life.augmented

STM32Trust

STM32H5 Security
Secure Manager - Part 5

Hands On:
Debug Authentication

Presenter: Rishi Shukla

Agenda

I Debug Authentication Overview

II Debug Authentication Ecosystem

III Hands-On: Debug Re-Opening and Regression

IV Resources

life.augmented

Debug Authentication Overview

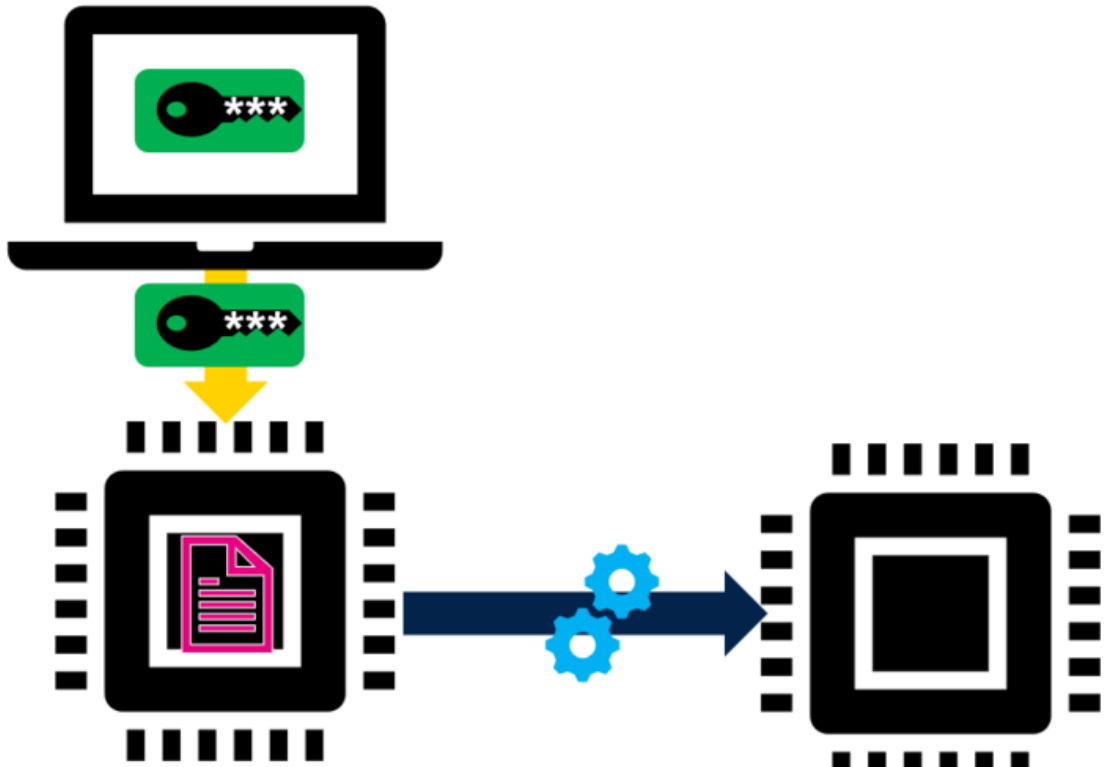
What is Debug Authentication?

- The user leverages the debug authentication security feature to perform:
  - Secure regression to OPEN (full regression) or TZ-CLOSED (partial regression) product states, erasing user data in user flash memory, SRAM and OBKeys.
  - Safely re-open debug access on the STM32

- Debug Authentication usage is different depending on the TrustZone activation:
  - Password based (In TZ disabled applications)
  - Certificate based (In TZ enabled applications)

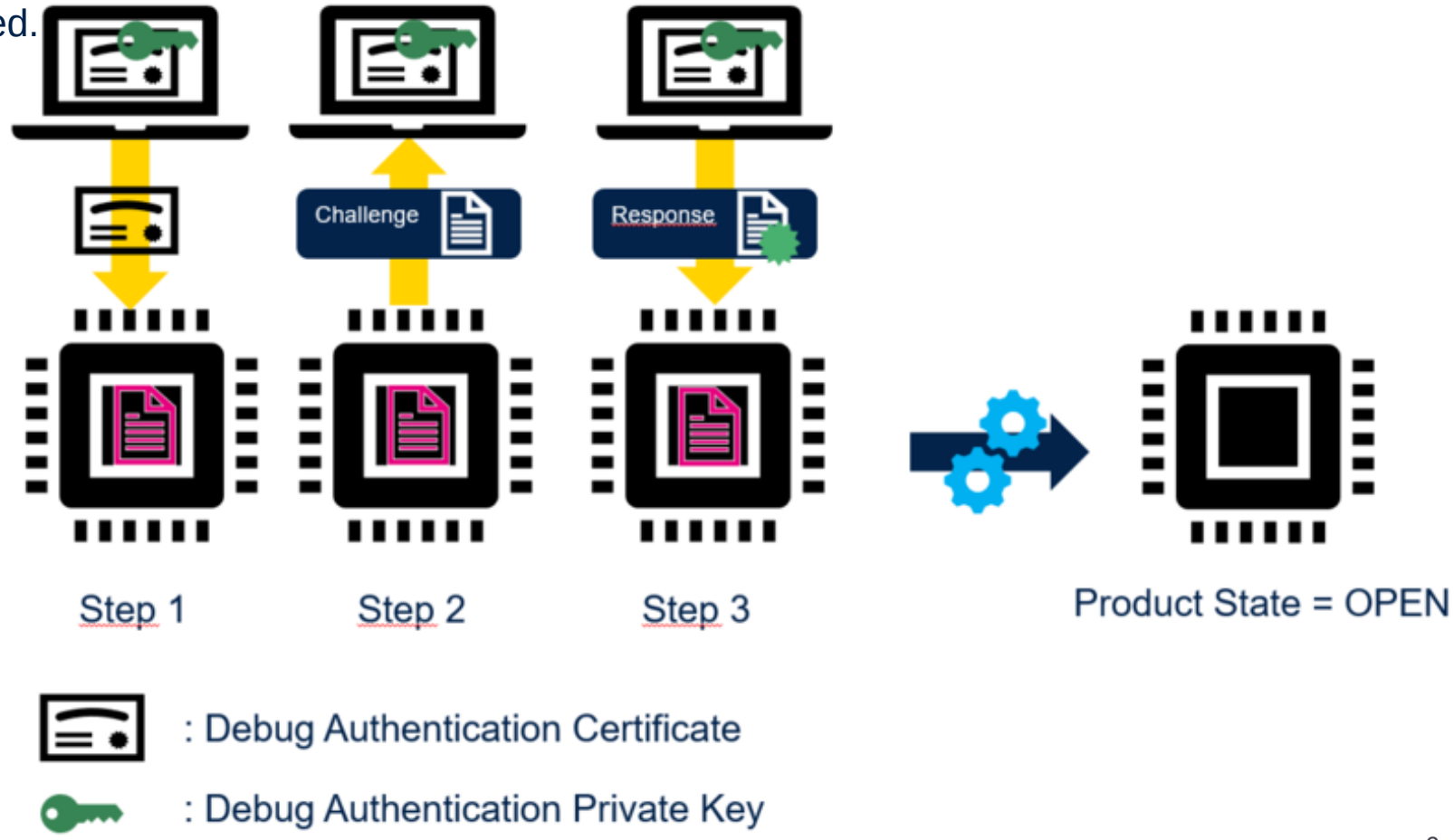
DA: Password based

- In order to access the debug authentication feature, the host sends the debug authentication password to the STM32. When the STM32 receives the hash of the password, it verifies that it corresponds to the one that is provisioned.

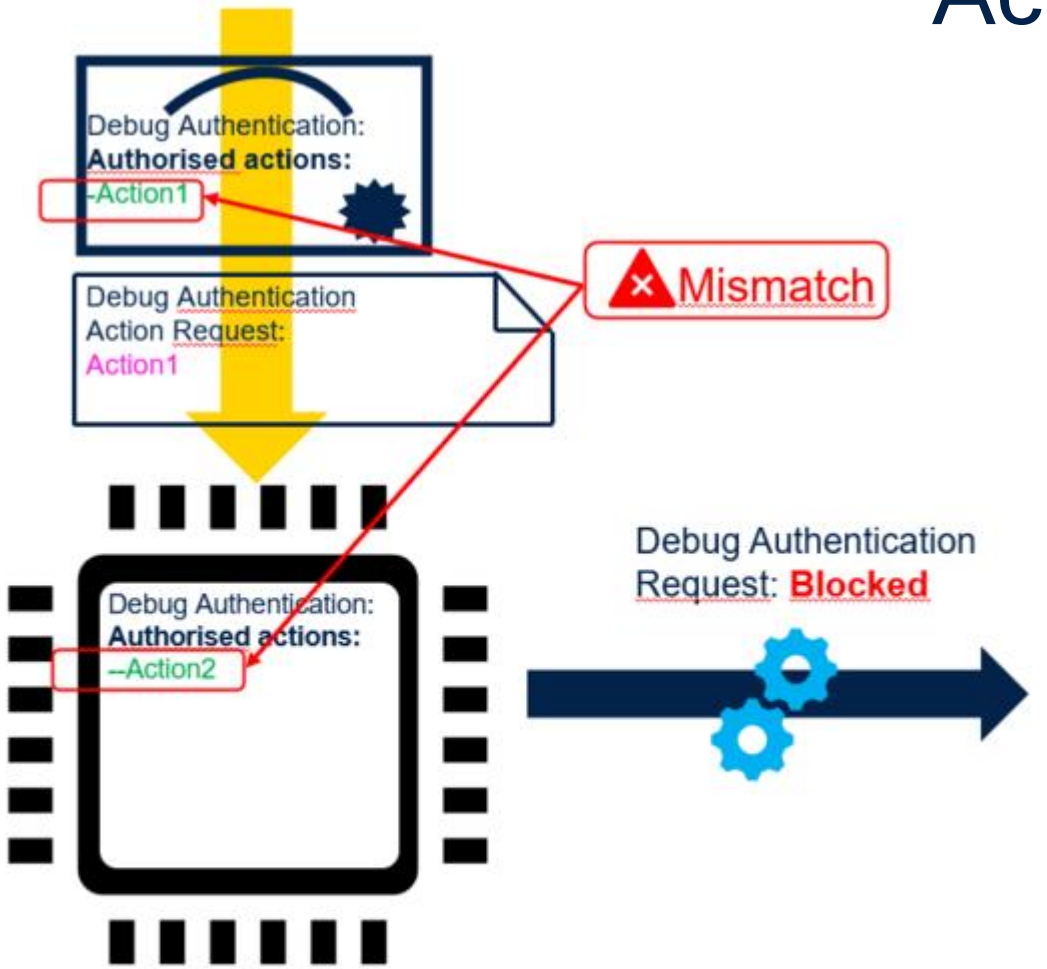


DA: Certificate based

- When the user access the debug authentication feature (regression or debug re-opening), he sends first a certificate and a debug authentication action request to the STM32. When the STM32 receives the certificate, it verifies that:
  - Certificate fits the one that is provisioned.
  - The authorized actions sent with the certificate match the ones provisioned.
  - The action request matches the authorized action list carried by the certificate.

