



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

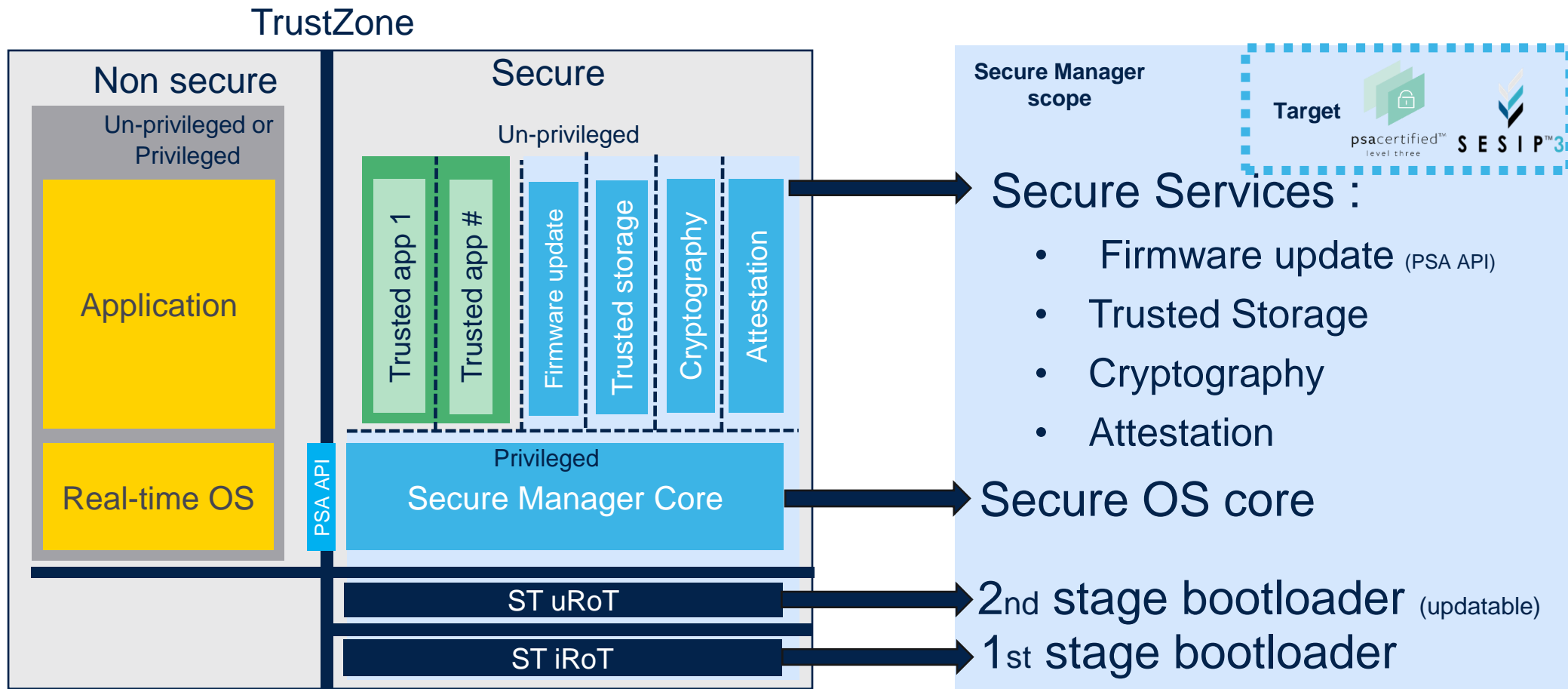
Hands-On: Install and get started
with Secure Manager

