life.augmented

STM32Trust

STM32H5 Security Secure Manager - Part 3

Hands On: Secure Manager Getting Started

Presenter: Massimo Panzica

Agenda

I Secure Manager features overview

II Hands-On: Install and get started with Secure Manager

III Resources

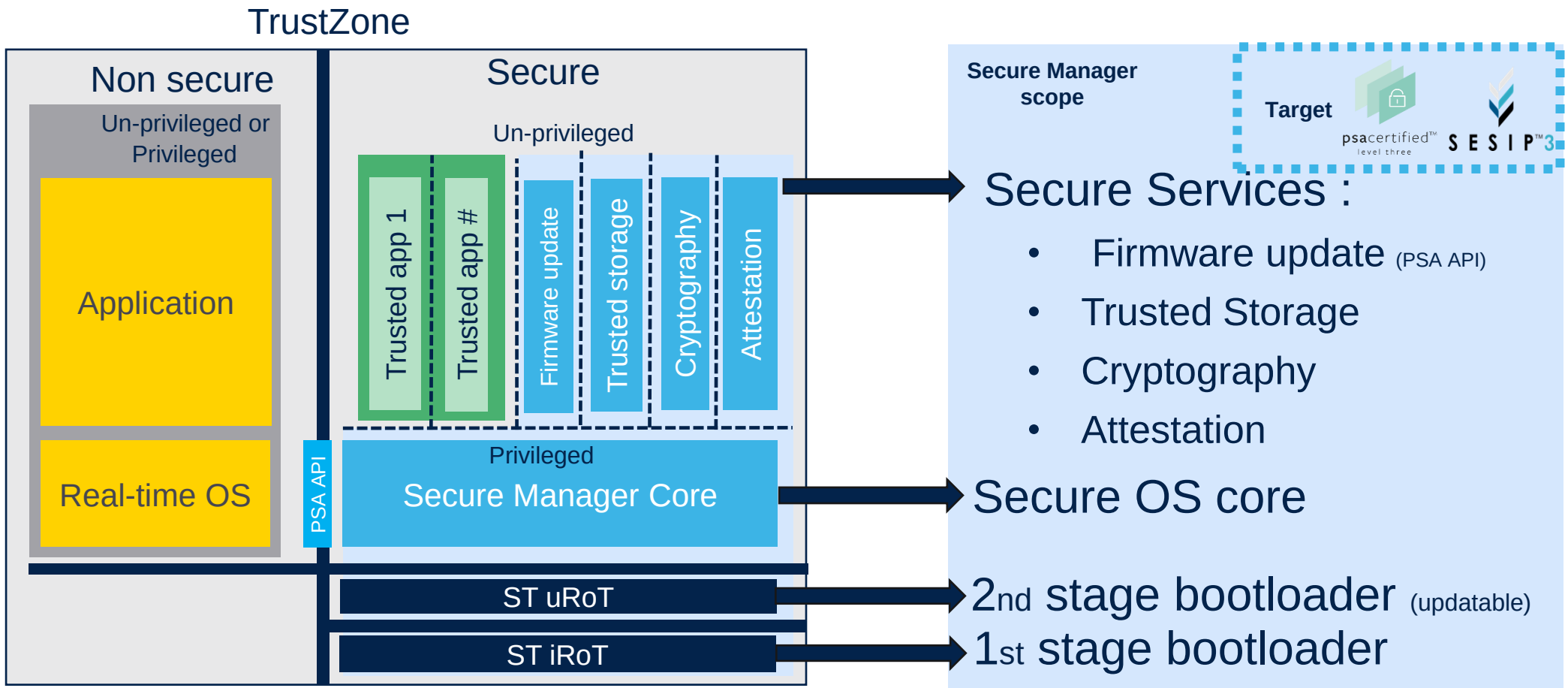
life.augmented

Secure Manager features overview

life.augmented

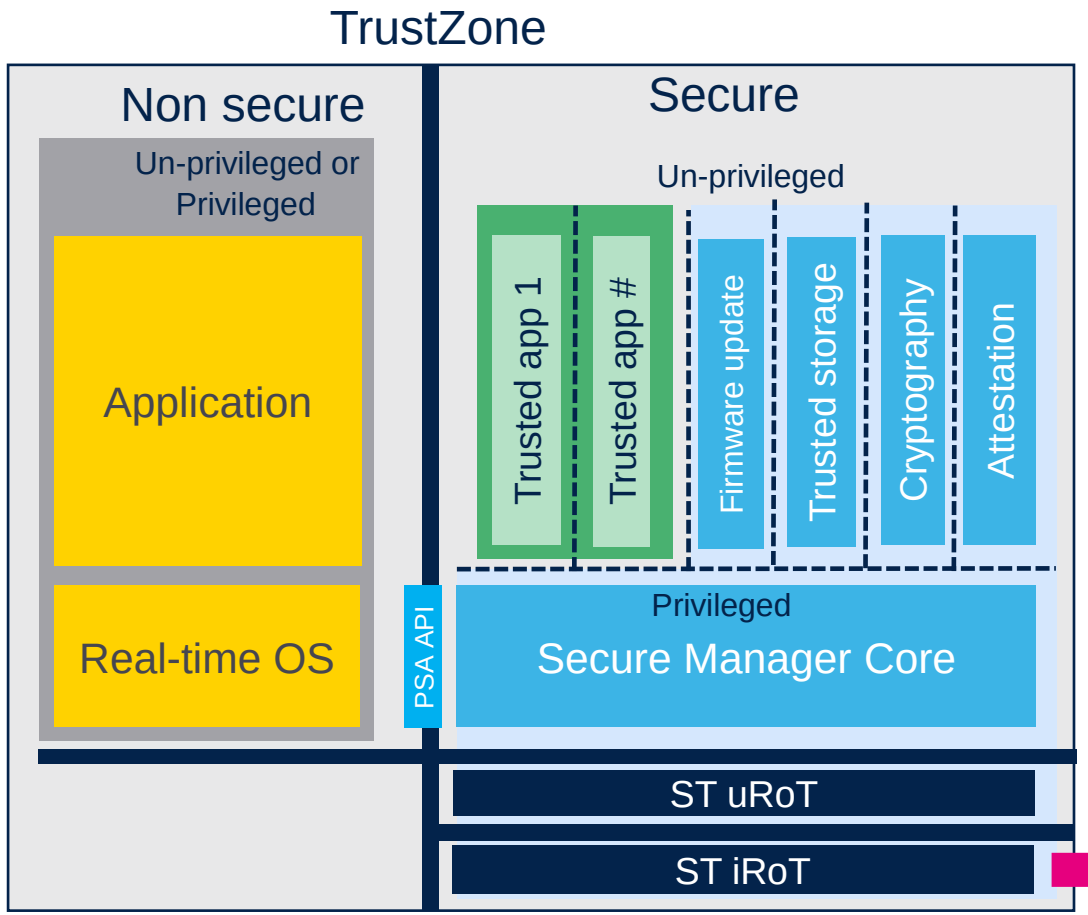
Secure Manager on STM32H5 platform

Protect IP and simplify security customer journey



Secure Manager on STM32H5 platform

Protect IP and simplify security customer journey



Secure Manager scope

Target psacertified™ level three SESIP™3

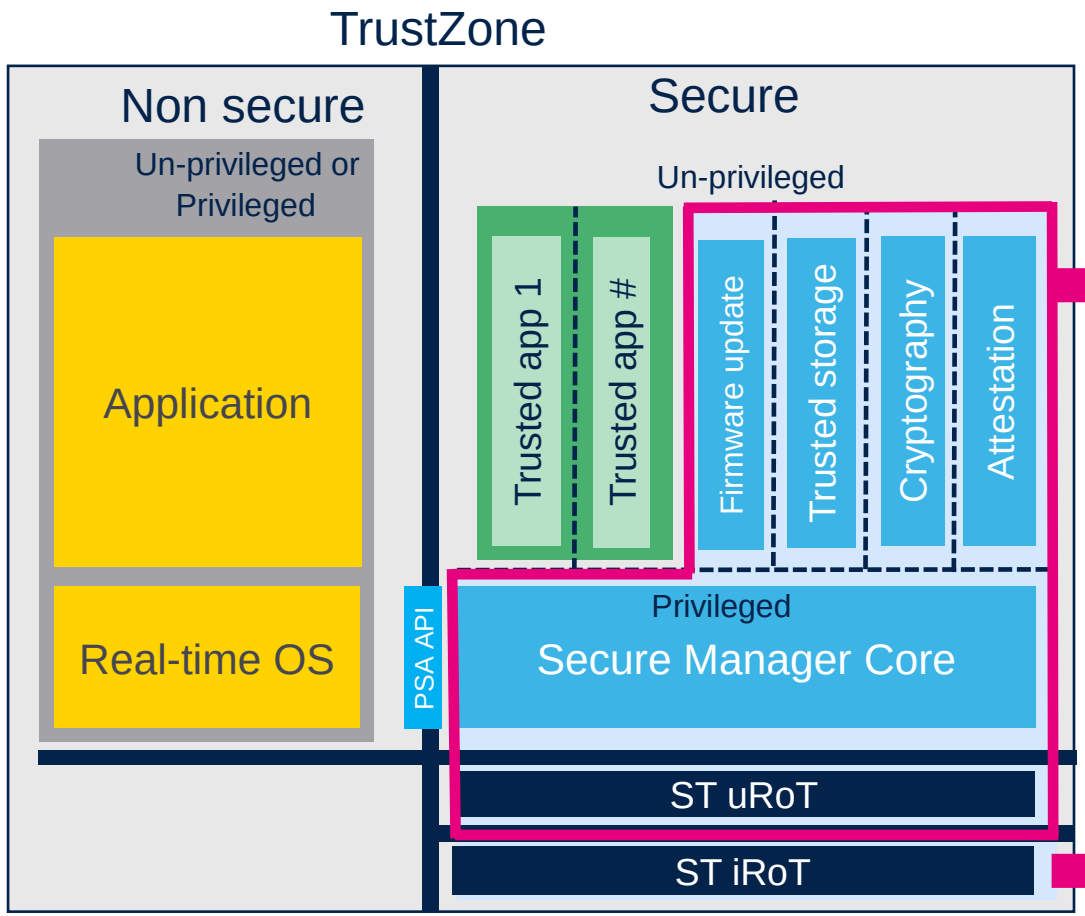
Secure Manager delivered as binary

- encrypted and signed by ST
- securely updatable
- provisioned with application

ROMed Secure bootloader

Secure Manager on STM32H5 platform

Protect IP and simplify security customer journey



Secure Manager scope

Target psacertified™ level three SESIP™3

Secure Manager delivered as binary

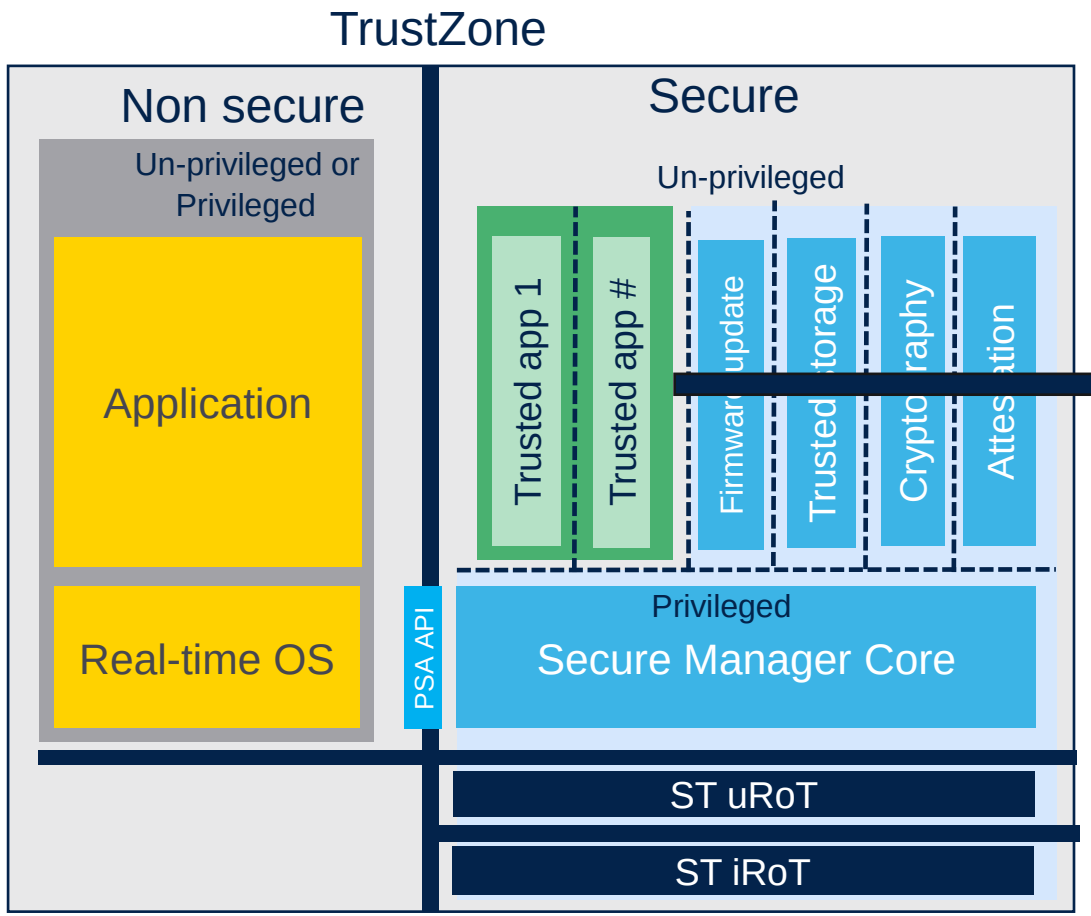
- encrypted and signed by ST
- securely updatable