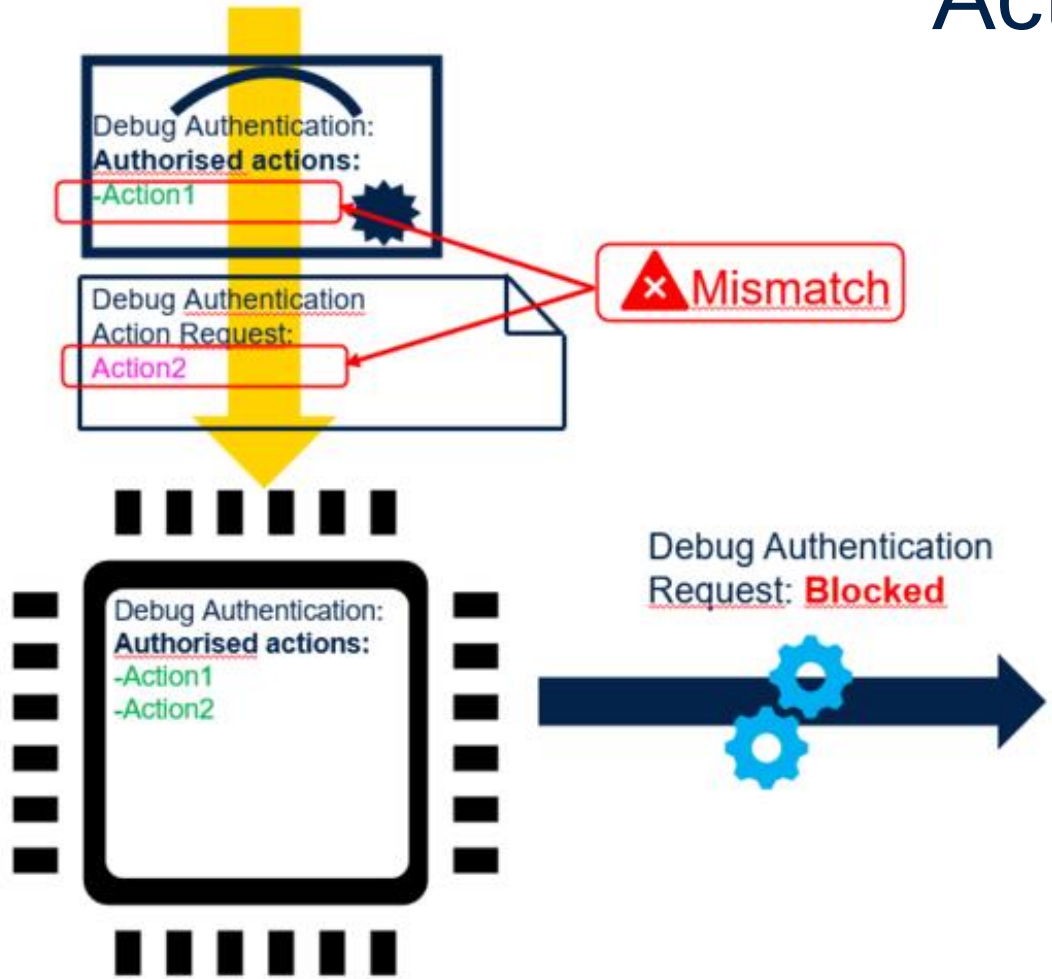


Actions Request 1/2



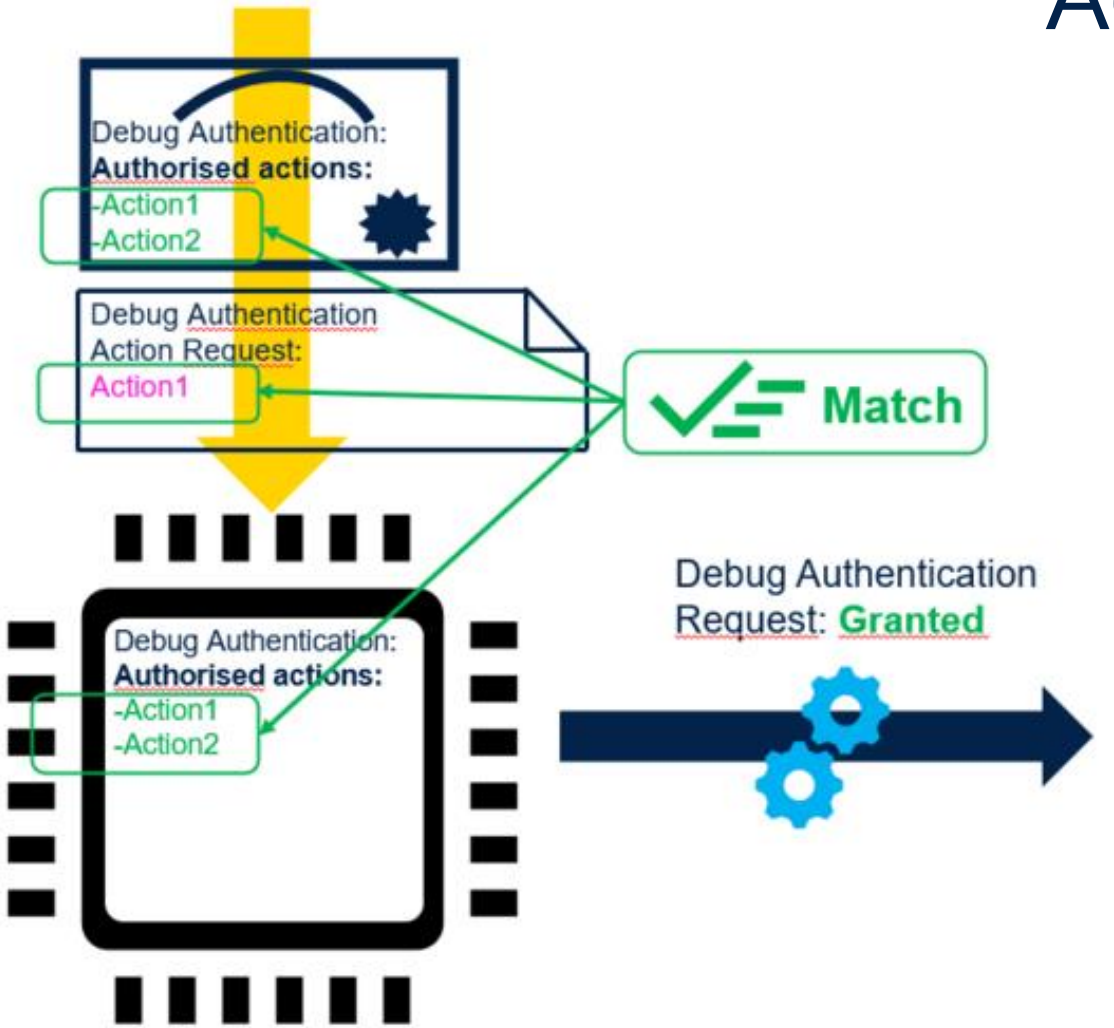
: Debug Authentication Certificate

Actions Request 2/2



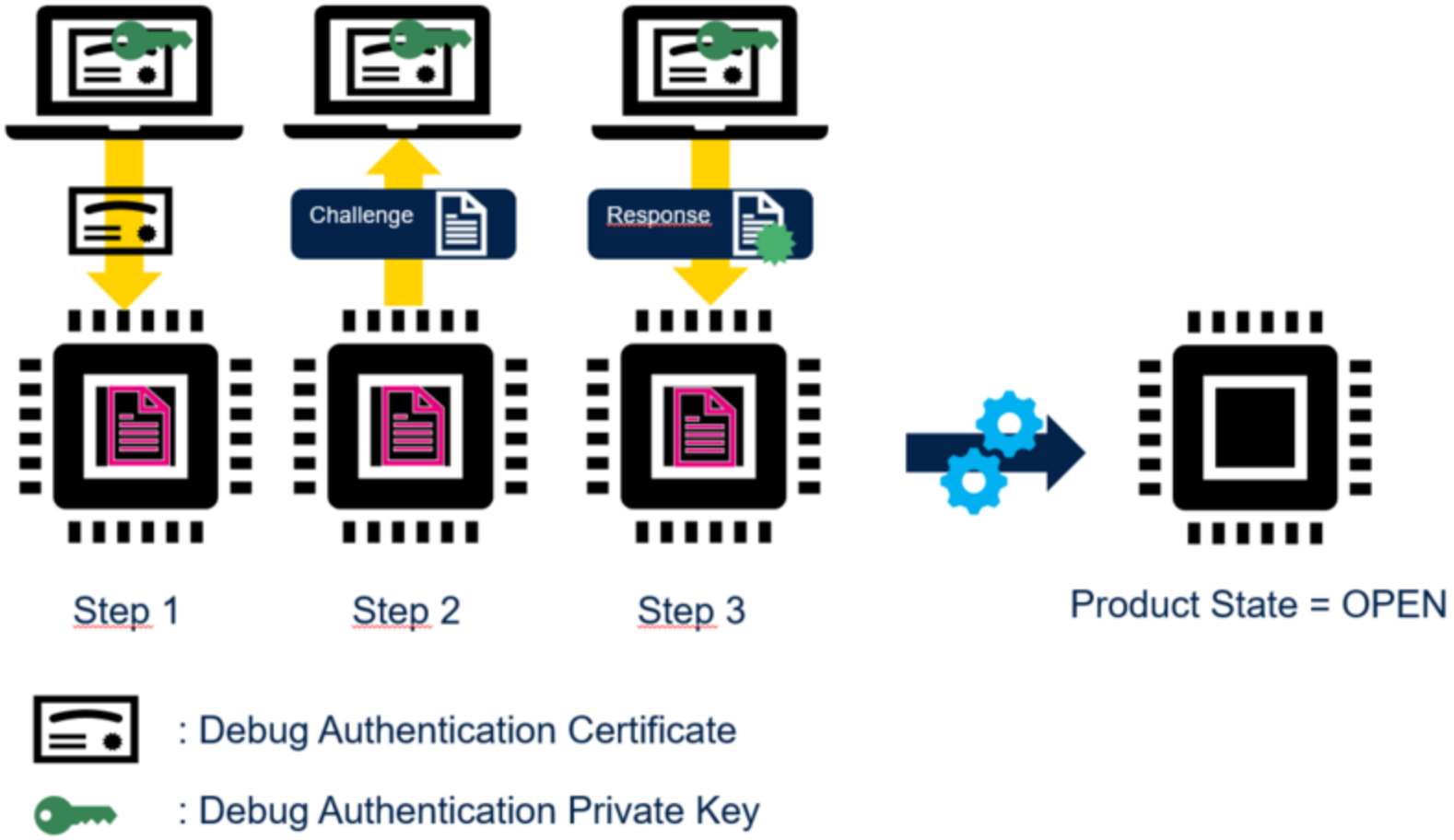
: Debug Authentication Certificate

Actions Request

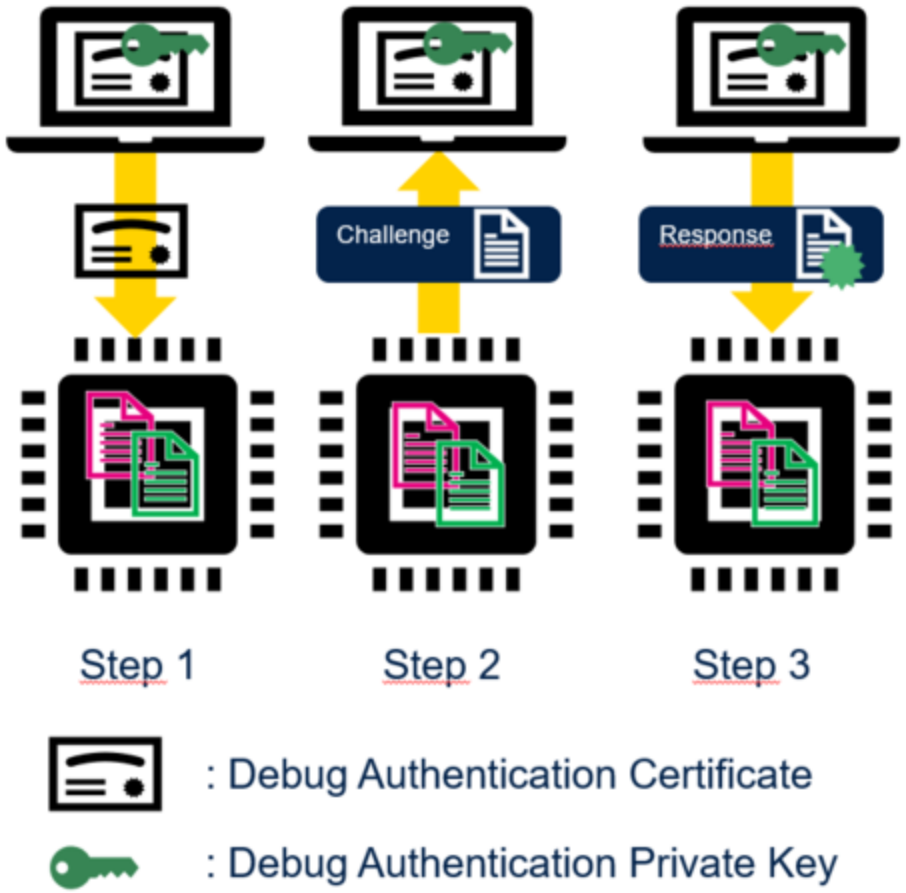


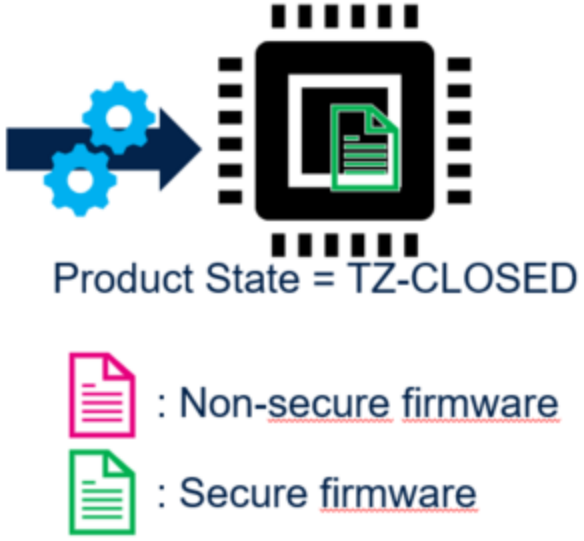
: Debug Authentication Certificate

Regression: Full

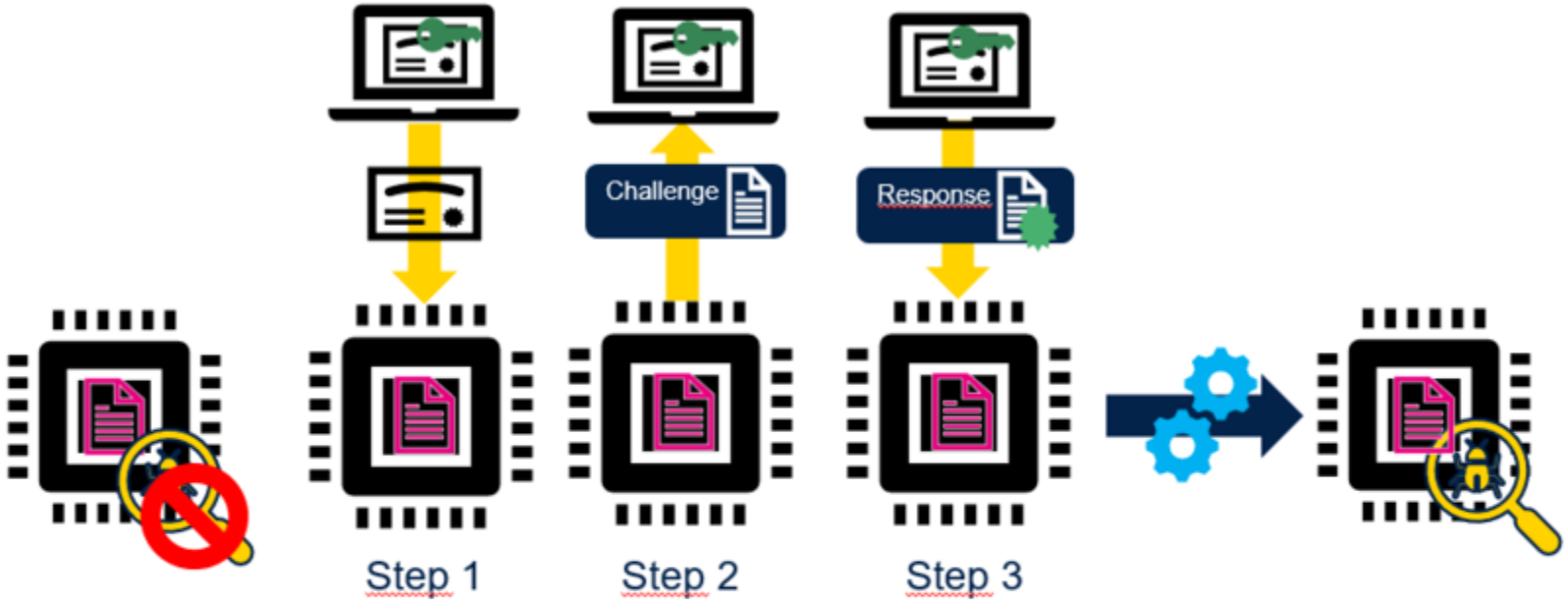


Regression: Partial





Debug Re-opening

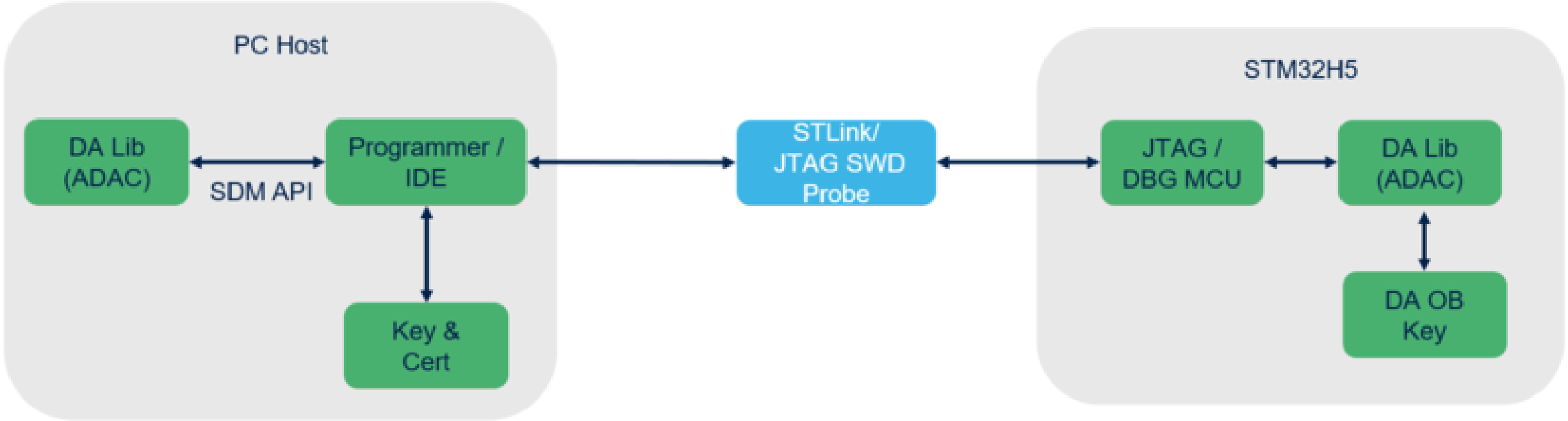


: Debug Authentication Certificate

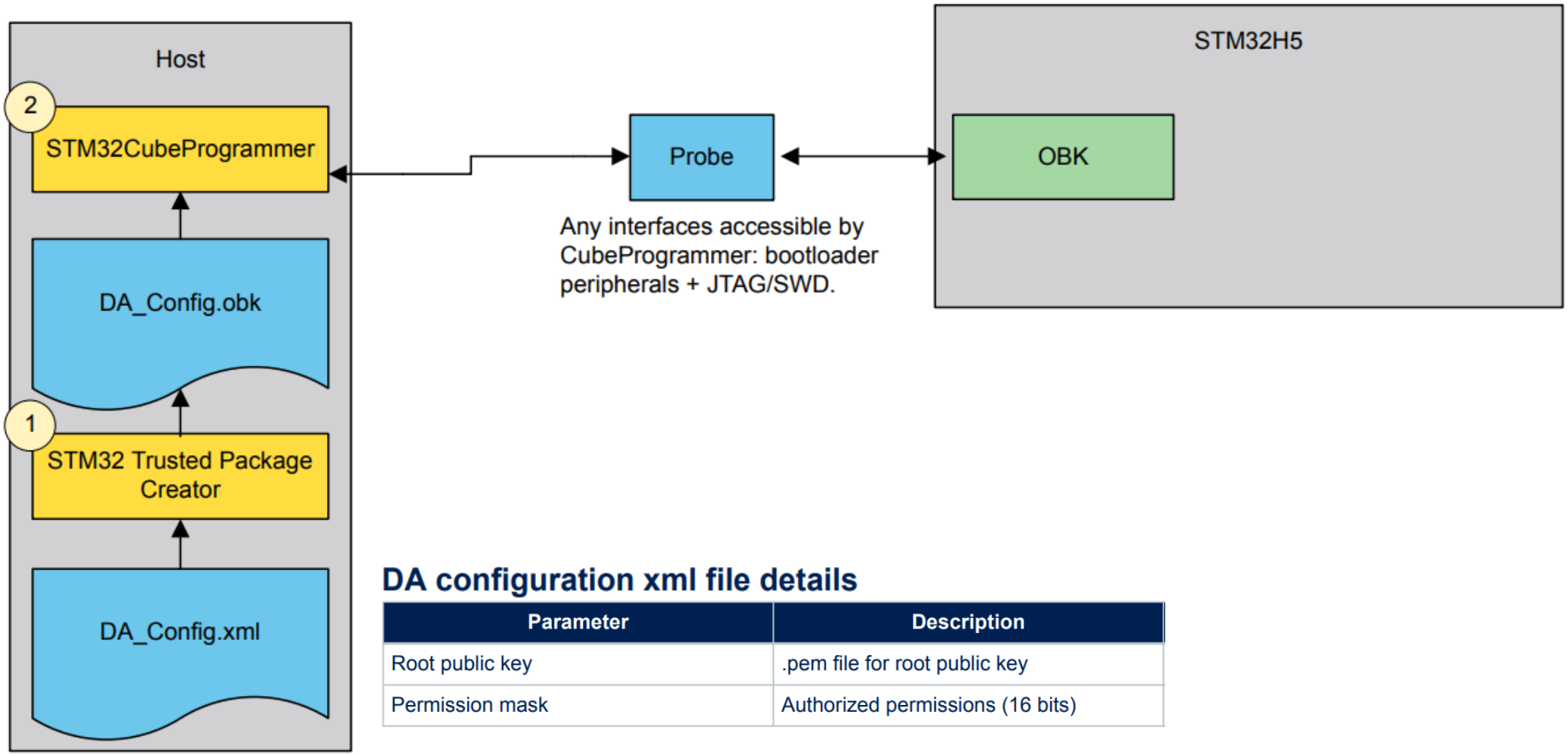
