



life.augmented



STM32Trust

STM32H5 Security Secure Manager - Part 4

Hands On: NS Application using Secure Manager services

Presenter: Massimo Panzica

Agenda

I Introduction

II Hands-On: NS Application
Compile and Debug

III Hands-On: NS Application
and Secure Manager services

IV Resources

Introduction

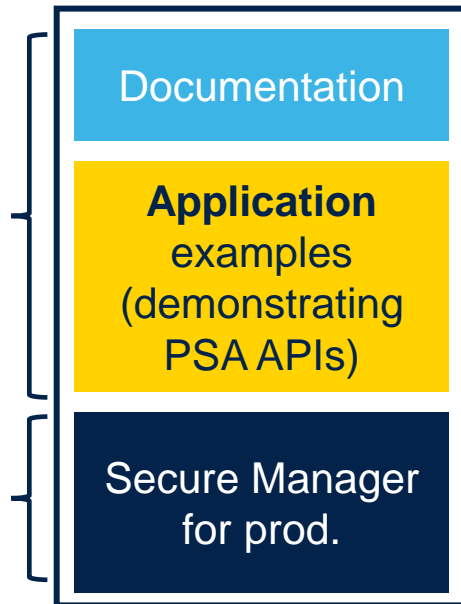
Simplify developer's experience

SMAK

To develop applications using security services

Downloaded from
[STM32CubeH5](#)
license [SLA0048](#)

Downloaded from
[STM32TRUSTEE-SM](#)
(encrypted binary)
license [SLA0044](#)

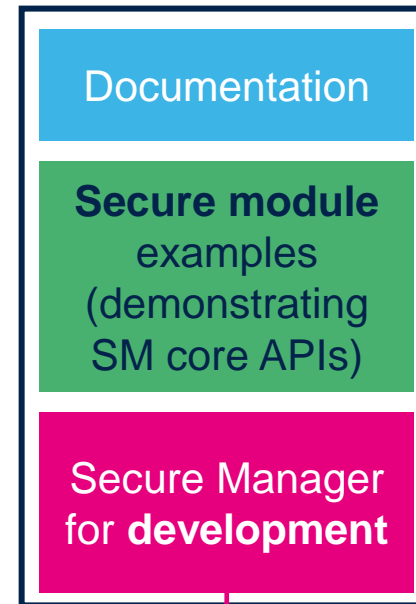


SMDK

To develop module inside TrustZone®

X-CUBE-SMDK-H5
Available on demand
(encrypted binary)

Signed LLA



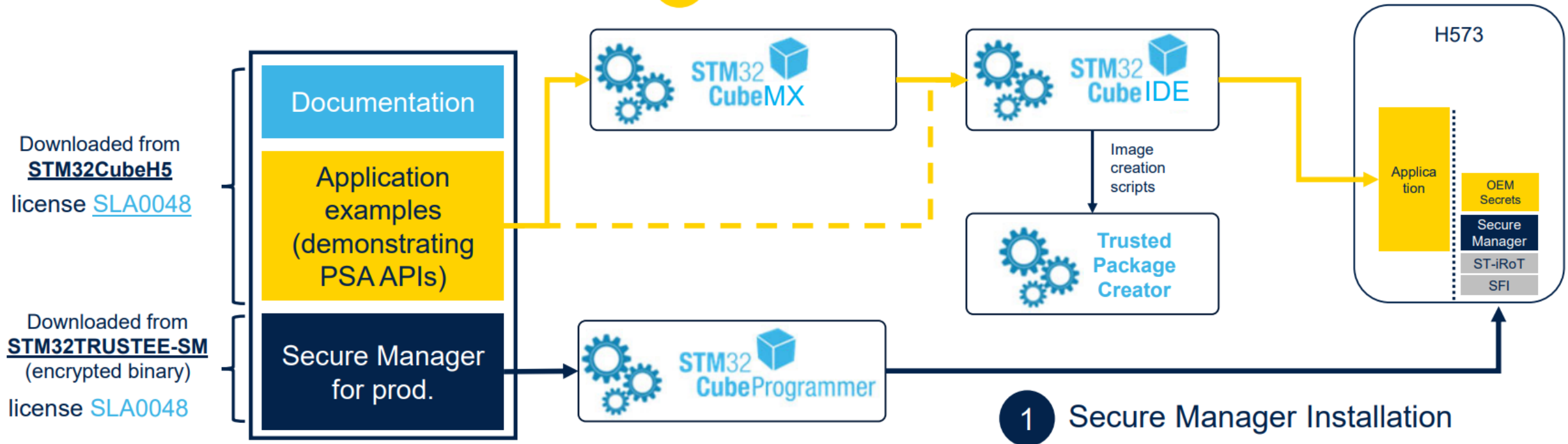
Only for development

Secure Manager Access Kit SMAK

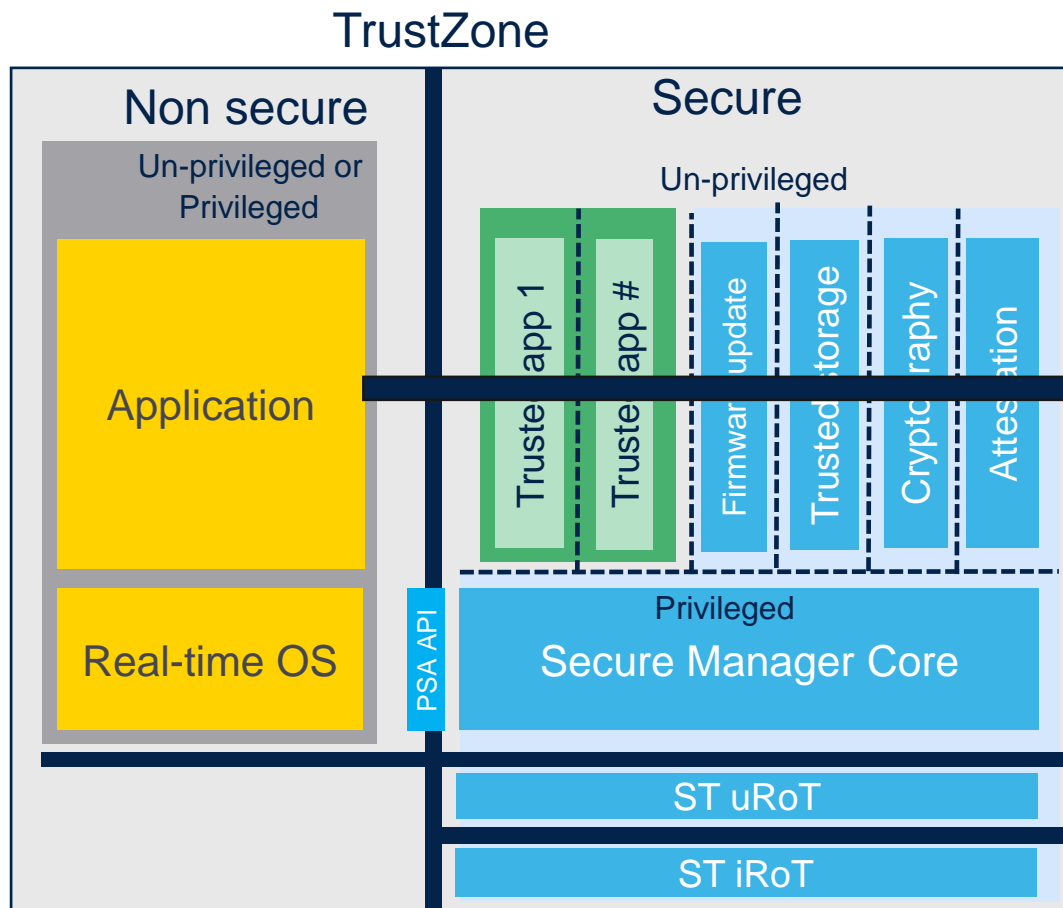
Development kit to develop **NS applications** using **security services**

