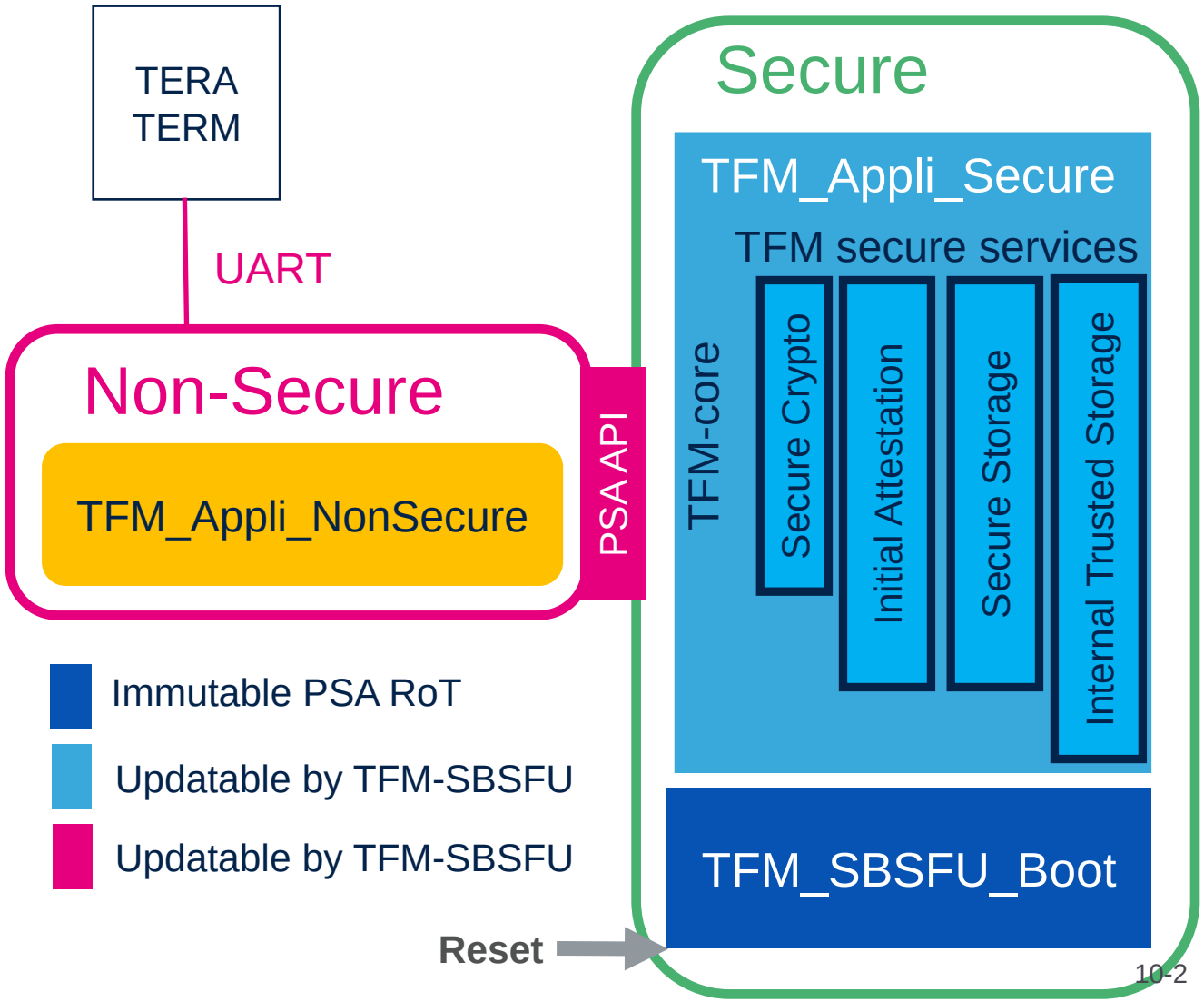
STM32 Security Workshop

PSA-TFM Homework

life.augmented

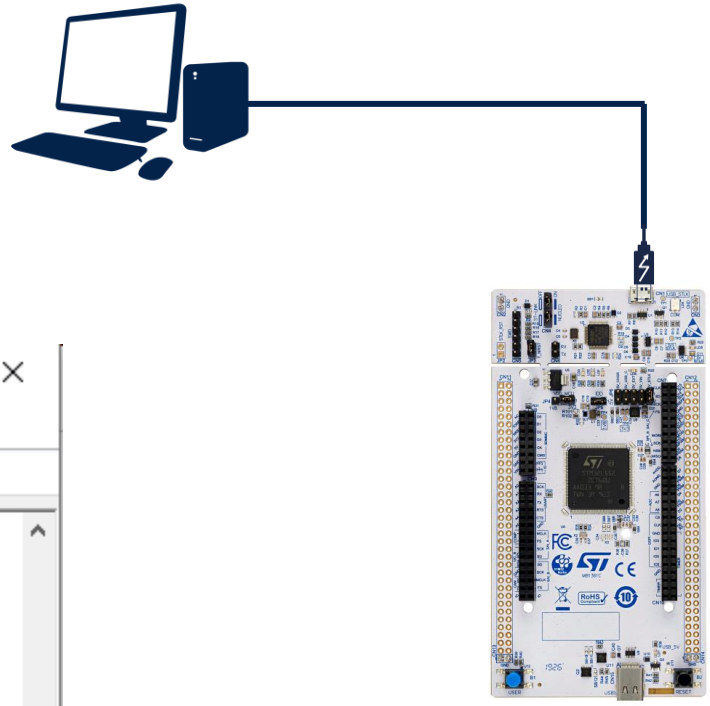
L5-TFM homework

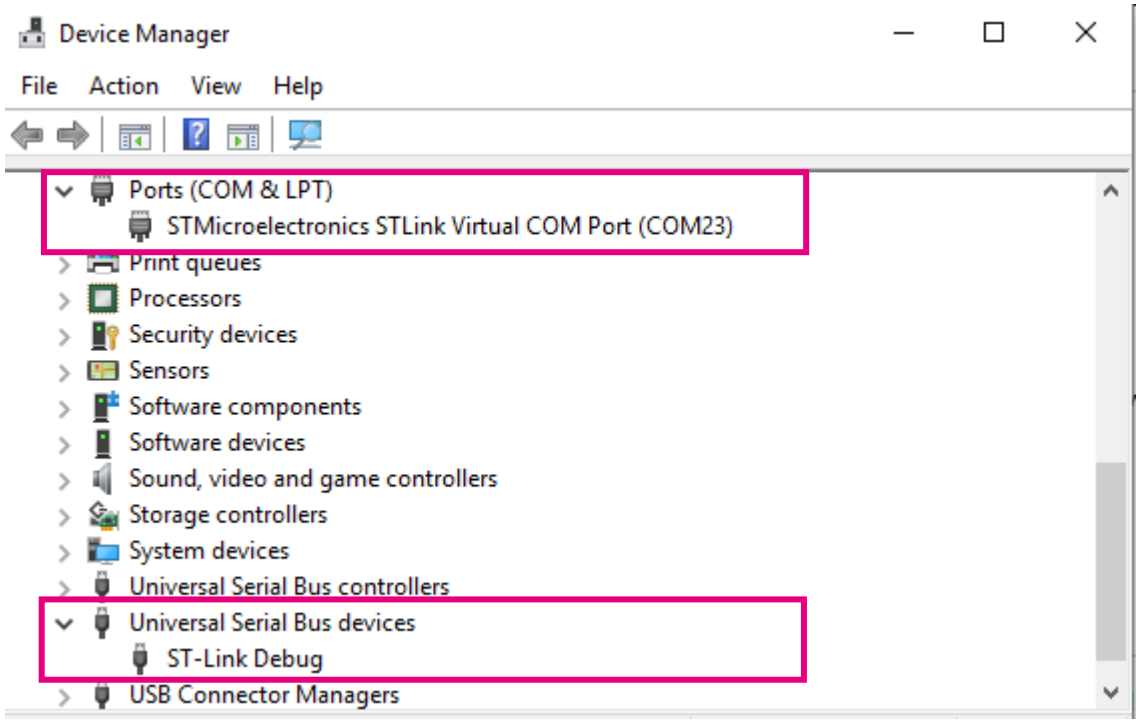
- Purpose :
  - Check the workshop environment (HW and SW) is ready for TFM Hands-on
- Scenario ;
  - configure STM32L5 board and flash a precompiled TFM thanks windows script 3 steps :
    - STEP1_Prepare_L5_for_TFM.bat
    - STEP2_flash_precompiled_TFM.bat
    - StartTeraTermL5