: Debug Authentication Private Key

Debug Authentication Ecosystem

Debug Authentication Ecosystem



Ecosystem: Provisioning phase

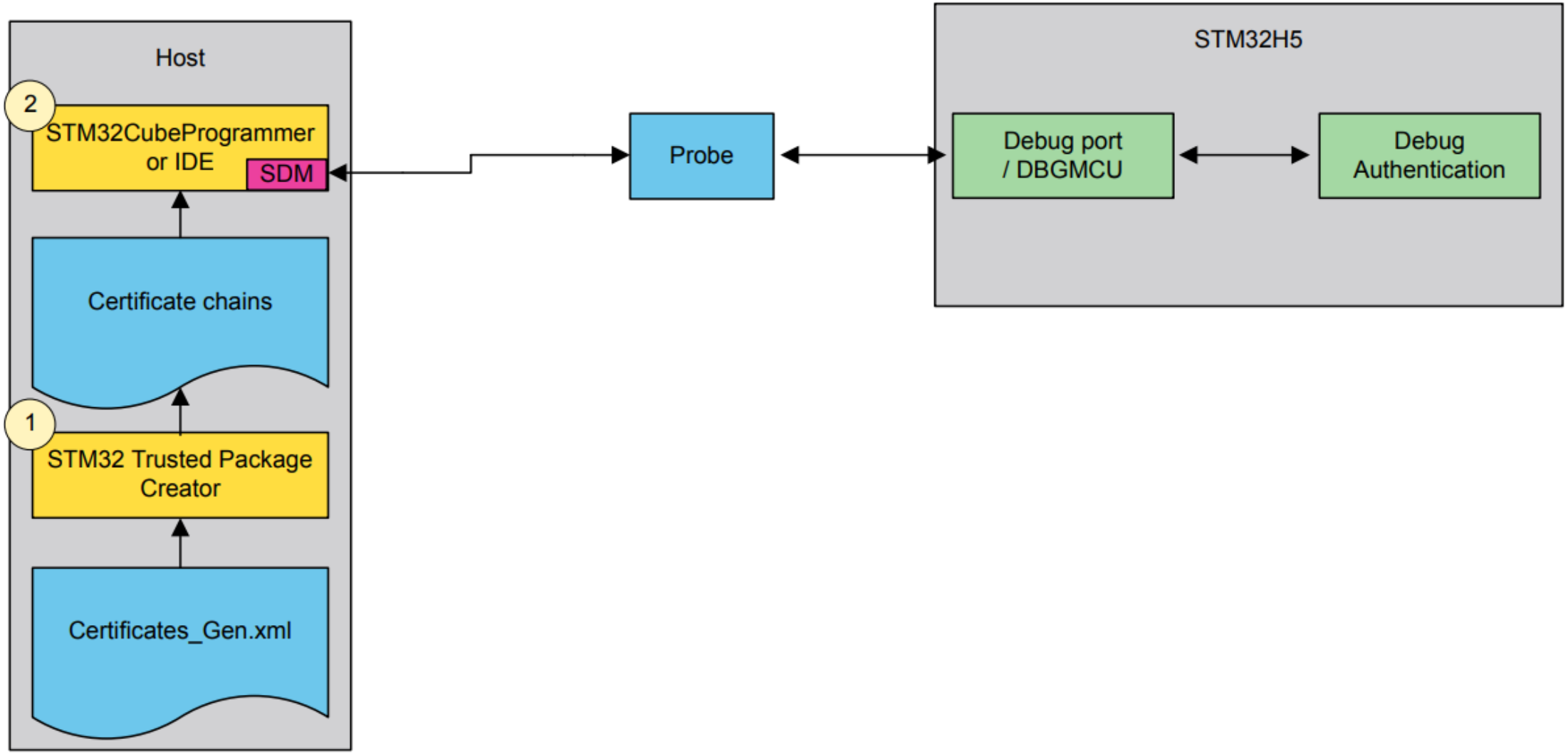


DA configuration xml file details

Parameter	Description
Root public key	.pem file for root public key
Permission mask	Authorized permissions (16 bits)

life.augmented

Ecosystem: Launch DA (certificate method)



How To: Create new certificate

- Instructions available in section 6.2 of the following Wiki page.

Use Case

- Development is completed and device is released in closed state