III

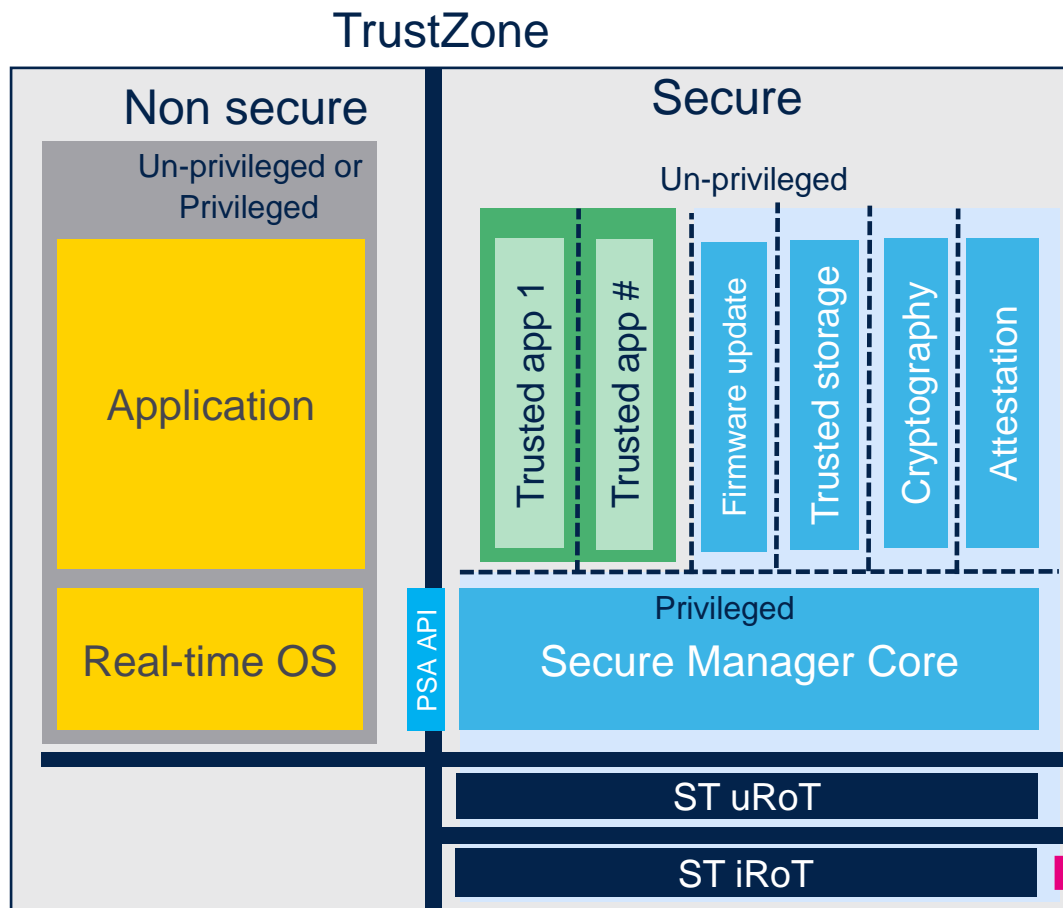
Resources

Secure Manager features overview

Protect IP and **simplify** security customer journey



Protect IP and **simplify** security customer journey



Secure Manager
scope

Target

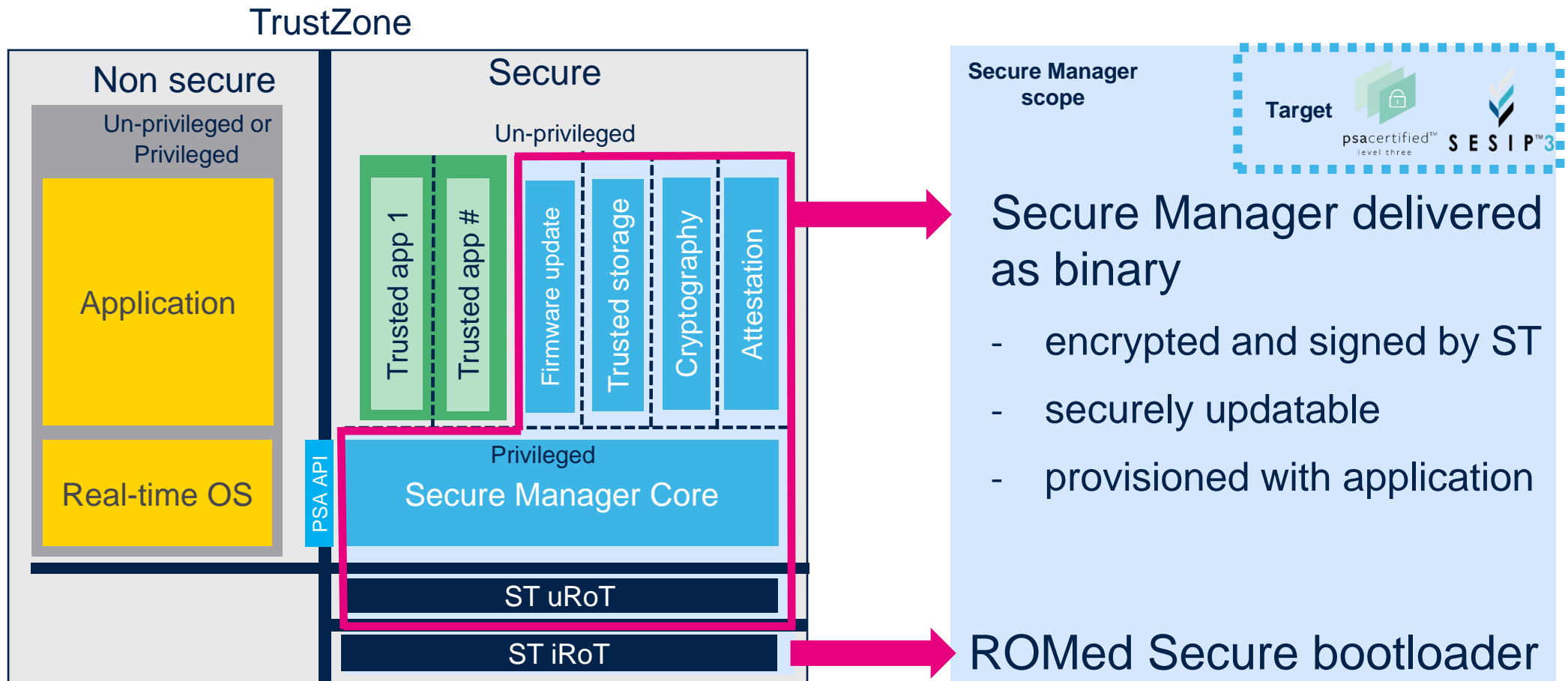


Secure Manager delivered
as binary

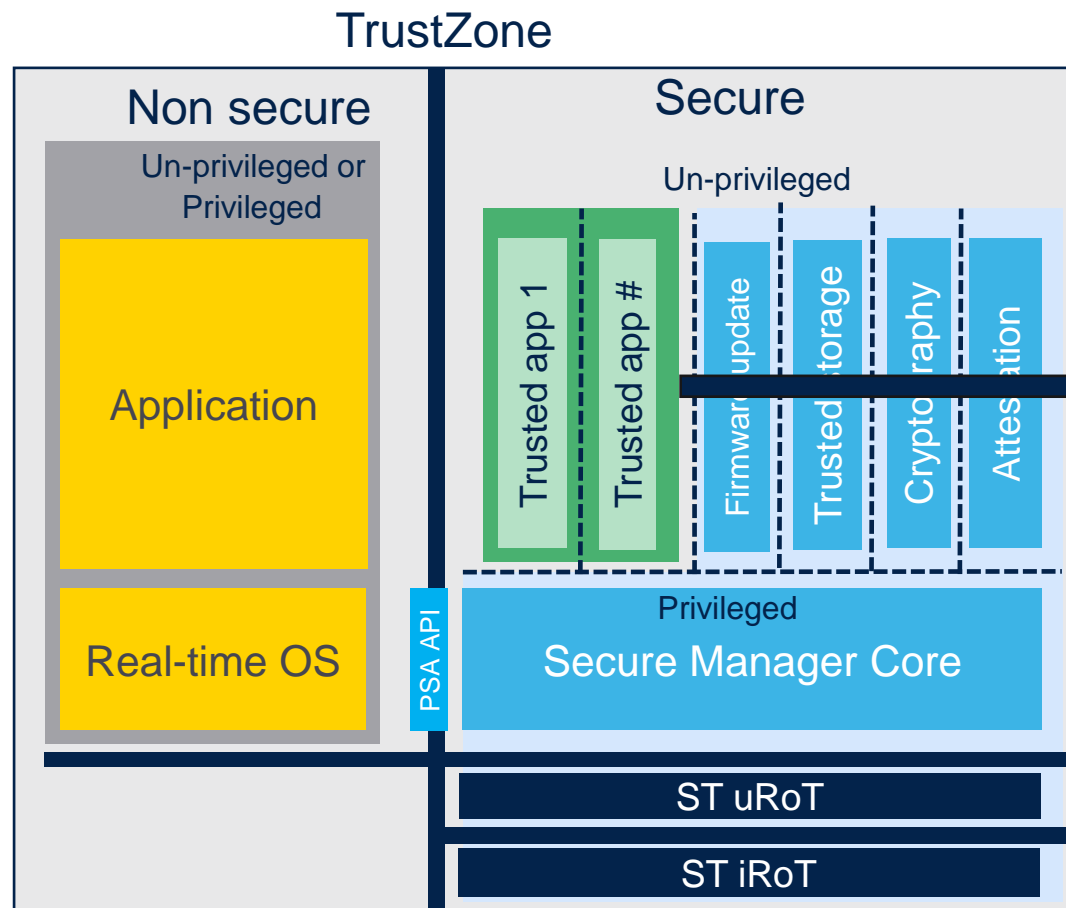
- encrypted and signed by ST
- securely updatable
- provisioned with application

