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

life.augmented

Introduction

STM32 Trust TEE

Secure Manager Ecosystem

Simplify developer's experience

SMAK
To develop applications using security services

Downloaded from **STM32CubeH5** license SLA0048

- Documentation
- **Application** examples (demonstrating PSA APIs)

Downloaded from **STM32TRUSTEE-SM** (encrypted binary) license SLA0044

- Secure Manager for prod.

SMDK
To develop module inside TrustZone®

- Documentation
- **Secure module** examples (demonstrating SM core APIs)
- Secure Manager for **development**

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

Signed LLA

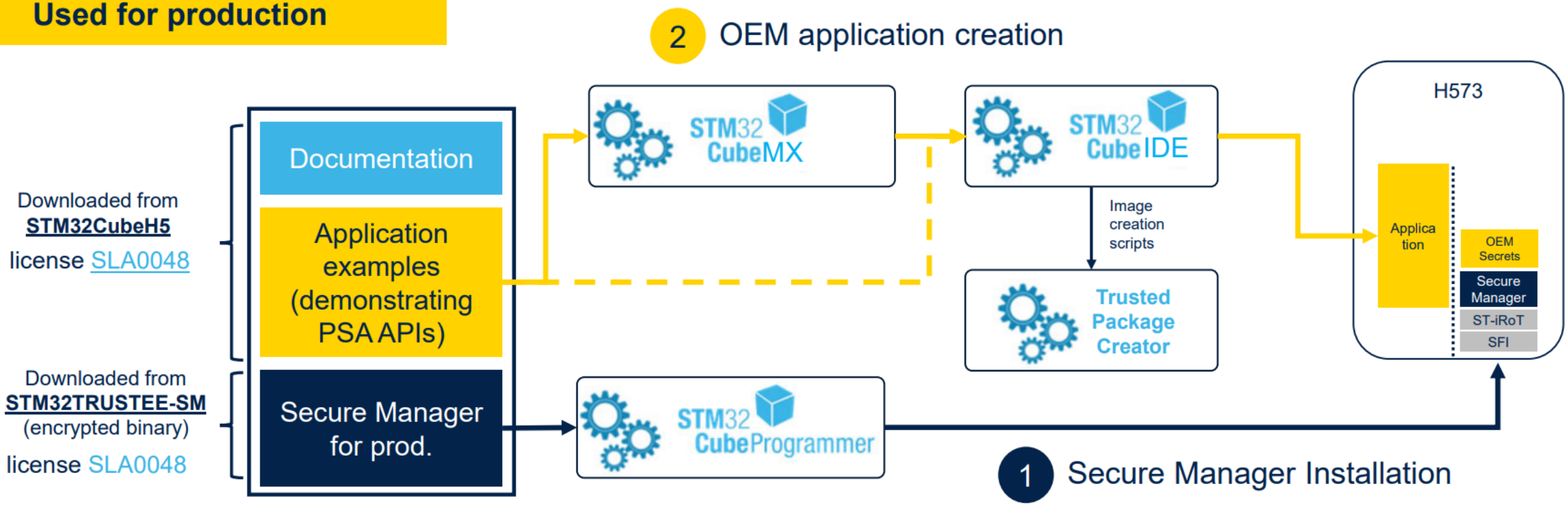
Only for development

life.augmented

Secure Manager Access Kit
SMAK

Development kit to develop NS applications using security services

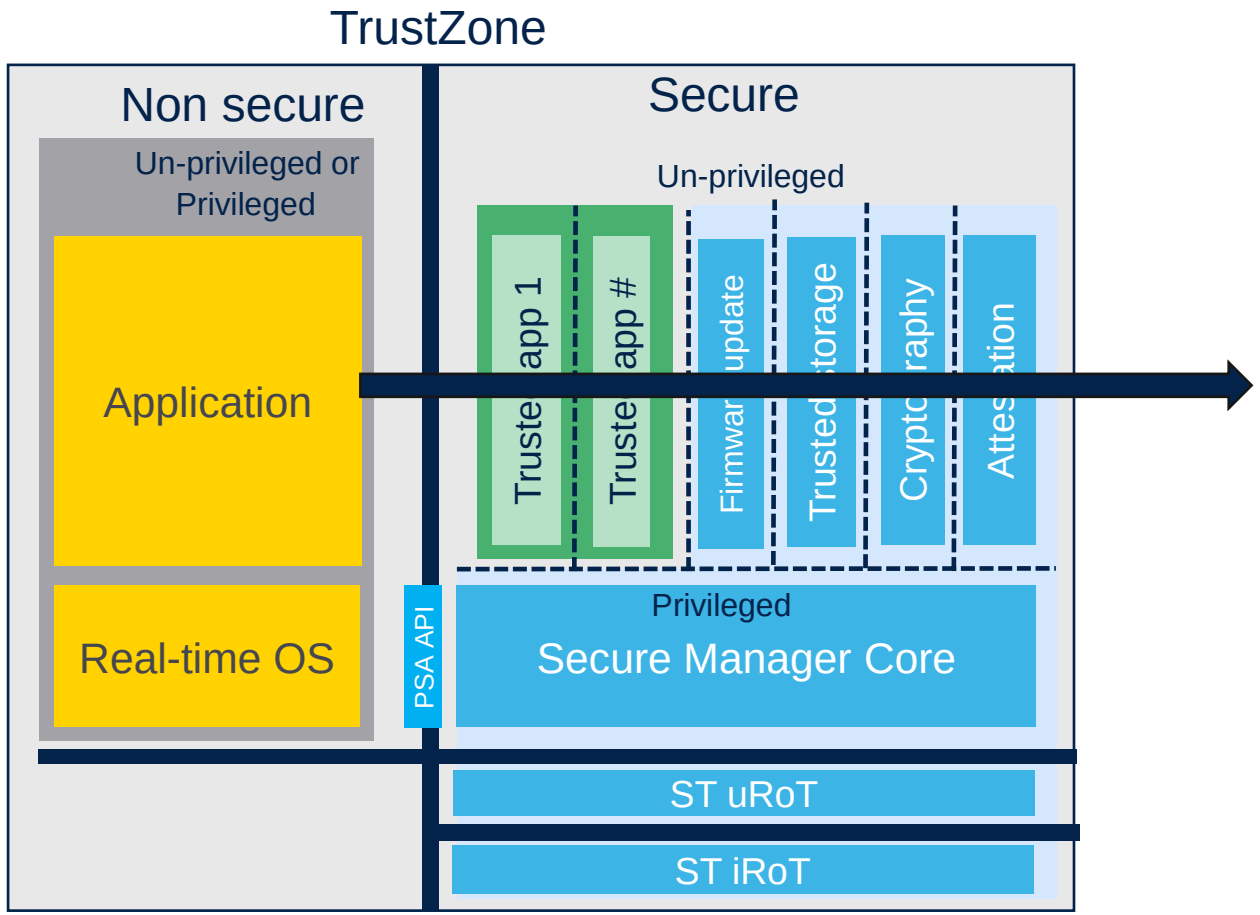
SMAK license SLA0048
Used for production