- provisioned with application

ROMed Secure bootloader

STM32 Trust TEE

Secure Manager on STM32H5 platform

Protect IP and simplify security customer journey



Third Party / OEM scope

Secure Modules: delivered as binary

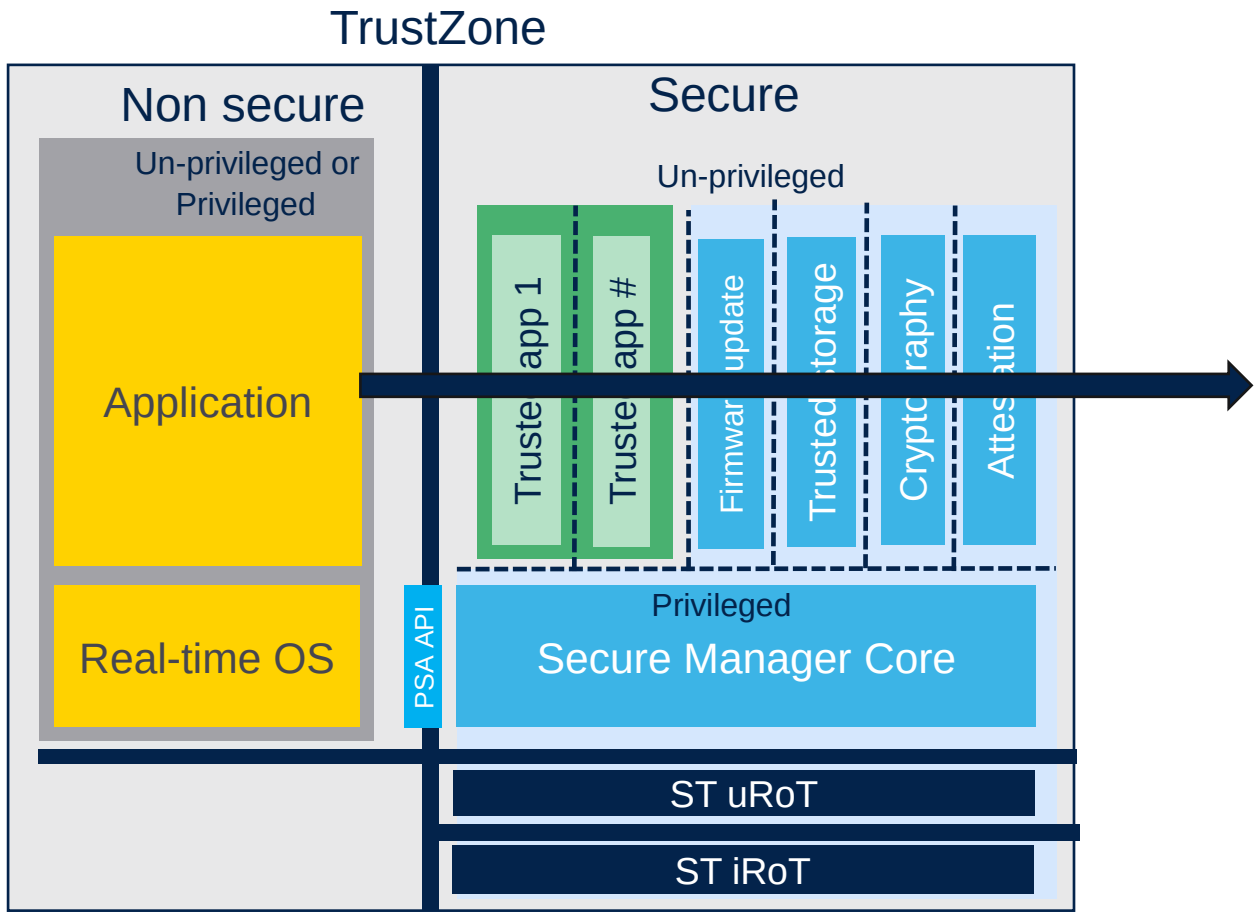
- encrypted and signed by OEM/3rd party
- securely & independently updatable

life.augmented

STM32 Trust TEE

Secure Manager on STM32H5 platform

Protect IP and simplify security customer journey



OEM scope

Non-Secure Application

- securely & independently updatable
- optionally encrypted

life.augmented

STM32 Trust TEE

Secure Manager on STM32H5 platform

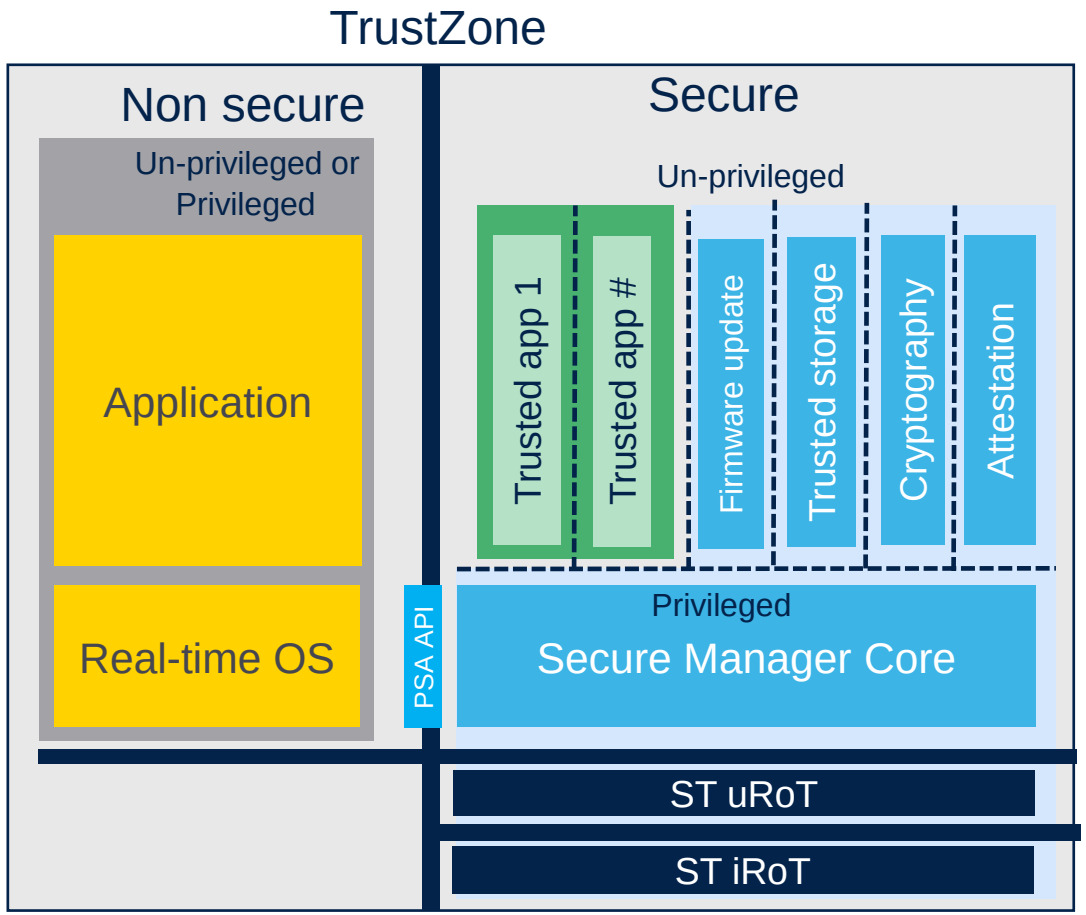
Protect IP and simplify security customer journey

psacertified™ level three

SESIP™3

Target

Scope of Secure Manager



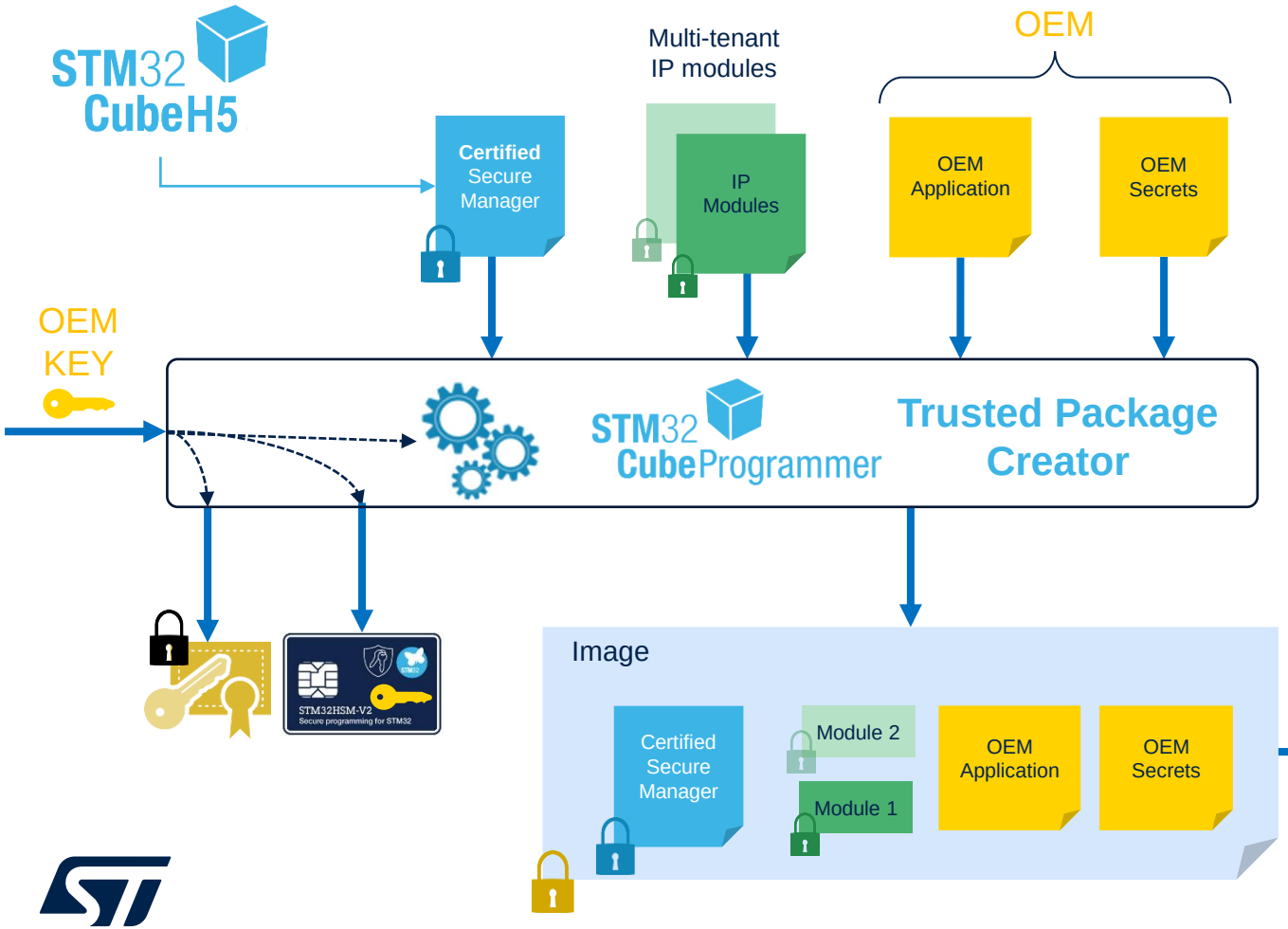
- ST platform ownership
- Turnkey set of security services
- Secure Manager Core to handle isolation
- Multi-tenant software IP protection
- Arm® PSA API compatible
- Designed for Long-Term-Support
- Modular secure update capable
- Optimized certification properties
- Certified and maintained by ST