ROMed Secure bootloader

Protect IP and **simplify** security customer journey



Protect IP and **simplify** security customer journey

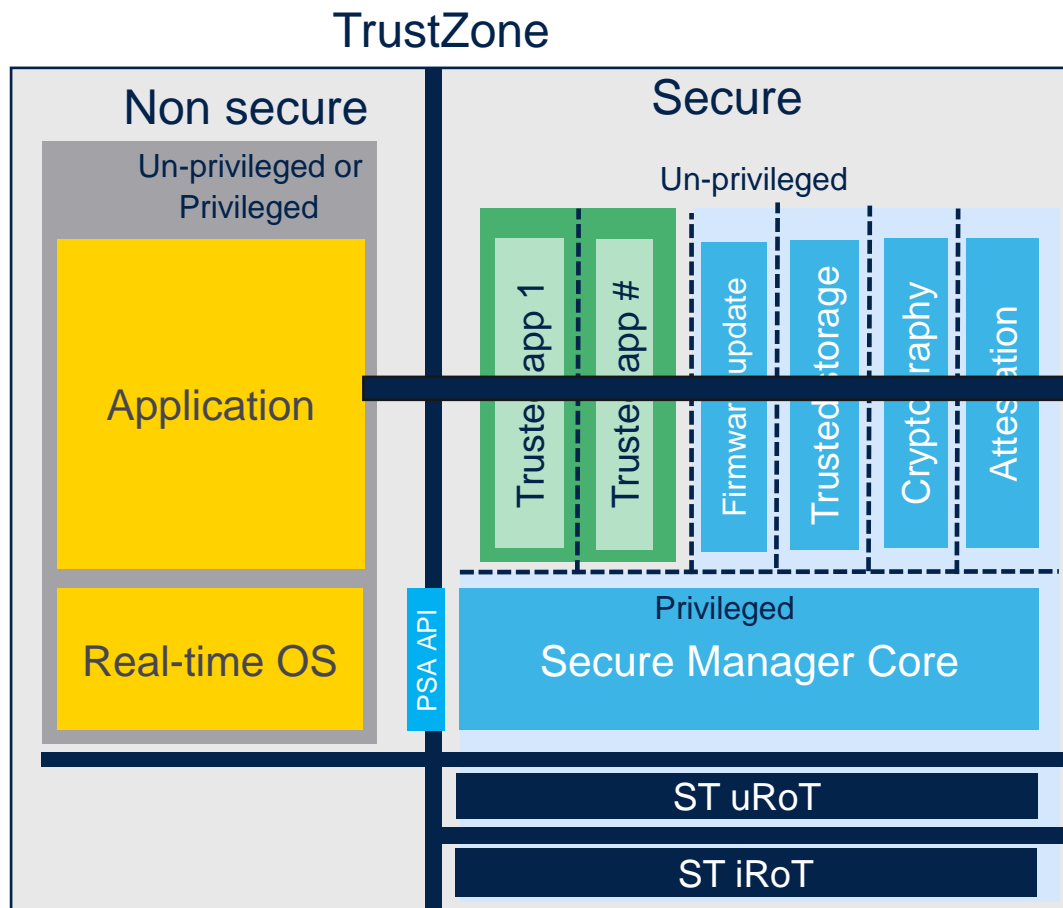


Third Party /
OEM scope

**Secure Modules:
delivered as binary**

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

Protect IP and **simplify** security customer journey

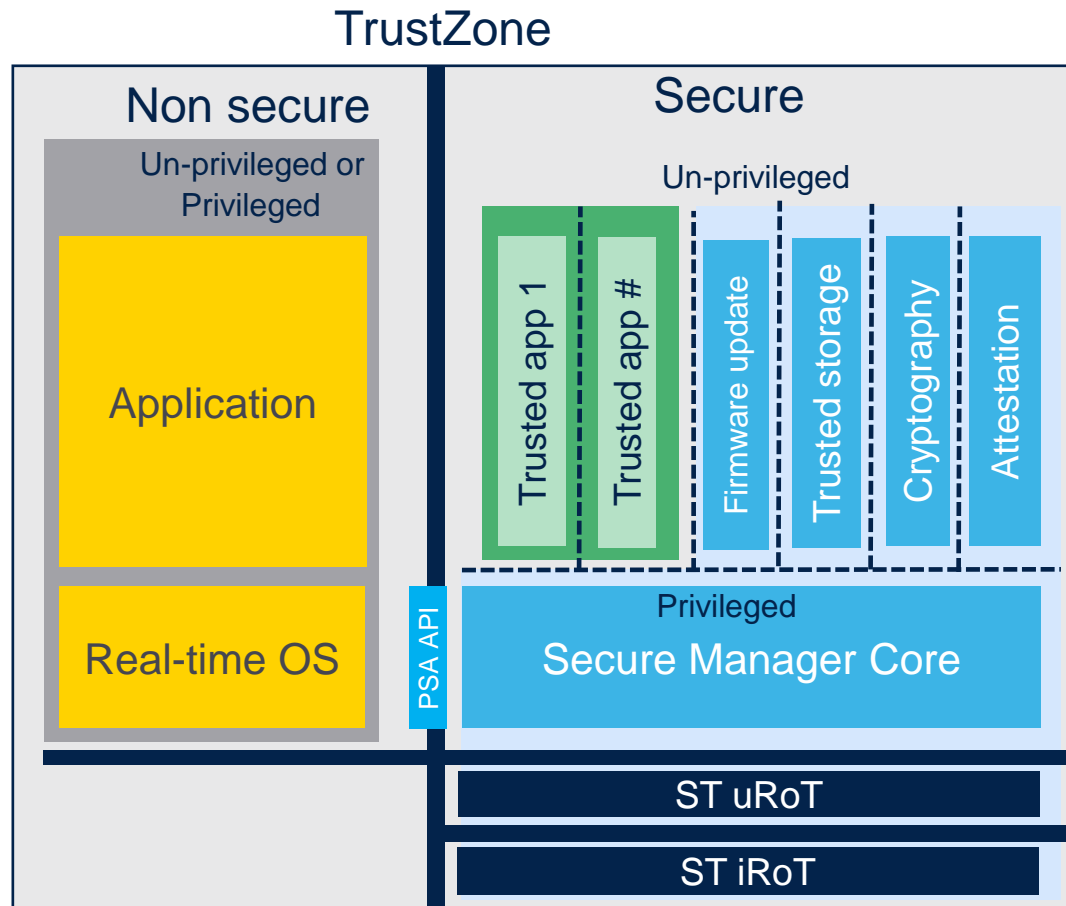


OEM scope

Non-Secure Application

- securely & independently updatable
- optionally encrypted

Protect IP and **simplify** security customer journey



- 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

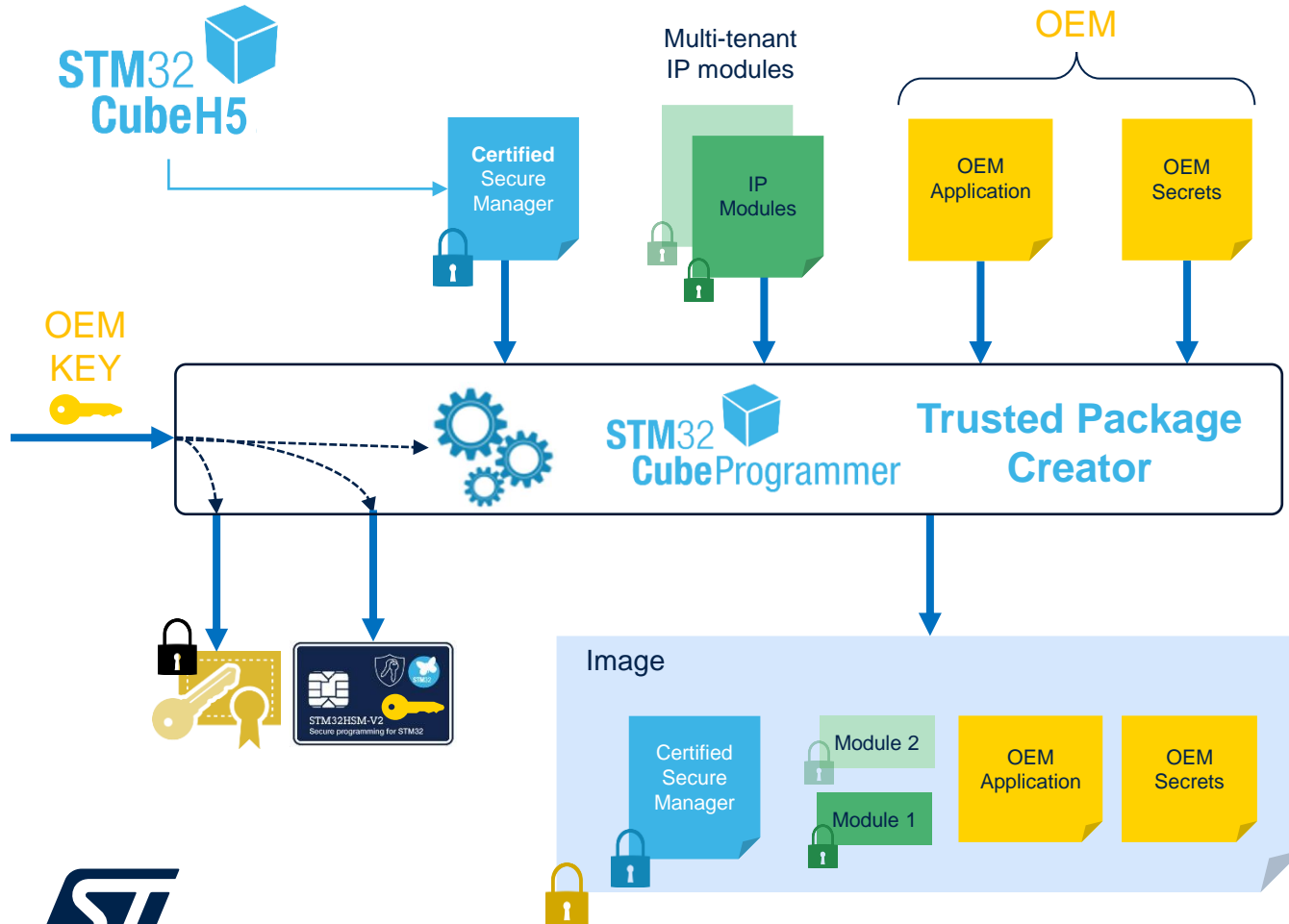


Scope of
Secure Manager

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

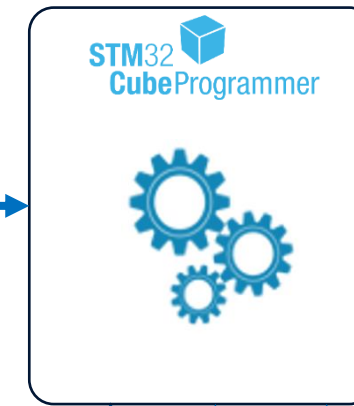
Secure Manager Configuration & Installation flow