life.augmented

Secure Manager Access Kit
NS and S partitioning

Simplify security customer journey



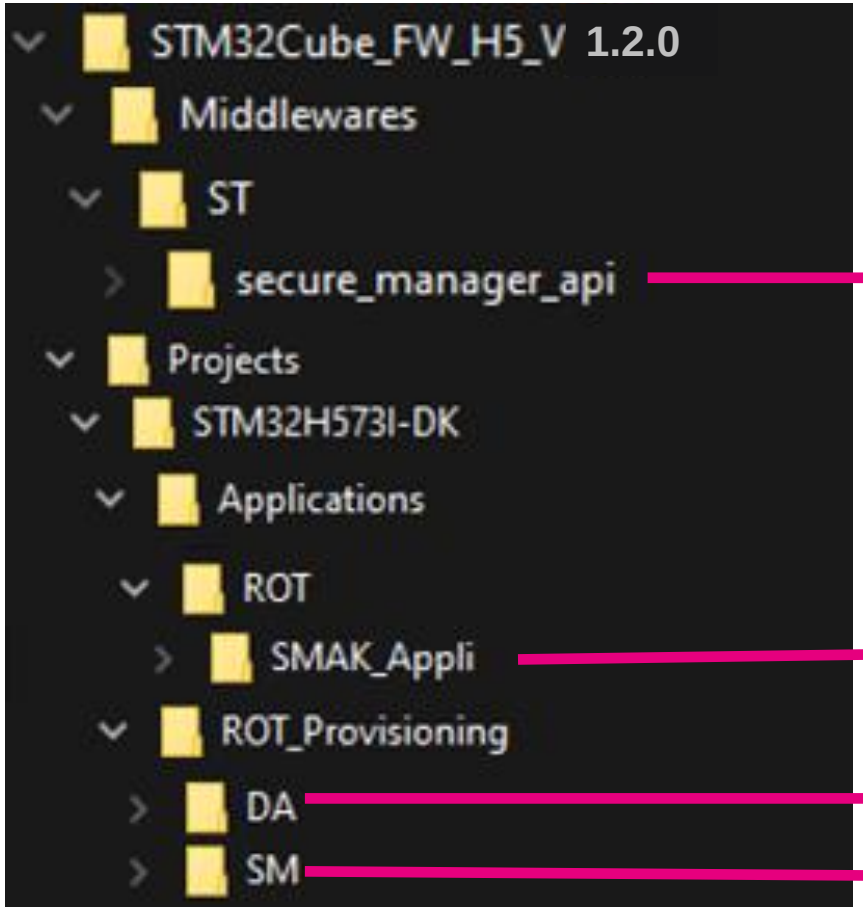
OEM scope

Non-Secure Application

- securely & independently updatable
- optionally encrypted

SMAK Delivery overview

Main resources



Secure Manager API Middleware provides callable standard PSA Services

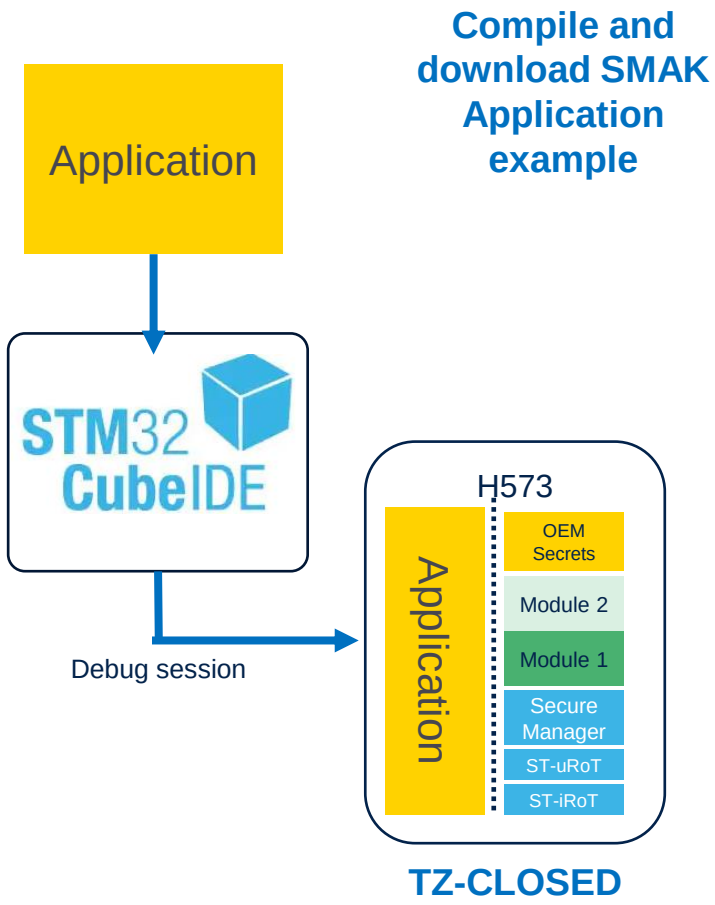
Application example with usage of the PSA API