life.augmented

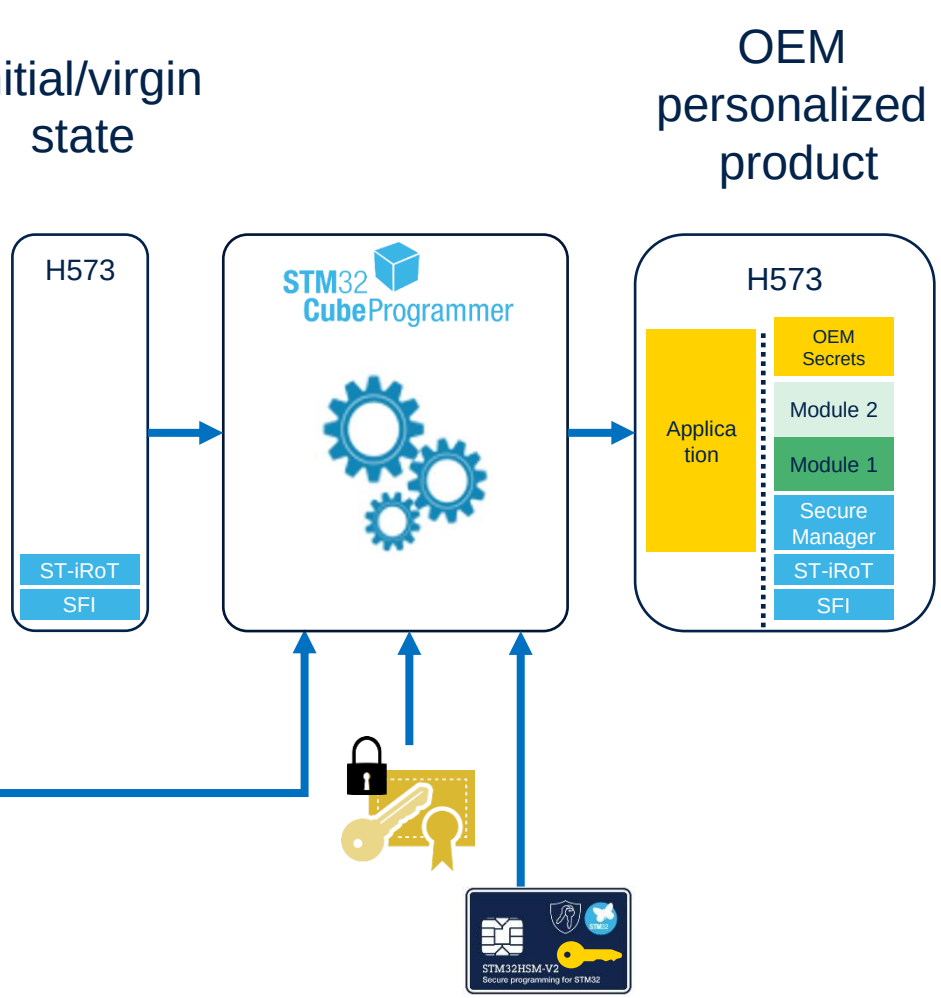
Protected by ST specific Key
Protected by Module Key
Protected by OEM Key
Protected by ST public Key for OEM

Secure Manager
Configuration & Installation flow

Creation Flow



Installation Flow



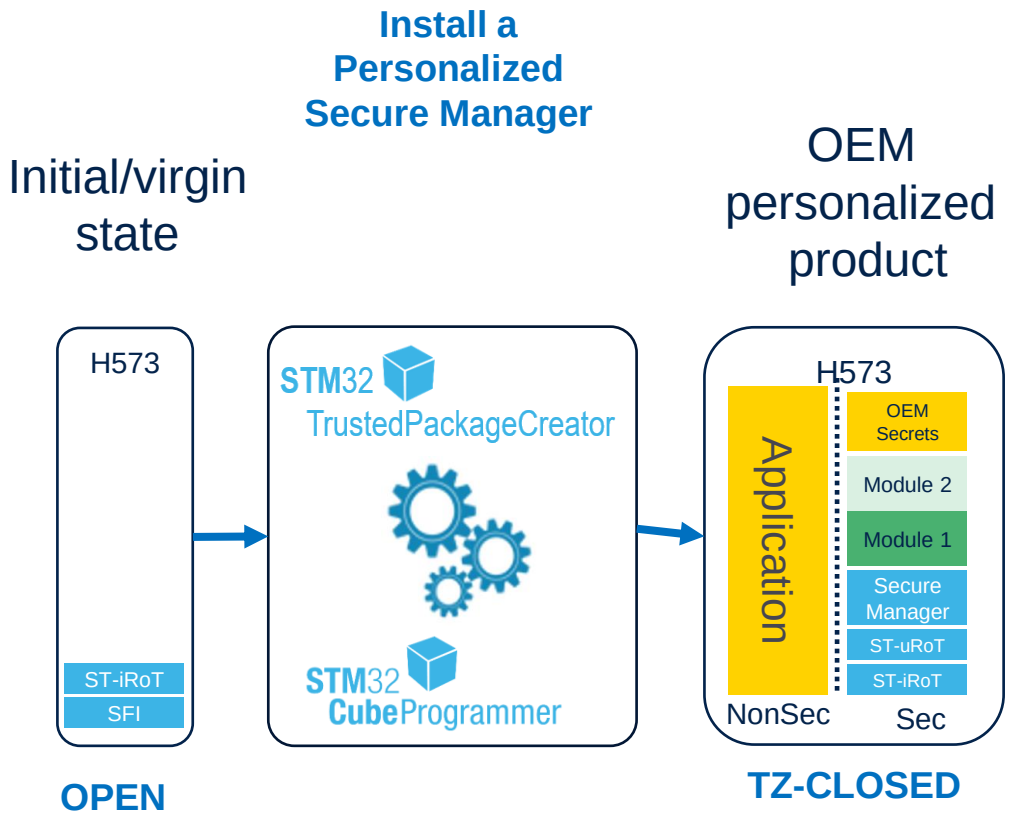
life.augmented

Hands-on: Install and get started with Secure Manager

life.augmented

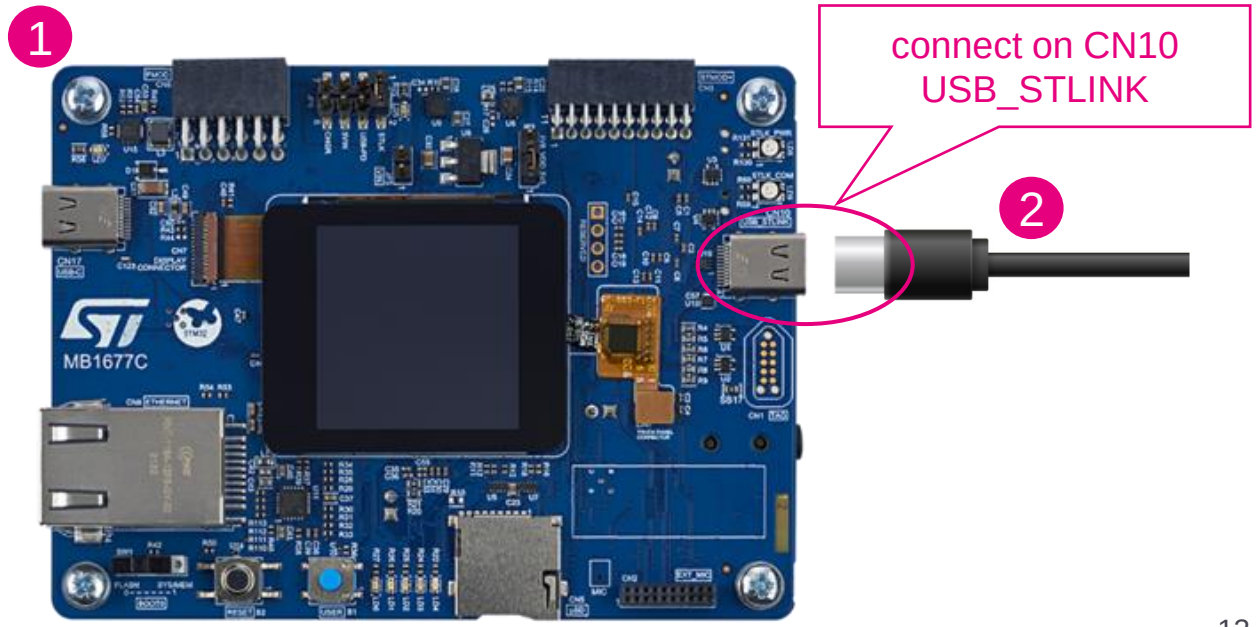
Hands-on

Configuration and Installation Flow



Hands-on: Requirements

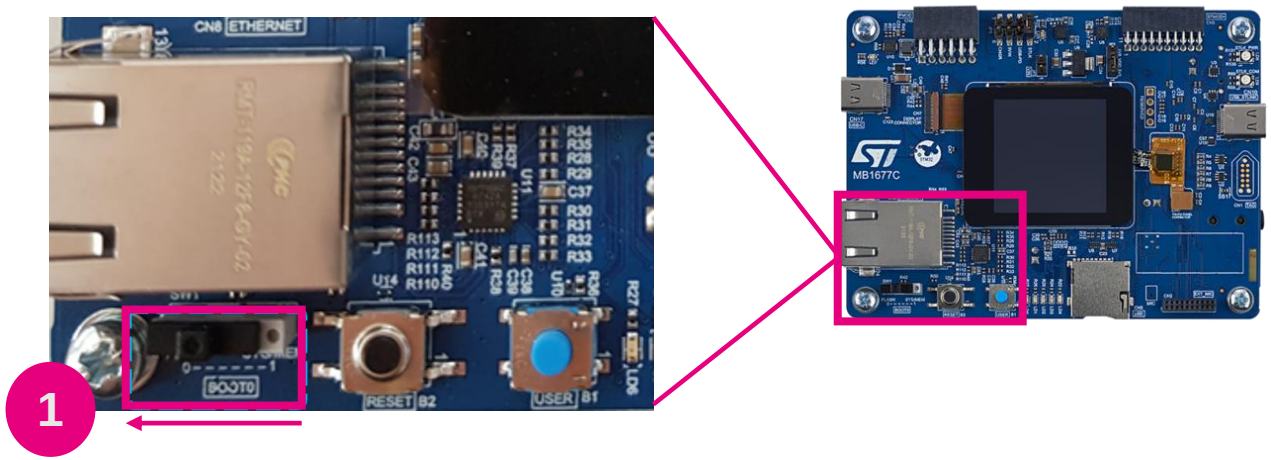
- SW Requirement :
  - STM32CubeH5 version 1.2.0 or upper
  - STM32TRUSTEE-SM version 1.1.2 or upper
  - STM32CubeIDE version 1.15.0 or upper
  - STM32CubeProgrammer version 2.15.0 (which includes STM32TrustePackageCreator)
  - Terminal application (TERATERM)
- HW Requirement :
  1. STM32H573-DK
  2. USB cable (Type C, or Type C-to-Type A)