Creation Flow

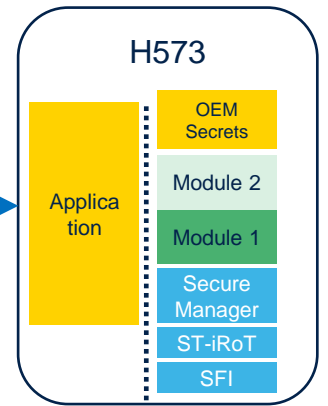


Installation Flow

Initial/virgin state

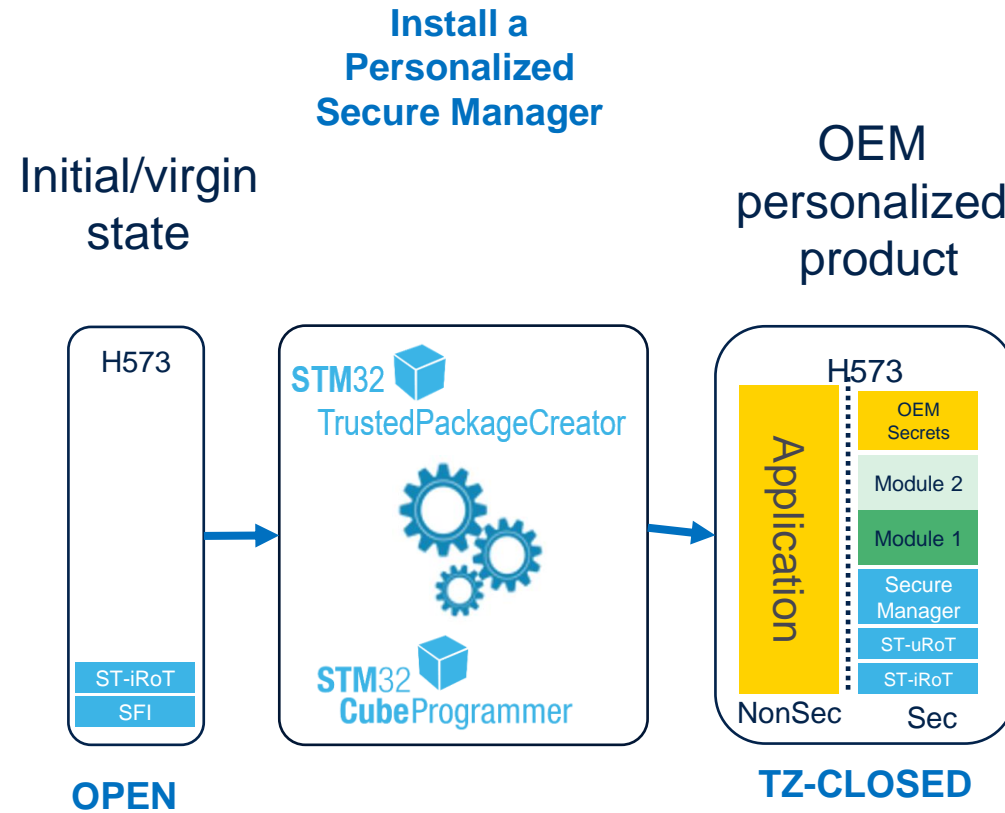


OEM personalized product



Hands-on: Install and get started with Secure Manager

Configuration and Installation Flow



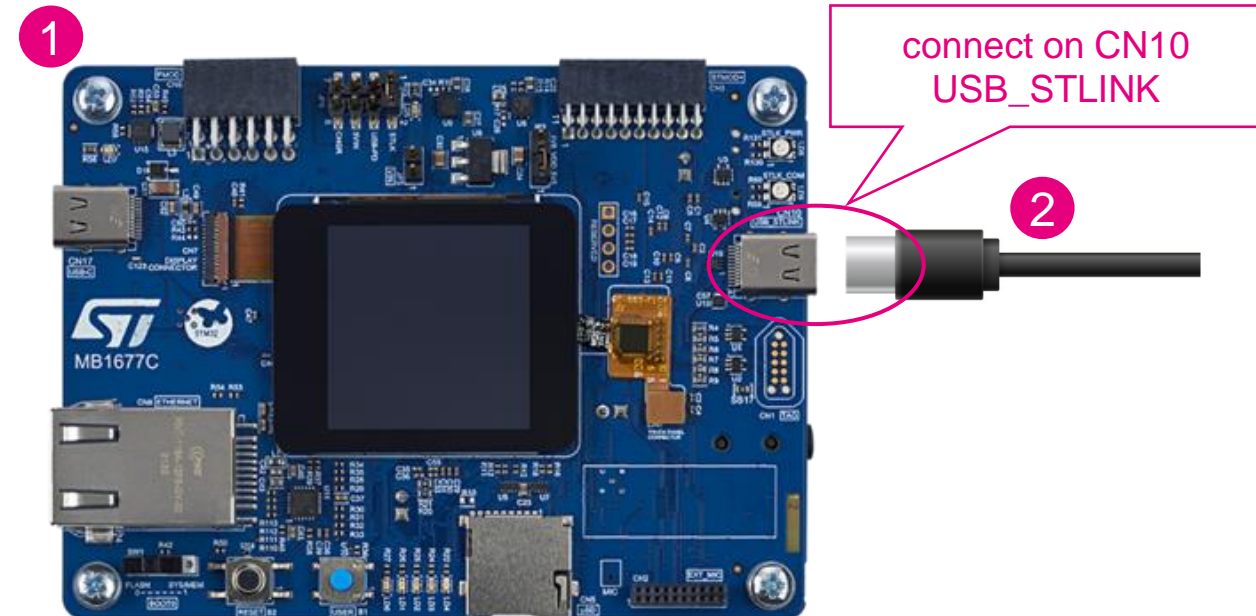
Hands-on: Requirements

- 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](#))

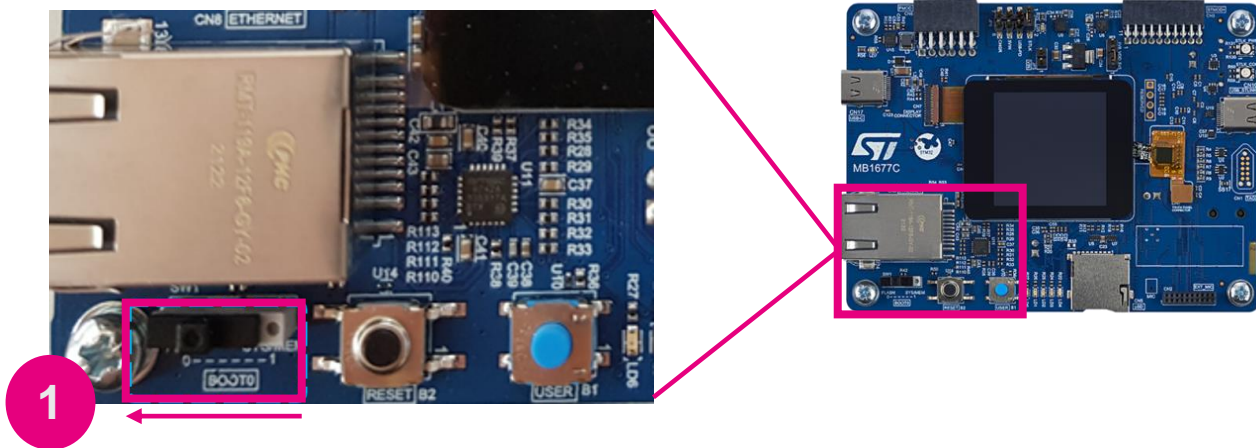
- HW Requirement :

1. STM32H573-DK
2. USB cable (Type C, or Type C-to-Type A)

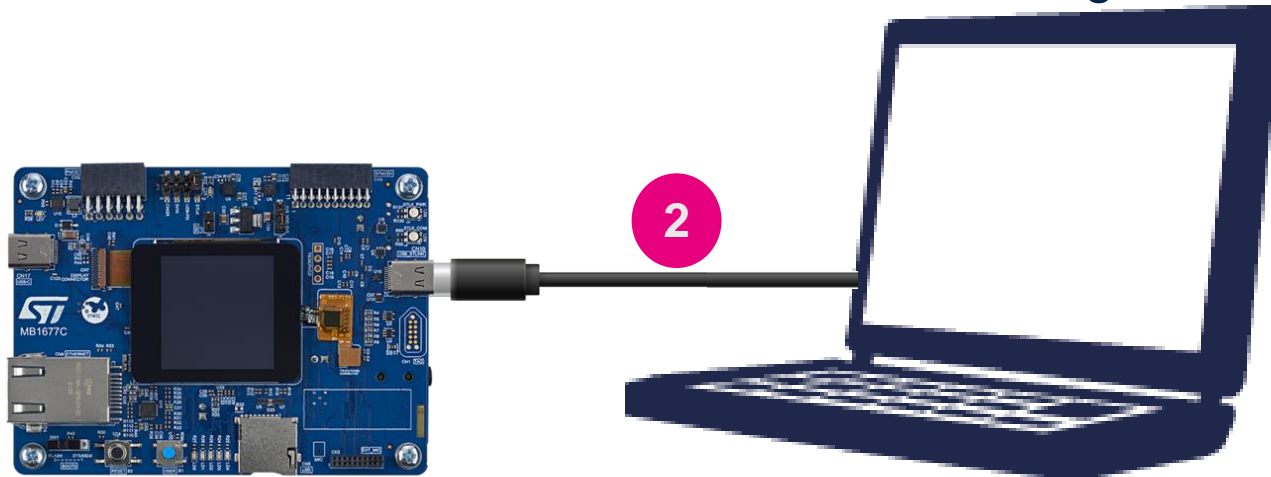


Hands-on: Hw configuration

- 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.