- Our product is on the field, unfortunately some devices are not working fine…
- Customer returned the product to the support team

Let’s see what the support team can do

Hands-on:
Debug re-opening and regression

First possibility: re-open the debug

- What do we need ?
  - A certificate that allows reopening the device for debug and regression (leaf certificate)

C:\...\ROT_Provisioning\DA\Certificates\cert_leaf_chain.b64

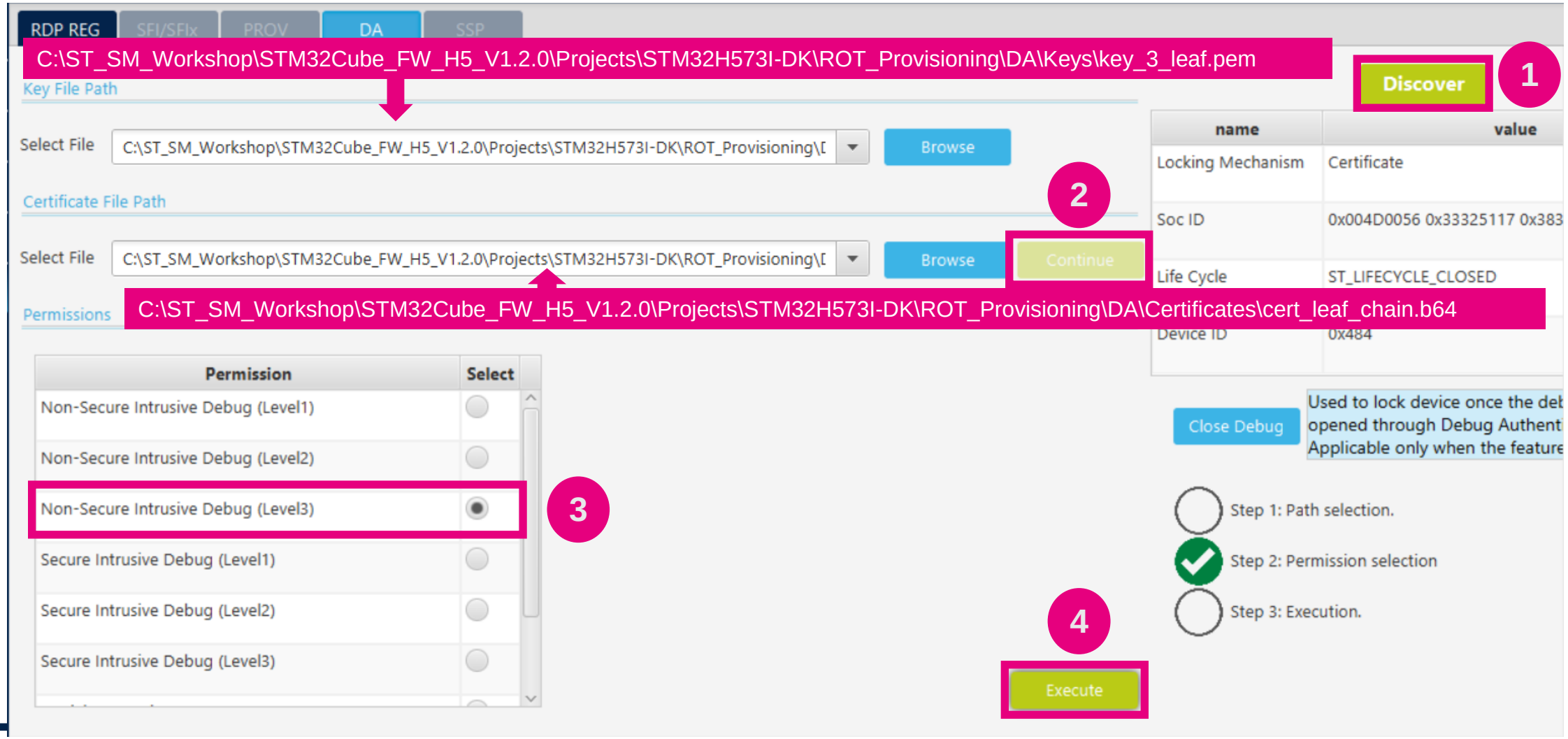
  - The associated private ECC key

C:\...\ROT_Provisioning\DA\Keys\key_3_leaf.pem

Let’s reopen the device for debug !