SMAK license [SLA0048](#)
Used for production

2 OEM application creation



Simplify security customer journey



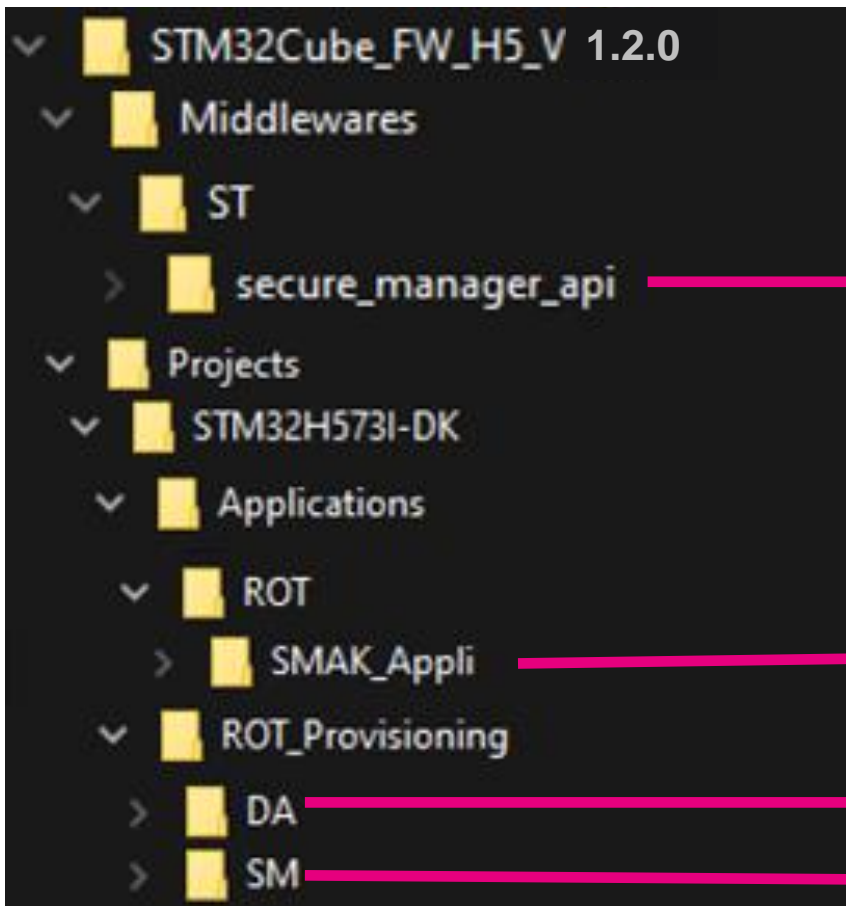
OEM scope

Non-Secure Application

- securely & independently updatable
- optionally encrypted

SMAK Delivery overview

Main resources



Secure Manager API Middleware provides callable standard PSA Services

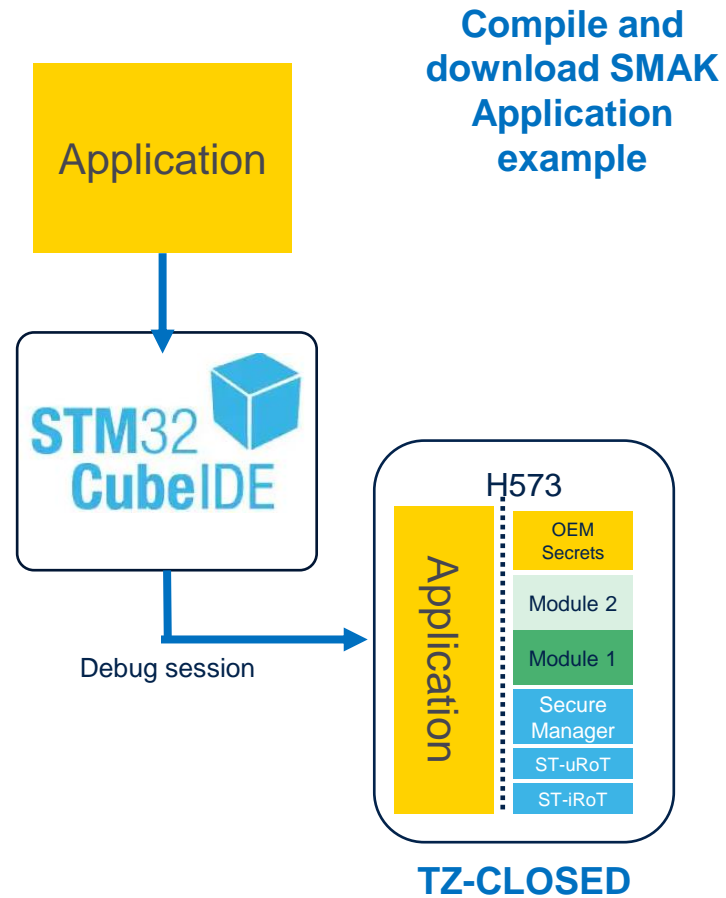
Application example with usage of the PSA API