1

2

Name	Date modified	Type	Size
DA	8/21/2023 3:20 AM	File folder	
OEMiROT	8/21/2023 3:20 AM	File folder	
SM	2/12/2024 10:58 AM	File folder	
STiROT	2/9/2024 10:39 AM	File folder	
STiROT OEMuROT	8/21/2023 3:20 AM	File folder	
env.bat	7/6/2023 1:27 PM	Windows Batch File	3 KB
env.sh	8/21/2023 3:20 AM	Shell Script	3 KB
img_config.bat	7/6/2023 1:27 PM	Windows Batch File	1 KB
ima_confia.sh	8/21/2023 3:20 AM	Shell Script	1 KB

```
:: =====  
::  
:: General  
:: =====  
:: Configure tools installation path  
set stm32programmercli="C:\Program Files\STMicroelectronics\STM32Cube\STM32CubeProgrammer\bin\STM32_Programmer_CLI.exe"  
set stm32tpcccli="C:\Program Files\STMicroelectronics\STM32Cube\STM32CubeProgrammer\bin\STM32TrustedPackageCreator_CLI.exe"
```

Hands-on: OB status check 1/3

STM32CubeProgrammer

Option bytes

Not connected

ST-LINK

Connect

ST-LINK configuration

Serial number: 004A00243...

Port: SWD

Frequency (kHz): 8000

Mode: Hot plug

Access port: 1

Reset mode: Hardware reset

Speed: Reliable

Shared: Disabled

Debug in Low Power mode: ☒

External loader: ☐

Target voltage: 3.27 V

Firmware version: V3J11M3

Firmware upgrade

Target information

Board: -

Device: -

Type: -

Device ID: -

Revision ID: -

Flash size: -

CPU: -

Bootloader Version: -

Some of the option bytes might be hidden or clipped, Use the mouse wheel or the touch pad to scroll down

Apply Read

Hands-on: OB status check 2/3

STM32CubeProgrammer

STM32CubeProgrammer

Data Information Notice

Connected

Option bytes

Product state

Name	Value	Description
PRODUCT_STATE	ED	Life state code. ED : Open 17 : Provisioning, Debug partially opened (only non-secure) 2E : iRoT-provisioned, Debug partially opened (only non-secure) C6 : TZ-Closed, Debug partially opened (only non-secure) 72 : Closed, Debug disabled, regression is possible 5C : Locked

BOR Level

User Configuration

User Configuration 2

Boot Configuration

Name	Value	Description
NSBOOTADD	Val... 0x80000 Addr... 0x08000000	Non secure unique boot entry address
NSBOOT_LOCK	C3	A field locking the values of SWAP_BANK, and NSBOOTADD settings C3 : The SWAP_BANK and NSBOOTADD can still be modified following their indi B4 : The NSBOOTADD is frozen. SWAP_BANK can only be modified with TZEN se
SECBOOT_LOCK	0	A field locking the values of UBE, SWAP_BANK, and SECBOOTADD settings. C3 : The BOOT_UBE, SWAP_BANK and SECBOOTADD can still be modified follow B4 : The BOOT_UBE and SECBOOTADD are frozen. SWAP_BANK can only be mod

Some of the option bytes might be hidden or clipped, Use the mouse wheel or the touch pad to scroll down

Apply Read

ST-LINK

Disconnect

ST-LINK configuration

Serial number 004A00243...

Port SWD

Frequency (kHz) 8000

Mode Hot plug

Access port 1

Reset mode Hardware reset

Speed Reliable

Shared Disabled

Debug in Low Power mode

External loader

Target voltage 3.27 V

Firmware version V3J11M3

Firmware upgrade

Target information

Board STM32H573I-DK

Device STM32H5xx

Type MCU

Device ID 0x484

Revision ID --

Flash size 2 MB

CPU Cortex-M33

Bootloader Version 0xE4

Hands-on: OB status check 3/3

STM32CubeProgrammer

STM32CubeProgrammer

Data Information Notice

Connected

Option bytes

Product state

Name	Value	Description
PRODUCT_STATE	ED	Life state code. ED : Open 17 : Provisioning, Debug partially opened (only non-secure) 2E : iRoT-provisioned, Debug partially opened (only non-secure) C6 : TZ-Closed, Debug partially opened (only non-secure) 72 : Closed, Debug disabled, regression is possible 5C : Locked

BOR Level

User Configuration

User Configuration 2

Boot Configuration

Name	Value	Description
NSBOOTADD	Val... 0x80000 Addr... 0x08000000	Non secure unique boot entry address
NSBOOT_LOCK	C3	A field locking the values of SWAP_BANK, and NSBOOTADD settings C3 : The SWAP_BANK and NSBOOTADD can still be modified following their indi B4 : The NSBOOTADD is frozen. SWAP_BANK can only be modified with TZEN se
SECBOOT_LOCK	0	A field locking the values of UBE, SWAP_BANK, and SECBOOTADD settings. C3 : The BOOT_UBE, SWAP_BANK and SECBOOTADD can still be modified follow B4 : The BOOT_UBE and SECBOOTADD are frozen. SWAP_BANK can only be mod

Some of the option bytes might be hidden or clipped, Use the mouse wheel or the touch pad to scroll down

Apply Read

ST-LINK

Disconnect

ST-LINK configuration

Serial number 004A00243...

Port SWD

Frequency (kHz) 8000

Mode Hot plug

Access port 1

Reset mode Hardware reset

Speed Reliable

Shared Disabled

Debug in Low Power mode

External loader

Target voltage 3.27 V

Firmware version V3J11M3

Firmware upgrade

Target information

Board STM32H573I-DK

Device STM32H5xx

Type MCU

Device ID 0x484

Revision ID --

Flash size 2 MB

CPU Cortex-M33

Bootloader Version 0xE4

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.

1

Name	Date modified	Type	Size
Binary	8/11/2023 4:26 AM	File folder	
Certificates	8/11/2023 4:26 AM	File folder	
Config	8/11/2023 4:26 AM	File folder	
Keys	8/11/2023 4:26 AM	File folder	
dbg_auth.bat	7/6/2023 1:27 PM	Windows Batch File	1 KB
dbg_auth.sh	8/21/2023 3:20 AM	Shell Script	1 KB
discovery.bat	7/6/2023 1:27 PM	Windows Batch File	1 KB
discovery.sh	8/21/2023 3:20 AM	Shell Script	1 KB
ob_programming.bat	7/6/2023 1:27 PM	Windows Batch File	3 KB
ob_programming.sh	8/21/2023 3:20 AM	Shell Script	3 KB
obk_provisioning.bat	7/6/2023 1:27 PM	Windows Batch File	3 KB
obk_provisioning.sh	8/21/2023 3:20 AM	Shell Script	3 KB
provisioning.bat	7/6/2023 1:27 PM	Windows Batch File	3 KB
provisioning.sh	8/21/2023 3:20 AM	Shell Script	3 KB
regression.bat	7/6/2023 1:27 PM	Windows Batch File	2 KB
regression.sh	8/21/2023 3:20 AM	Shell Script	2 KB

2

Use it only if device is NOT in OPEN state
or
if you run into issues/blocks moving forward

Hands-on: Secure Manager Configuration and Installation

Hands-on: provisioning scripts

1

File Explorer path: This PC > Windows (C:) > ST_SM_Workshop > STM32Cube_FW_H5_V1.1.0 > Projects > STM32H573I-DK > ROT_Provisioning > SM