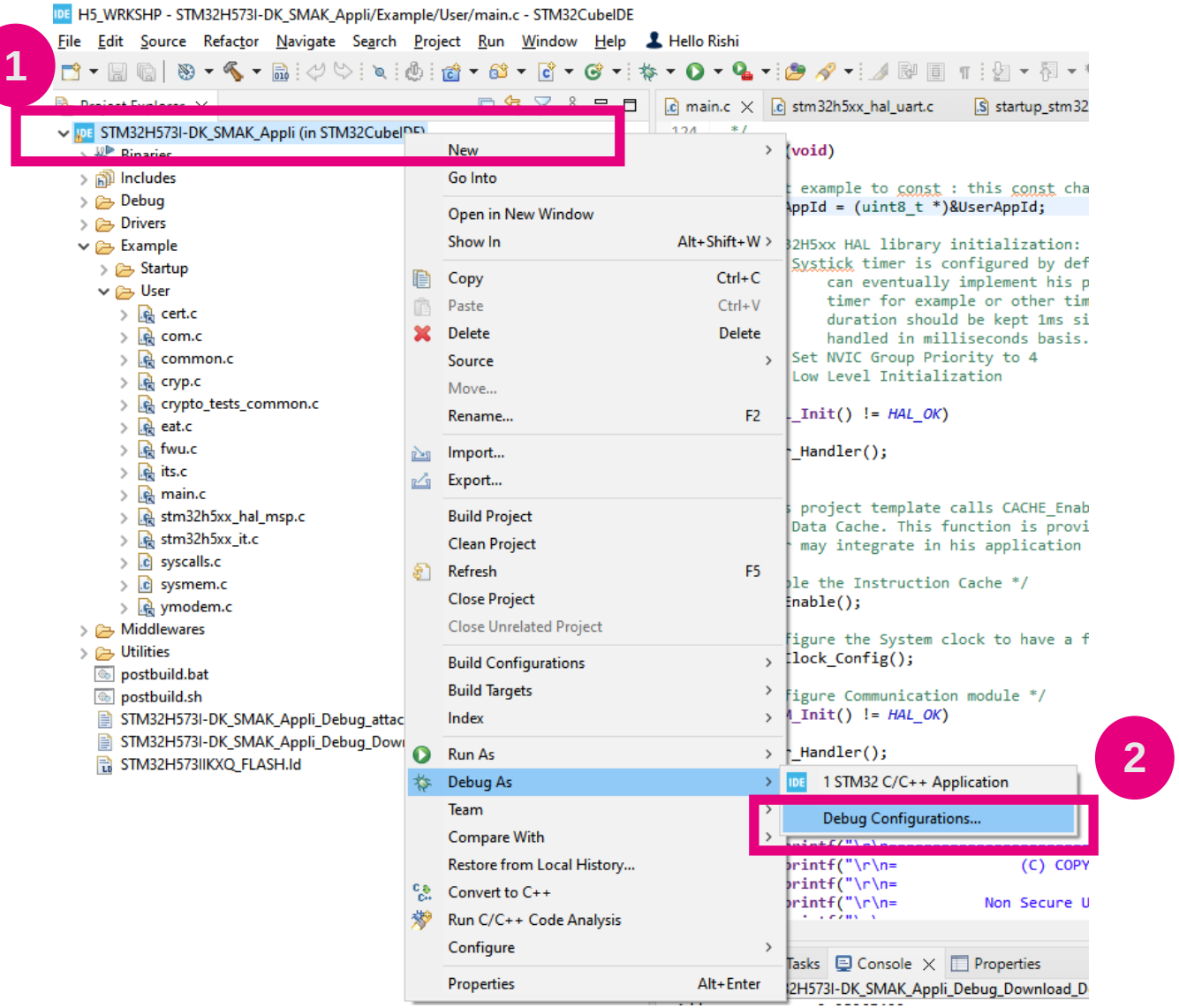
life.augmented

Debug Reopening

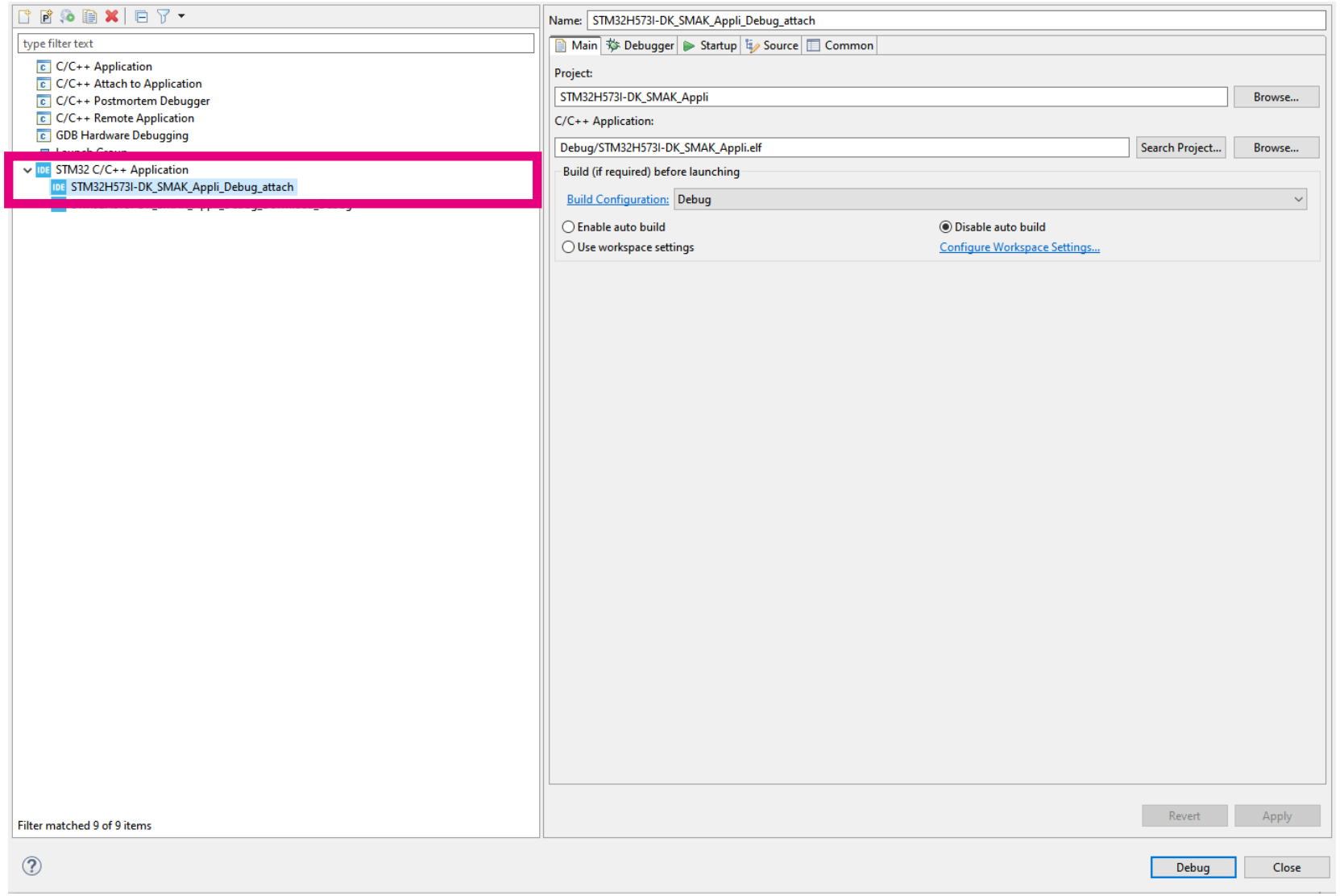


Modify the debug configuration

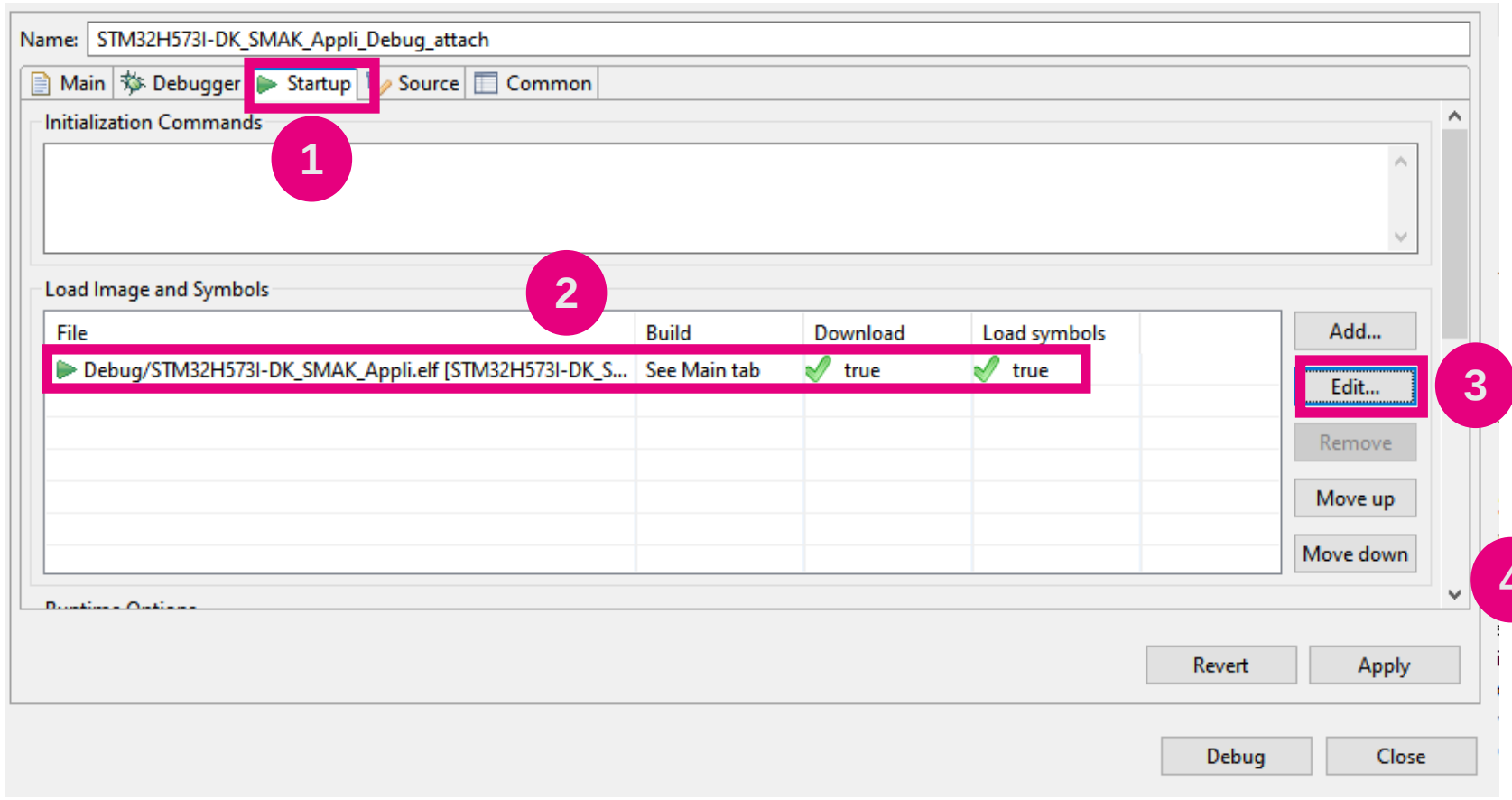
Right click

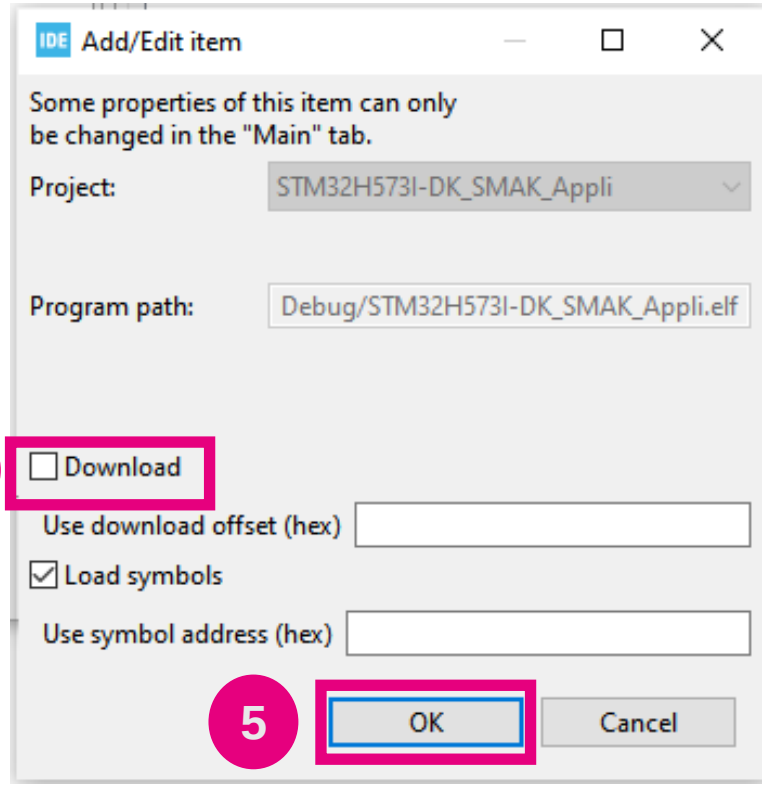


Debug Configuration

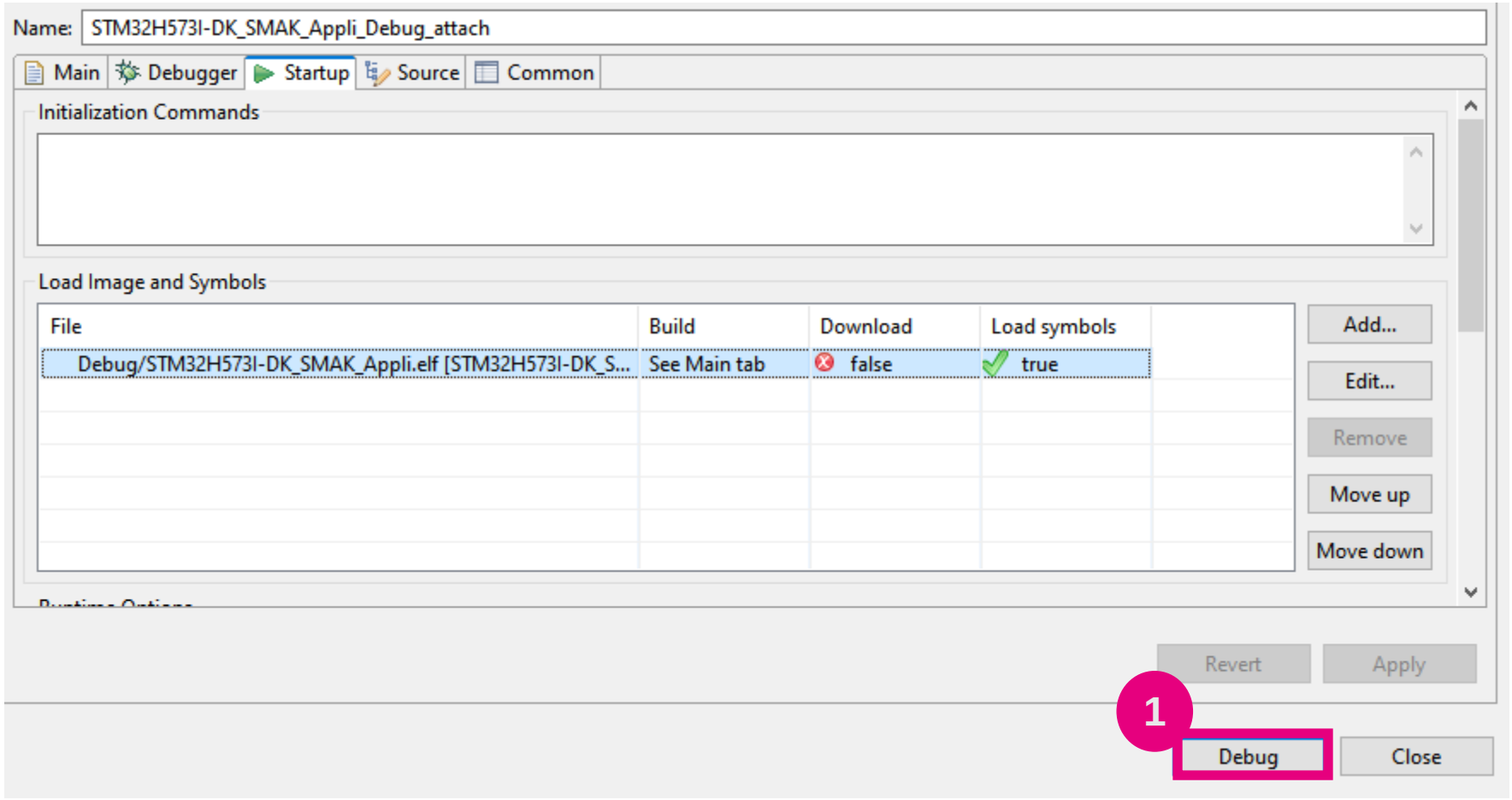


Remove ‘download’ option of the firmware