Debug Authentication : all the scripts and resource associated

Secure Manager : all the scripts and resource associated

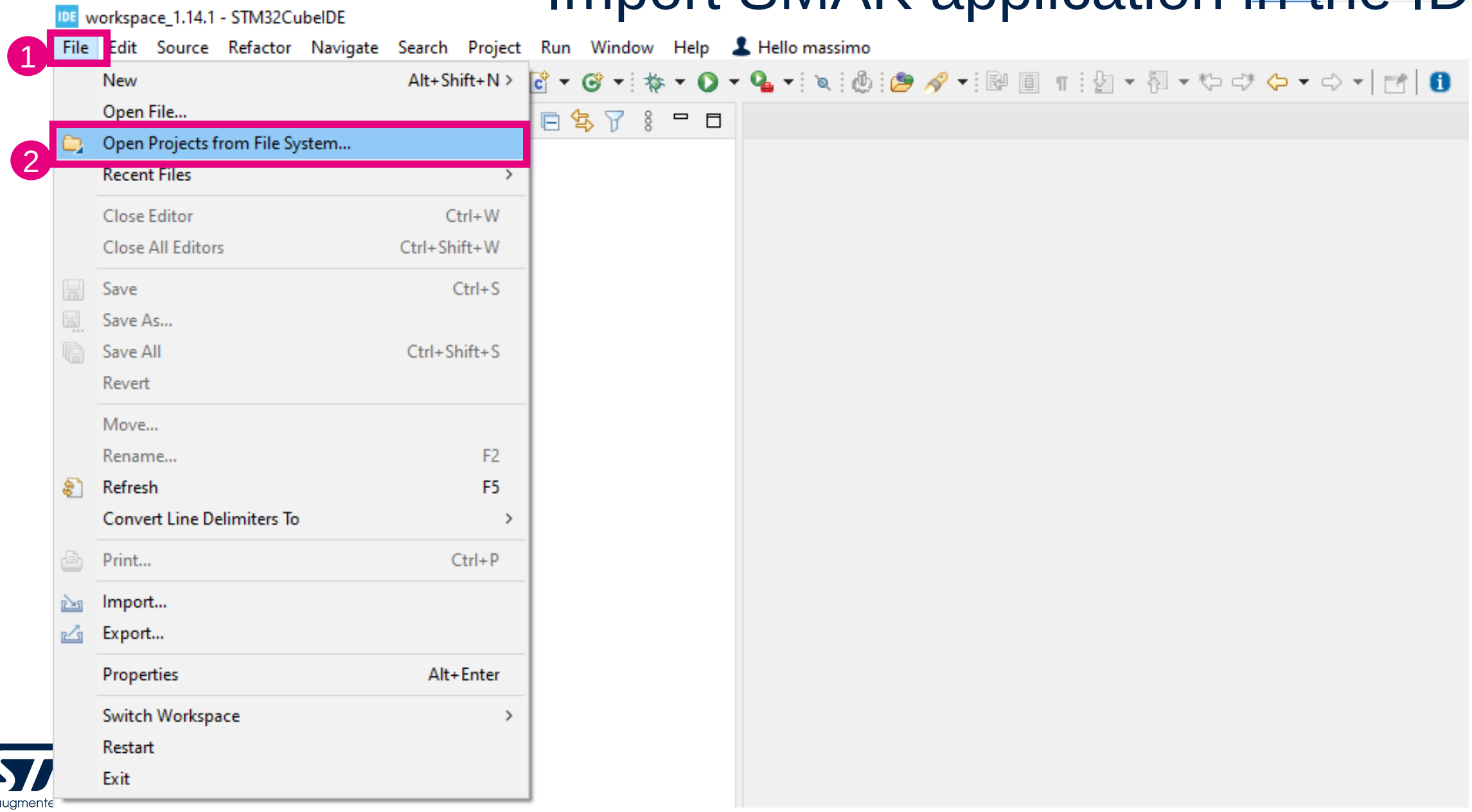
SMAK Development Flow

Application Development Flow

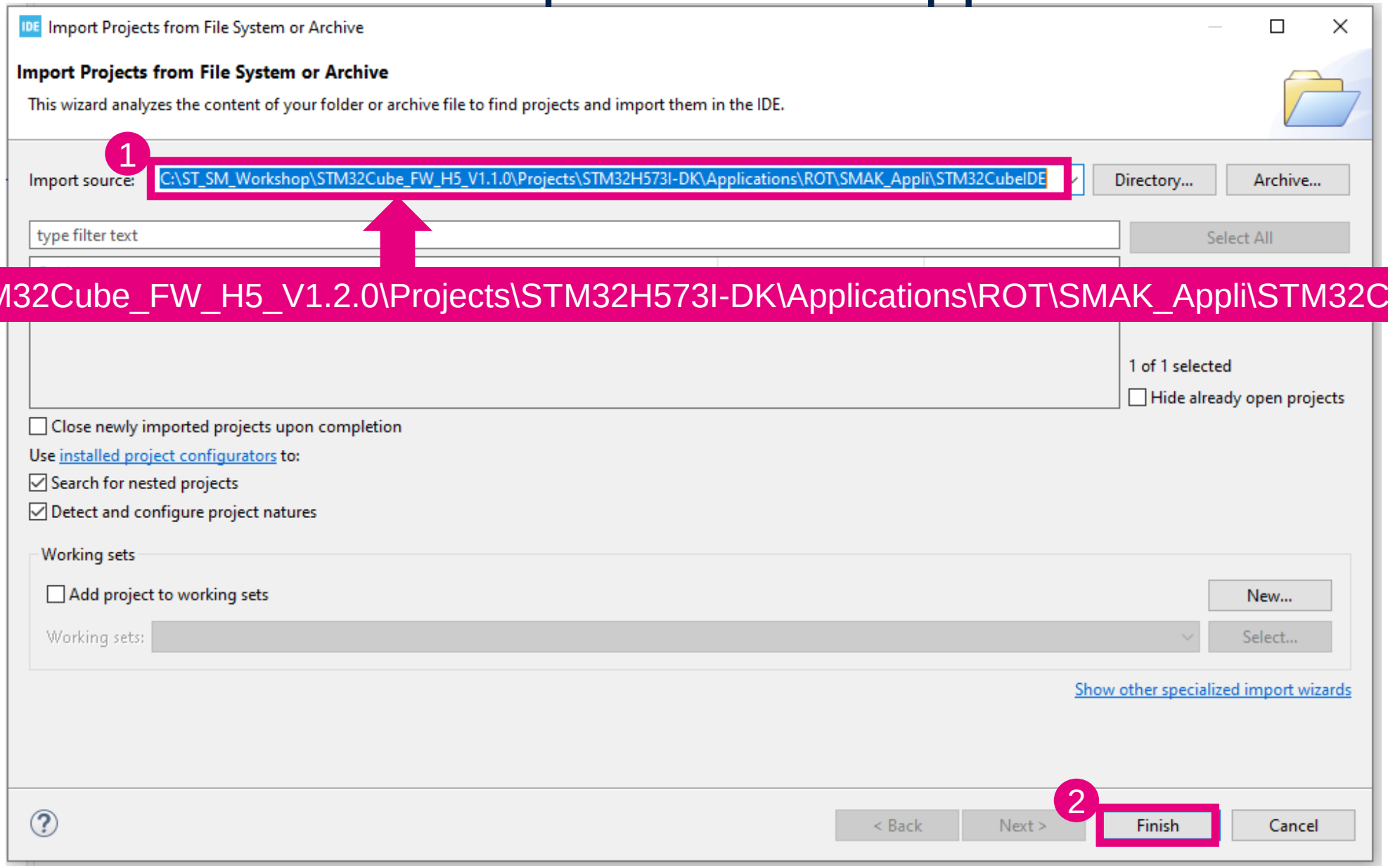


Hands-on: NS Application Compile and Debug

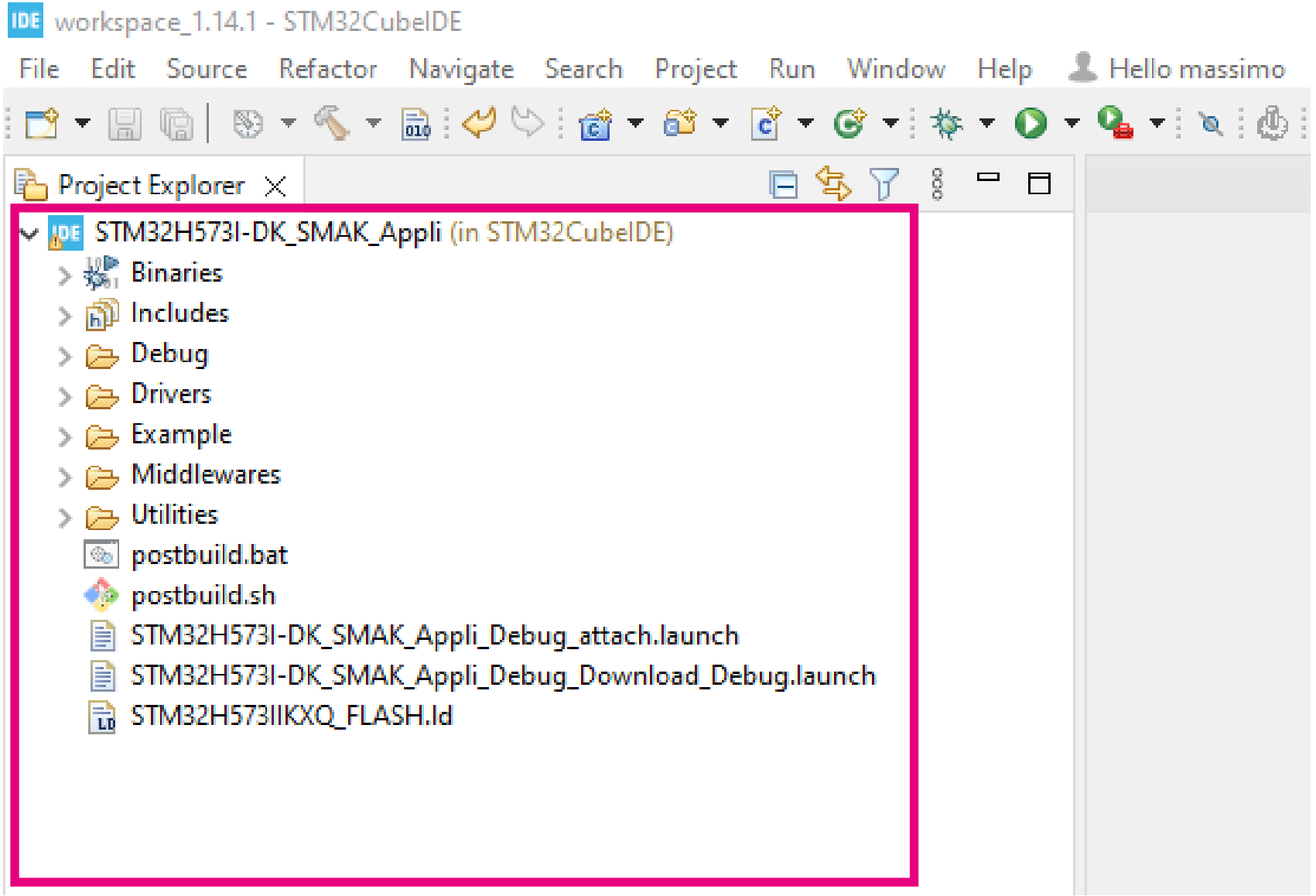
Import SMAK application in the IDE