Name	Date modified	Type	Size
Binary	2/12/2024 10:49 AM	File folder	
Config	2/12/2024 10:49 AM	File folder	
Helper	8/21/2023 3:20 AM	File folder	
Images	2/12/2024 10:51 AM	File folder	
Keys	8/11/2023 4:26 AM	File folder	
License			
ST			
its_blob.bat		File	3 KB
its_blob.sh	8/21/2023 3:20 AM	Shell Script	4 KB
provisioning.bat	8/7/2023 2:17 PM	Windows Batch File	28 KB
provisioning.sh	8/21/2023 3:20 AM	Shell Script	29 KB
provisioning_auto.bat	7/6/2023 1:27 PM	Windows Batch File	1 KB

Install the Secure Manager

2

Hands-on: Secure Manager

STEP1 - Configuration

```
C:\WINDOWS\system32\cmd.exe
run config Appli with Windows executable
=====
===== Provisioning of Secure Manager Package
=====
SSFI version: SecureManagerPackage_PROD_v1.1.1.ssfi
RSSe SFI version: enc_signed_RSse_SFI_STM32H5_v2.0.0.0.bin
=====
Product state must be Open. Execute \ROT_Provisioning\DA\regression.bat if not the case.
=====

Step 1 : Configuration

* General configuration:
  From TrustedPackageCreator (tab H5-OBkey)
  Select SM_Config_General.xml (in \ROT_Provisioning\SM\Config)
  Update the configuration (if/as needed) then generate SM_Config_General.obk file
  Press any key to continue...
  Processing OBKey file...
  Successful SM_Config_General.obk file generation

* OEM Keys configuration:
  From TrustedPackageCreator (tab H5-OBkey)
  Select SM_Config_Keys.xml (in \ROT_Provisioning\SM\Config)
  Warning: Default keys must NOT be used in a product. Make sure to regenerate your own keys
  Update the configuration (if/as needed) then generate OBkey file
  Press any key to continue...
  Processing OBKey file...
  Successful SM_Config_Keys.obk file generation

* Other configuration:
  From TrustedPackageCreator (tab H5-OBkey)
  Select SM_Config_Other1.xml (in \ROT_Provisioning\SM\Config)
  Update the configuration (if/as needed) then generate SM_Config_Other.obk file
  Press any key to continue...
  Processing OBKey file...
  Successful SM_Config_Other.obk file generation

* DA configuration:
  Warning: Default keys must NOT be used in a product. Make sure to regenerate your own keys
  From TrustedPackageCreator (tab H5-DA CertifGen),
  update the keys(s) (in \ROT_Provisioning\DA\Keys) and permissions (if/as needed)
  then regenerate the certificate(s)
  From TrustedPackageCreator (tab H5-OBkey),
  Select DA_Config.xml (in \ROT_Provisioning\DA\Config)
  Update the configuration (if/as needed) then generate DA_Config.obk file
  Press any key to continue...

* Option Bytes configuration:
  From TrustedPackageCreator (tab H5-SFI Option Bytes)
  Select STM32H5xx, then Open Option_Bytes.csv file (in \ROT_Provisioning\SM\Config)
  Update the configuration (if/as needed) then generate Option_Bytes.csv file
```

Information to configure secure manager capabilities

Information to configure OEM keys

Information to configure secure manager behaviour

Information to configure debug authentication keys

Hands-on: Secure Manager

STEP1 - Configuration

```
C:\ Select C:\WINDOWS\system32\cmd.exe

1 * Option Bytes configuration:
  From TrustedPackageCreator (tab H5-SFI Option Bytes)
  Select STM32H5xx, then Open Option_Bytes.csv file (in \ROT_Provisioning\SM\Config)
  Update the configuration (if/as needed) then generate Option_Bytes.csv file
  Press any key to continue...

2 * Factory ITS blob preparation:
  Personalize (if/as needed) ITS blob content (in \ROT_Provisioning\its_blob.bat)
  then regenerate the blob (ROT_Provisioning\SM\Binary\ITS_Factory_Blob.bin) by running its_blob script.
  Press any key to continue...

3 * SFI global license configuration:
  From TrustedPackageCreator (tab H5-License Gen)
  Select SFIG in the "License Type" list
  Open encryption key file (\ROT_Provisioning\SM\Keys\SFI_Encryption_Key.bin)
  and nonce file (\ROT_Provisioning\SM\Keys\SFI_Encryption_Nonce.bin),
  then regenerate them (if/as needed) with same name.
  Select Output license file (\ROT_Provisioning\SM\Keys\SFI_Global_License.bin)
  then Generate License (if/as needed) with same name.
  Press any key to continue...

4 * Flash layout processing
  Processing...

  * SFI file generation:
  Processing...

  Successful SFI file generation
```

Option bytes
configuration

Internal trusted storage
configuration

SFI license setup

Build big SFI binary

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

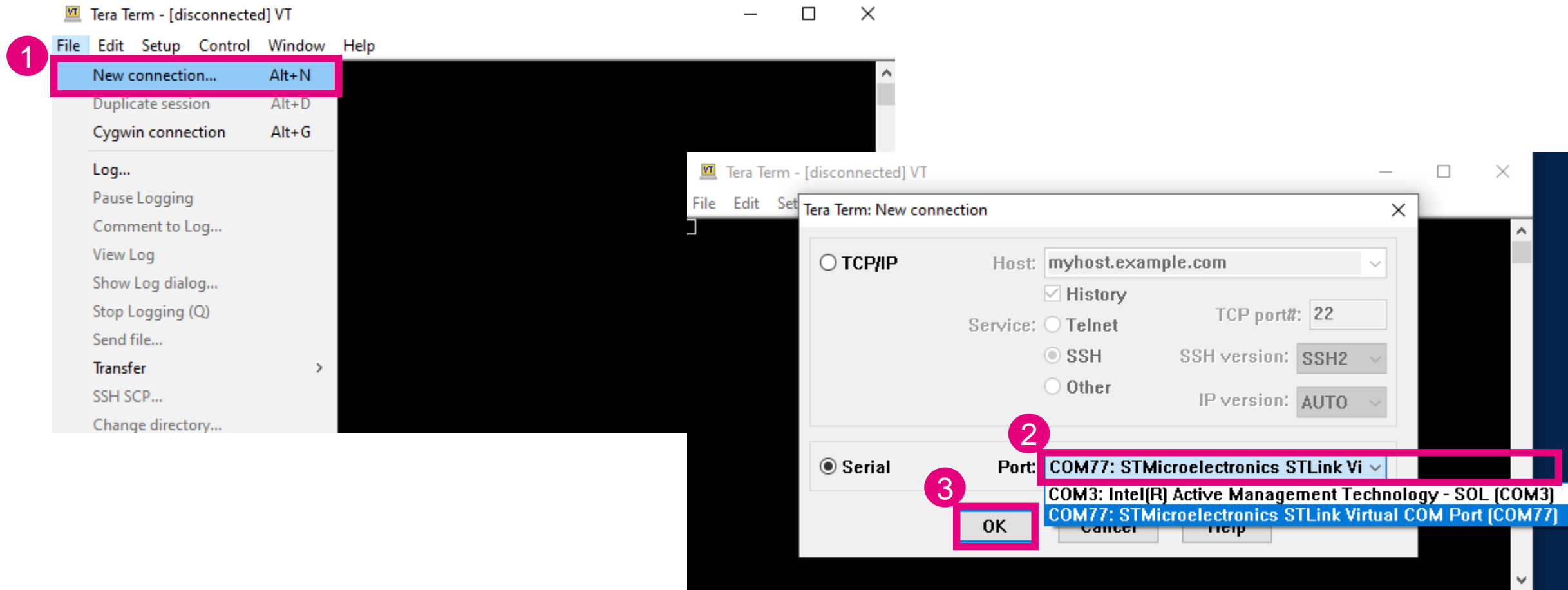
```
* Secure installation
  Installation starting (might take up to 15 seconds)...
  Installation completion...
  Successful installation
```

Secure manager installation
securely !