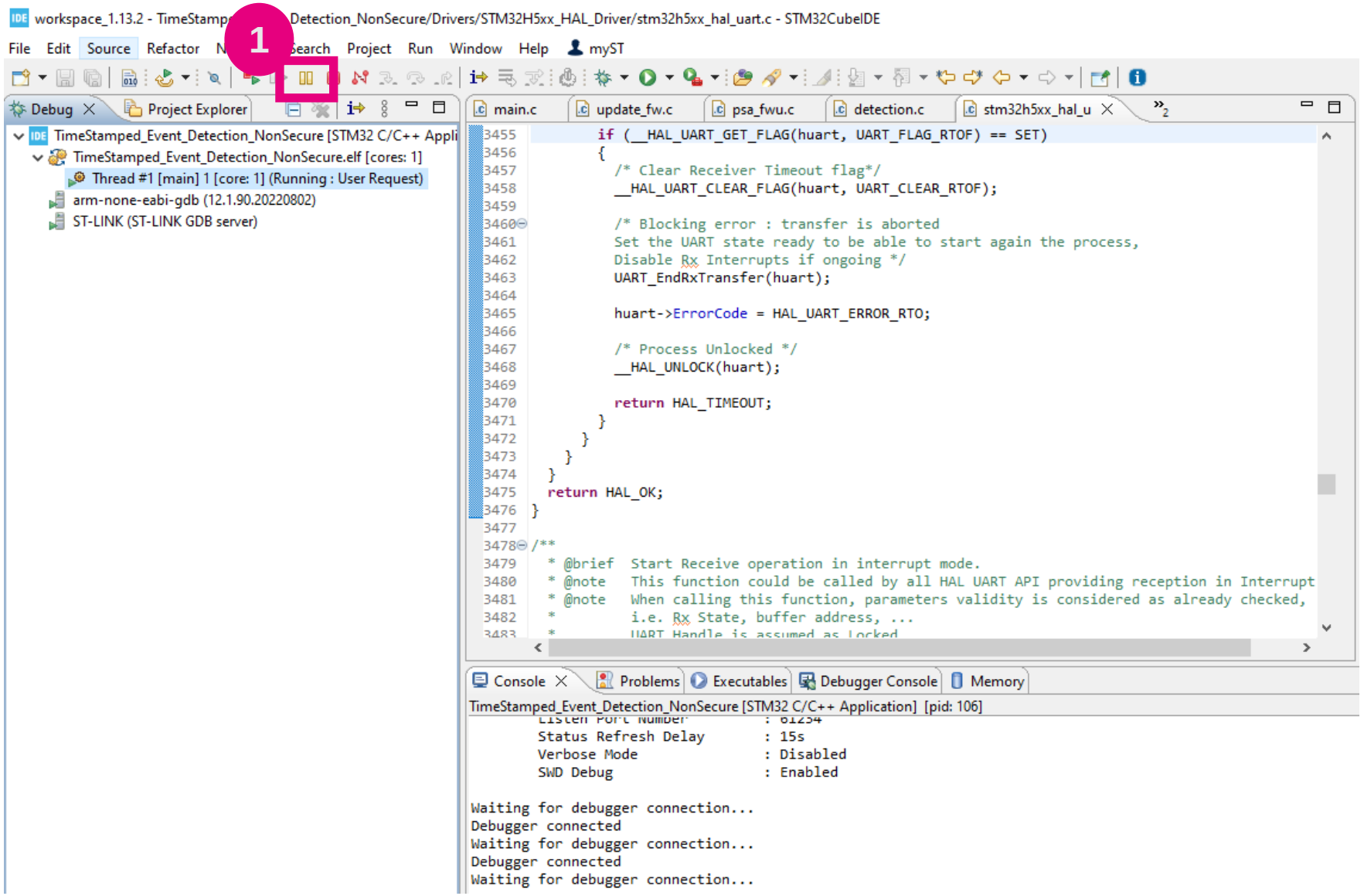




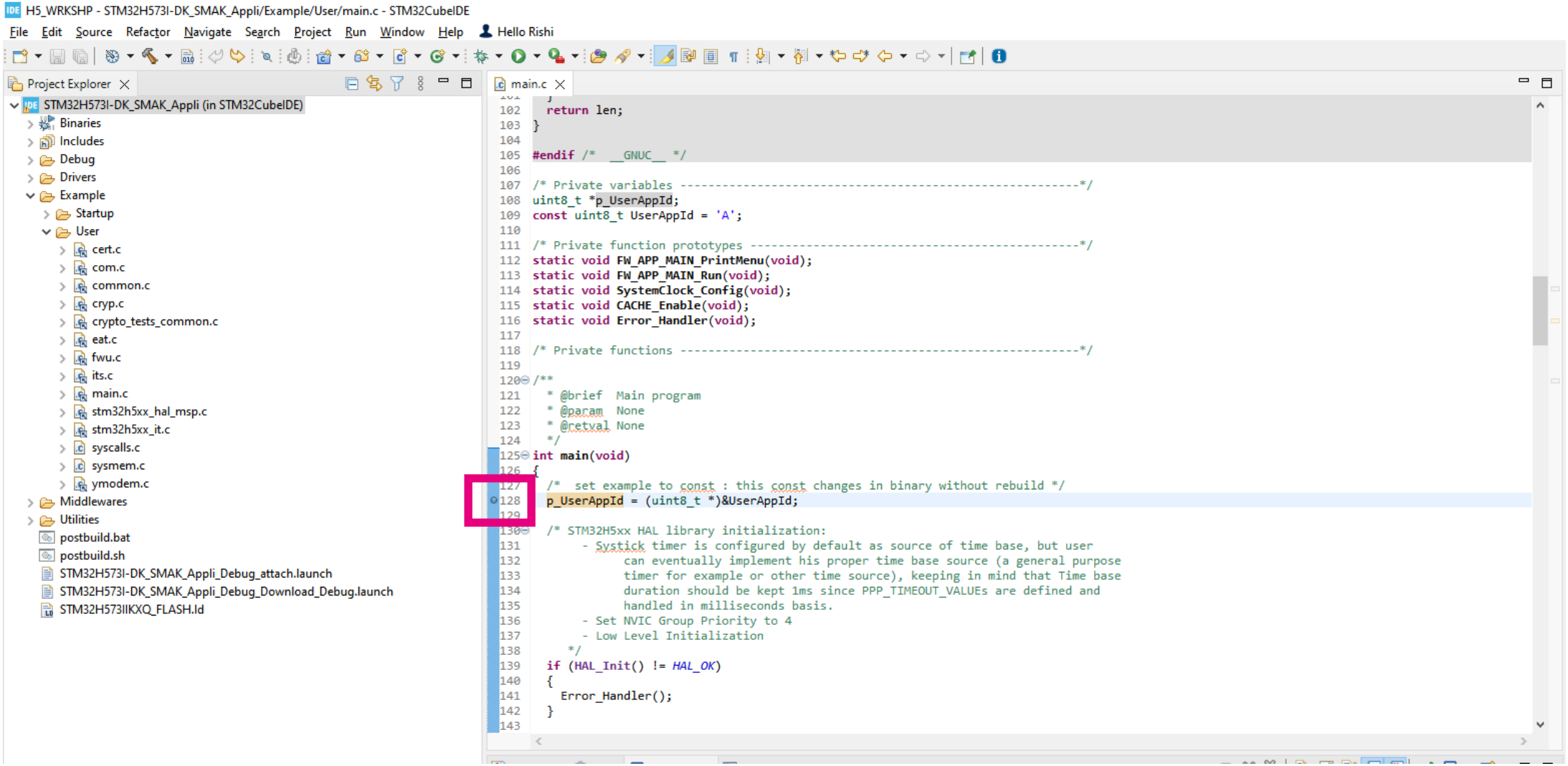
Launch debug



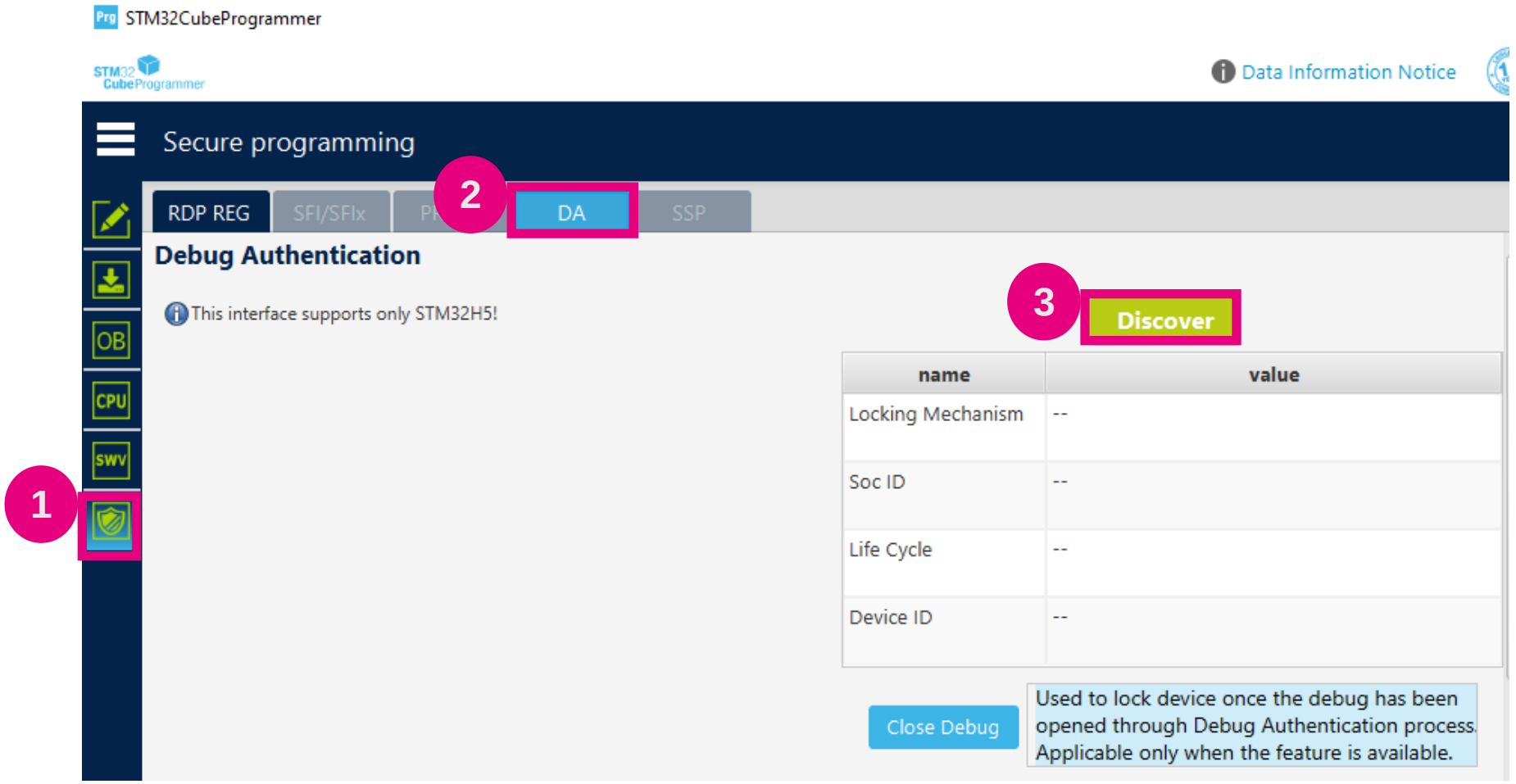
Break execution



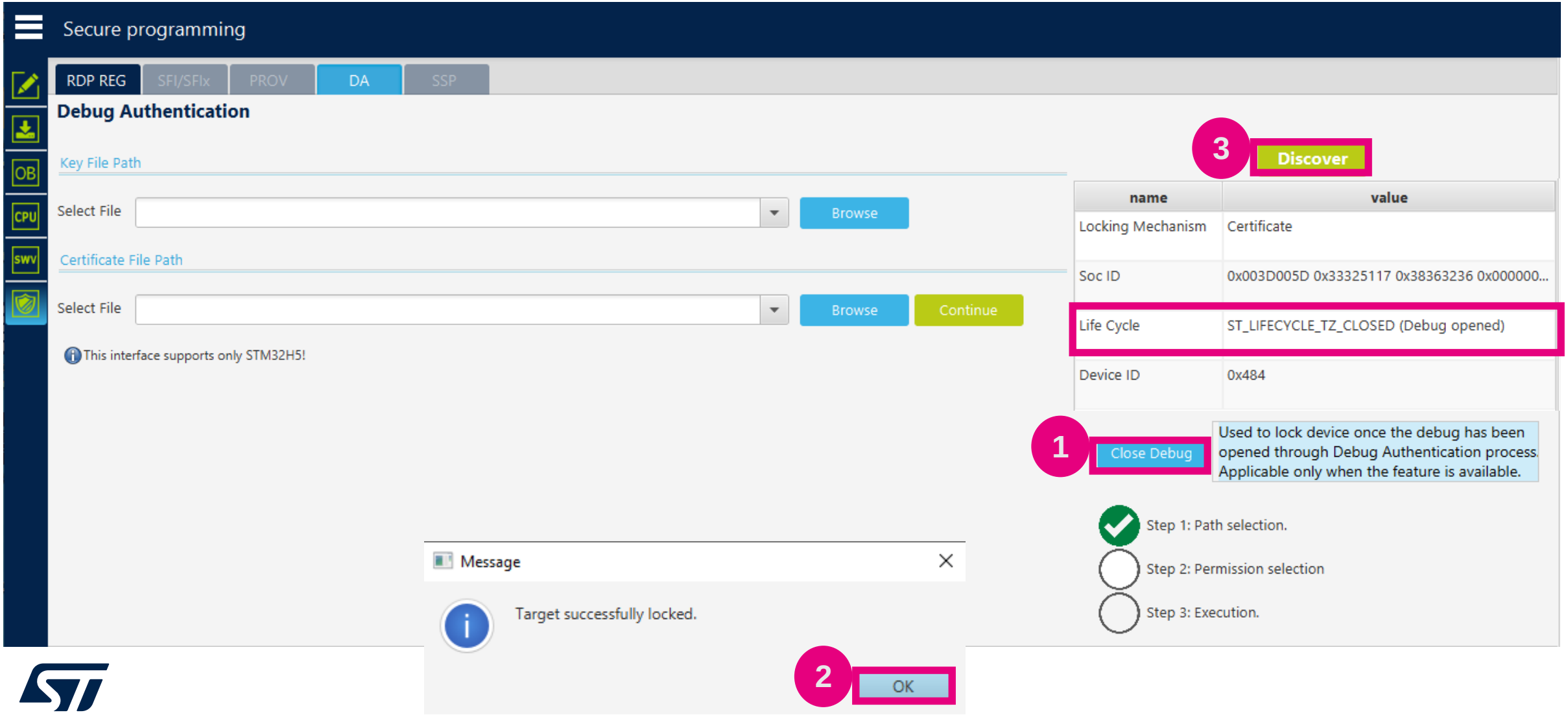
You can set breakpoint and debug…



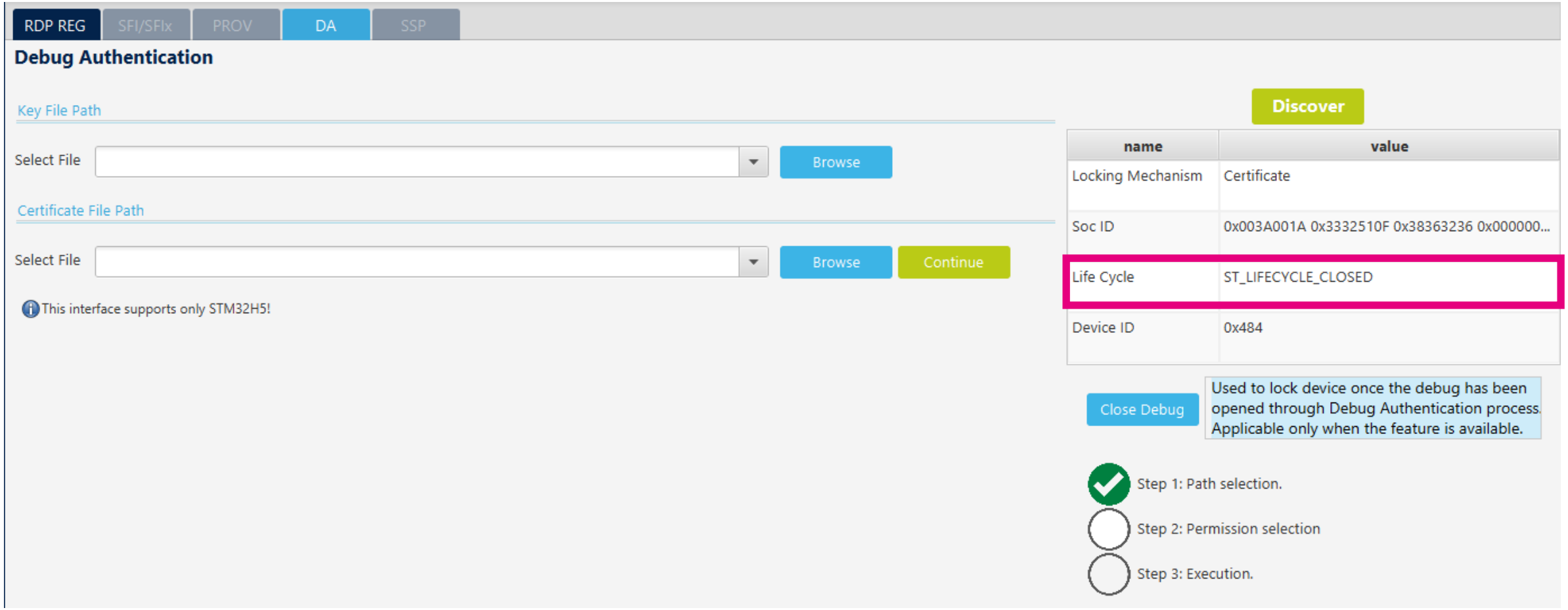
Let’s close the debug



Close Debug Procedure



Debug is now closed



STM32H5 Security