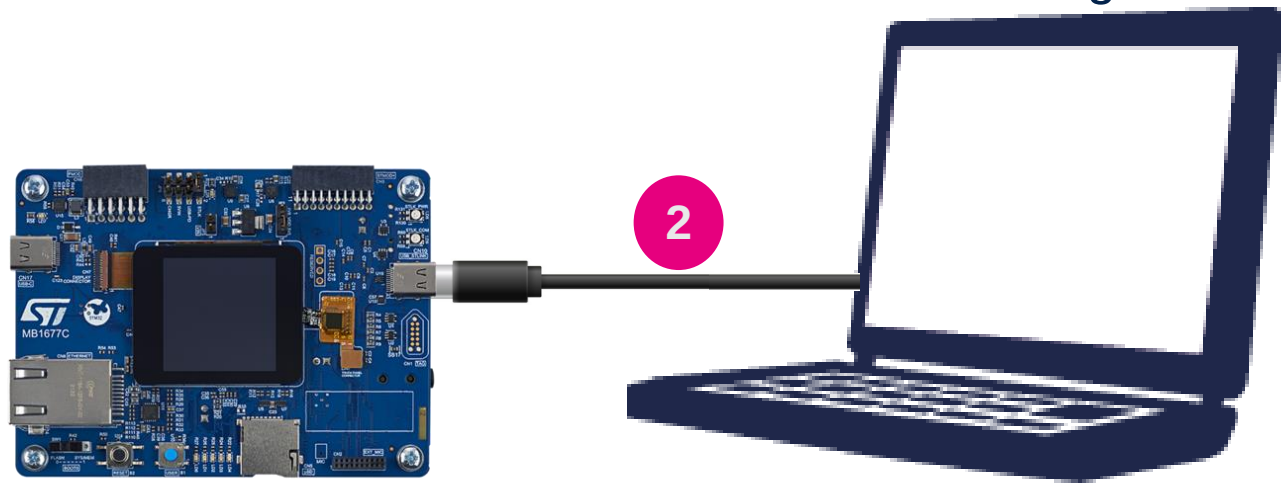
life.augmented

Hands-on: Hw configuration

- On the STM32H573-DK, check that the SW1 BOOT0 switch is set to 0 to boot from user flash

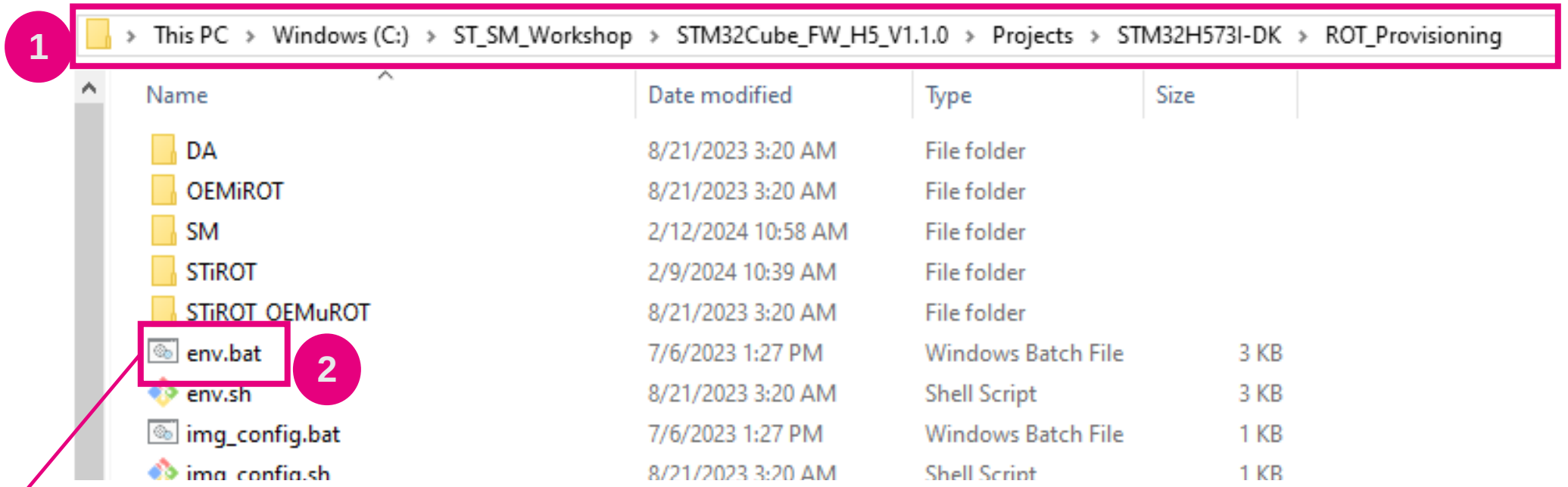


- Connect the STM32H573-DK to the Windows PC using the USB-C cable



Hands-on: Tools/Scripts configuration

Warning: If STM32CubeProgrammer is not installed in the default folder, the customized installation path must be updated in the environment variables script files: **“env.bat”** for our hands-on.

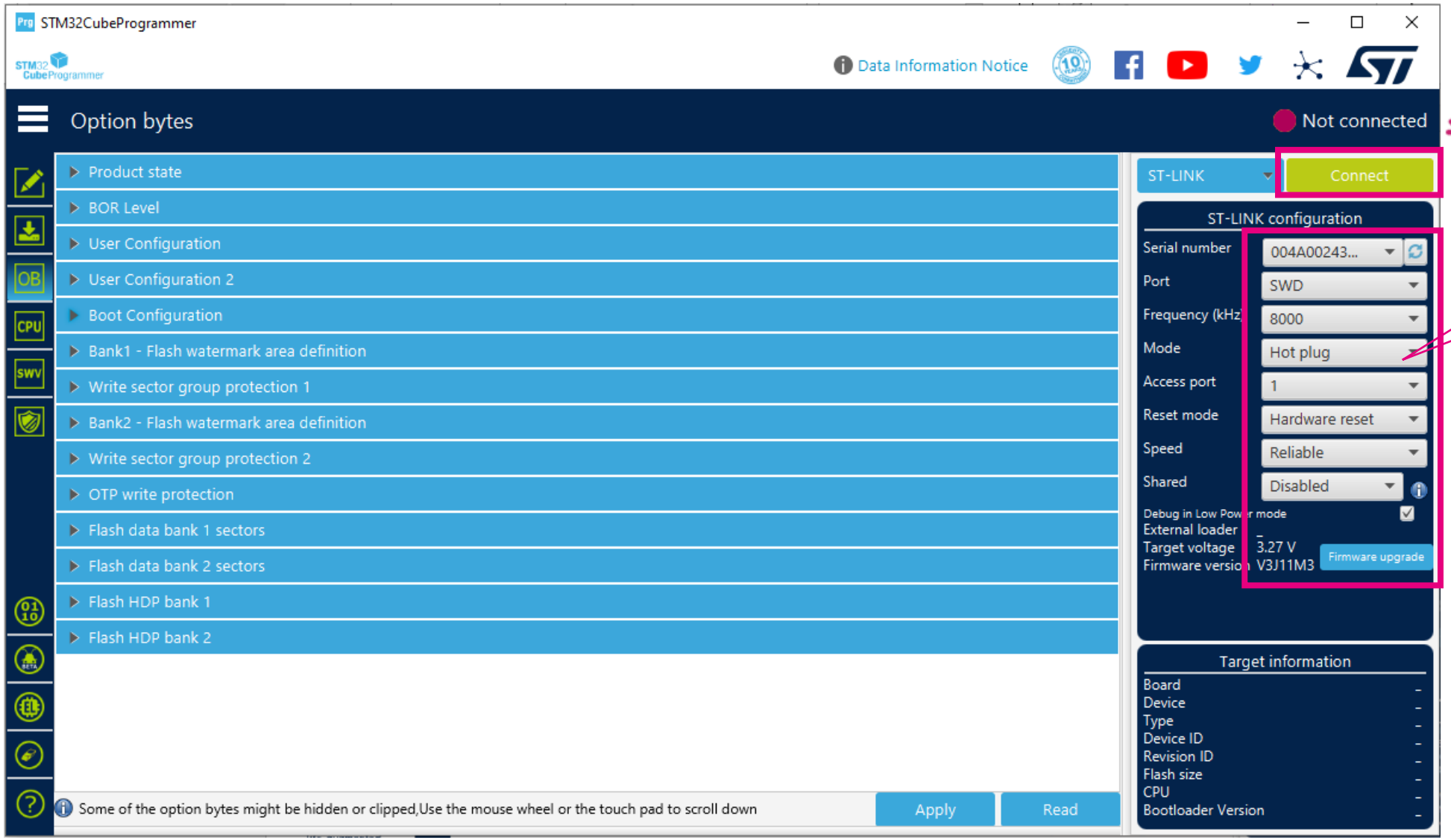



```
:: ============================================================================
::                              General
:: ============================================================================
:: Configure tools installation path
set stm32programmercli="C:\Program Files\STMicroelectronics\STM32Cube\STM32CubeProgrammer\bin\STM32_Programmer_CLI.exe"
set stm32tpccli="C:\Program Files\STMicroelectronics\STM32Cube\STM32CubeProgrammer\bin\STM32TrustedPackageCreator_CLI.exe"
```