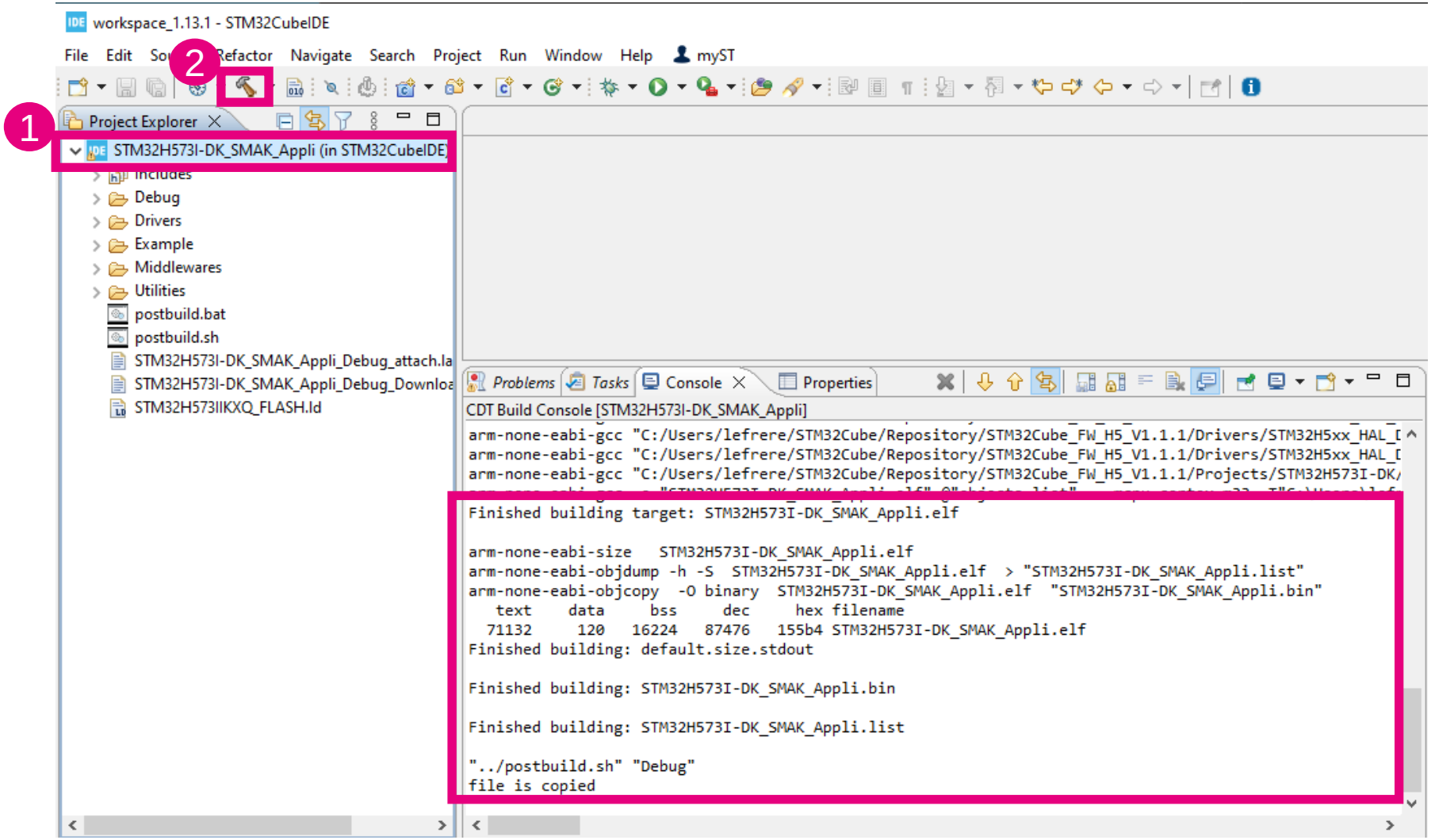
Import SMAK application in the IDE



Import SMAK application in the IDE

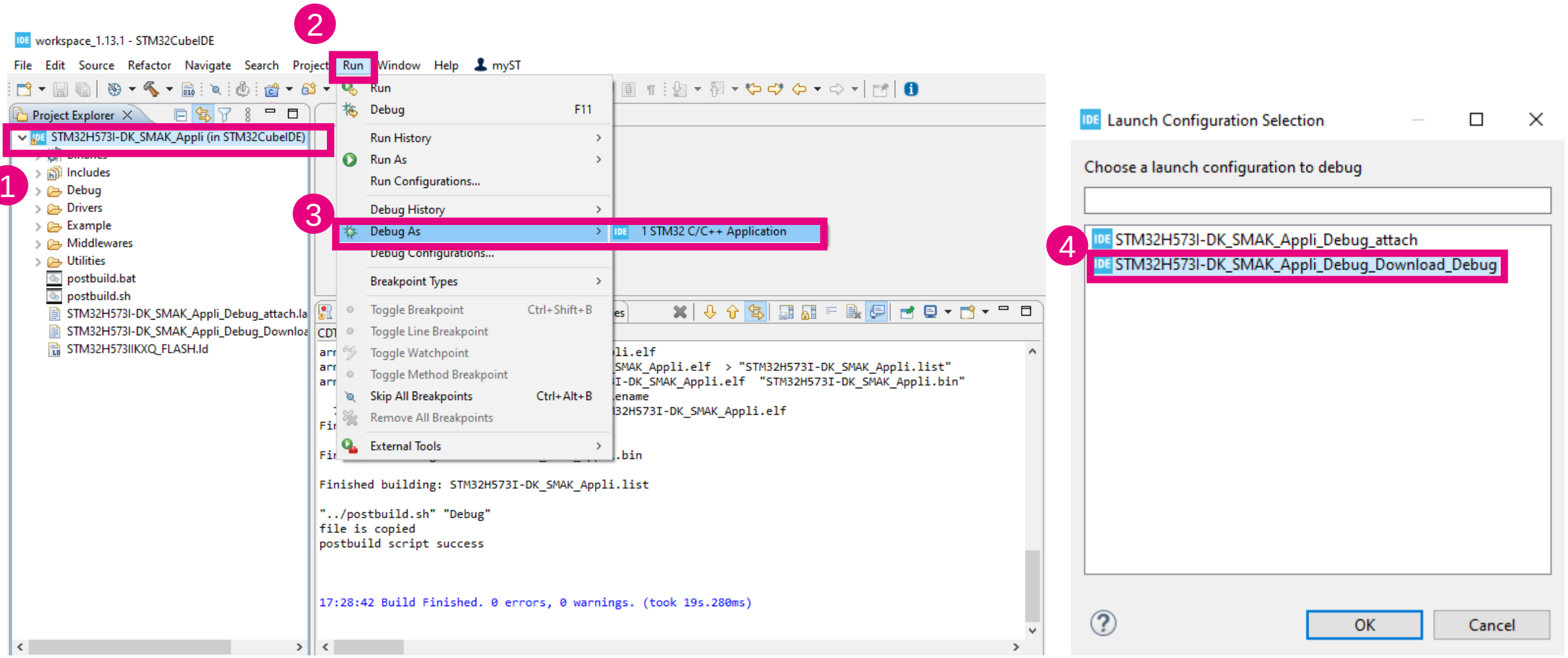


Compile SMAK application

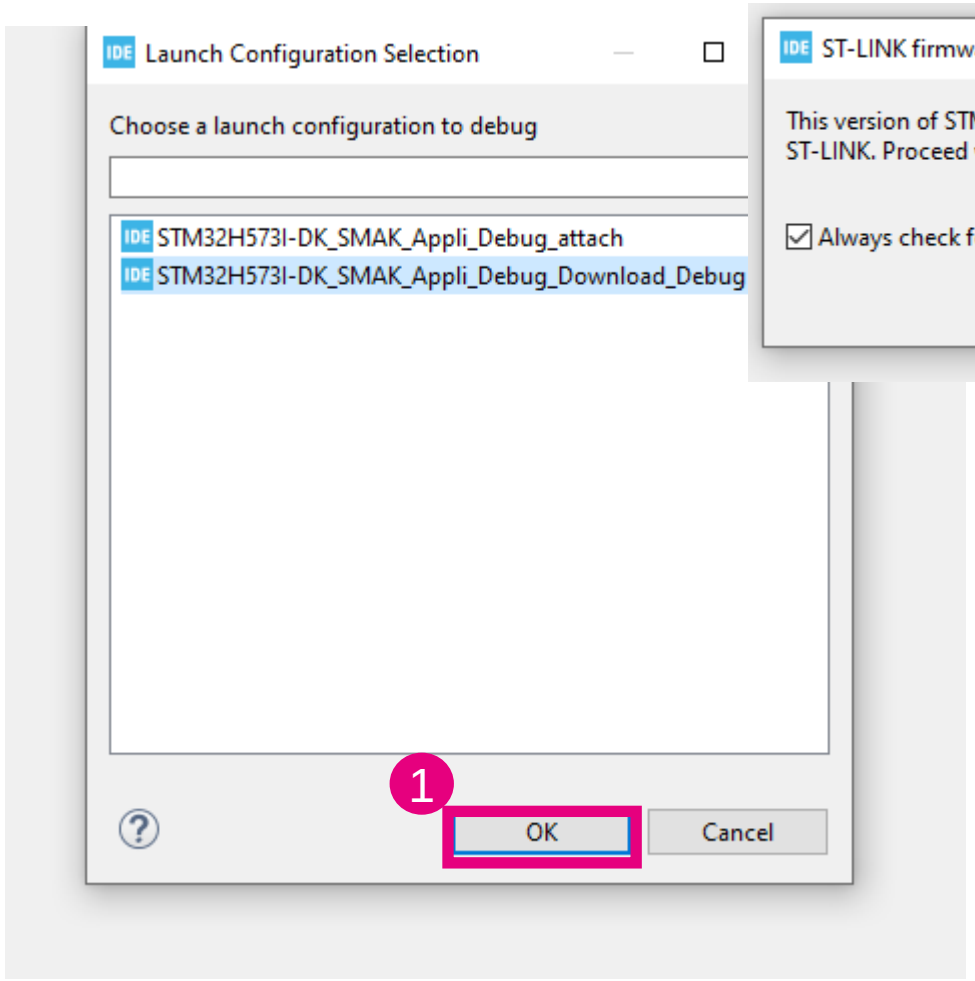


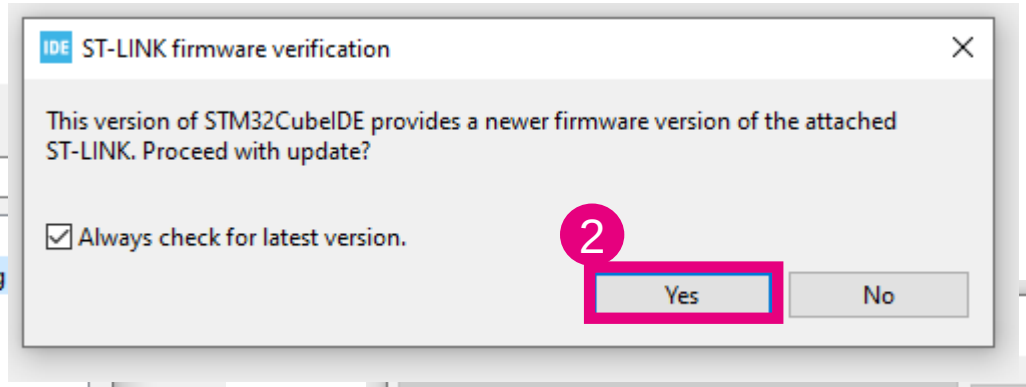
life.augmented

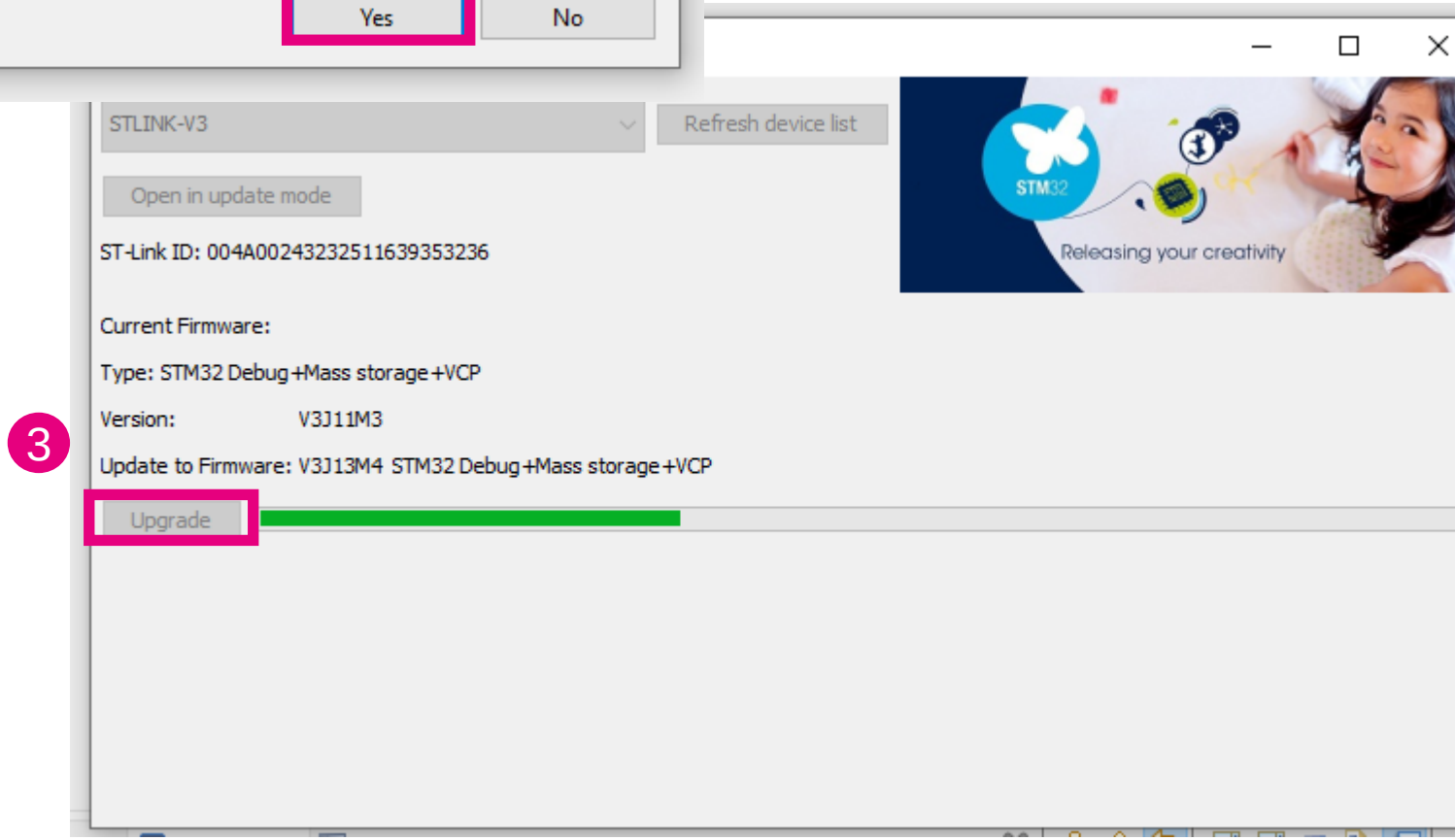