Connect the Nucleo-L552ZE

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

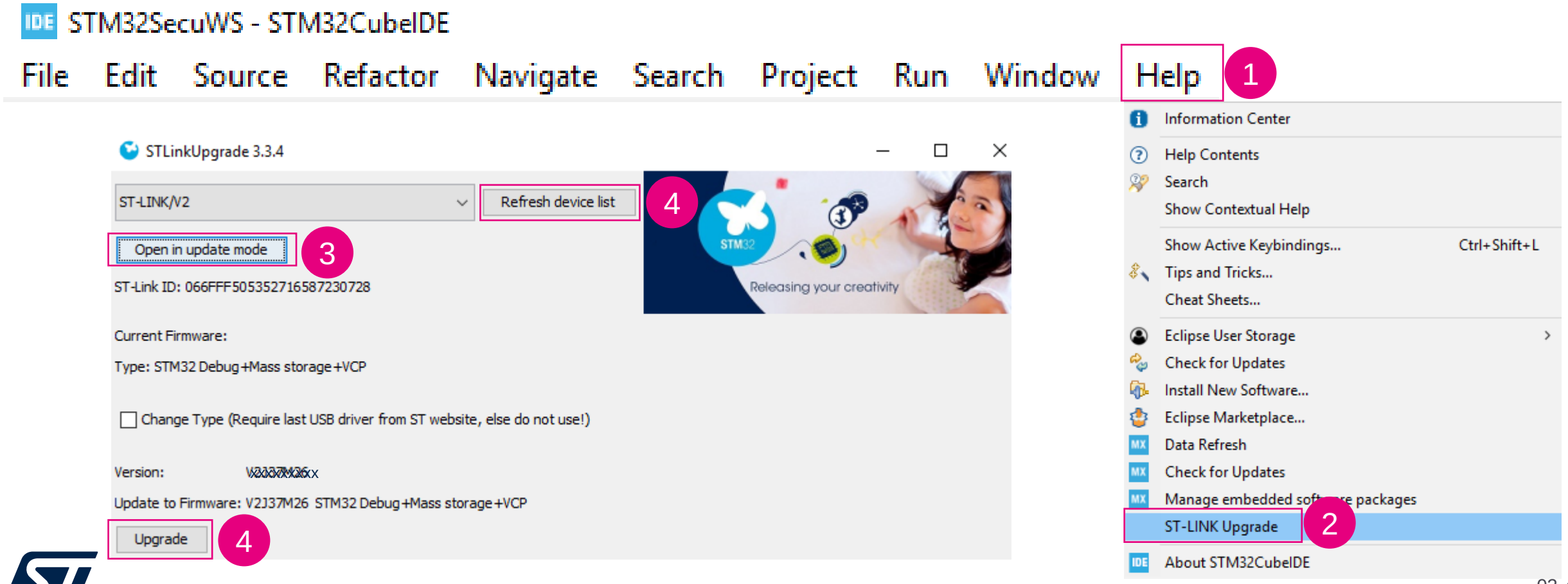




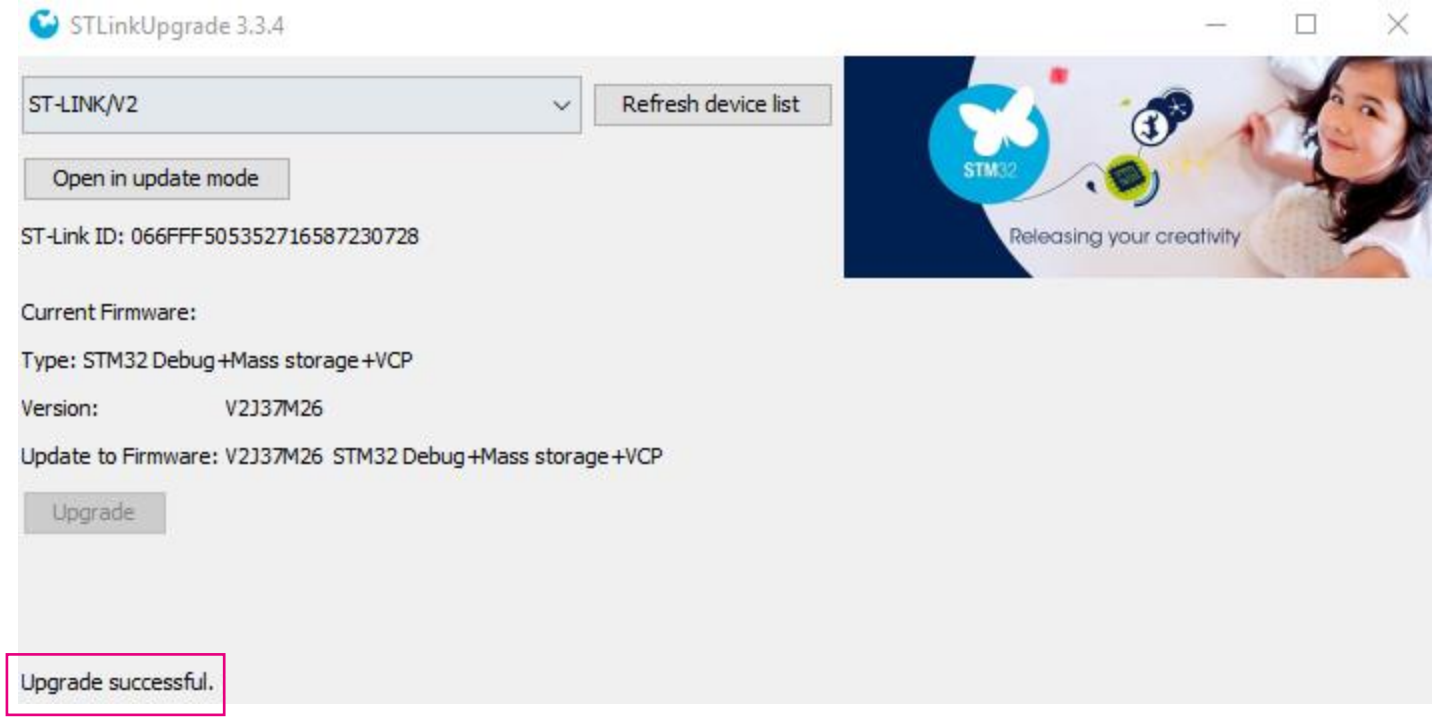
life.augmented

Update the ST-Link firmware