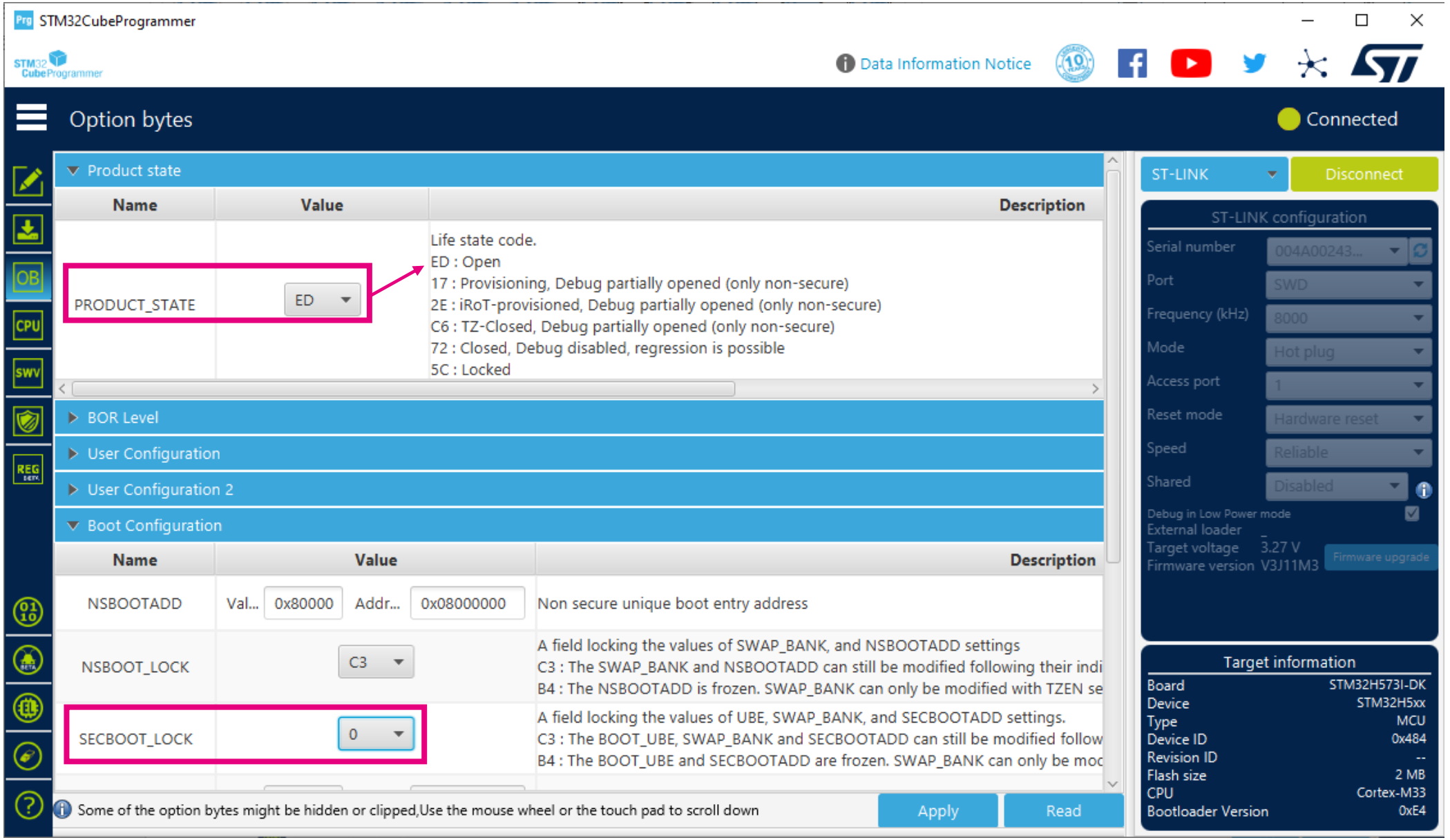
IMPORTANT: This workshop was initially created using the STM32CubeH5 V1.1.x. Every time you see the path STM32Cube_FW_H5_V1.1.x, it is in fact “STM32Cube_FW_H5_V1.2.0” or any newer version/path you are using.

life.augmented

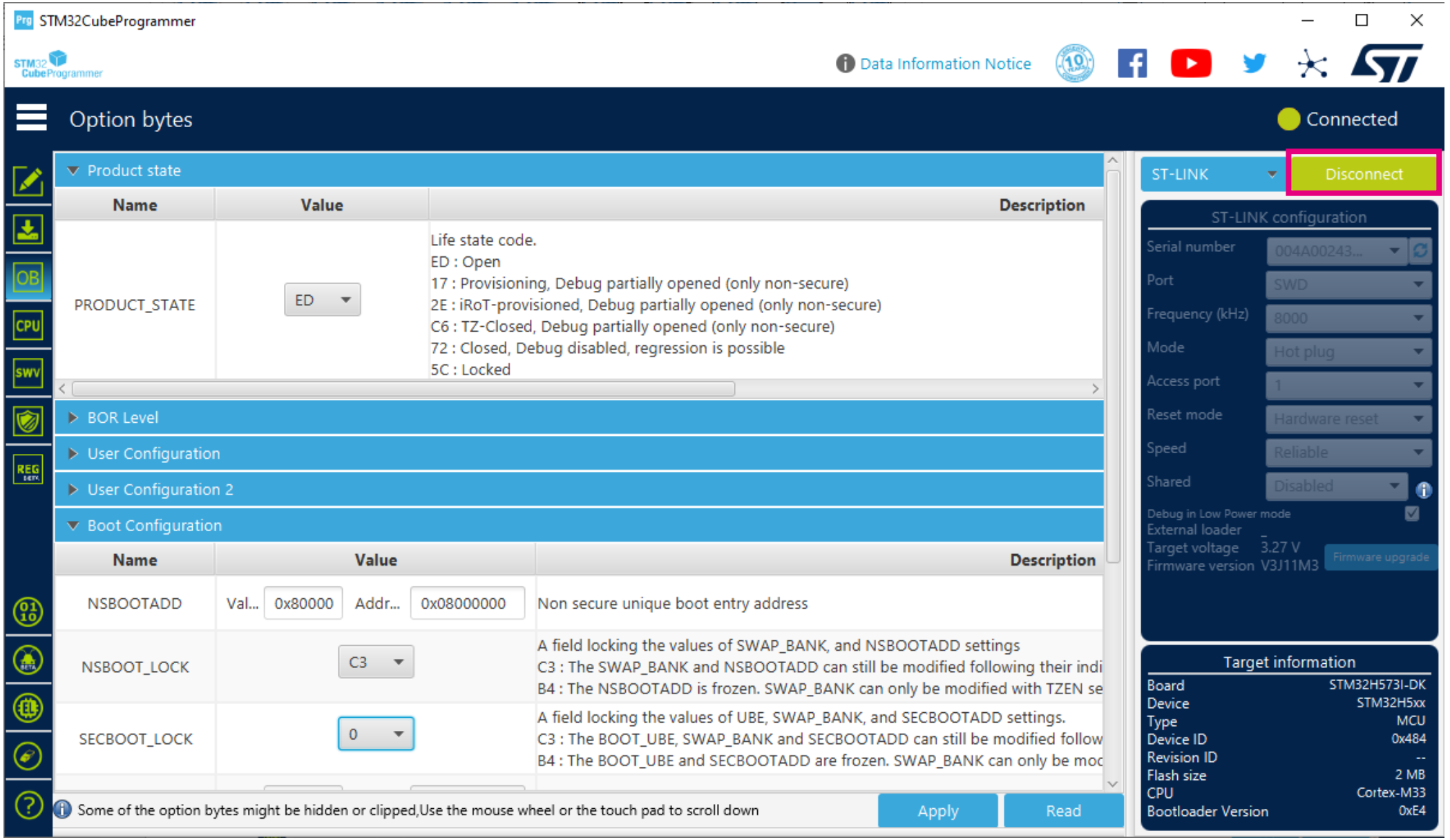
Hands-on: OB status check 1/3



Hands-on: OB status check 2/3

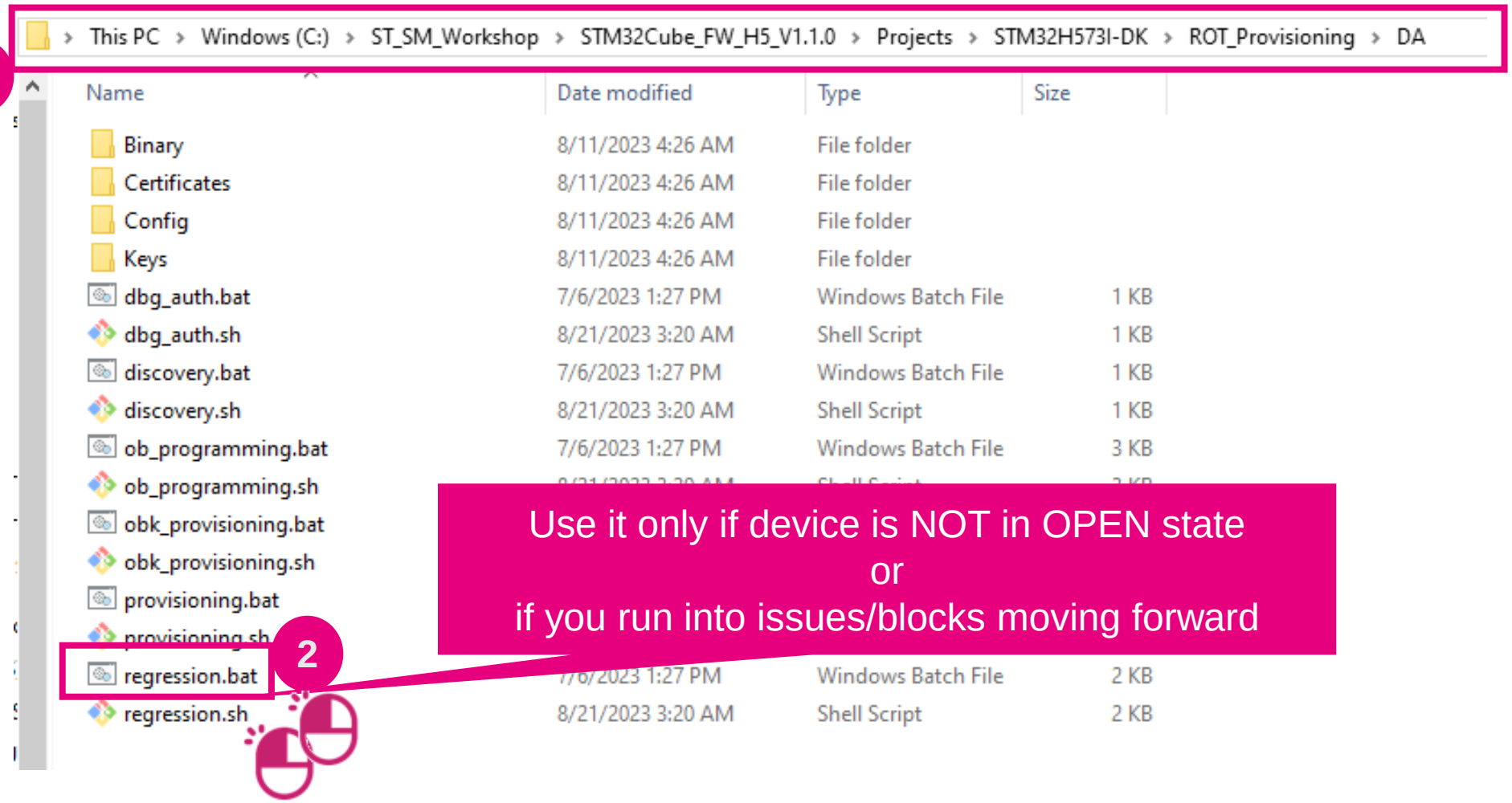


Hands-on: OB status check 3/3



Hands-on: OB status check ONLY IF NEEDED

WARNING: Use the regression script only if you find out that your device is not in OPEN state.
Or if you run into issues/block moving forward because board already used/configured etc.