Load and debug the SAMK application



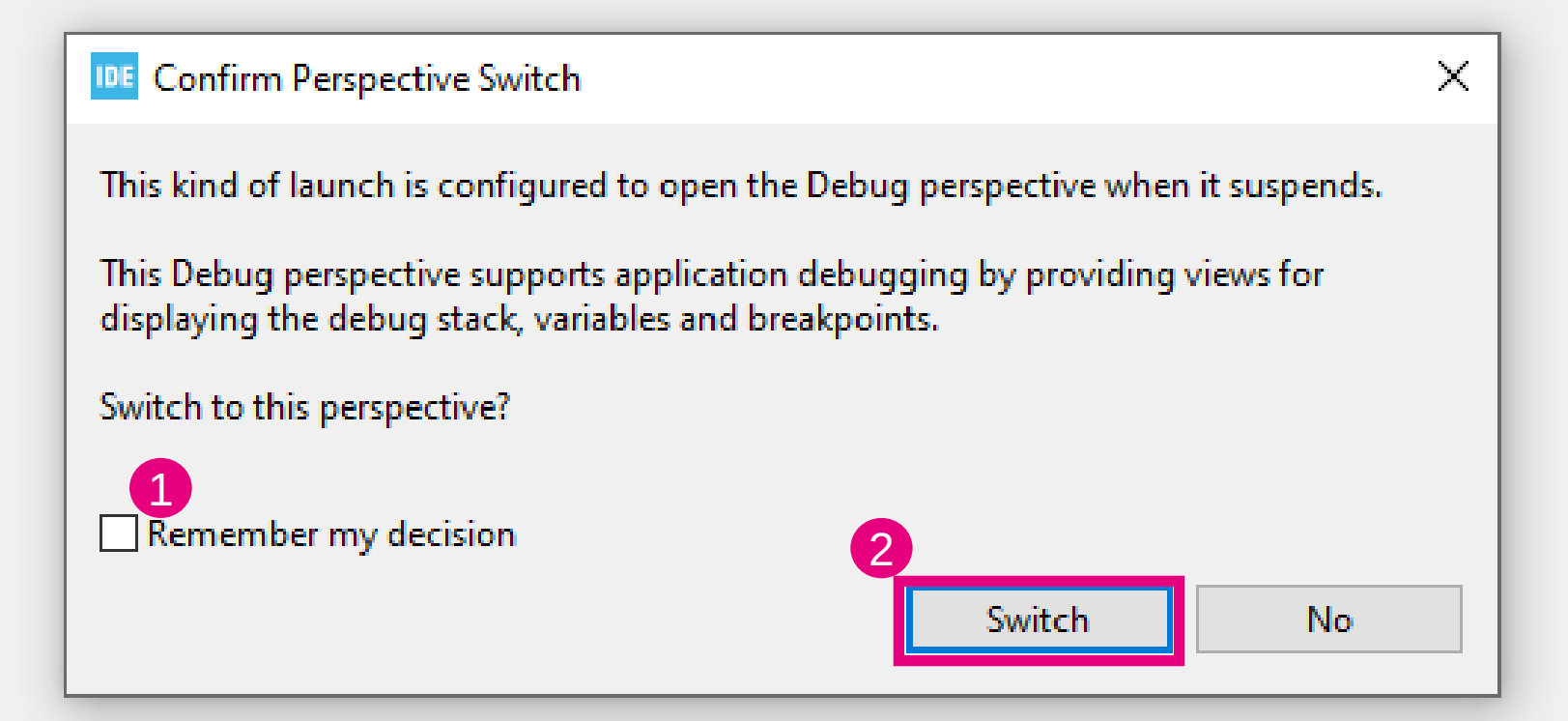
Update ST-LINK if asked







Activate Debug Perspective

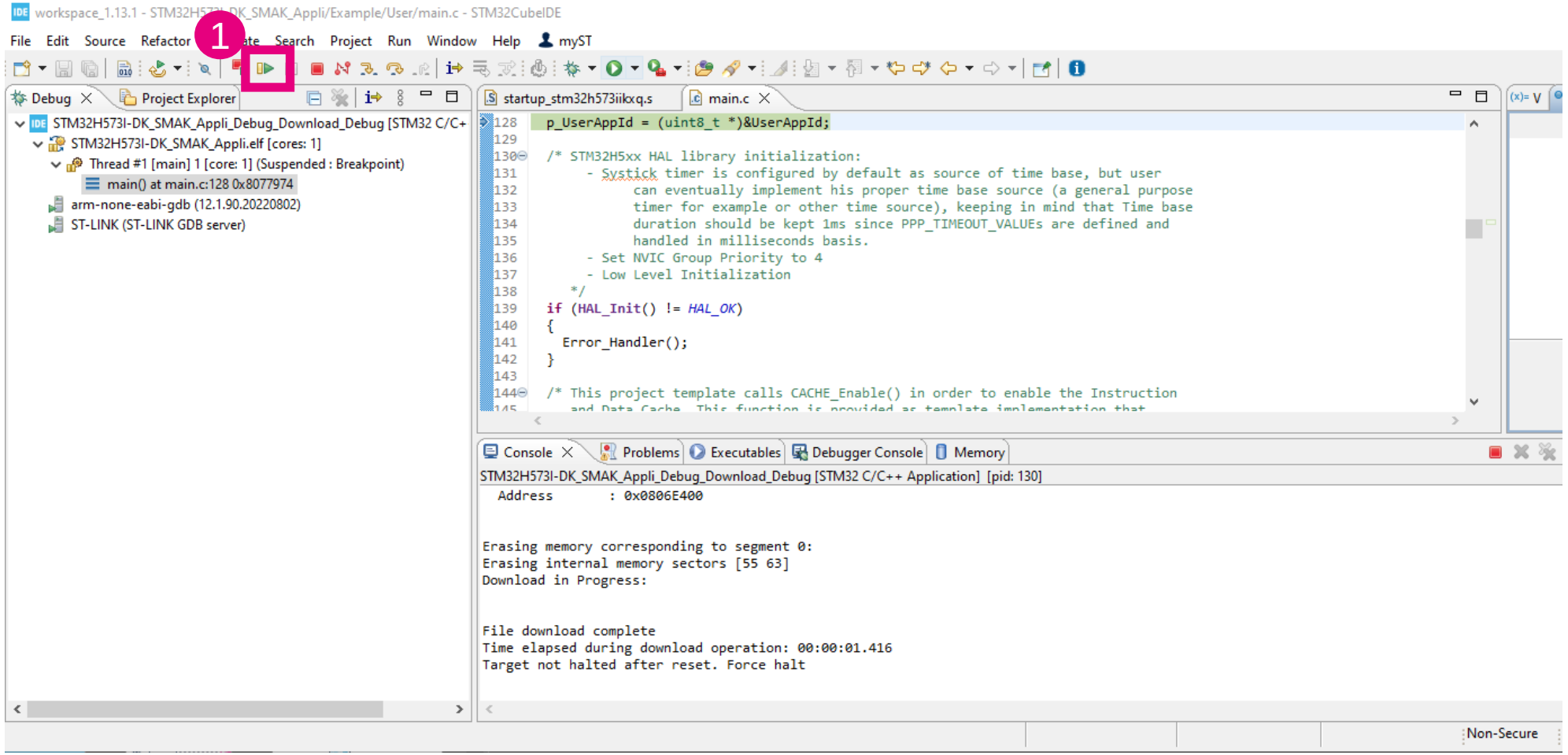


SMAK application debug

- 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

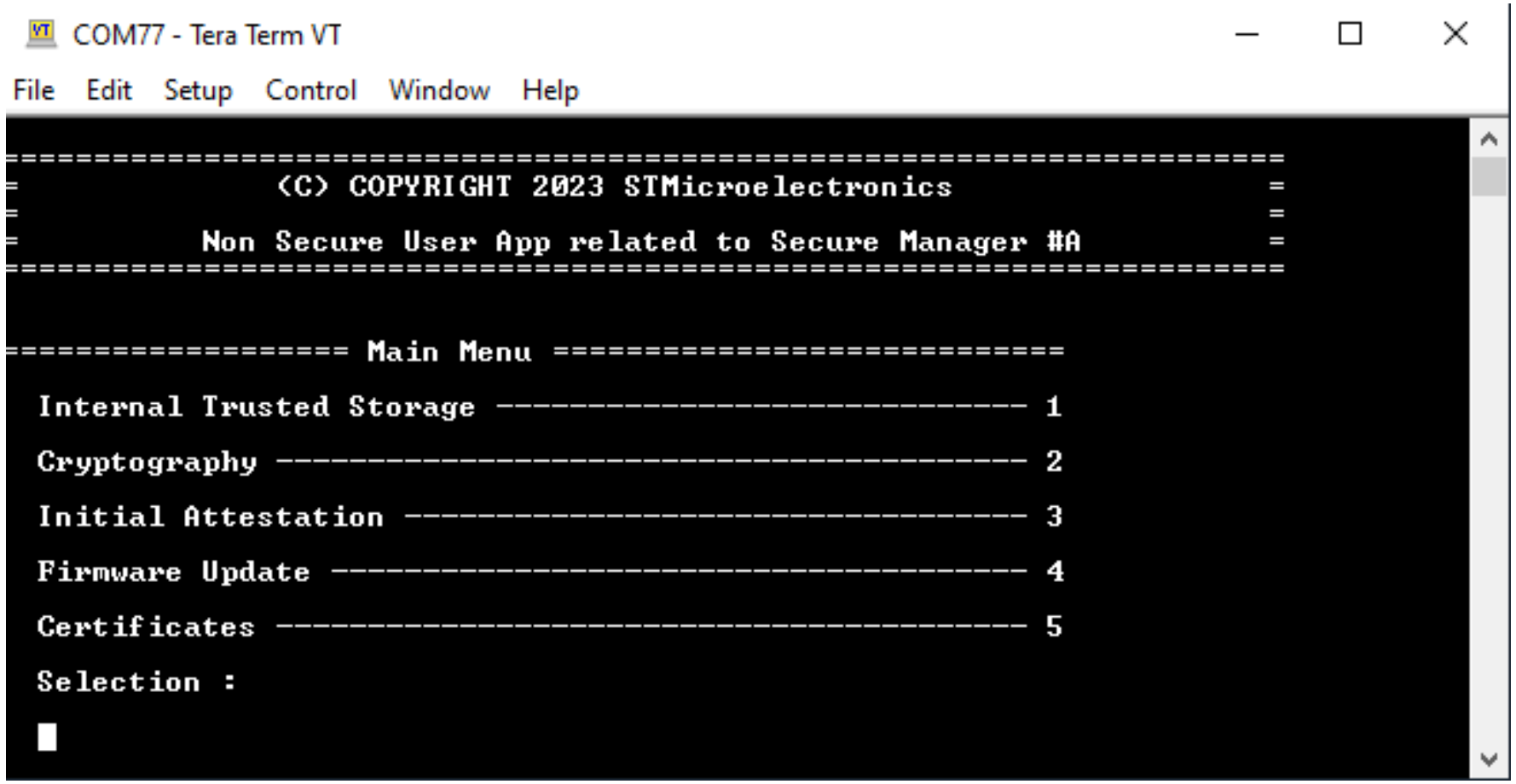
Launch the SMAK appli



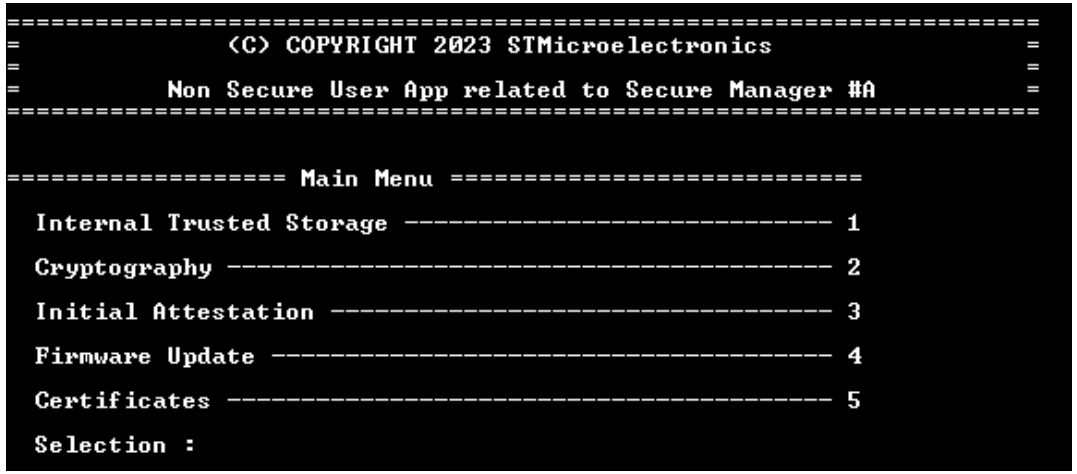