Debug Authentication : all the scripts and resource associated

Secure Manager : all the scripts and resource associated

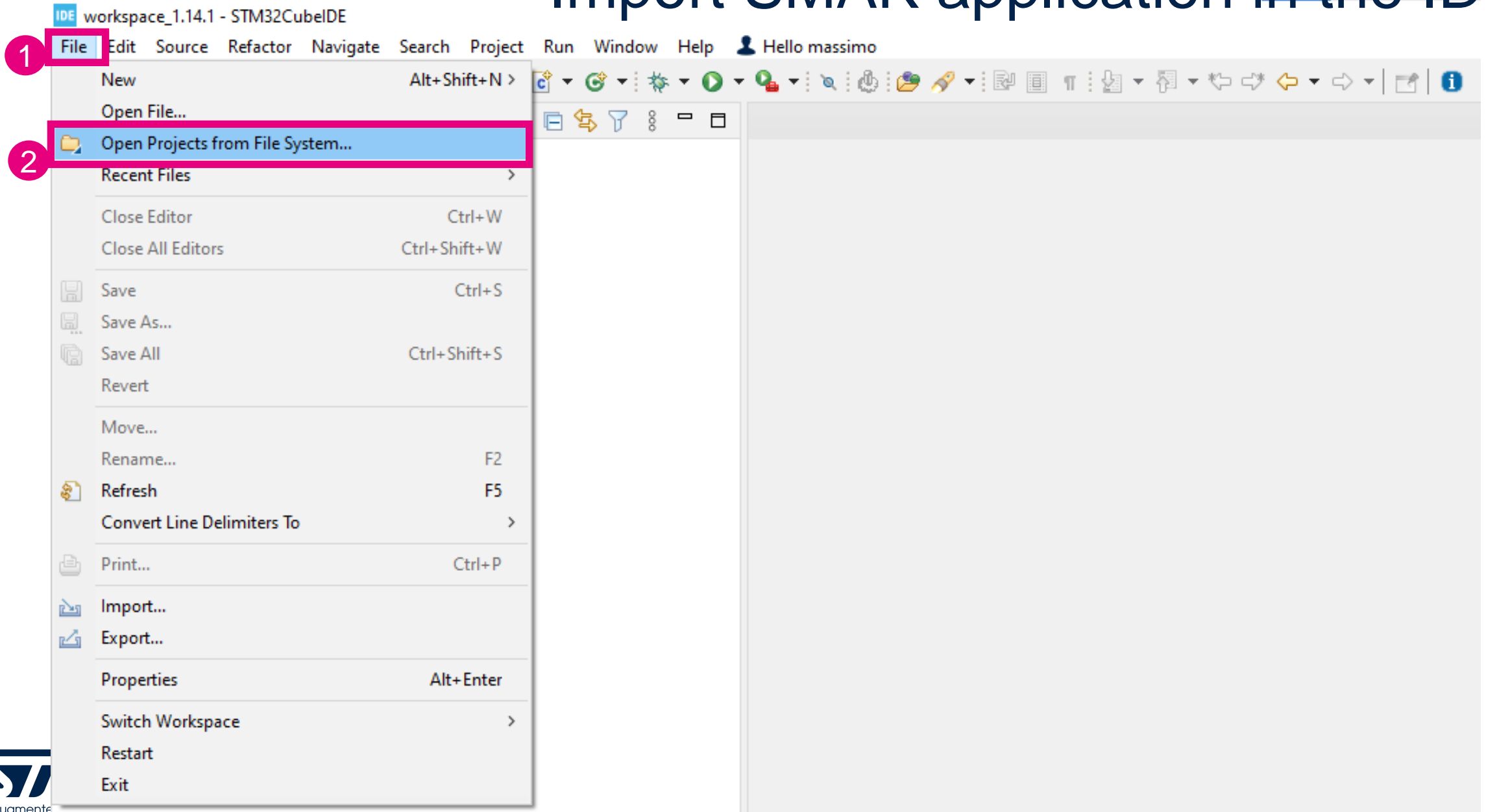
SMAK Development Flow

Application Development Flow

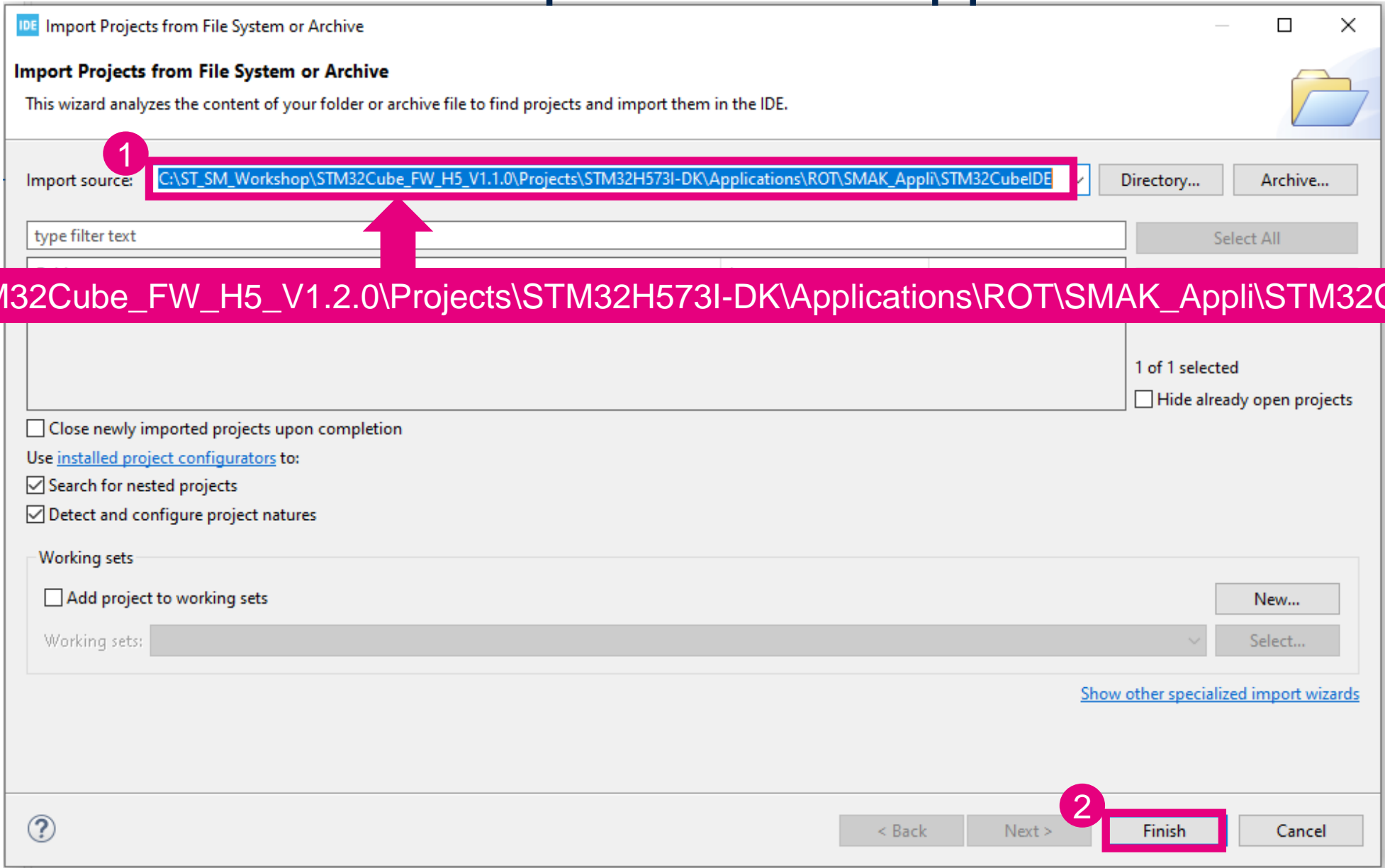


Hands-on: NS Application Compile and Debug

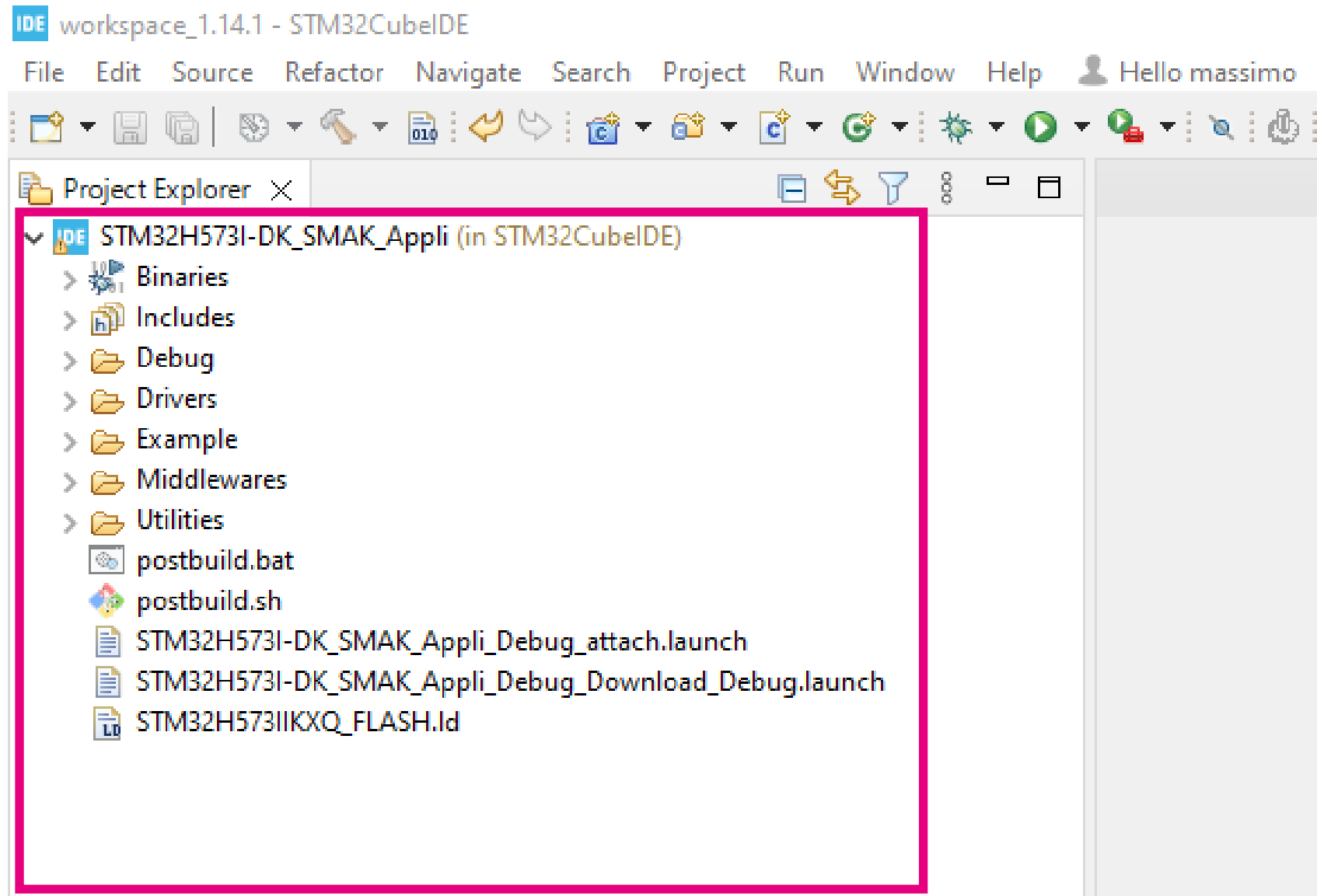
Import SMAK application in the IDE



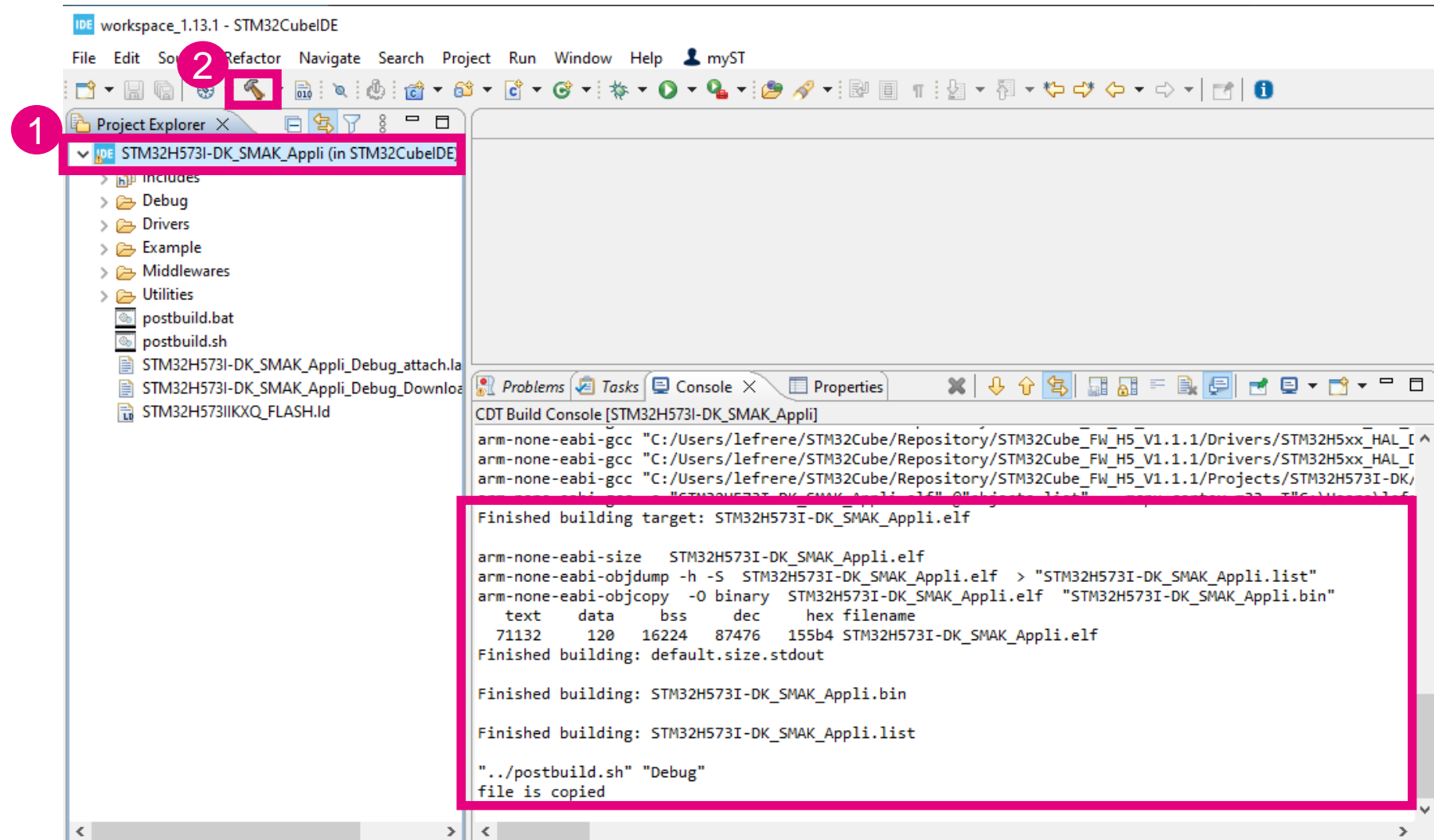
Import SMAK application in the IDE



Import SMAK application in the IDE



Compile SMAK application



Load and debug the SAMK application

The screenshot illustrates the steps to load and debug the SAMK application in STM32CubeIDE. The interface is divided into several panels:

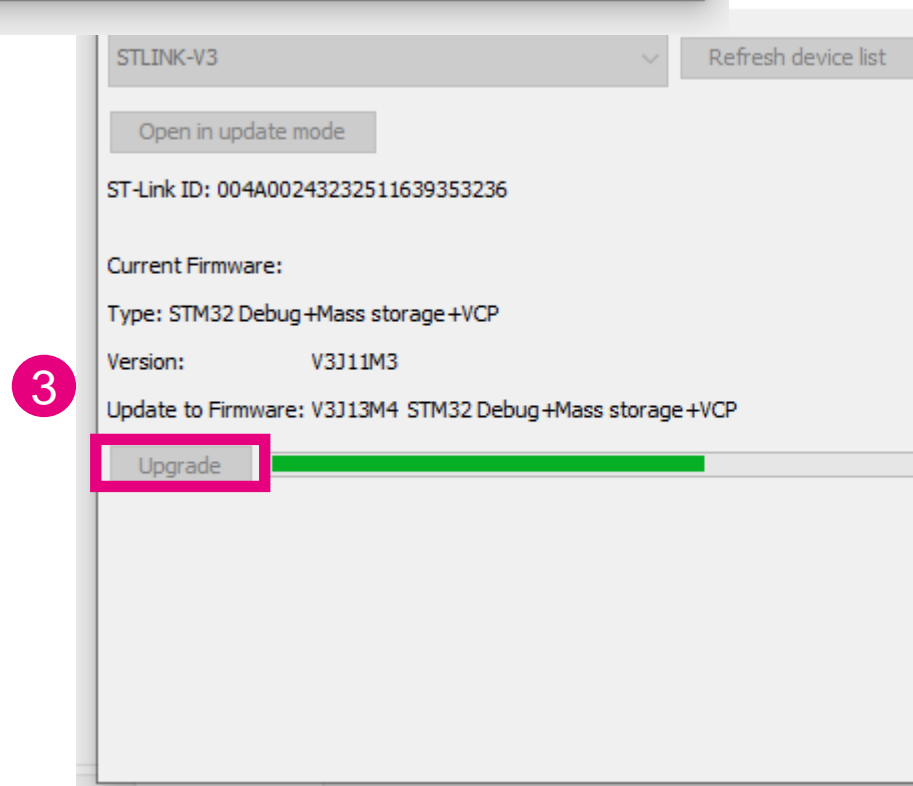
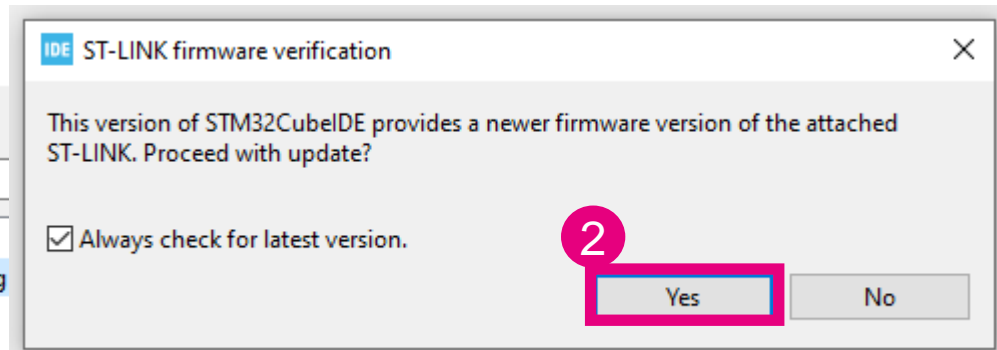
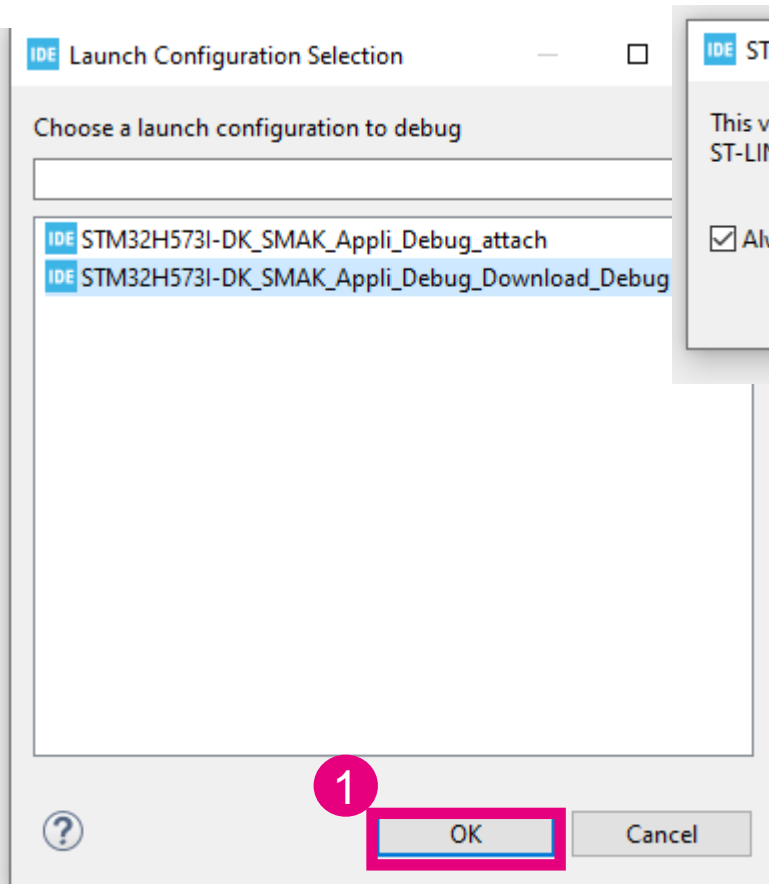
- Project Explorer:** Shows the project structure. The project name "STM32H573I-DK_SMAK_Appli (in STM32CubeIDE)" is highlighted with a red box and labeled with a red circle 1.
- Run and Debug Menu:** The "Run" menu is open, showing options like "Run", "Debug", "Run History", "Run As", "Run Configurations...", "Debug History", "Debug As", "Debug Configurations...", "Breakpoint Types", "Toggle Breakpoint", "Toggle Line Breakpoint", "Toggle Watchpoint", "Toggle Method Breakpoint", "Skip All Breakpoints", "Remove All Breakpoints", and "External Tools". The "Debug As" option is highlighted with a red box and labeled with a red circle 3. The "1 STM32 C/C++ Application" option is also highlighted with a red box and labeled with a red circle 4.
- Launch Configuration Selection Dialog:** A dialog box titled "Launch Configuration Selection" is shown. It contains a list of launch configurations. The configuration "STM32H573I-DK_SMAK_Appli_Debug_Download_Debug" is highlighted with a red box and labeled with a red circle 4.