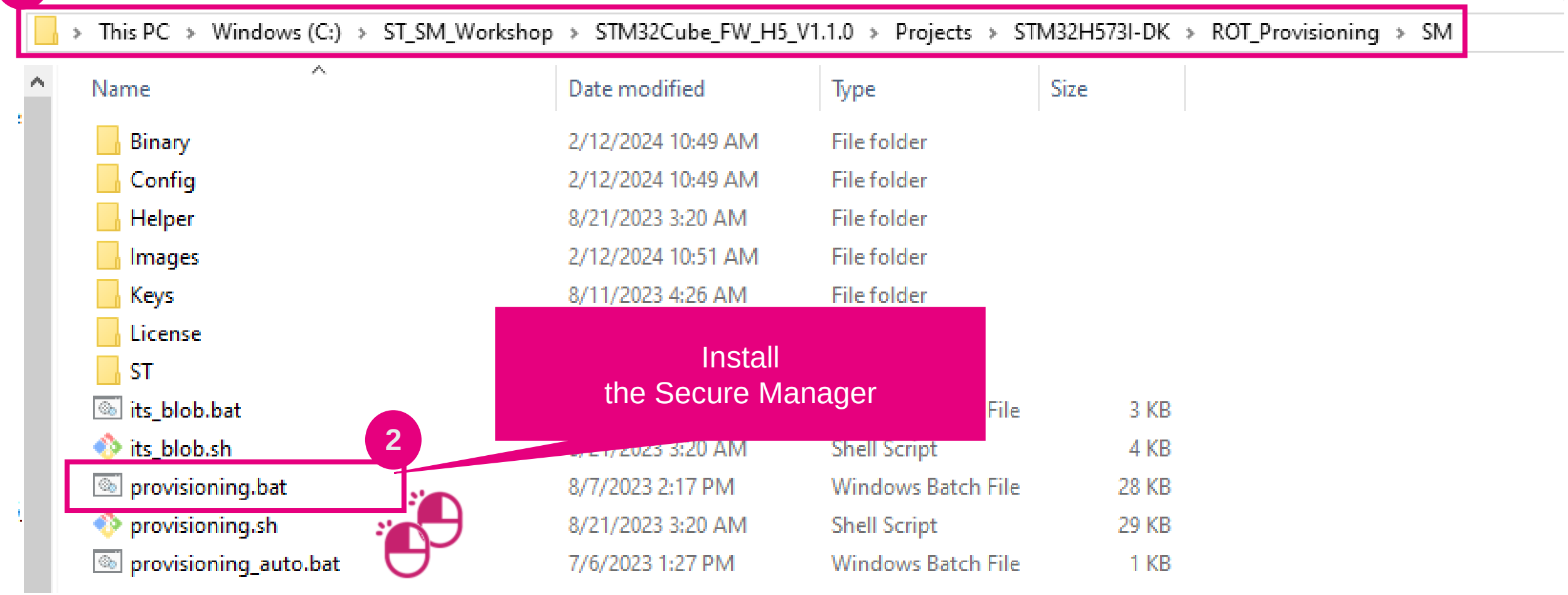


Hands-on: Secure Manager Configuration and Installation

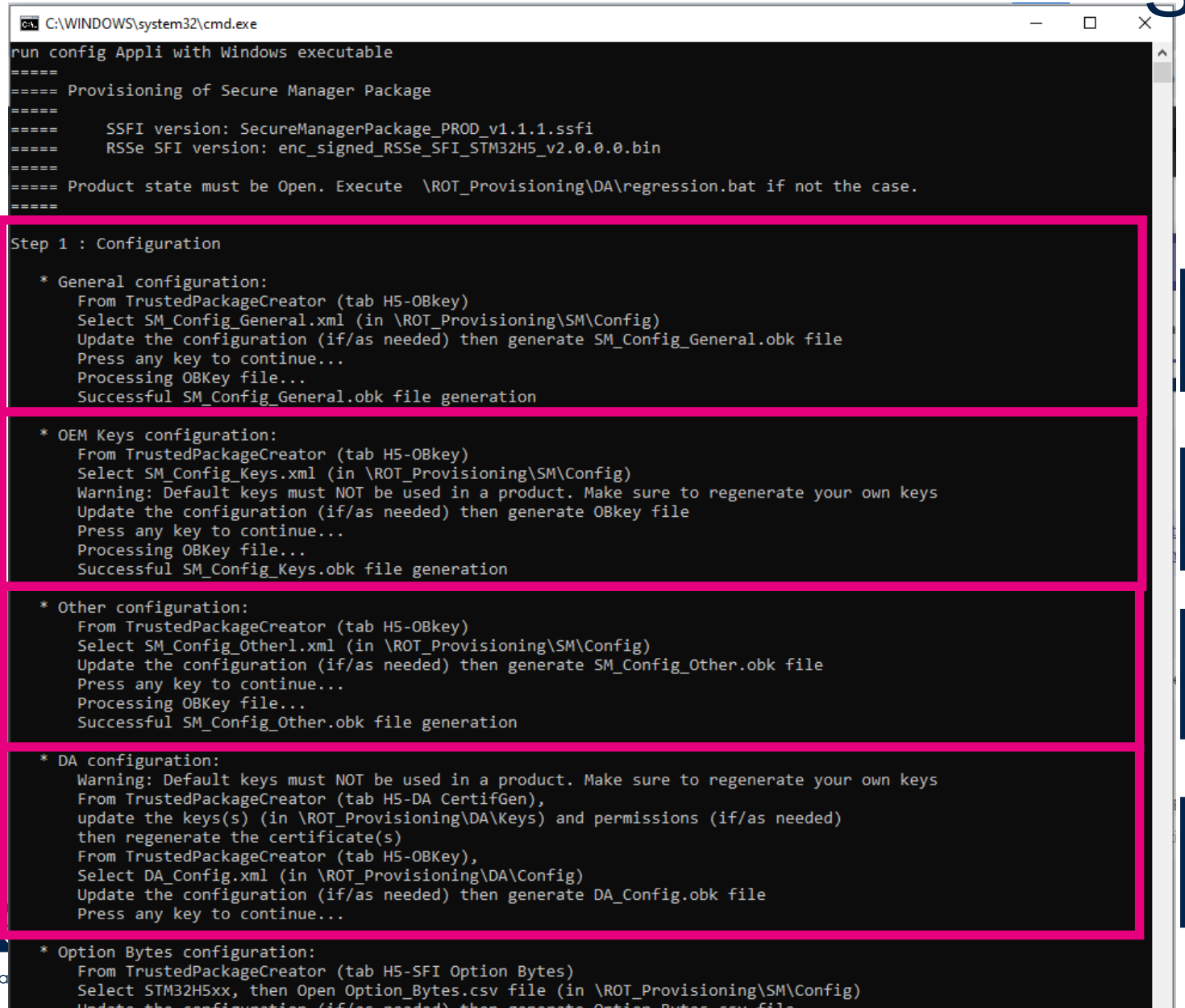
life.augmented

Hands-on: provisioning scripts

1

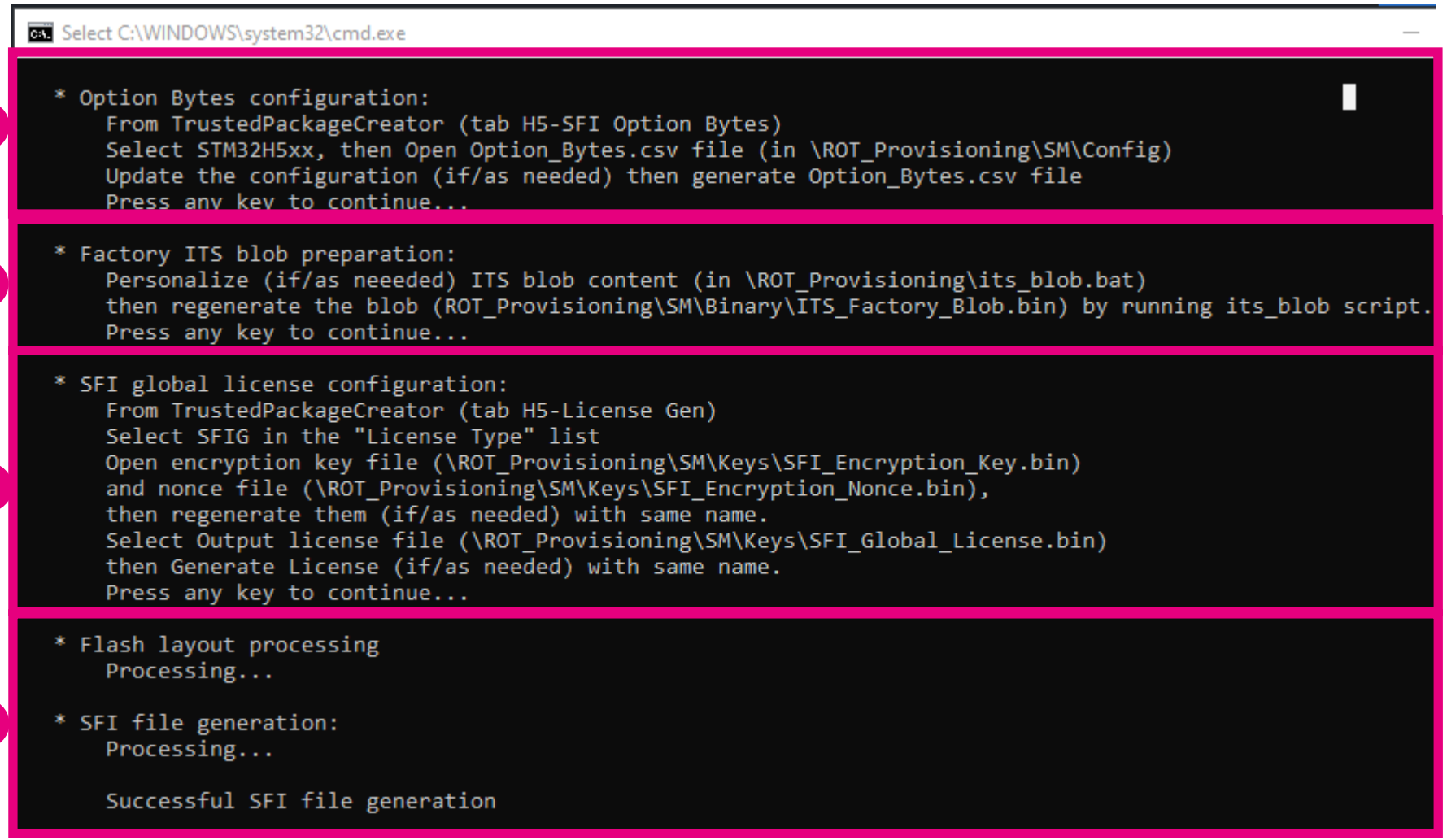


Hands-on: Secure Manager STEP1 - Configuration



1. Information to configure secure manager capabilities
2. Information to configure OEM keys
3. Information to configure secure manager behaviour
4. Information to configure debug authentication keys

Hands-on: Secure Manager STEP1 - Configuration



Option bytes configuration

Internal trusted storage configuration

SFI license setup

Build big SFI binary

life.augmented

Hands-on: Secure Manager STEP2 - Installation

1

```
Step 2 : Installation

   * BOOT0 pin should be disconnected from VDD
     (STM32H573I-DK: set SW1 to position 0)
     Press any key to continue...
```

Ensure switch SW1 (close to ETH connector) is set on FLASH (0)