Debug Authentication partial regression

private ECC key

PERM_MASK_CERT

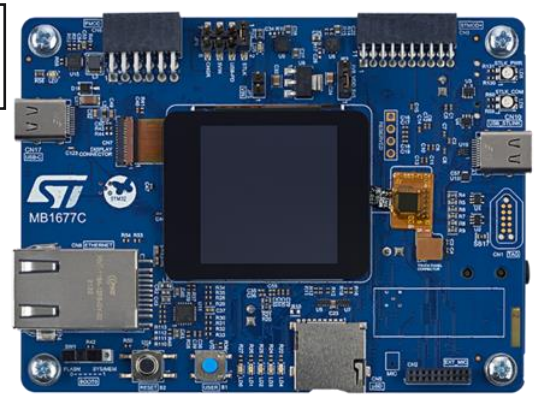
LEAF certificate

Request partial regression

Authentication

Action requested

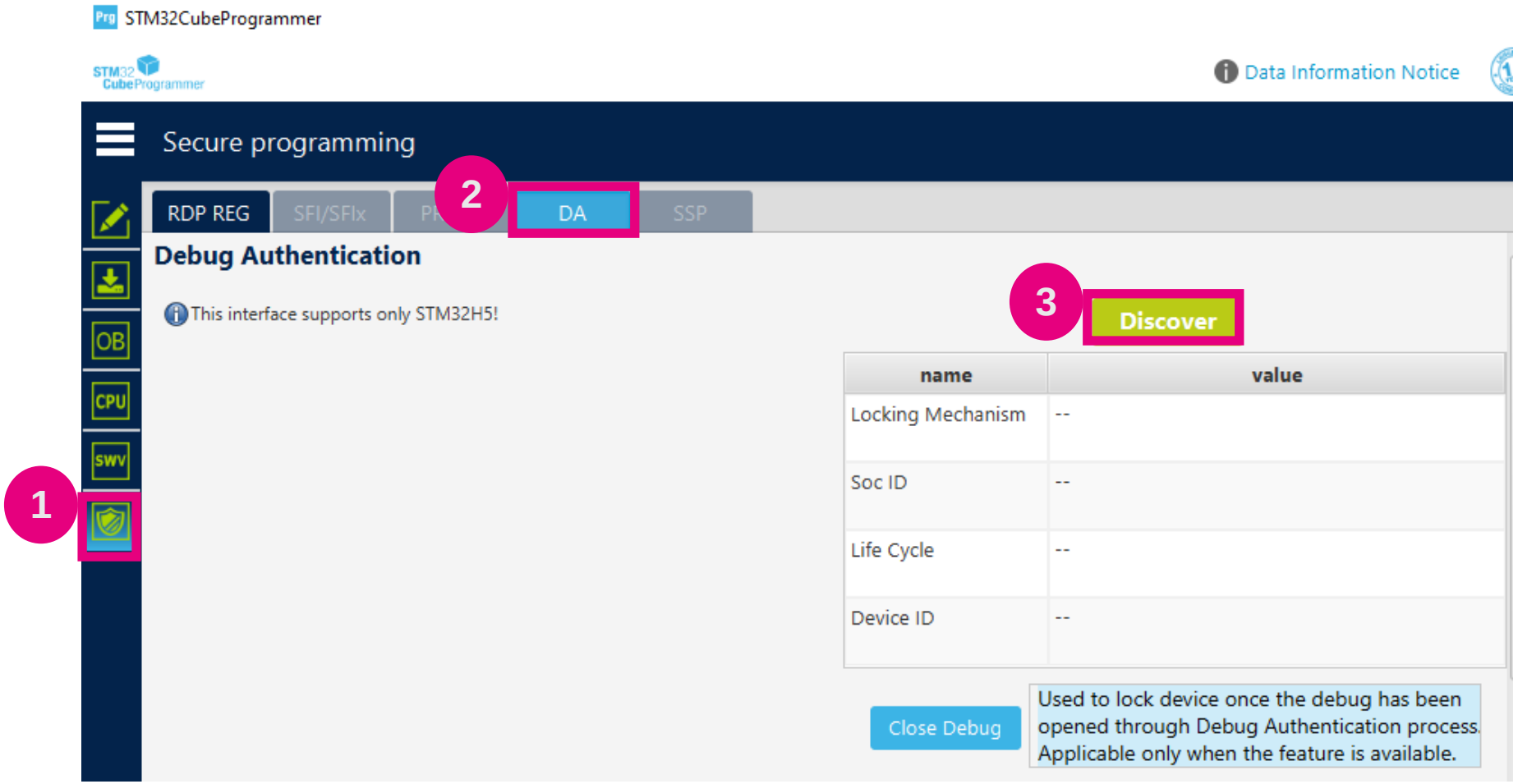
HASH(Key1_root_pub)
SOC Permission Mask



Closed

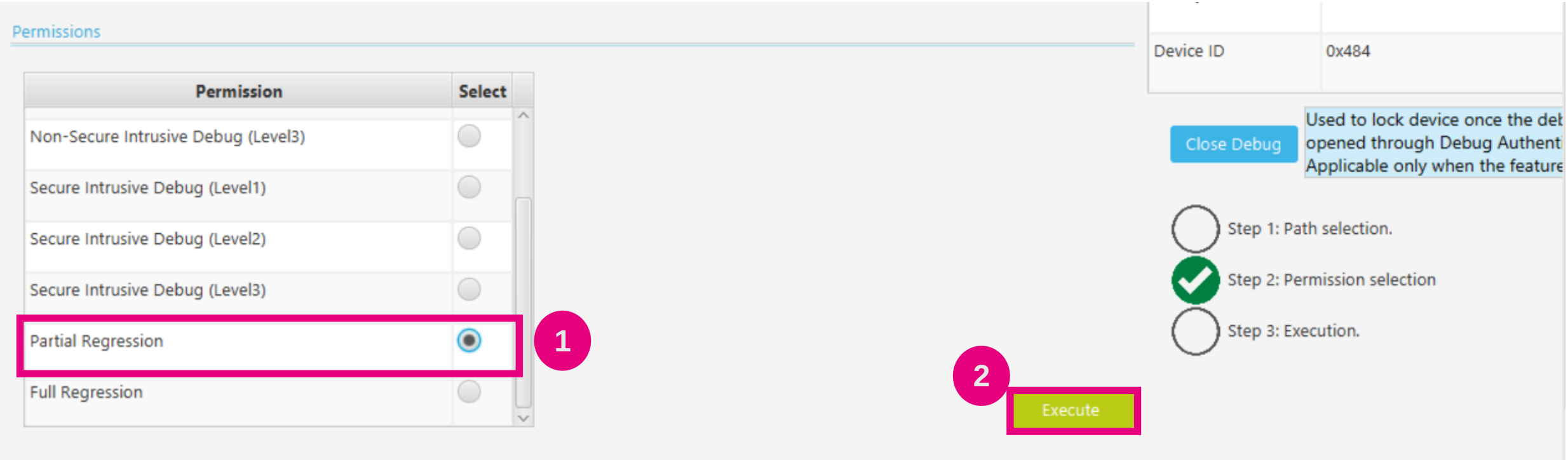
TZ-Closed

Partial Regression

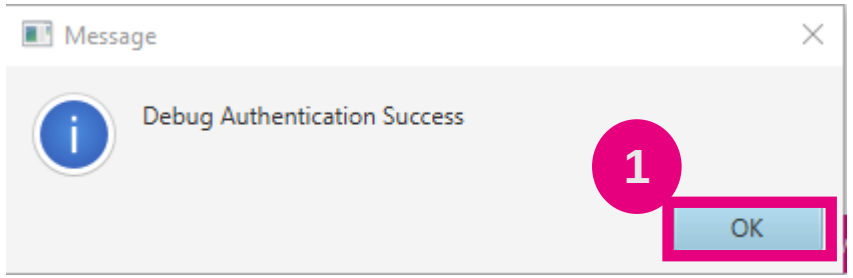