The console output shows the build process:

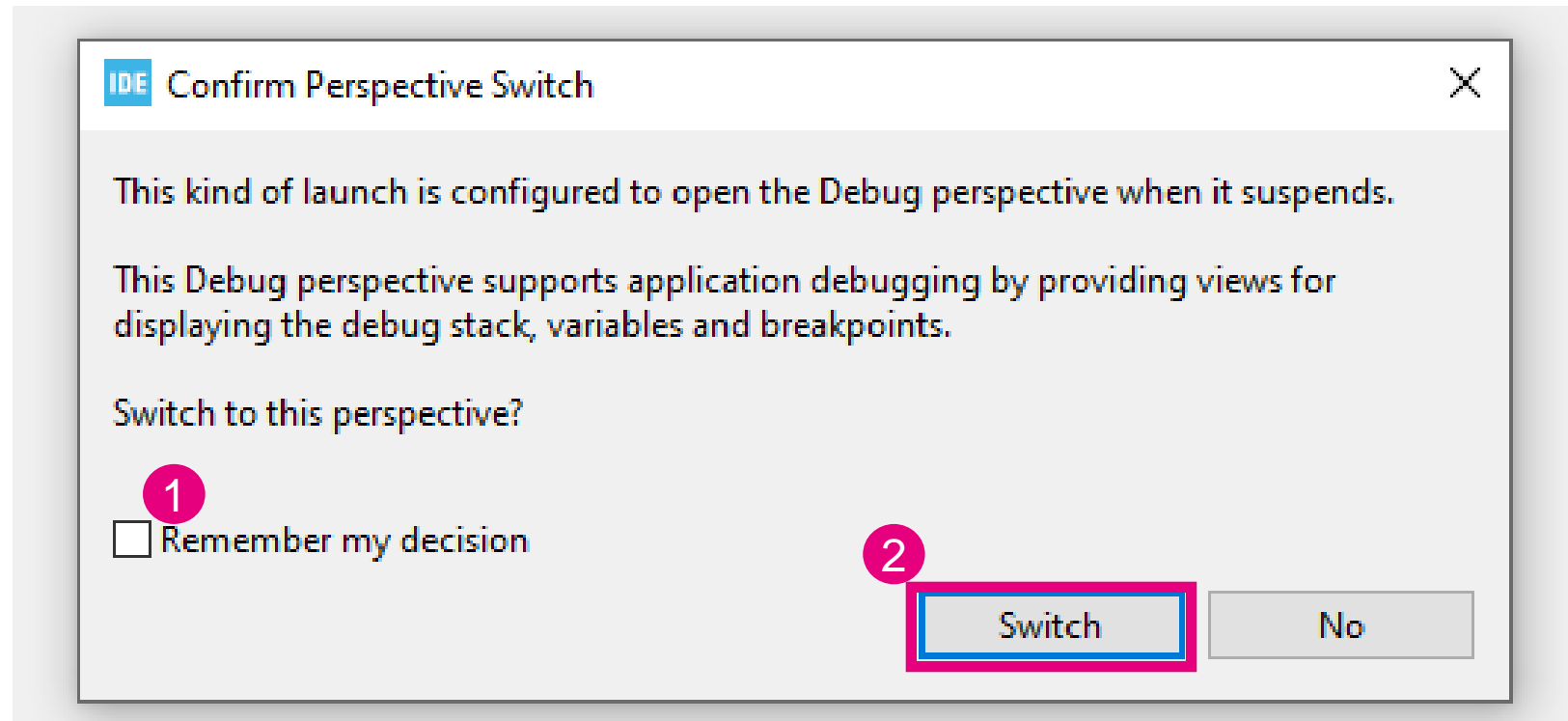
```
Finished building: STM32H573I-DK_SMAK_Appli.list
"../postbuild.sh" "Debug"
file is copied
postbuild script success

17:28:42 Build Finished. 0 errors, 0 warnings. (took 19s.280ms)
```