2

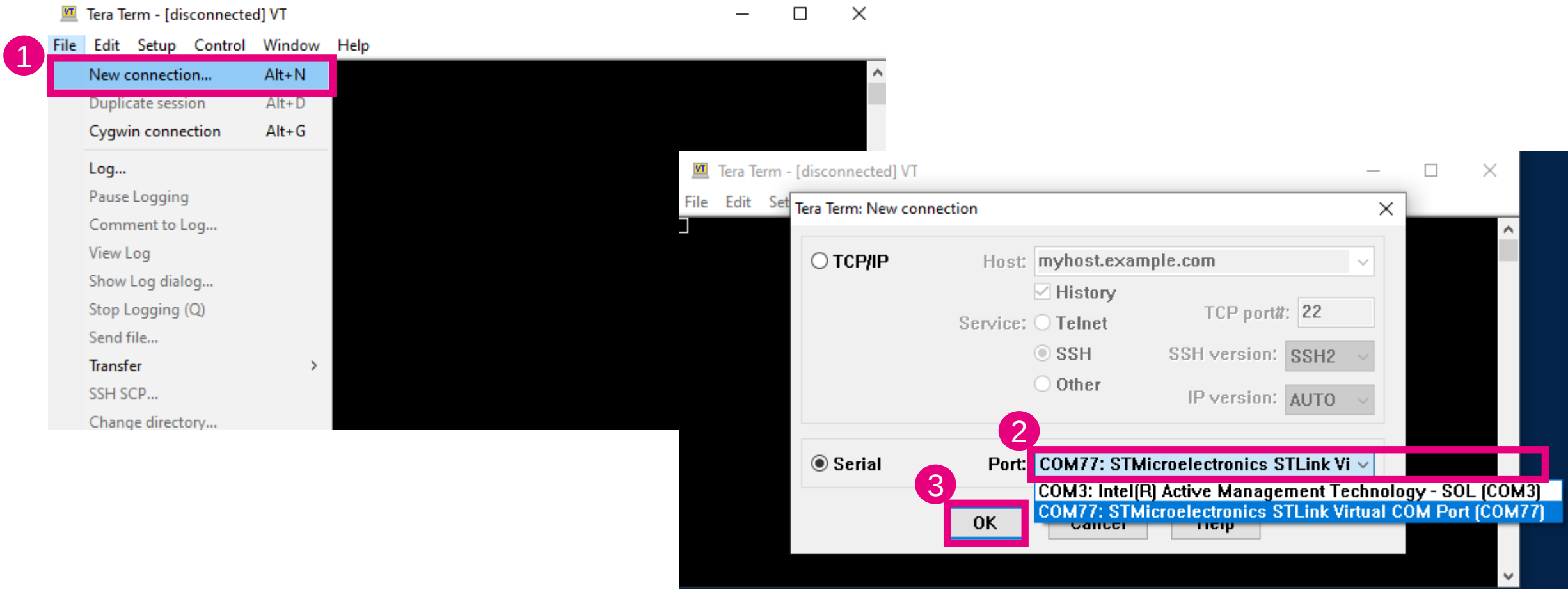
```
   * Secure installation
     Installation starting (might take up to 15 seconds)...
     Installation completion...
     Successful installation

=====
===== The board is correctly configured with ST Secure Manager Package
=====
```

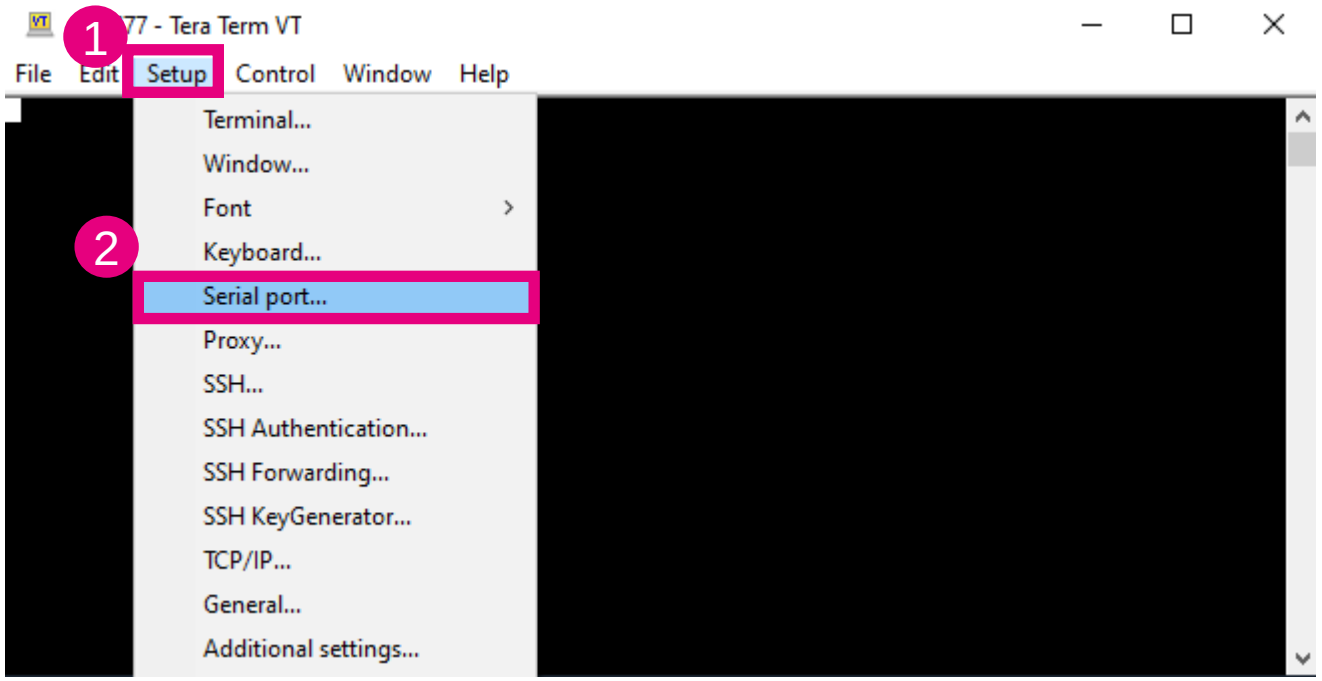
Secure manager installation securely !

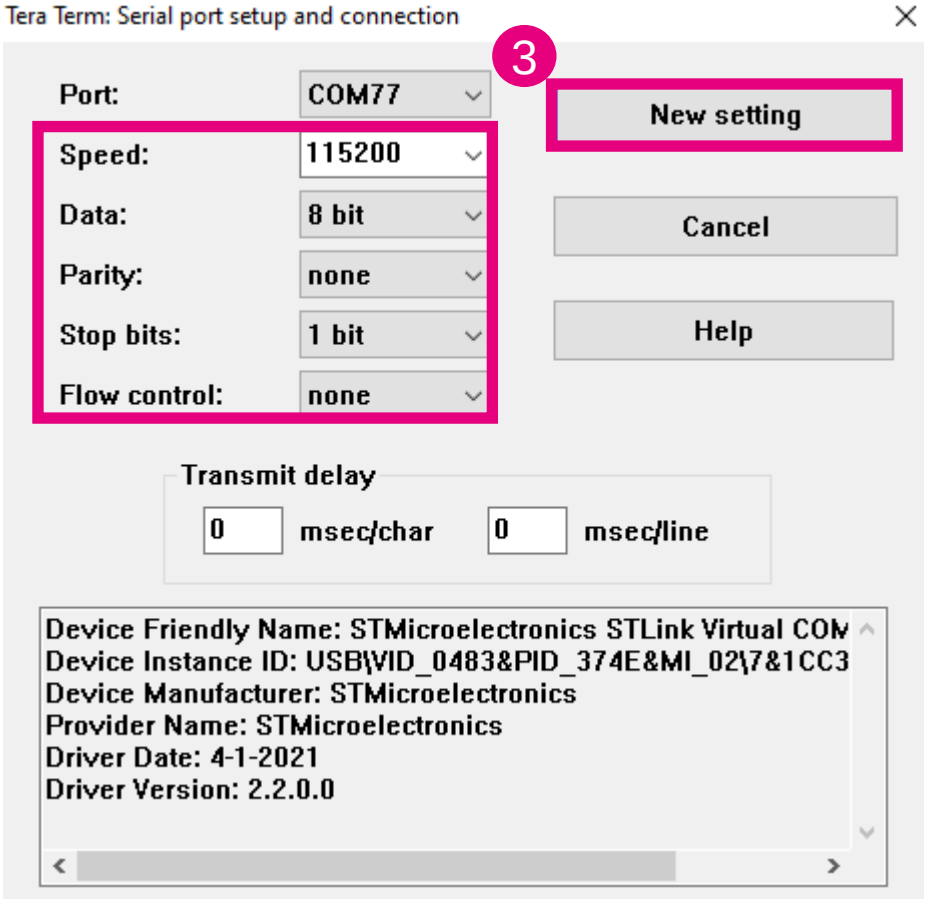
Board LEDs are blinking !