Hands-on: NS Application and Secure Manager services

life.augmented

SMAK appli UI

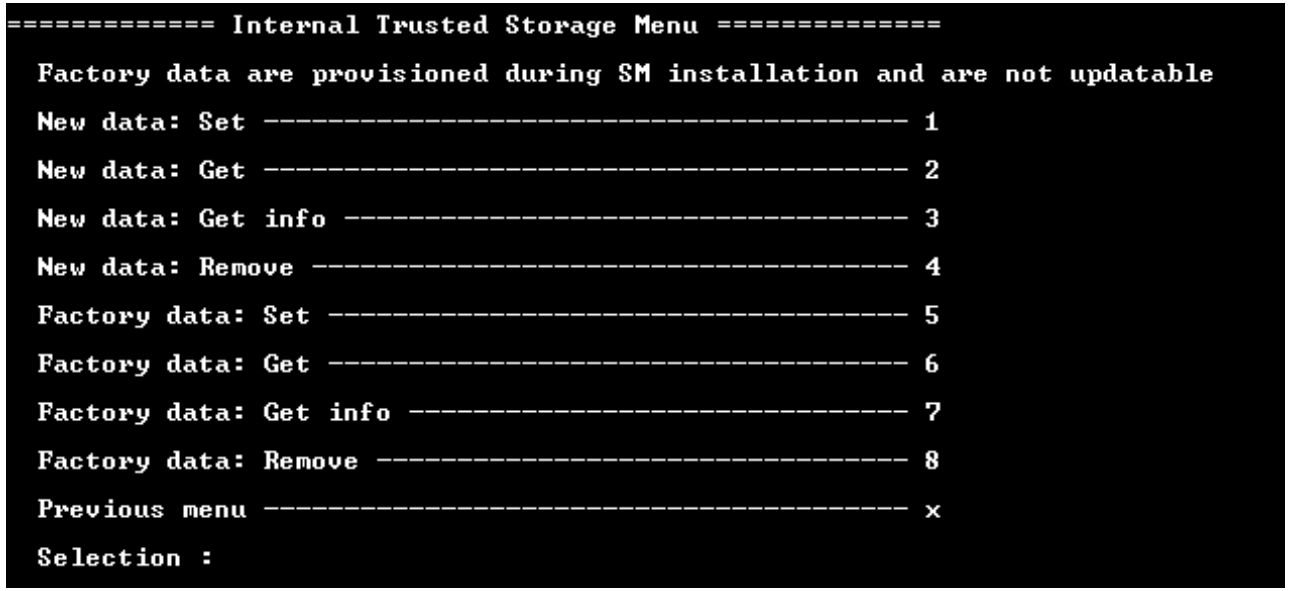


SMAK appli UI



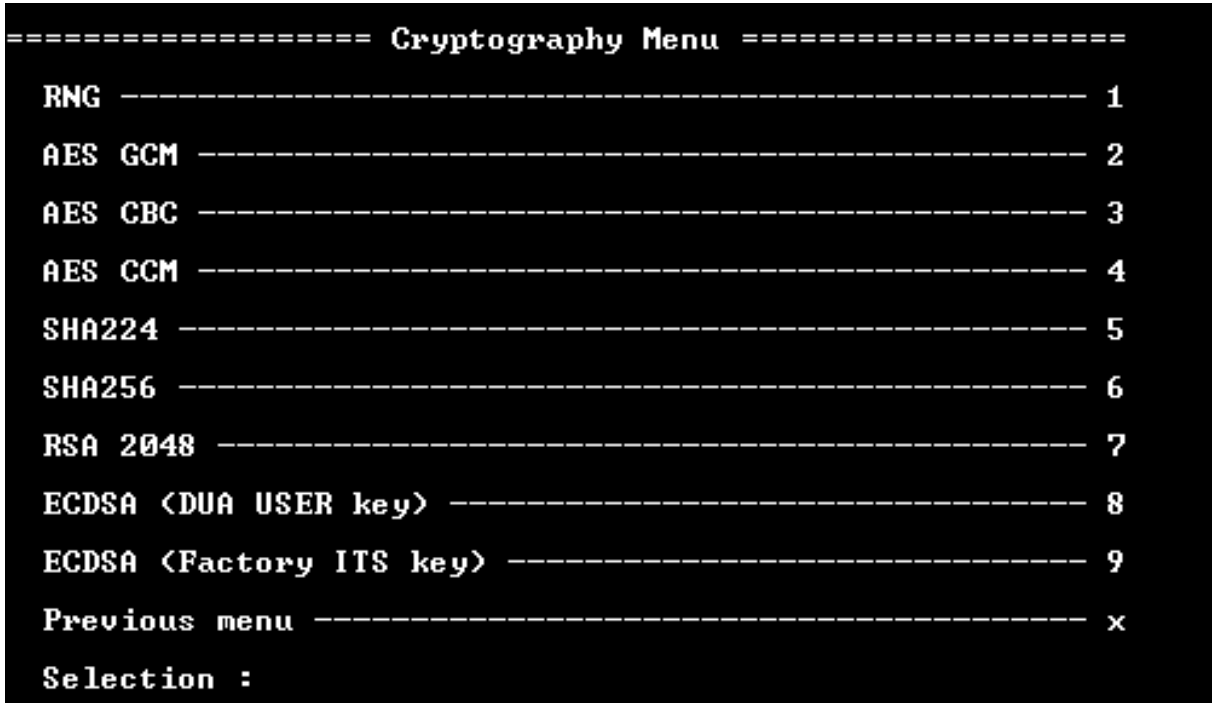
- SMAK example application provides implementation of PSA API for each service category (1 to 4)
- Item 5 does not use PSA API. Just displays the X509 certificates provided by the platform