Update ST-LINK if asked



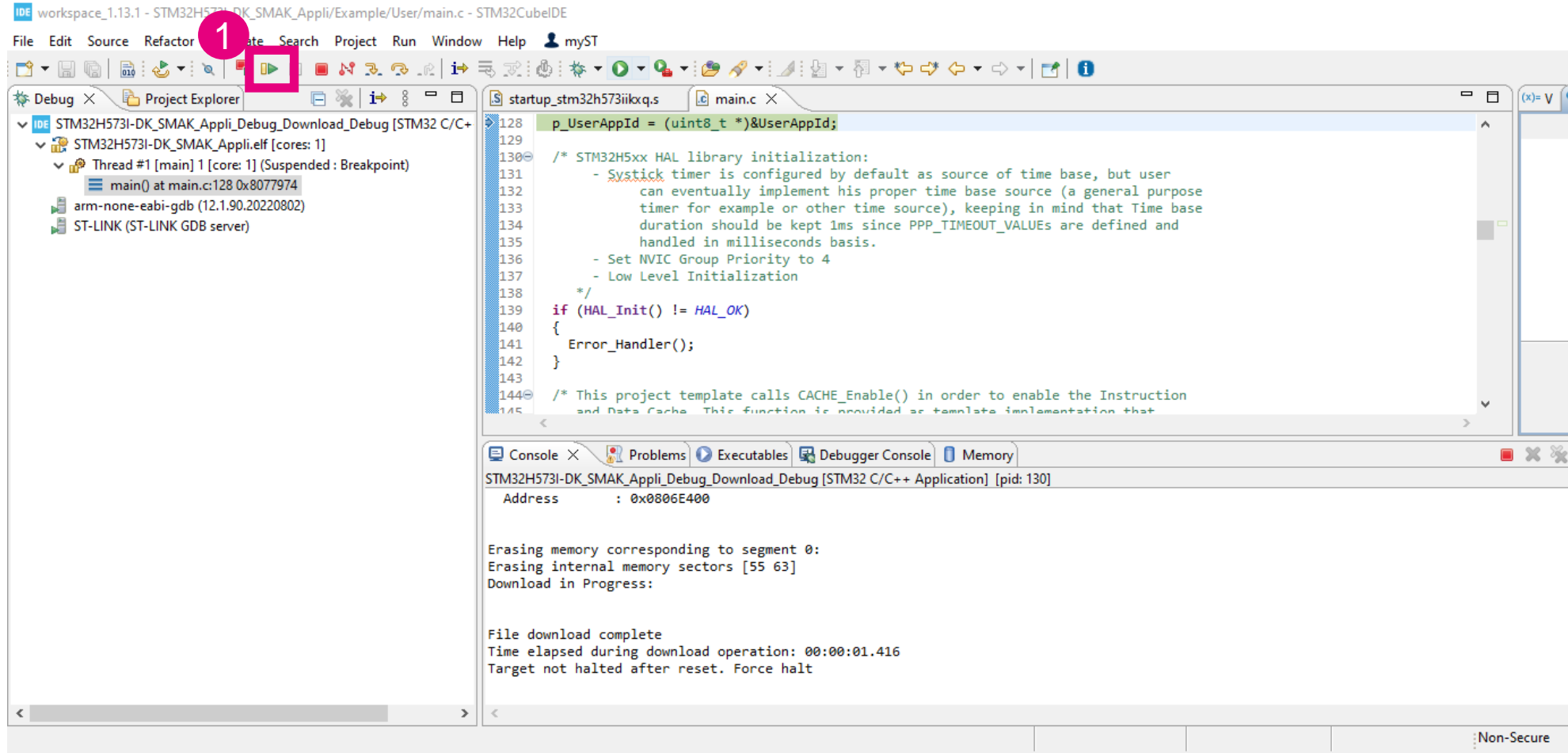
Activate Debug Perspective



SMAK application debug

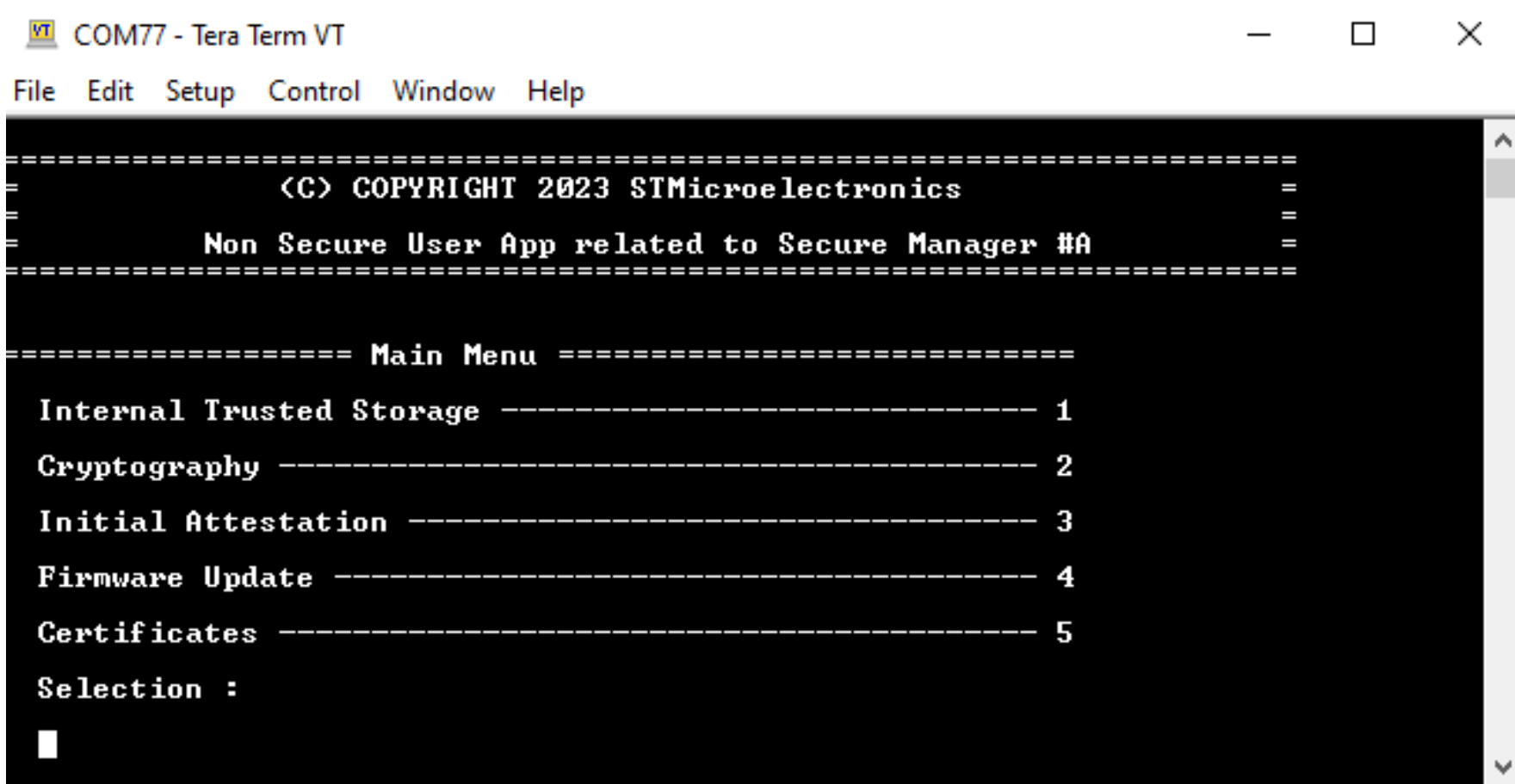
- Add breakpoint line 162 which is first printf line : double click on “162”
- Run/Resume of F8
- Then press F6 and see the lines printing in TeraTerm
- => You can download and debug the SMAK example application as if you were developing on a STM32 without TrustZone in open state

Launch the SMAK appli



Hands-on: NS Application and Secure Manager services

SMAK appli UI

A screenshot of a terminal window titled "COM77 - Tera Term VT". The window has a menu bar with "File", "Edit", "Setup", "Control", "Window", and "Help". The terminal content is as follows:

```
=====
<C> COPYRIGHT 2023 STMicroelectronics
Non Secure User App related to Secure Manager #A
=====

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

Internal Trusted Storage ----- 1
Cryptography ----- 2
Initial Attestation ----- 3
Firmware Update ----- 4
Certificates ----- 5

Selection :
█
```

SMAK appli UI

```
=====
(C) COPYRIGHT 2023 STMicroelectronics
=====
Non Secure User App related to Secure Manager #A
=====

===== Main Menu =====
Internal Trusted Storage ----- 1
Cryptography ----- 2
Initial Attestation ----- 3
Firmware Update ----- 4
Certificates ----- 5
Selection :
```