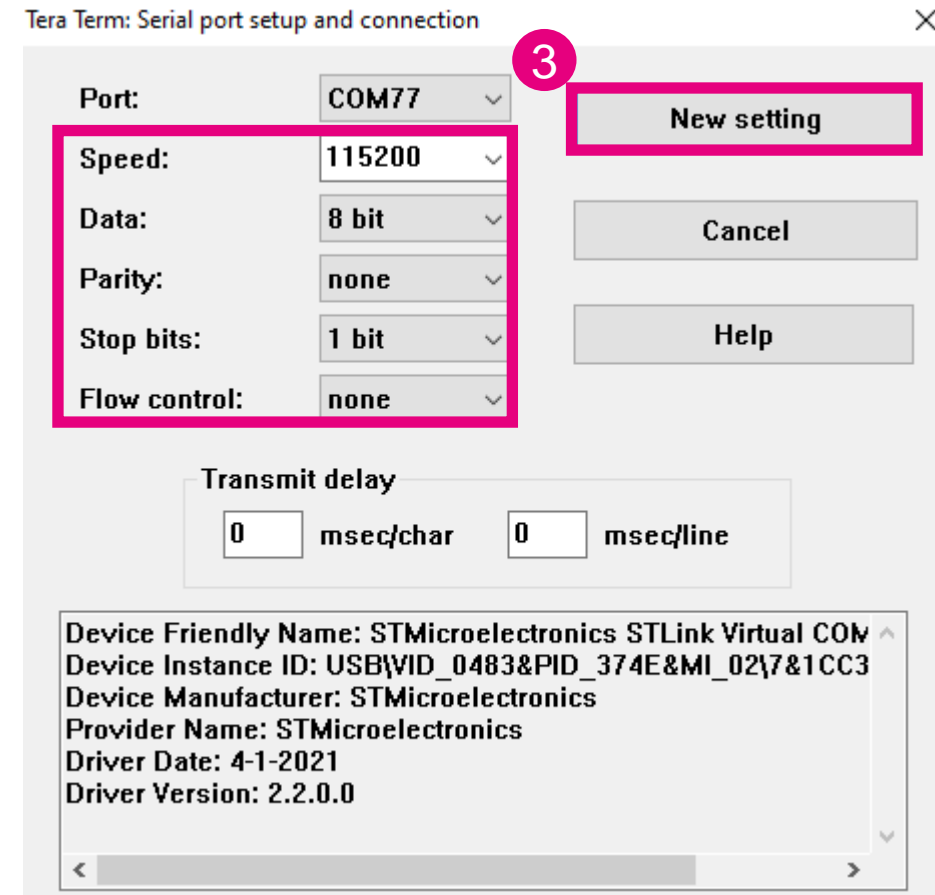
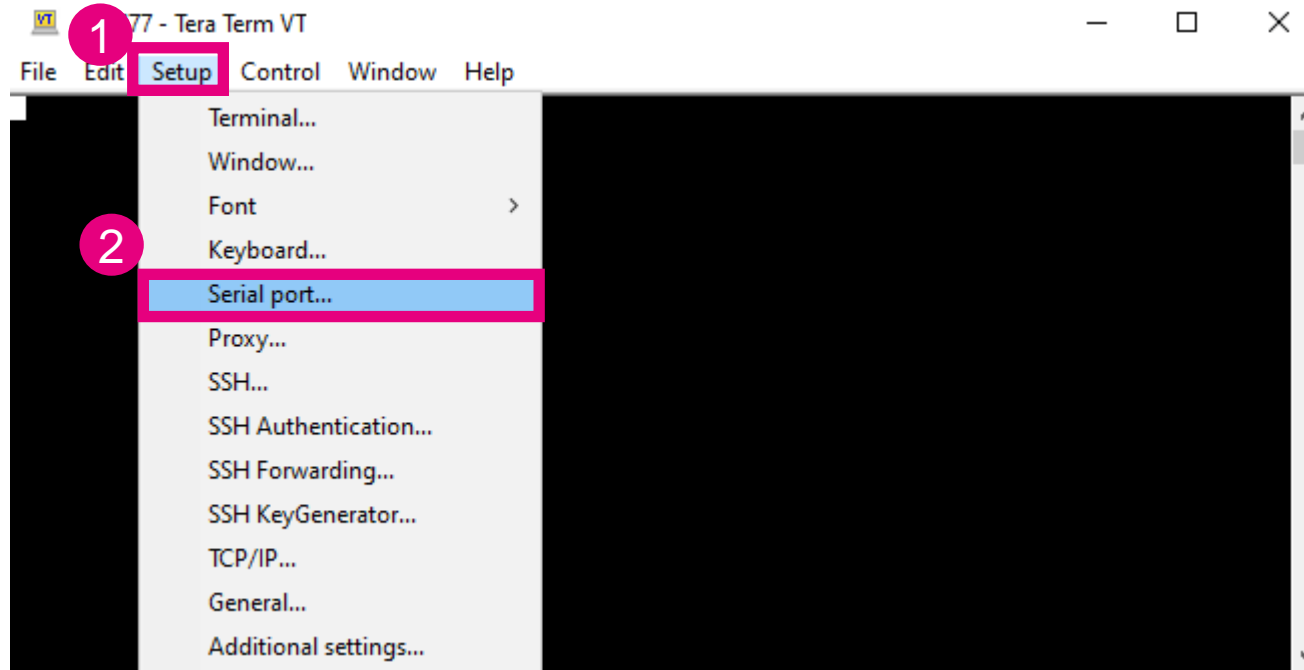
```
====
==== The board is correctly configured with ST Secure Manager Package
====
```

Board LEDs are blinking !

Open UART terminal serial port

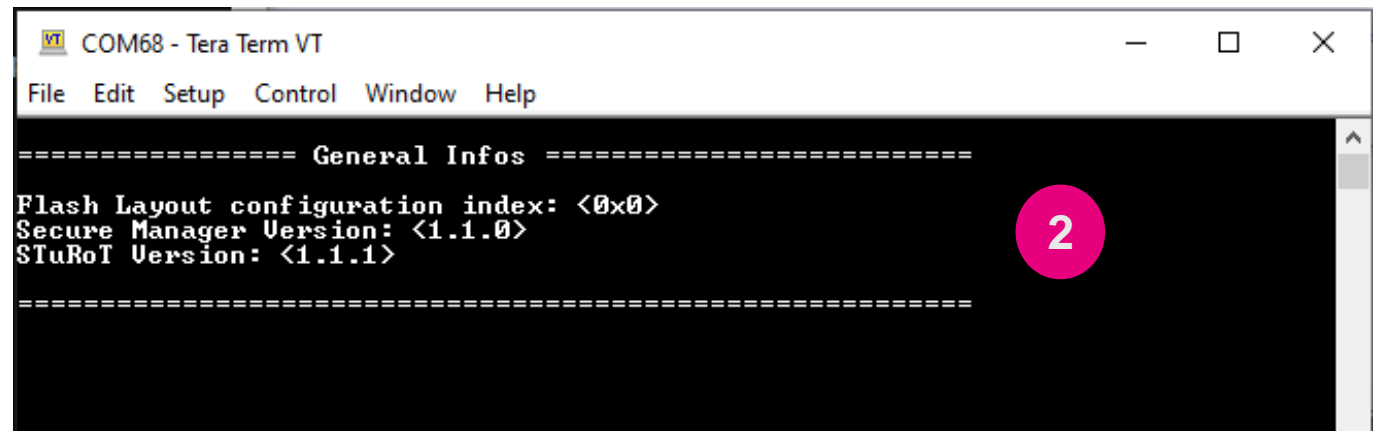
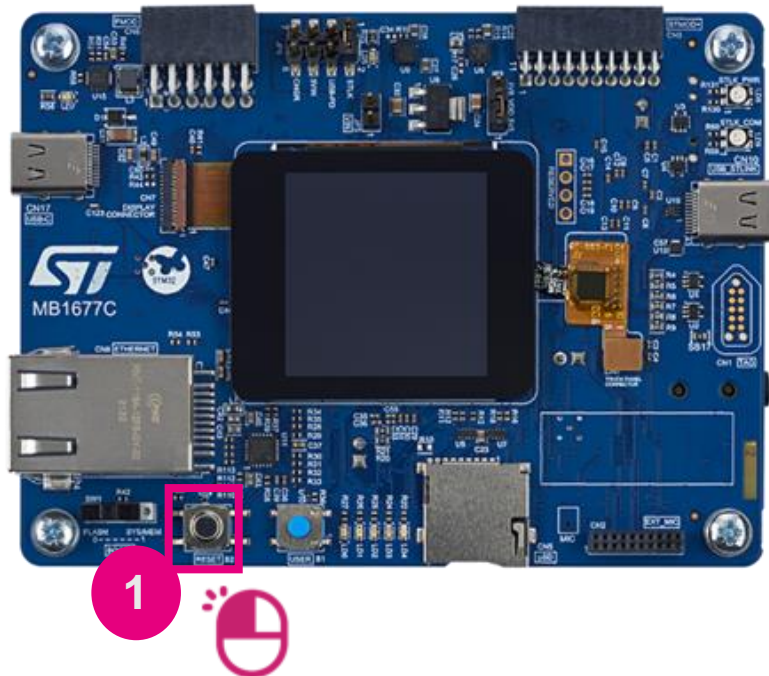