Open UART terminal serial port



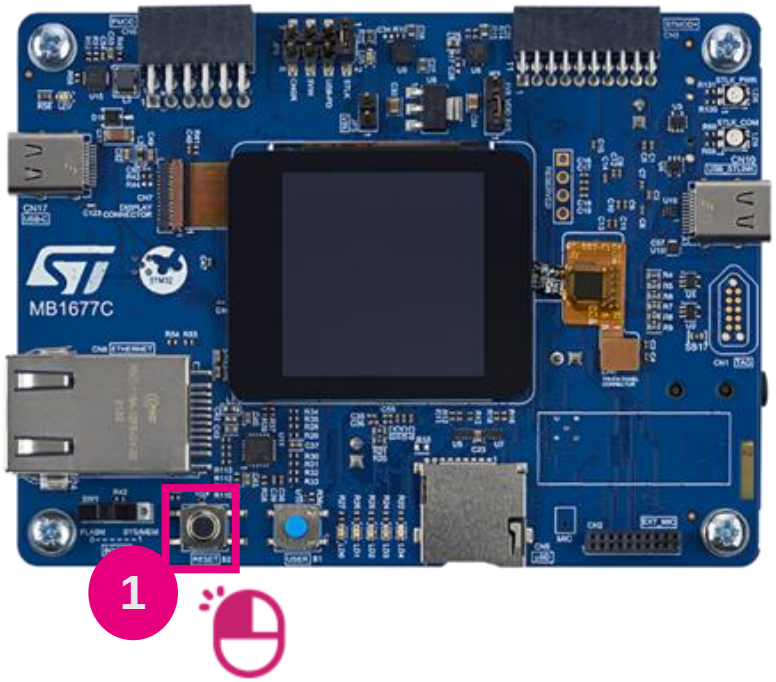
Serial port configuration

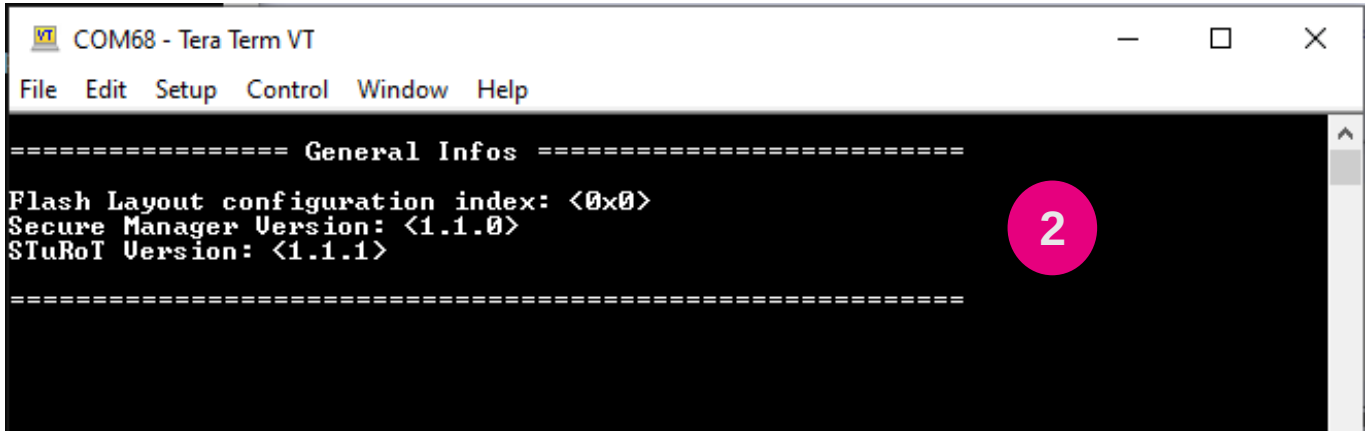




Check terminal connection

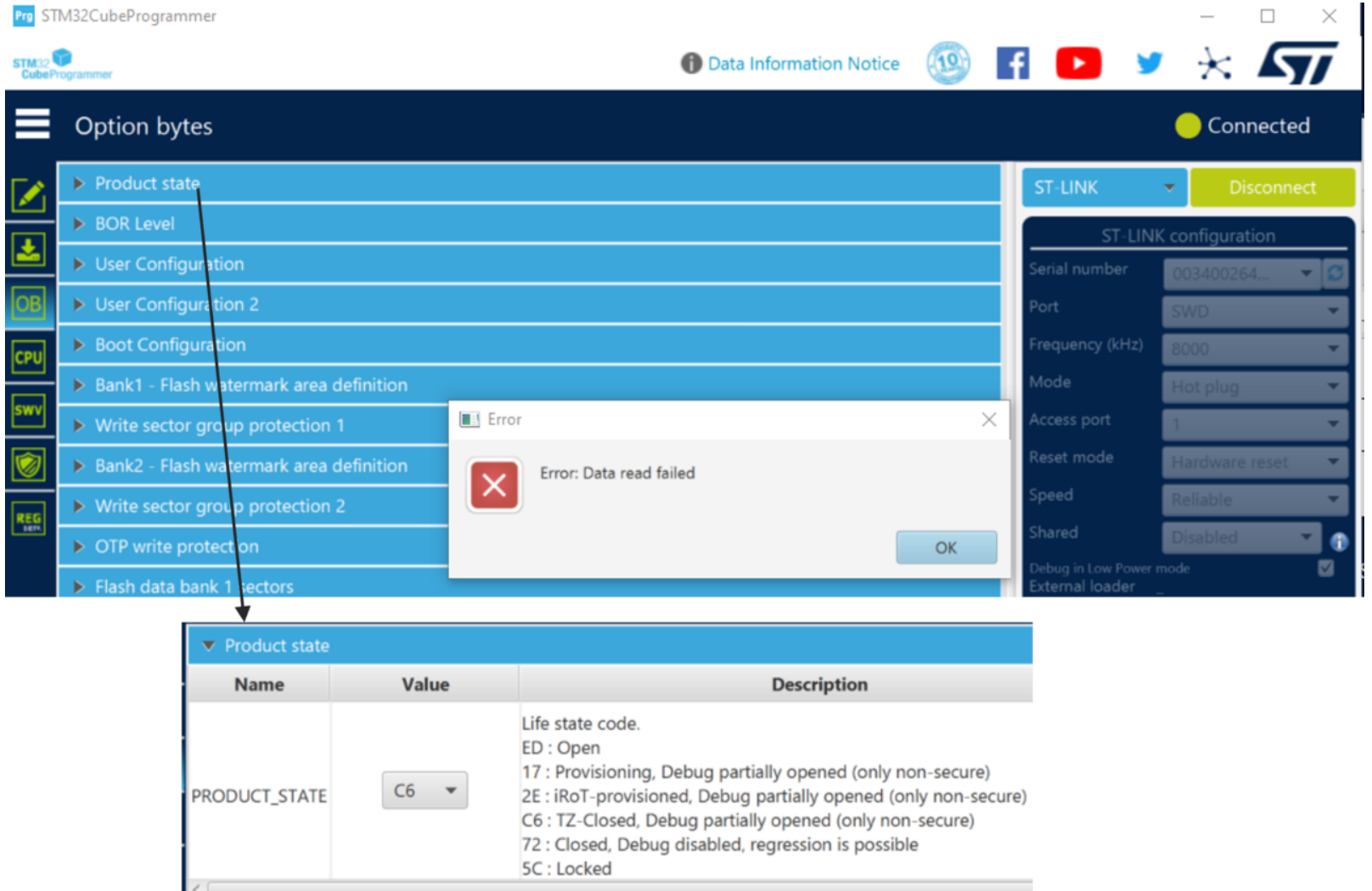
- Press the reset button on the board





Check product state

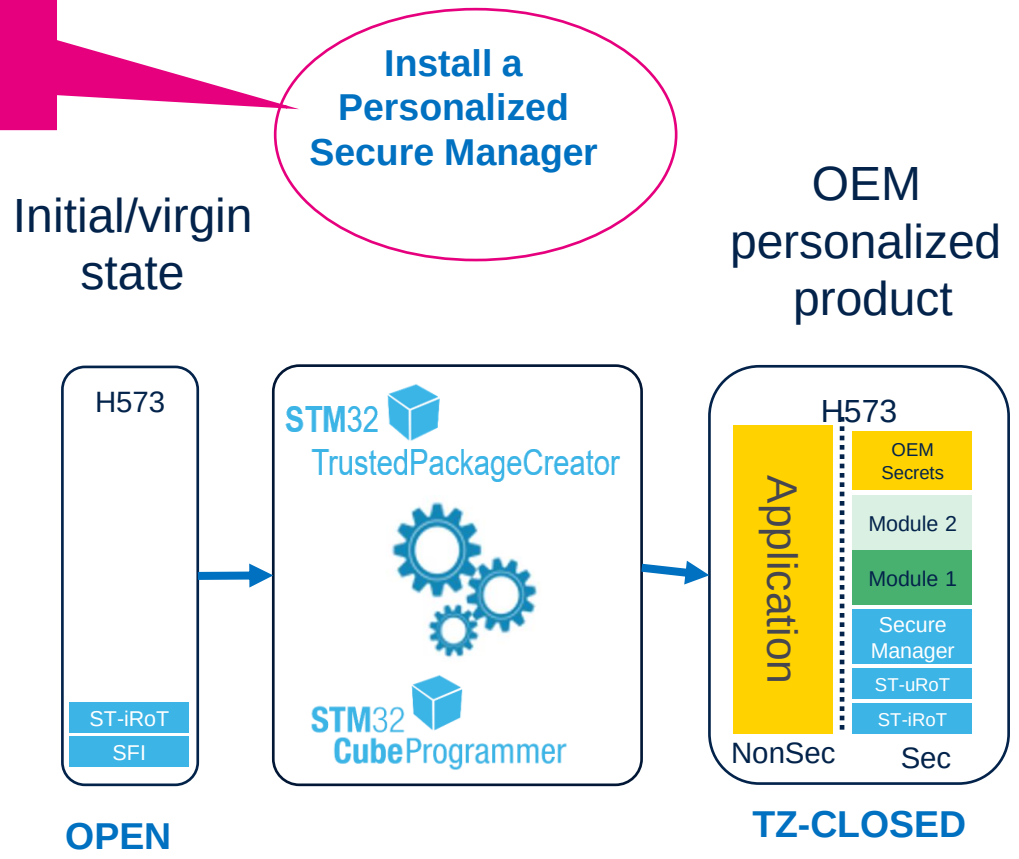
- Connect to the board through STM32CubeProg to check the new TZ-Closed product state (you can check accessibility of S and NS flash). Then Disconnect



Hands-on Completed

Configuration and Installation Flow

COMPLETED



Resources

Resources

Links

- STM32Trust: Web page
- Security with STM32H5: Wiki pages
- Getting Started with STM32H5 security: Wiki pages
- STM32 Embedded Security Learning Journey: Web page

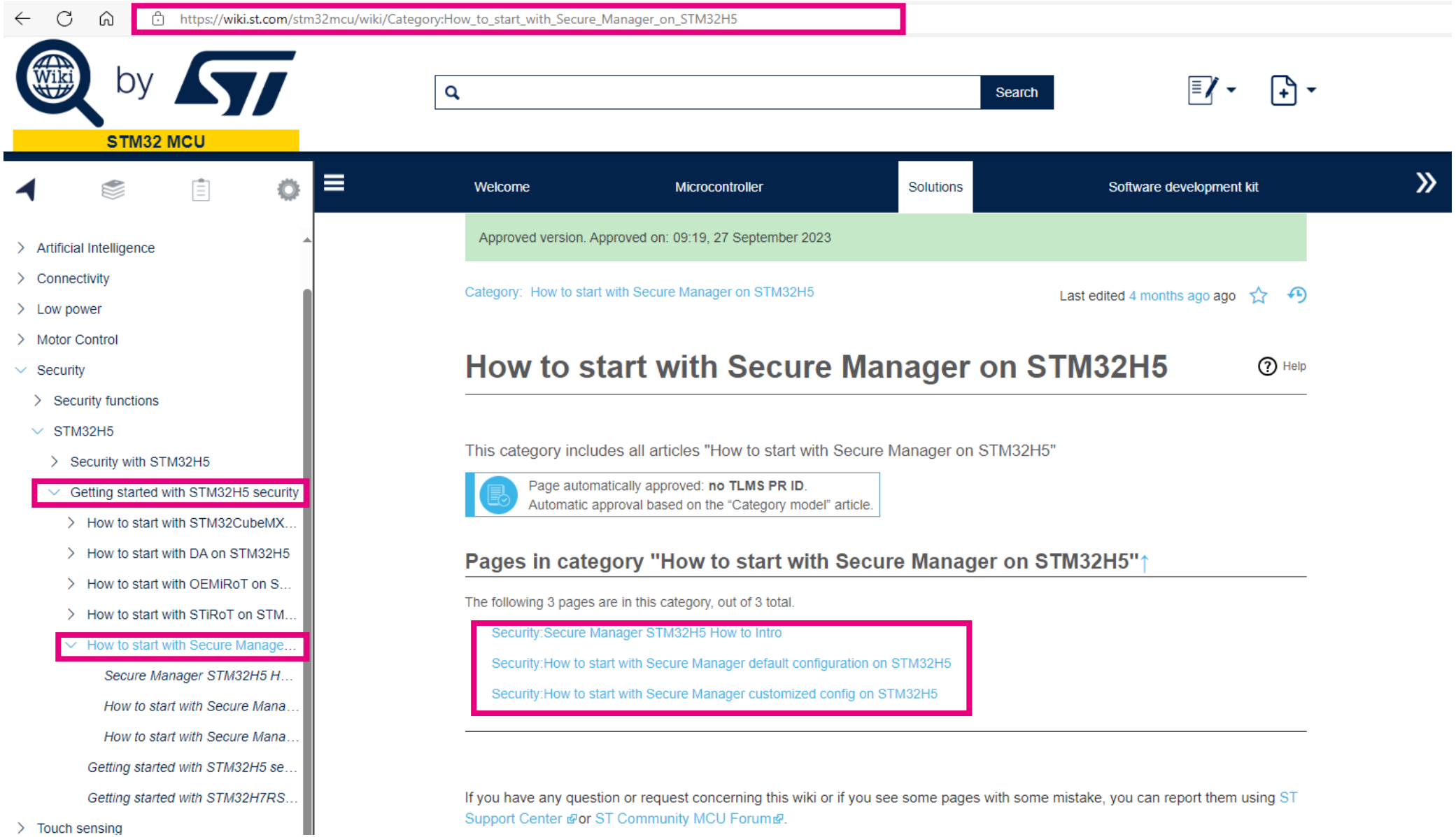
Videos

- STM32H5 Training: Online Training
- STM32 Security MOOC: Online Course
- Secure Manager MOOC: Online Course

Docs

- AN5156 : Introduction to STM32 microcontrollers security
- AN6007 : Getting Started with STiRoT for STM32H5 MCUs
- AN6008 : Getting Started with Debug Authentication for STM32H5 MCUs
- UM3254 : Secure manager for STM32H573xx microcontrollers
- RM0481 : STM32H563/H573 Reference Manual

Wiki: How to start with Secure Manager



life.augmented

Agenda

1 Introduction

2 STM32H5 security features overview

3 Hands-On: Getting started with Secure Manager

4 Hands-On: SMAK Develop and Debug

5 Hands-On: Debug Authentication

6 Conclusion & takeaways

life.augmented

Our technology starts with You

Find out more at www.st.com

life.augmented