- SMAK example application provides implementation of PSA API for each service category (1 to 4)
- Item 5 does not use PSA API. Just displays the X509 certificates provided by the platform

Internal Trusted Storage

```
===== Internal Trusted Storage Menu =====  
Factory data are provisioned during SM installation and are not updatable  
New data: Set ----- 1  
New data: Get ----- 2  
New data: Get info ----- 3  
New data: Remove ----- 4  
Factory data: Set ----- 5  
Factory data: Get ----- 6  
Factory data: Get info ----- 7  
Factory data: Remove ----- 8  
Previous menu ----- x  
Selection :
```

- Example of dynamic writing into secure store
- Example of accessing pre-provisioned data (Factory data)
- Secure manager provides the ability to pre-provision the Internal Trusted Storage using a simple tool (we will use it later)

Cryptography

```
===== Cryptography Menu =====  
RNG ----- 1  
AES GCM ----- 2  
AES CBC ----- 3  
AES CCM ----- 4  
SHA224 ----- 5  
SHA256 ----- 6  
RSA 2048 ----- 7  
ECDSA <DUA USER key> ----- 8  
ECDSA <Factory ITS key> ----- 9  
Previous menu ----- x  
Selection :
```

- Set of examples of PSA Crypto API usage

Initial Attestation

```
===== Initial Attestation Menu =====  
Token ----- 1  
Previous menu ----- x  
Selection :
```

- Provides Initial Attestation token signed by Device Unique Authentication DUA1 key



Firmware Update

```
===== Firmware Update Menu =====
Get all applications Status ----- 1
Install all requested Applications <reboot> ----- 2
Download Non-Secure App ----- 3
Request Install Non-Secure App ----- 4
Accept Non-Secure App ----- 5
Abort Download Non Secure App ----- 6
Download Secure Manager ----- 7
Request Install Secure Manager ----- 8
Accept Secure Manager ----- 9
Abort Download Secure Manager ----- A
Download STuRoT ----- B
Request Install STuRoT ----- C
Abort Download STuRoT ----- D
Previous menu ----- x
Selection :
```

Secure User application update

Secure manager update

Secure ST-uROT (2nd stage bootloader) update



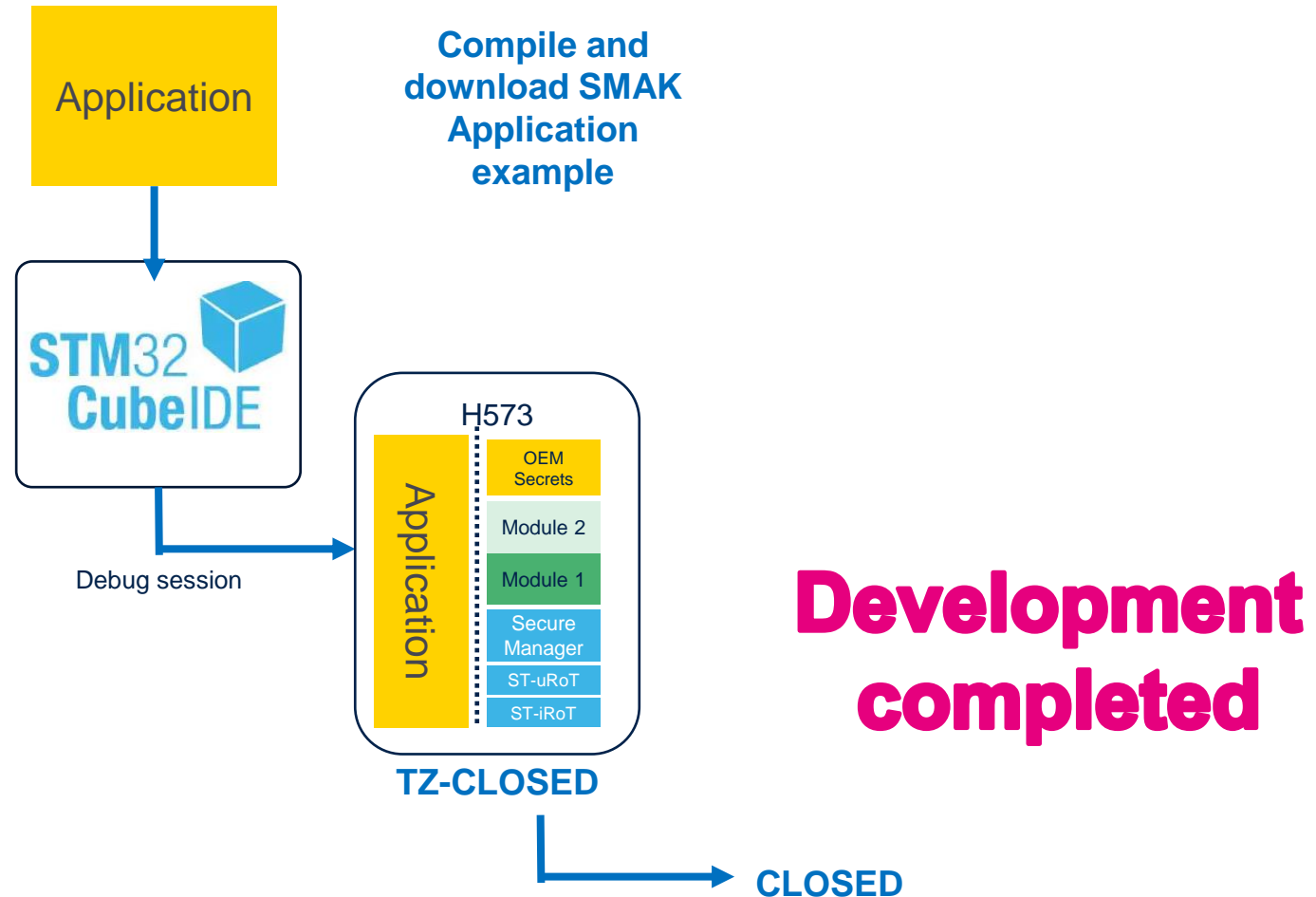
Certificate

```
===== Certificates Menu =====  
DUA USER X509 certificate ----- 1  
DUA Initial Attestation X509 certificate ----- 2  
Previous menu ----- x  
Selection :
```