Internal Trusted Storage



- 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

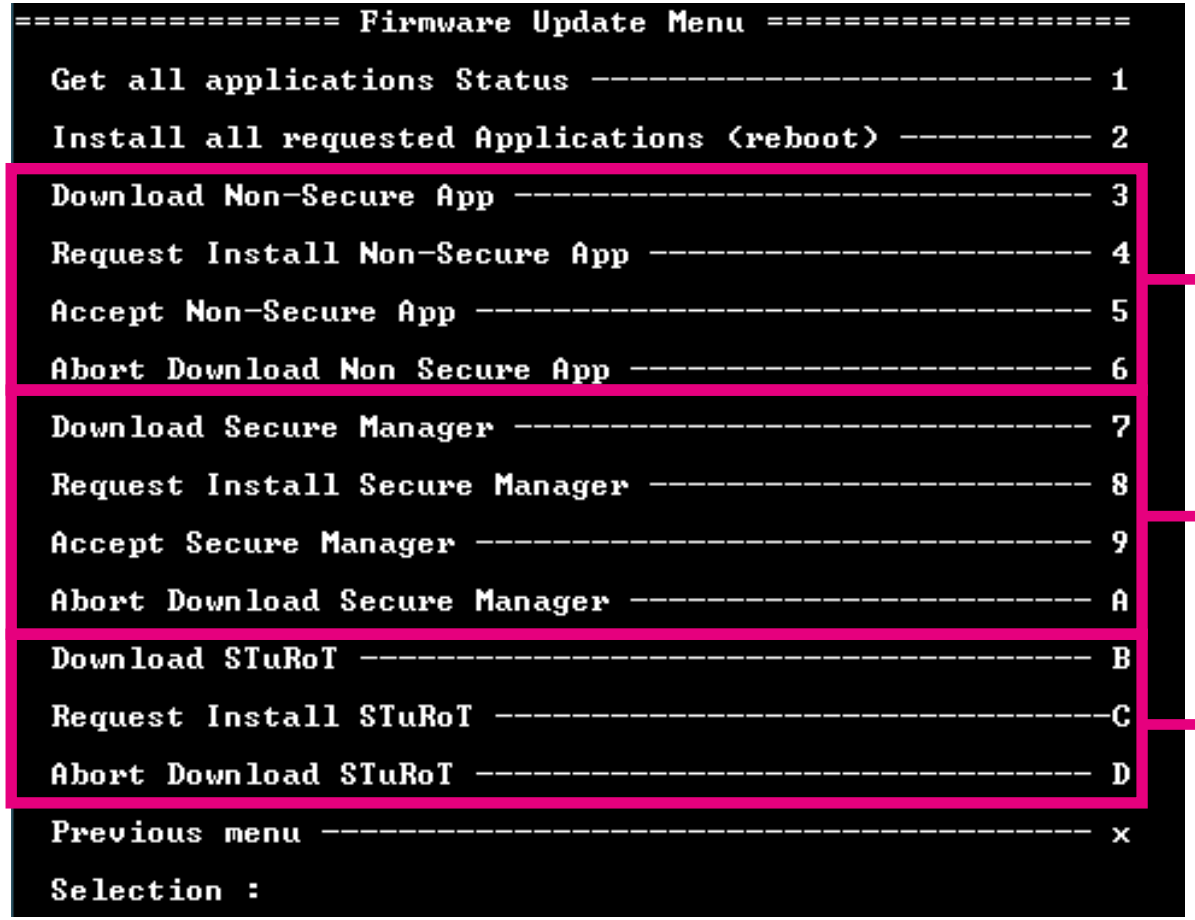


- Set of examples of PSA Crypto API usage

Initial Attestation

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

Firmware Update



→ Secure User application update

→ Secure manager update

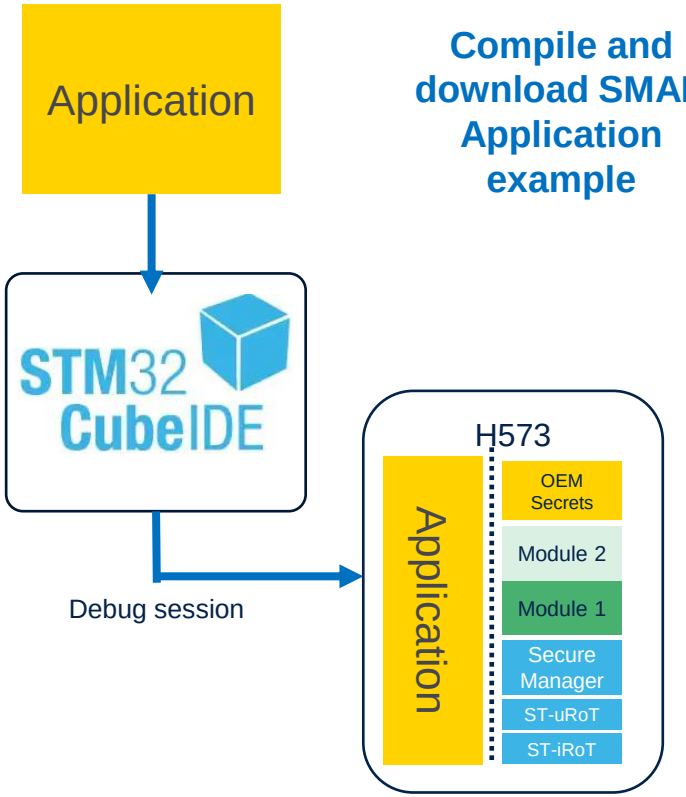
→ Secure ST-uROT (2nd stage bootloader) update