- Launch CubeIDE



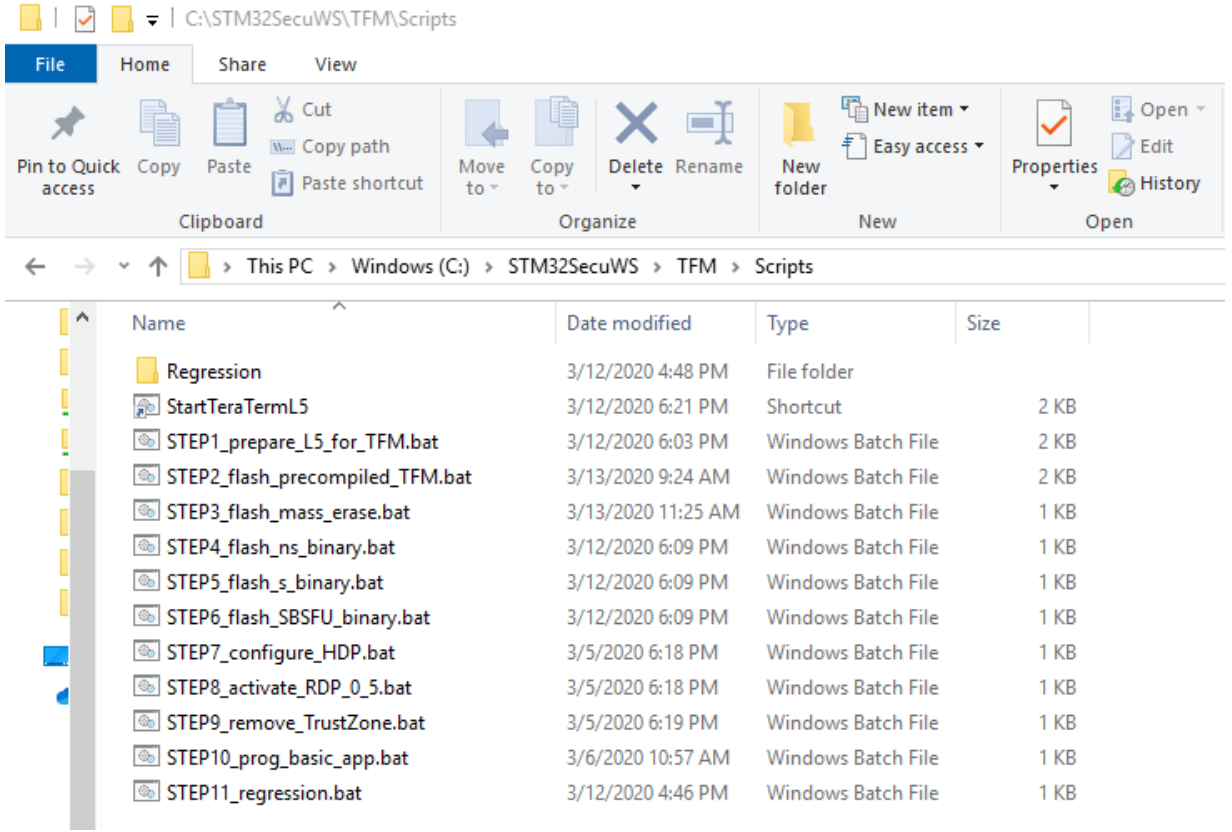
Update the ST-Link firmware

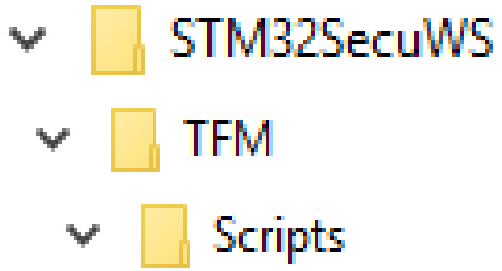


- Quit Cube IDE

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:





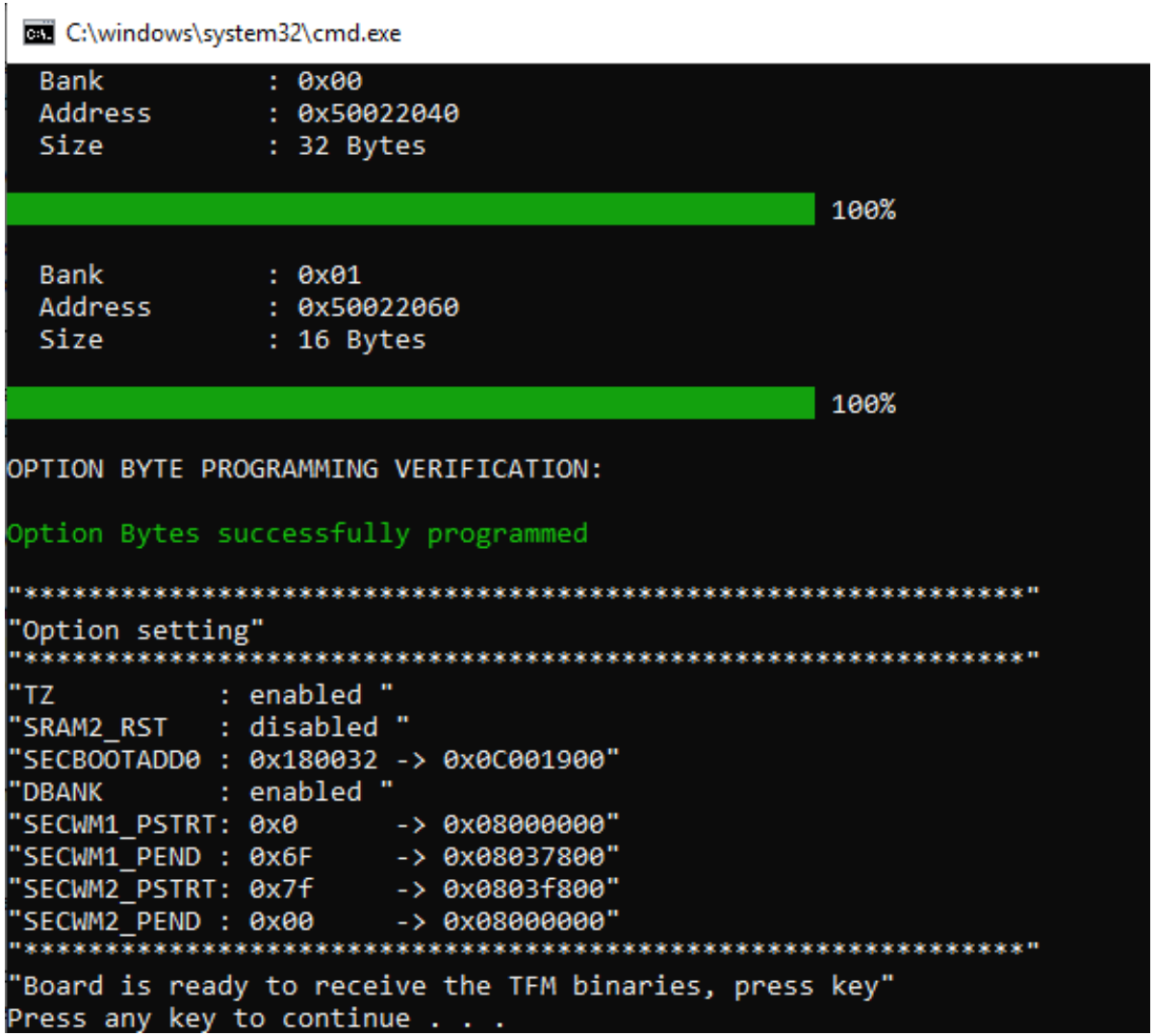
STM32L5 option byte settings

- Activate TrustZone and configure the flash split between secure and non-secure.

- Please launch and check the traces :
  C:\STM32SecuWS\TFM\Scripts
  STEP1_Prepare_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 !



- 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

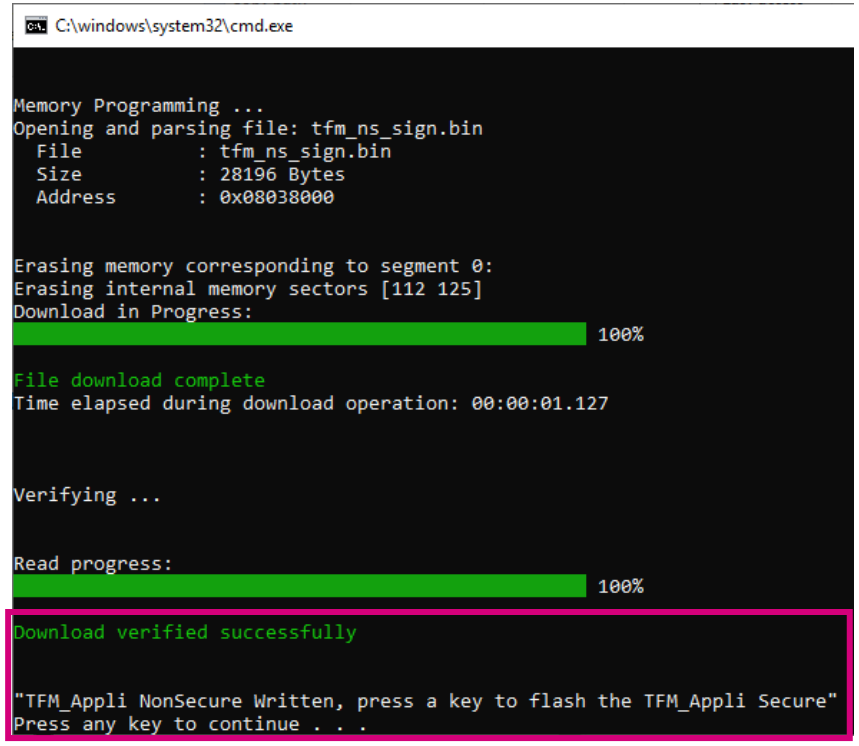
  TFM_Appli_NonSecure + associated metadata : tfm_ns_sign.bin