- Display both certificate content in X509 pem format

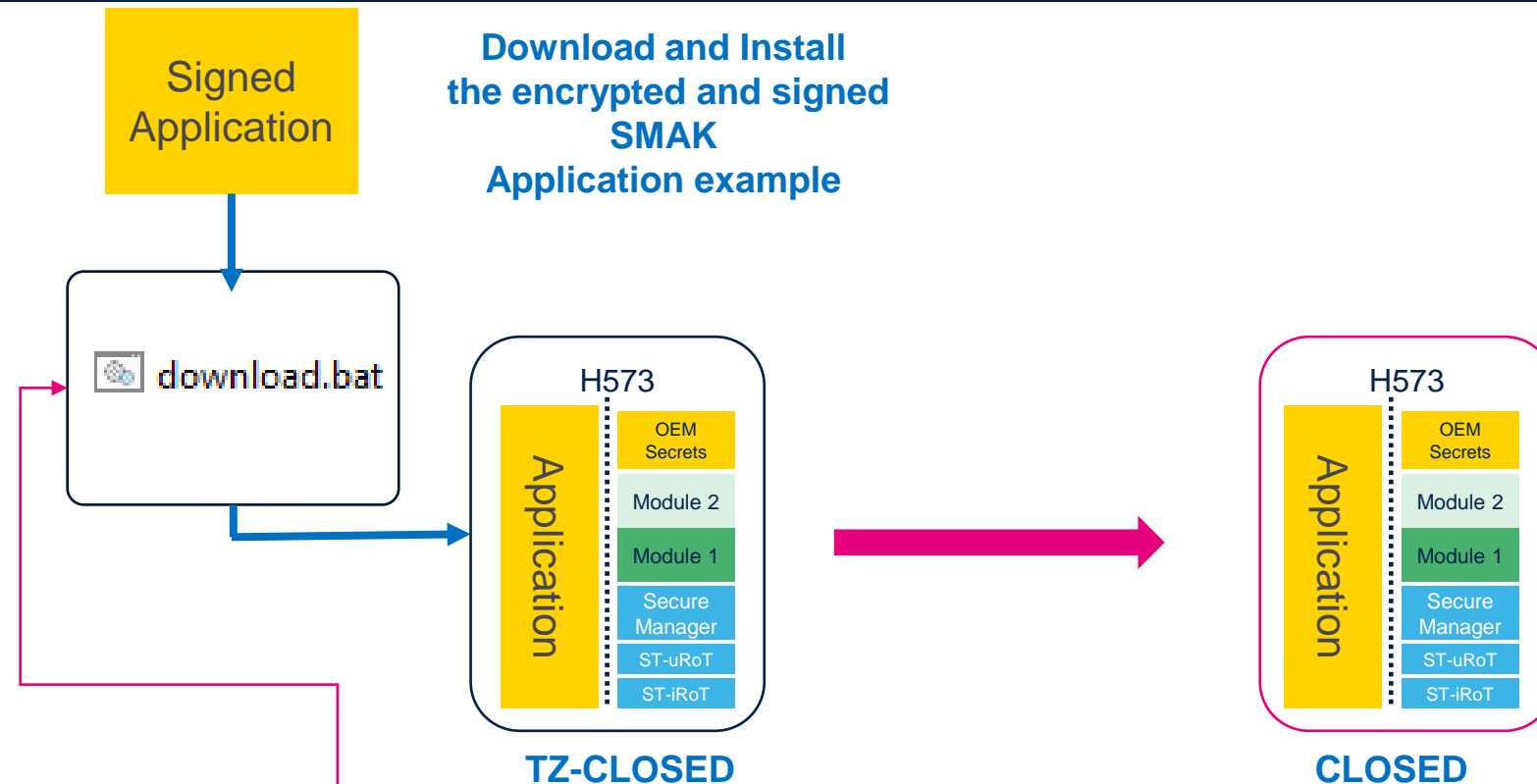
SMAK Development Flow

Application Development Flow



SMAK Installation Flow

Application Installation Flow



`STM32Cube_FW_H5_V1.2.0\Projects\STM32H573I-DK\Applications\ROT\SMAK_Appli`

C:\WINDOWS\system32\cmd.exe

```
=====  
==== The non-secure application is correctly updated  
=====  
C:\ST_SM_Workshop\STM32Cube_FW_H5_V1.1.0\Projects\STM32H573I-DK\Applications\ROT\SMAK_Appli>
```

Secure Manager Ecosystem

Set device in CLOSED state

The screenshot displays the STM32CubeProgrammer application window. The 'Option bytes' section is active, showing a list of configuration items. The 'PRODUCT_STATE' item is selected, and its dropdown menu is open, showing the value '72' highlighted with a pink box. The description for '72' is 'Closed, Debug disabled, regression is possible', also highlighted with a pink box. The 'ST-LINK' configuration panel on the right shows the device is connected and provides details about the target hardware and firmware.

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 : T2-Closed, Debug partially opened (only non-secure) 72 : Closed, Debug disabled, regression is possible 5C : Locked
BOR Level	C6	
User Configuration	72	
User Configuration 2	5C	
Boot Configuration		
Bank1 - Flash watermark area definition		
Write sector group protection 1		

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

Apply Read

Log

Live Update Verbosity level 1 2 3

12:25:26 : Address : 0x8000000
12:25:26 : Read progress:
12:25:26 : Data read successfully
12:25:26 : Time elapsed during the read operation is: 00:00:00.005

100%

ST-LINK configuration

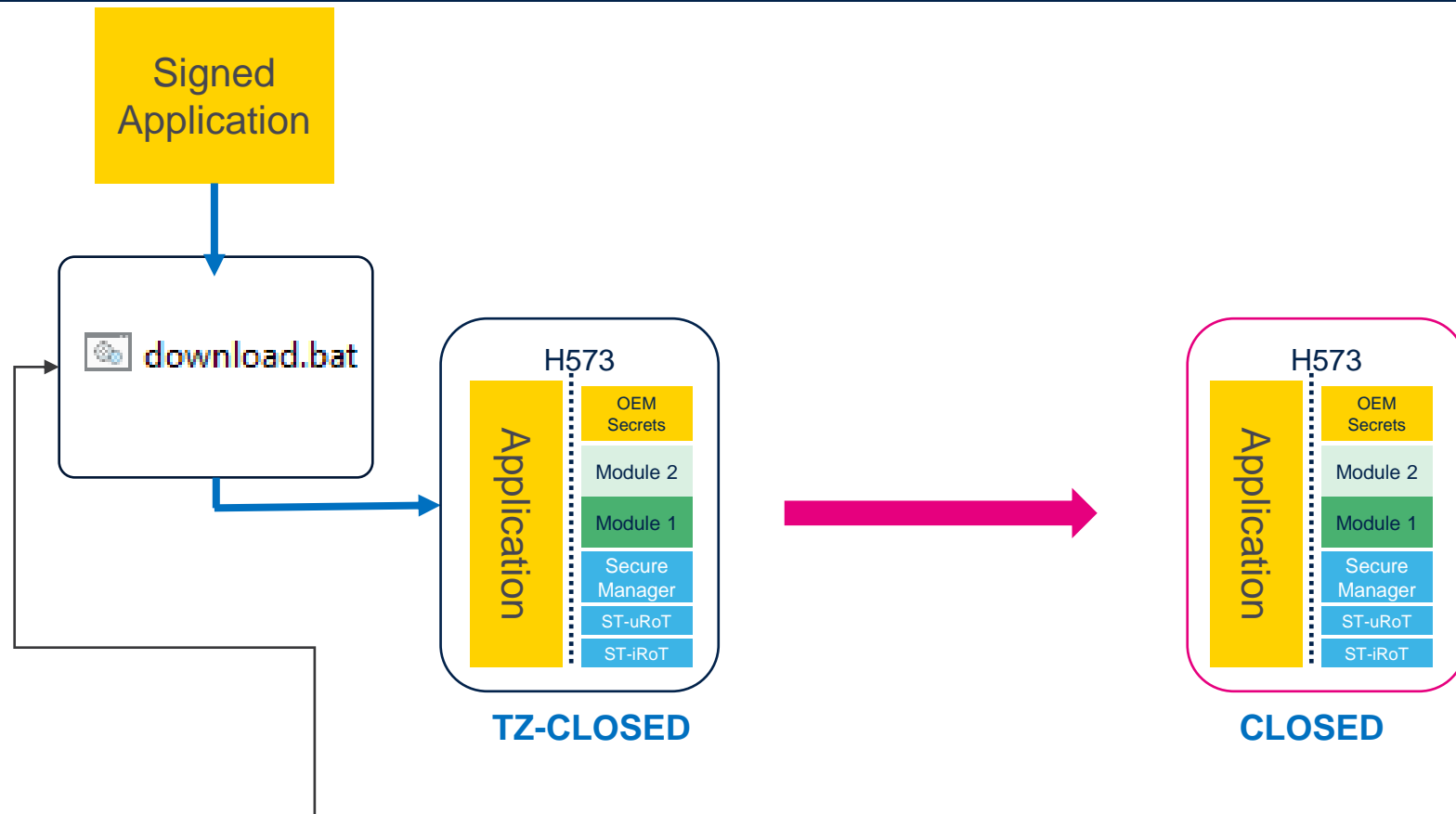
Serial number 0003001E4...
Port SWD
Frequency (kHz) 8000
Mode Hot plug
Access port 1
Reset mode Hardware reset
Speed Reliable
Shared Disabled
Debug in Low Power mode
External loader
Target voltage 3.27 V
Firmware version V3J10M3

Target information

Board STM32H573I-DK
Device STM32H5xx
Type MCU
Device ID 0x484
Revision ID Rev Z
Flash size 2 MB
CPU Cortex-M33
Bootloader Version 0xFF

SMAK Installation Flow

Application Installation Flow



STM32Cube_FW_H5_V1.2.0\Projects\STM32H573I-DK\Applications\ROT\SMAK_Appli

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

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