Serial port configuration



Check terminal connection

- Press the reset button on the board

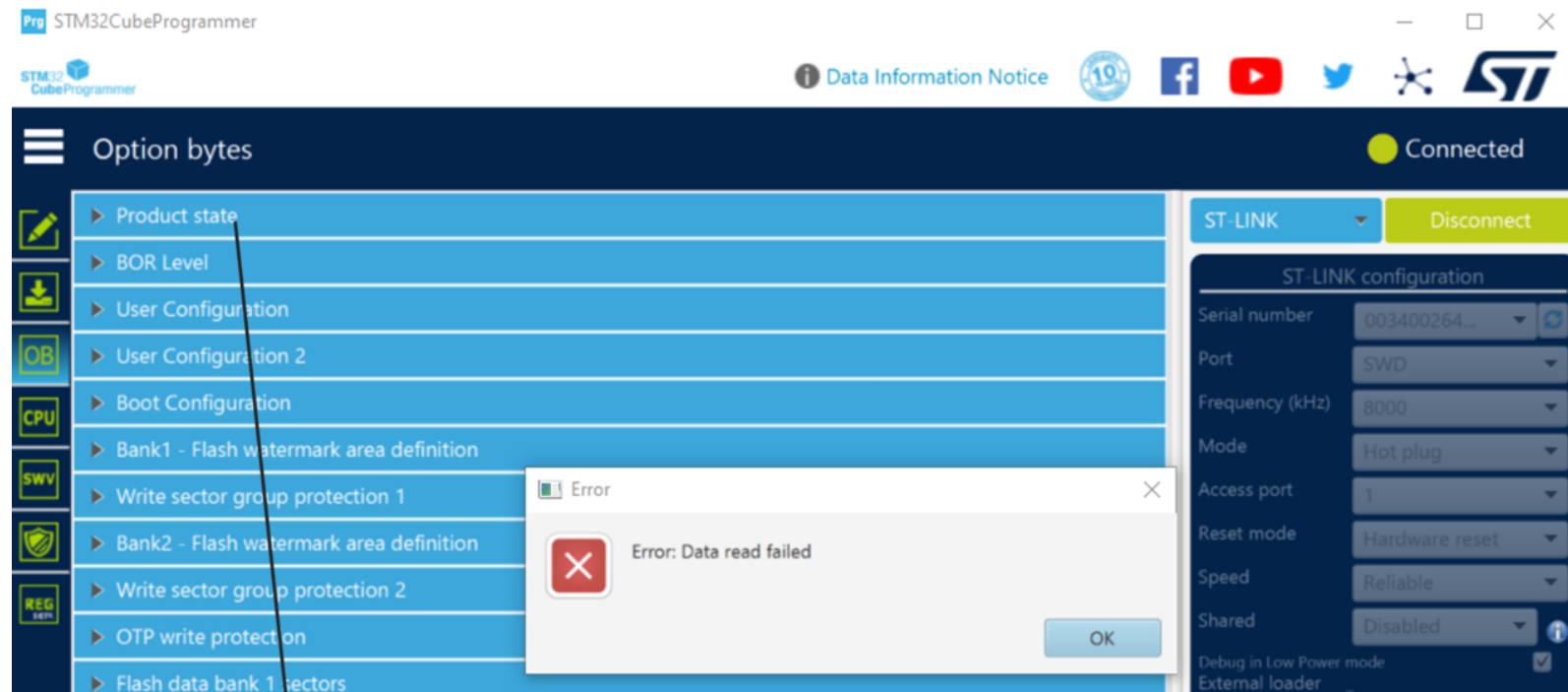
A screenshot of a terminal window titled 'COM68 - Tera Term VT'. The window has a menu bar with 'File', 'Edit', 'Setup', 'Control', 'Window', and 'Help'. The terminal output shows the following text:

```
===== General Infos =====  
Flash Layout configuration index: <0x0>  
Secure Manager Version: <1.1.0>  
STuRoT Version: <1.1.1>  
=====
```

A red circle with the number '2' is overlaid on the right side of the terminal window.

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



Product state		
Name	Value	Description
PRODUCT_STATE	C6	Life state code. ED : Open 17 : Provisioning, Debug partially opened (only non-secure) 2E : iRoT-provisioned, Debug partially opened (only non-secure) C6 : TZ-Closed, Debug partially opened (only non-secure) 72 : Closed, Debug disabled, regression is possible 5C : Locked

Hands-on Completed

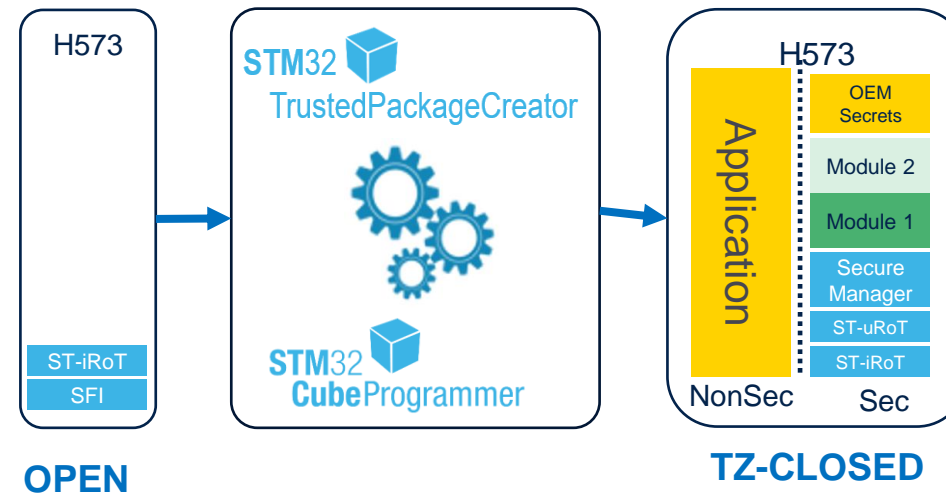
Configuration and Installation Flow

COMPLETED

Install a
Personalized
Secure Manager

Initial/virgin
state

OEM
personalized
product



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

← ↻ 🏠 https://wiki.st.com/stm32mcu/wiki/Category:How_to_start_with_Secure_Manager_on_STM32H5



STM32 MCU

🏠 📁 📄 ⚙️ ☰


Welcome Microcontroller **Solutions** Software development kit >>

Approved version. Approved on: 09:19, 27 September 2023

Category: [How to start with Secure Manager on STM32H5](#) Last edited 4 months ago ago ☆ ↺

How to start with Secure Manager on STM32H5 ? Help

This category includes all articles "How to start with Secure Manager on STM32H5"

 Page automatically approved: **no TLMS PR ID**.
Automatic approval based on the "Category model" article.

Pages in category "How to start with Secure Manager on STM32H5"↑

The following 3 pages are in this category, out of 3 total.

- [Security:Secure Manager STM32H5 How to Intro](#)
- [Security:How to start with Secure Manager default configuration on STM32H5](#)
- [Security:How to start with Secure Manager customized config on STM32H5](#)

If you have any question or request concerning this wiki or if you see some pages with some mistake, you can report them using [ST Support Center](#) or [ST Community MCU Forum](#).

🔍 by **ST**

STM32 MCU

🏠 📁 📄 ⚙️ ☰

- > Artificial Intelligence
- > Connectivity
- > Low power
- > Motor Control
- ✓ Security
 - > Security functions
 - ✓ STM32H5
 - > Security with STM32H5
 - ✓ **Getting started with STM32H5 security**
 - > How to start with STM32CubeMX...
 - > How to start with DA on STM32H5
 - > How to start with OEMiRoT on S...
 - > How to start with STiRoT on STM...
 - ✓ **How to start with Secure Manage...**
 - Secure Manager STM32H5 H...
 - How to start with Secure Mana...
 - How to start with Secure Mana...
 - Getting started with STM32H5 se...
 - Getting started with STM32H7RS...
- > Touch sensing

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

Our technology starts with You



Find out more at www.st.com

© STMicroelectronics - All rights reserved.

ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.

For additional information about ST trademarks, please refer to www.st.com/trademarks.

All other product or service names are the property of their respective owners.



life.augmented