  TFM_Appli_Secure + associated metadata : tfm_s_sign.bin

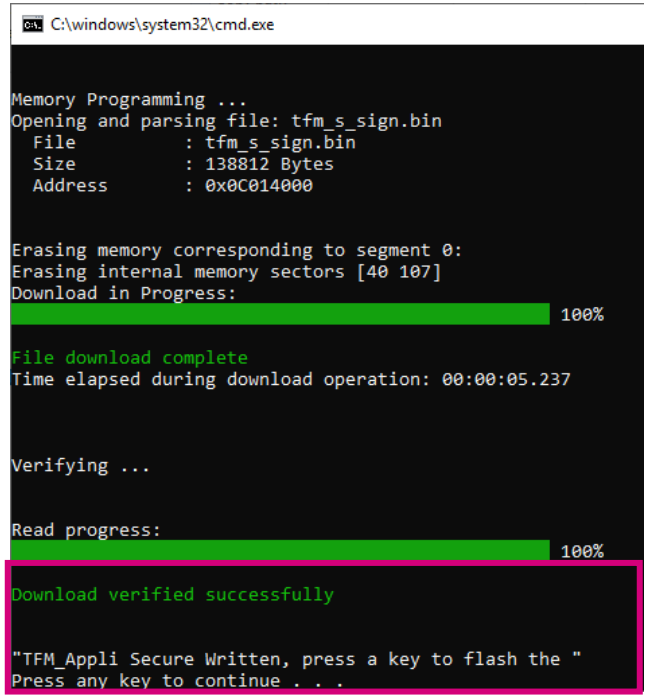
  TFM_SBSFU_Boot : TFM_SBSFU_Boot.bin

- Please launch and check the traces :
  C:\STM32SecuWS\TFM\Scripts
  STEP2_flash_precompiled_TFM.bat