Certificate

- Display both certificate content in X509 pem format

SMAK Development Flow

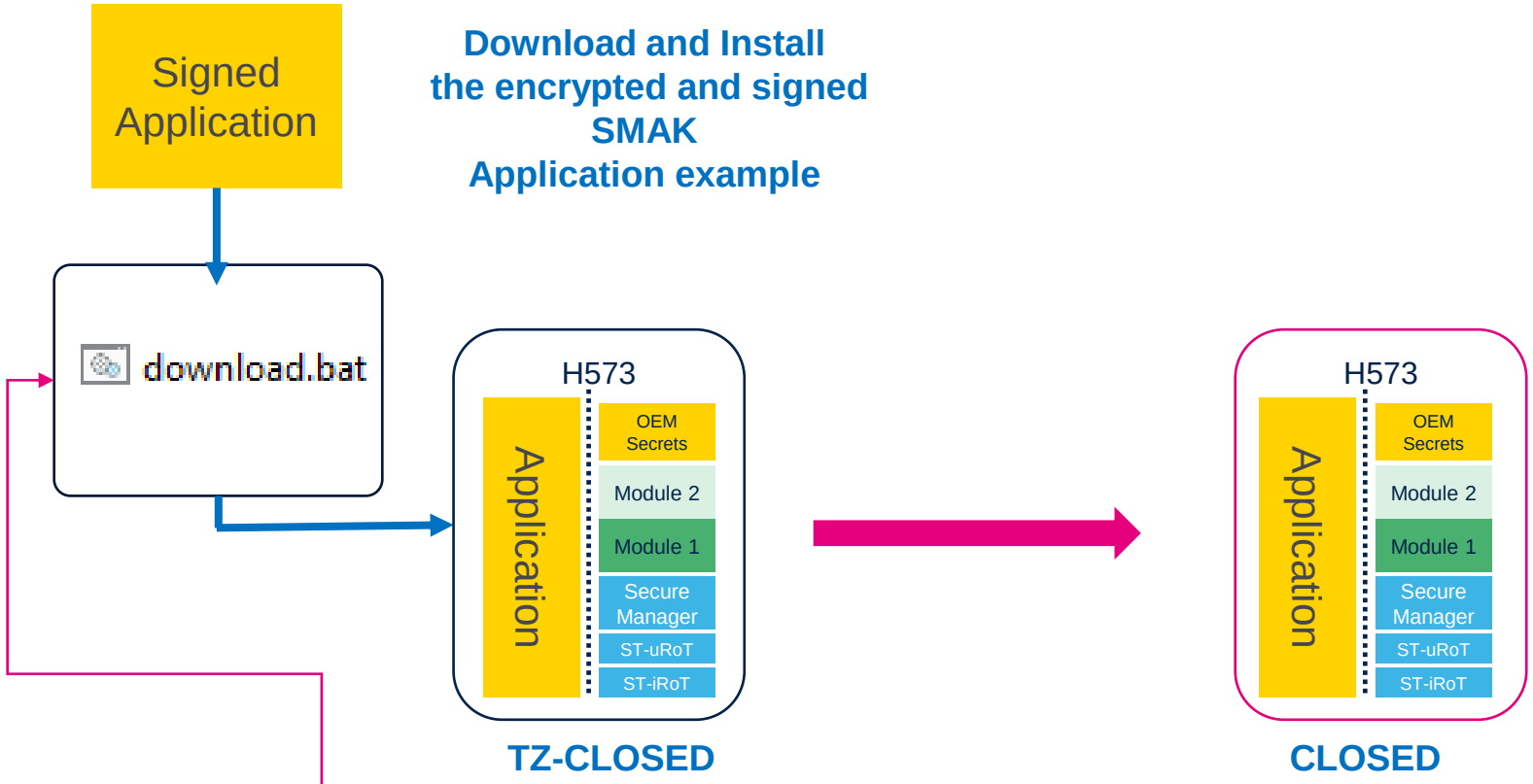
Application Development Flow



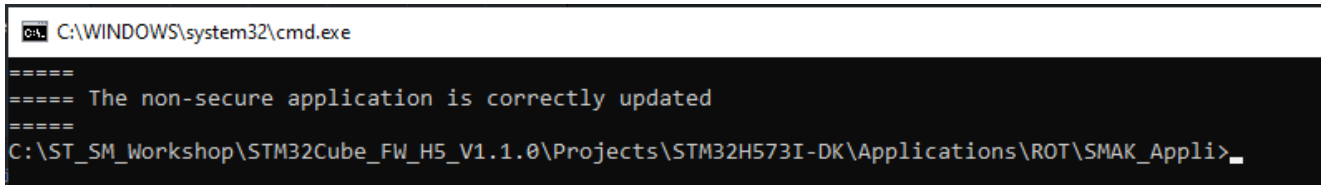
Development completed

SMAK Installation Flow

Application Installation Flow



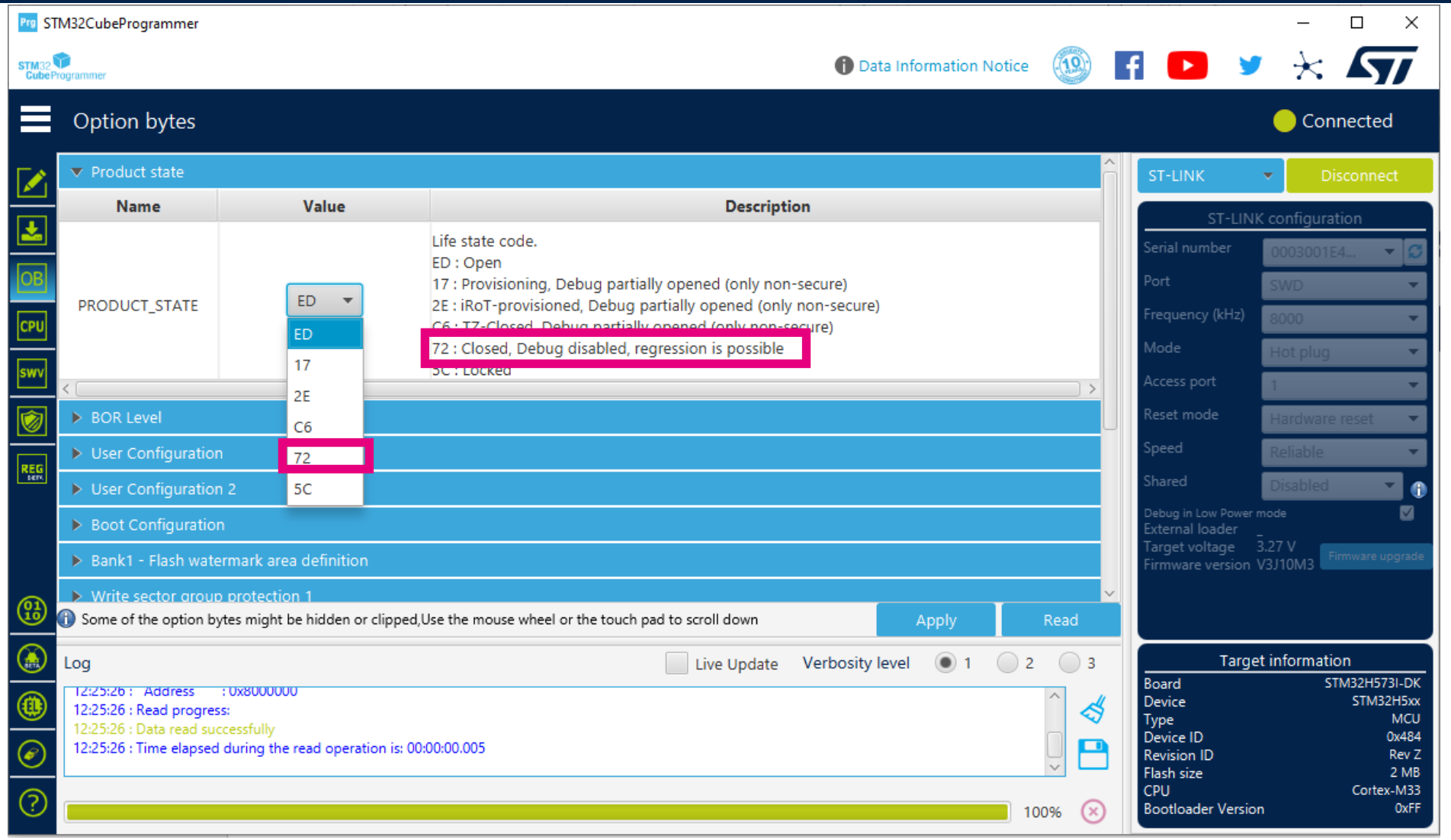
STM32Cube_FW_H5_V1.2.0\Projects\STM32H573I-DK\Applications\ROT\SMAK_Appli



life.augmented

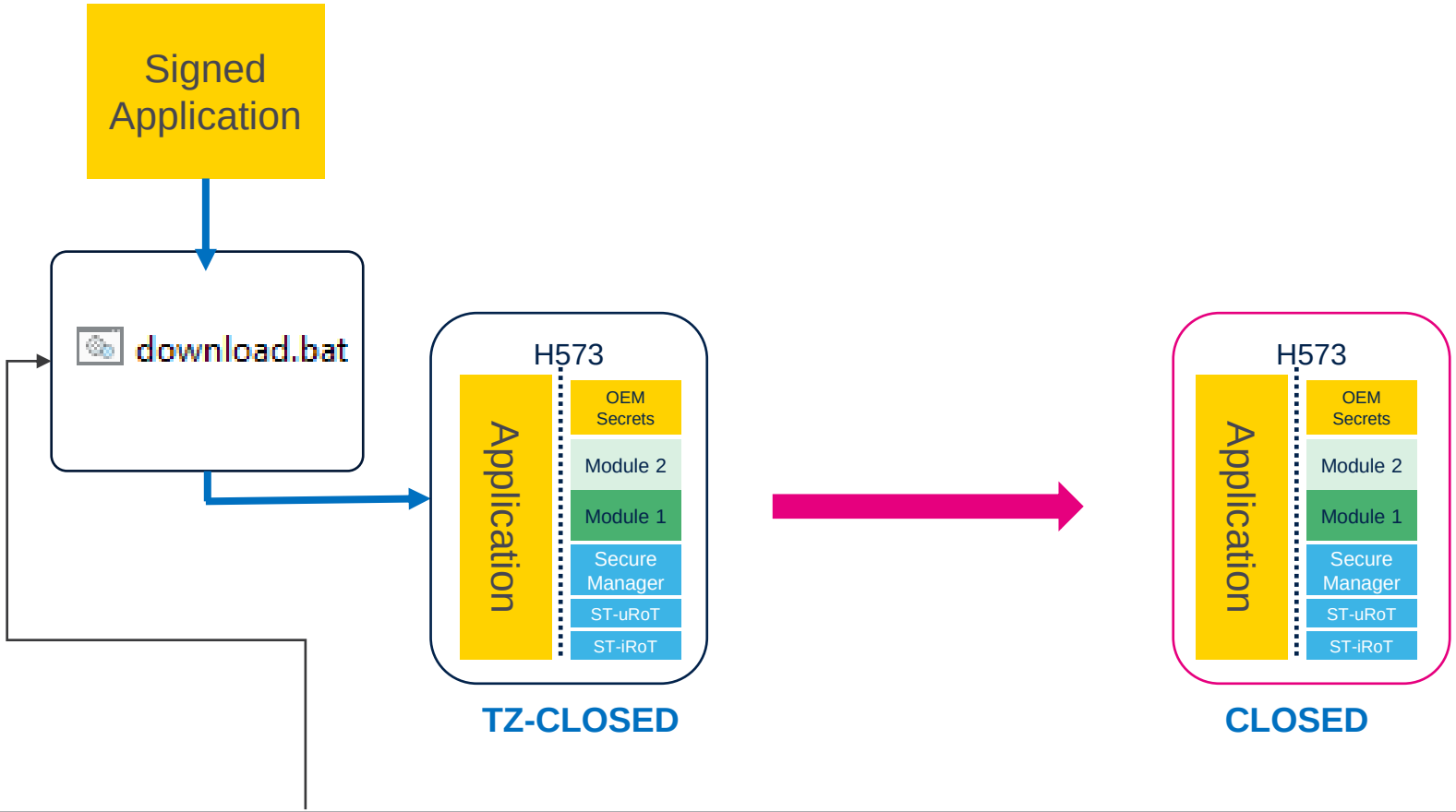
Secure Manager Ecosystem

Set device in CLOSED state



SMAK Installation Flow

Application Installation Flow



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

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

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