled "
"SRAM2_RST : disabled "
"SECBOOTADD0 : 0x180032 -> 0x0C001900"
"DBANK    : enabled "
"SECWM1_PSTRT: 0x0      -> 0x08000000"
"SECWM1_PEND : 0x6F     -> 0x08037800"
"SECWM2_PSTRT: 0x7f     -> 0x0803f800"
"SECWM2_PEND : 0x00     -> 0x08000000"
*****
"Board is ready to receive the TFM binaries, press key"
Press any key to continue . . .
```

- You could ignore : Warning: Option Byte: xxxx, value: 0xx, was not modified ( those option byte has been already set)



# Flash the TFM software

- To flash precompiled version of TFM

TFM\_Appli\_NonSecure + associated metadata : tfm\_ns\_sign.bin

TFM\_Appli\_Secure + associated metadata : tfm\_s\_sign.bin

TFM\_SBSFU\_Boot : TFM\_SBSFU\_Boot.bin

- Please launch and check the traces :  
**C:\STM32SecuWS\TFM\Scripts\  
STEP2\_flash\_precompiled\_TFM.bat**

# Flash the TFM software

```
C:\windows\system32\cmd.exe
```

```
Memory Programming ...  
Opening and parsing file: tfm_ns_sign.bin  
File       : tfm_ns_sign.bin  
Size      : 28196 Bytes  
Address   : 0x08038000  
  
Erasing memory corresponding to segment 0:  
Erasing internal memory sectors [112 125]  
Download in Progress:  
██████████████████████████████████████████████████████████████████████████ 100%  
  
File download complete  
Time elapsed during download operation: 00:00:01.127  
  
Verifying ...  
  
Read progress:  
██████████████████████████████████████████████████████████████████████████ 100%  
  
Download verified successfully  
  
"TFM_Appli NonSecure Written, press a key to flash the TFM_Appli Secure"  
Press any key to continue . . .
```

1 Press any key

```
C:\windows\system32\cmd.exe
```

```
Memory Programming ...  
Opening and parsing file: tfm_s_sign.bin  
File       : tfm_s_sign.bin  
Size      : 138812 Bytes  
Address   : 0x0C014000  
  
Erasing memory corresponding to segment 0:  
Erasing internal memory sectors [40 107]  
Download in Progress:  
██████████████████████████████████████████████████████████████████████████ 100%  
  
File download complete  
Time elapsed during download operation: 00:00:05.237  
  
Verifying ...  
  
Read progress:  
██████████████████████████████████████████████████████████████████████████ 100%  
  
Download verified successfully  
  
"TFM_Appli Secure Written, press a key to flash the "  
Press any key to continue . . .
```

2 Press any key

```
C:\windows\system32\cmd.exe

Memory Programming ...
Opening and parsing file: TFM_SBSFU_Boot.bin
File       : TFM_SBSFU_Boot.bin
Size      : 55930 Bytes
Address   : 0x0C001000

Erasing memory corresponding to segment 0:
Erasing internal memory sectors [2 29]
Download in Progress:
██████████████████████████████████████████████████████████████████████████ 100%

File download complete
Time elapsed during download operation: 00:00:02.158

Verifying ...

Read progress:
██████████████████████████████████████████████████████████████████████████ 100%

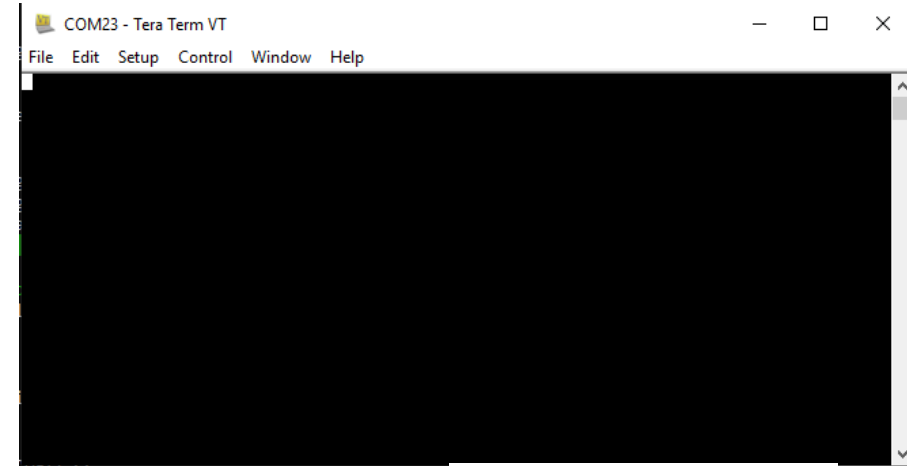
Download verified successfully

"TFM SBSFU Done, press a key"
Press any key to continue . . .
```

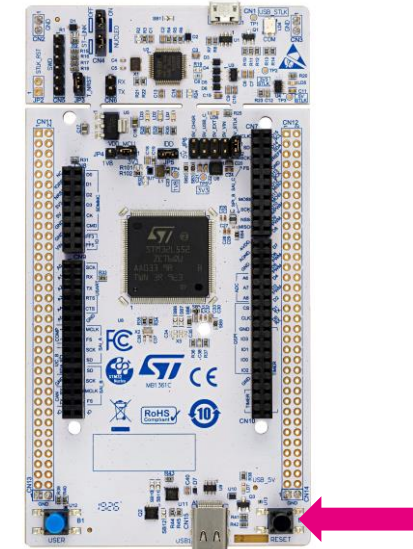
3 Press any key

# Flash the TFM software

- Please launch :  
**C:\STM32SecuWS\TFM\Scripts\  
StartTeraTermL5**



- Reset the board : press the black button on the board



# Check the TFM traces on the Teramterm

```
[INF] Starting bootloader
[INF] Initializing BL2 NU area : Power down/reset not supported...
[INF] Init BL2 NU Header area: Done
[INF] Initializing BL2 NU Counters
[INF] Init BL2 NU counters to 0 : Done
[INF] BL2 NU Area Initialized : Power Down/reset supported
[INF] Checking BL2 NU area
[INF] Checking BL2 NU area header
[INF] Checking BL2 NU Counter consistency
[INF] Consistent BL2 NU Counter 3 = 0x0
[INF] Consistent BL2 NU Counter 4 = 0x0
[INF] Swap type: none
[INF] Swap type: none
[INF] verify counter 0 1000000 0
[INF] counter 0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] Counter 3 set to 0x1000000
[INF] verify counter 1 1000000 0
[INF] counter 1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Counter 4 set to 0x1000000
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2_HUK_STM32L652XX_HUK_CUSTOMIZATION_
set to BL2_SHARED_DATA
[INF] Code c001900 c00ea7a
[INF] hash TFM_SBSFU_Boot 8b114fc3 .. 87de87c
[Sec Thread] Secure image initializing!
```

TFM\_SBSFU traces

TFM\_Appli\_Secure traces

TFM\_Appli\_NonSecure traces

```
=====
=                (C) COPYRIGHT 2019 STMicroelectronics                =
=                                                                    =
=                User App #A                                          =
=====

===== Main Menu =====

Test Protections ----- 1
Test TFM ----- 2
Download a new Fw Image ----- 3
Selection :
```

# Conclusion

- If you seen the previous screen, you are ready for STM32 Security Workshop PSA-TFM hands-on.
- Please keep the board with this configuration for the workshop.
- If you face any issue during the setup, <https://community.st.com/stm32-security-workshop>

# 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.



life.augmented