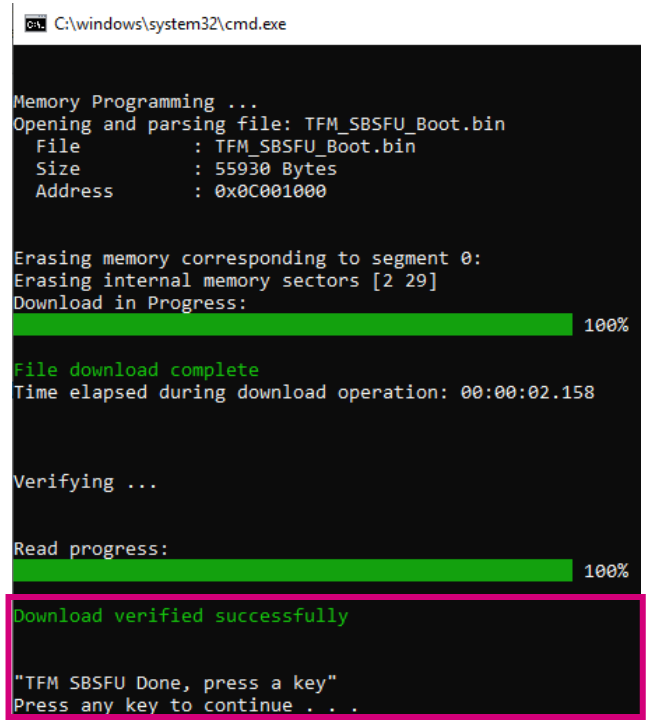
Flash the TFM software



1 Press any key



2 Press any key

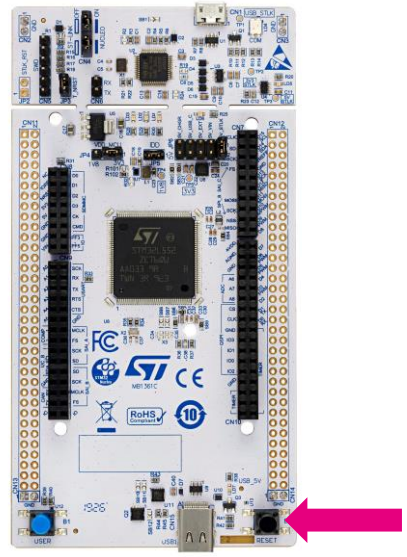


3 Press any key

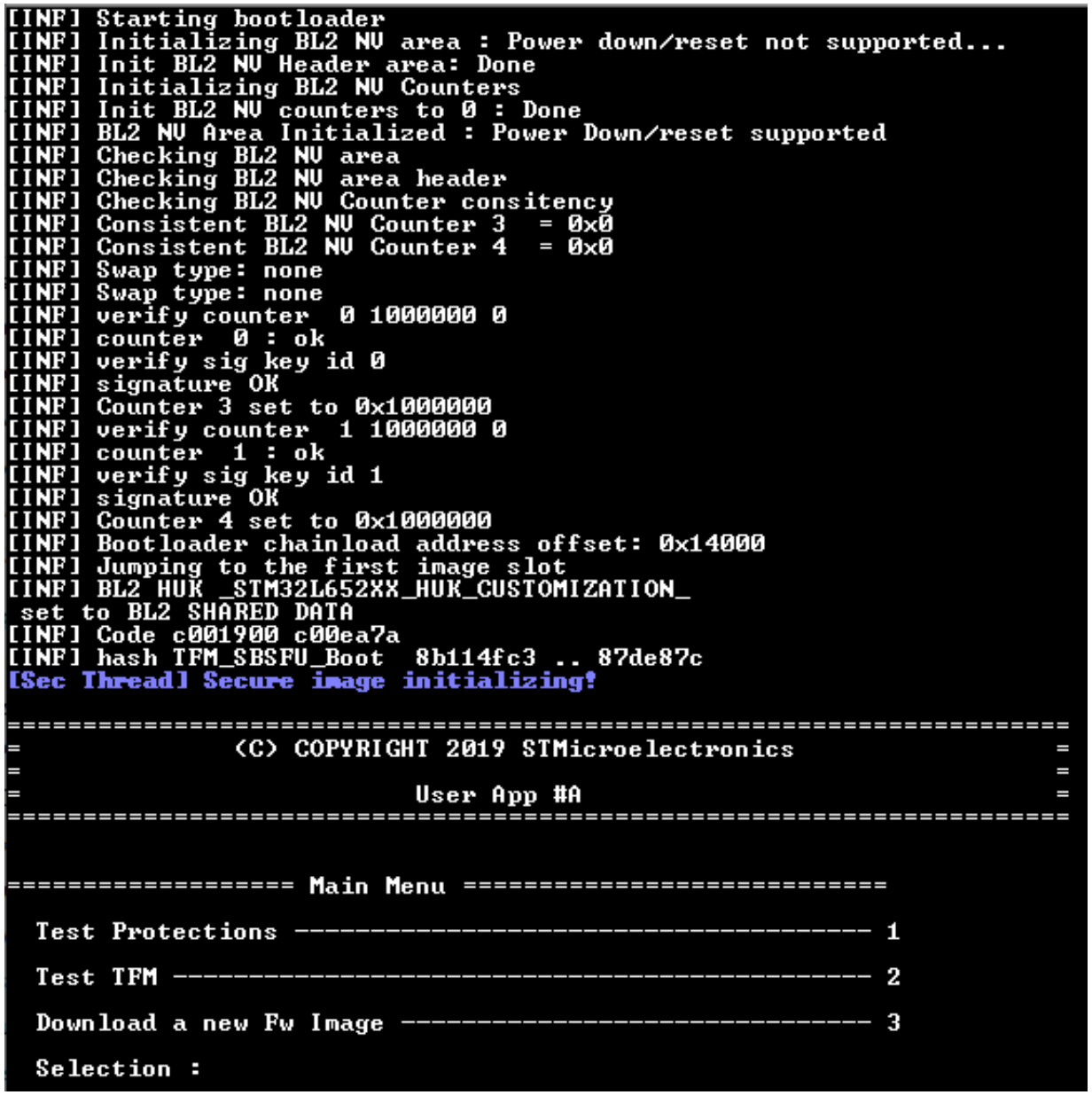
Flash the TFM software

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

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



Check the TFM traces on the Teramterm



TFM_SBSFU traces

TFM_Appli_Secure traces

TFM_Appli_NonSecure traces

life.augmented

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

life.augmented