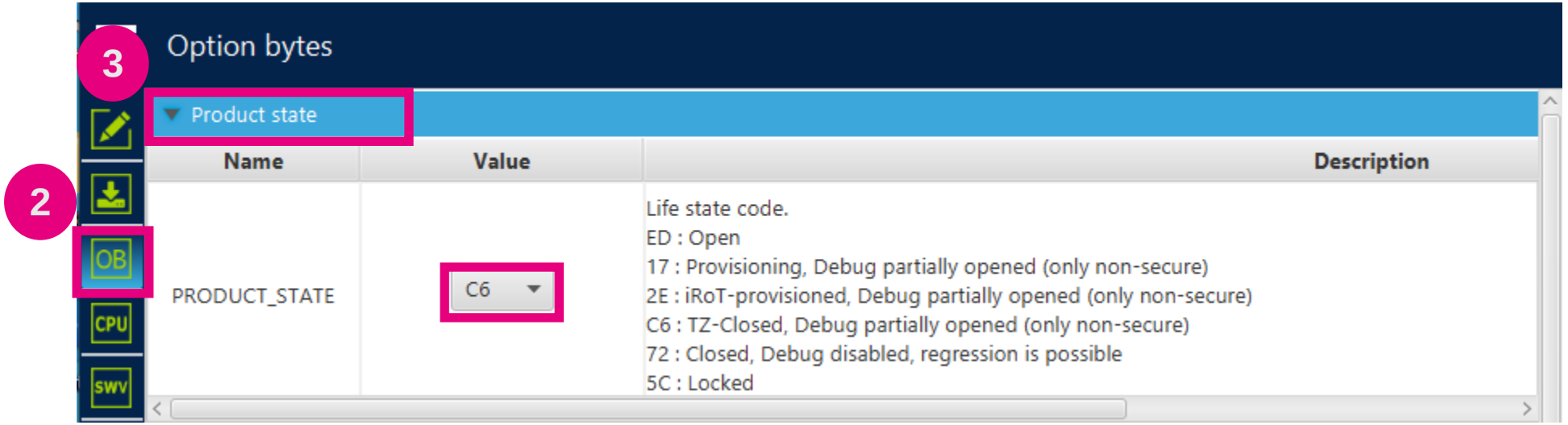
Partial Regression: Keys and Certificates

Partial Regression: Permission Selection

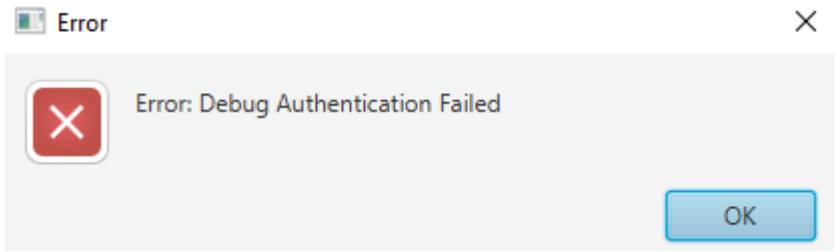


Partial Regression: Success

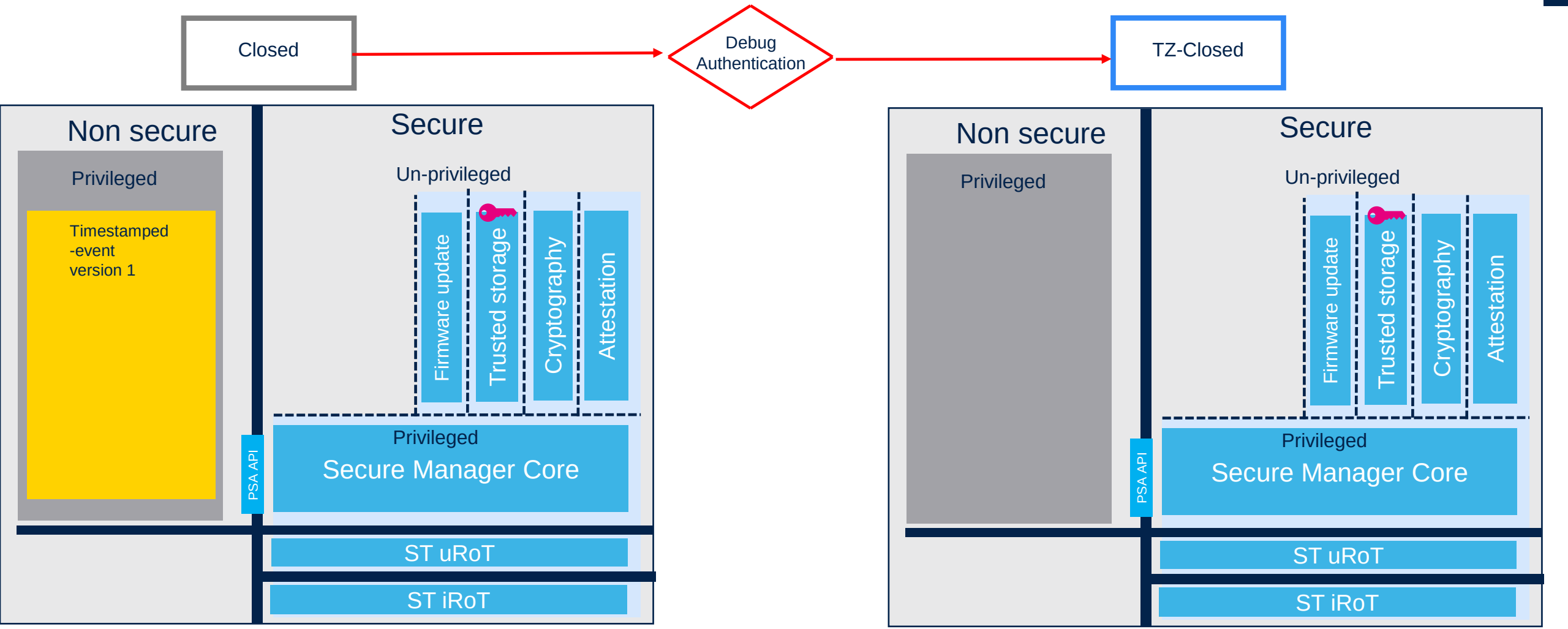




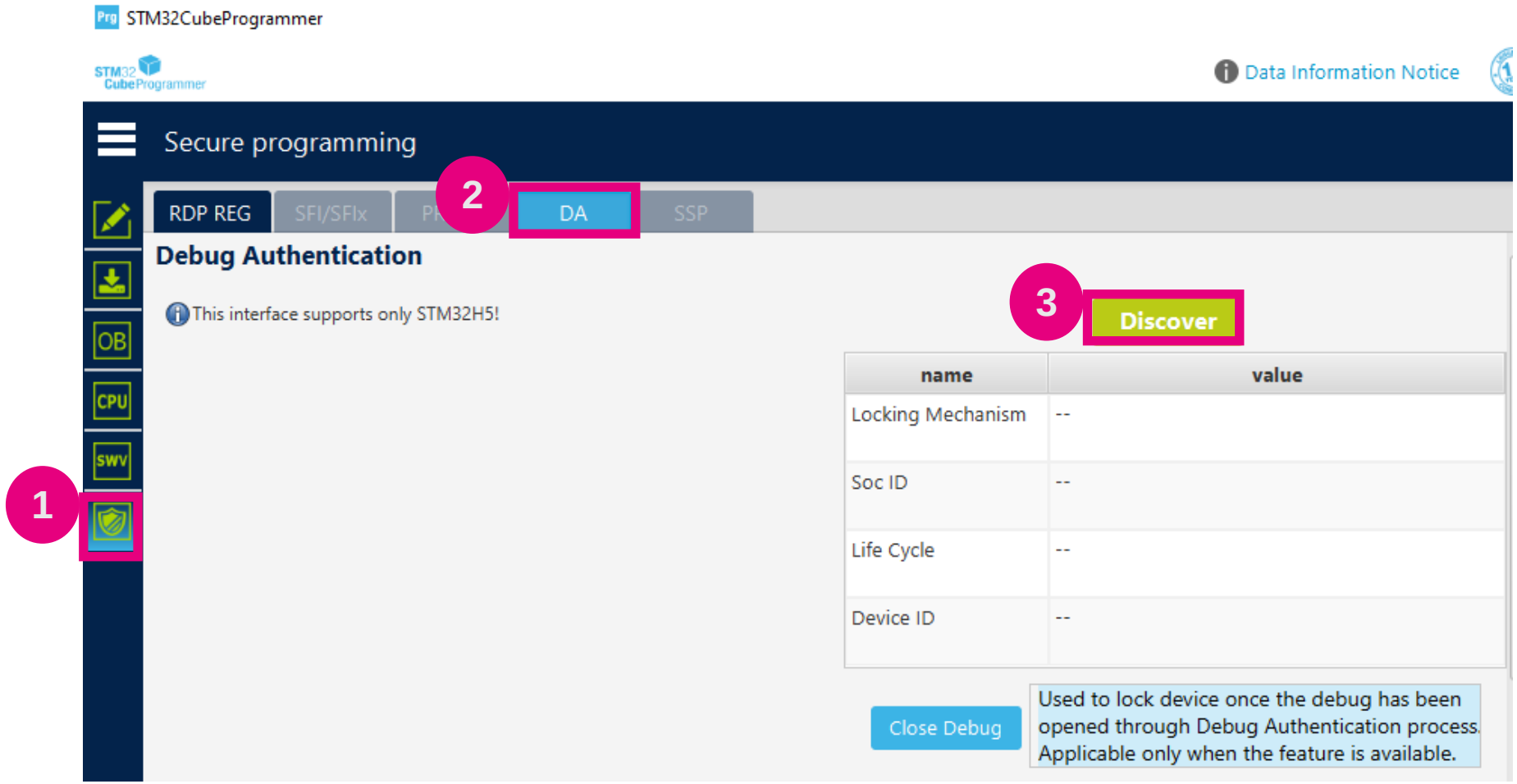
If you try any unauthorize action…



STM32H5 NS-Regression (partial) Result

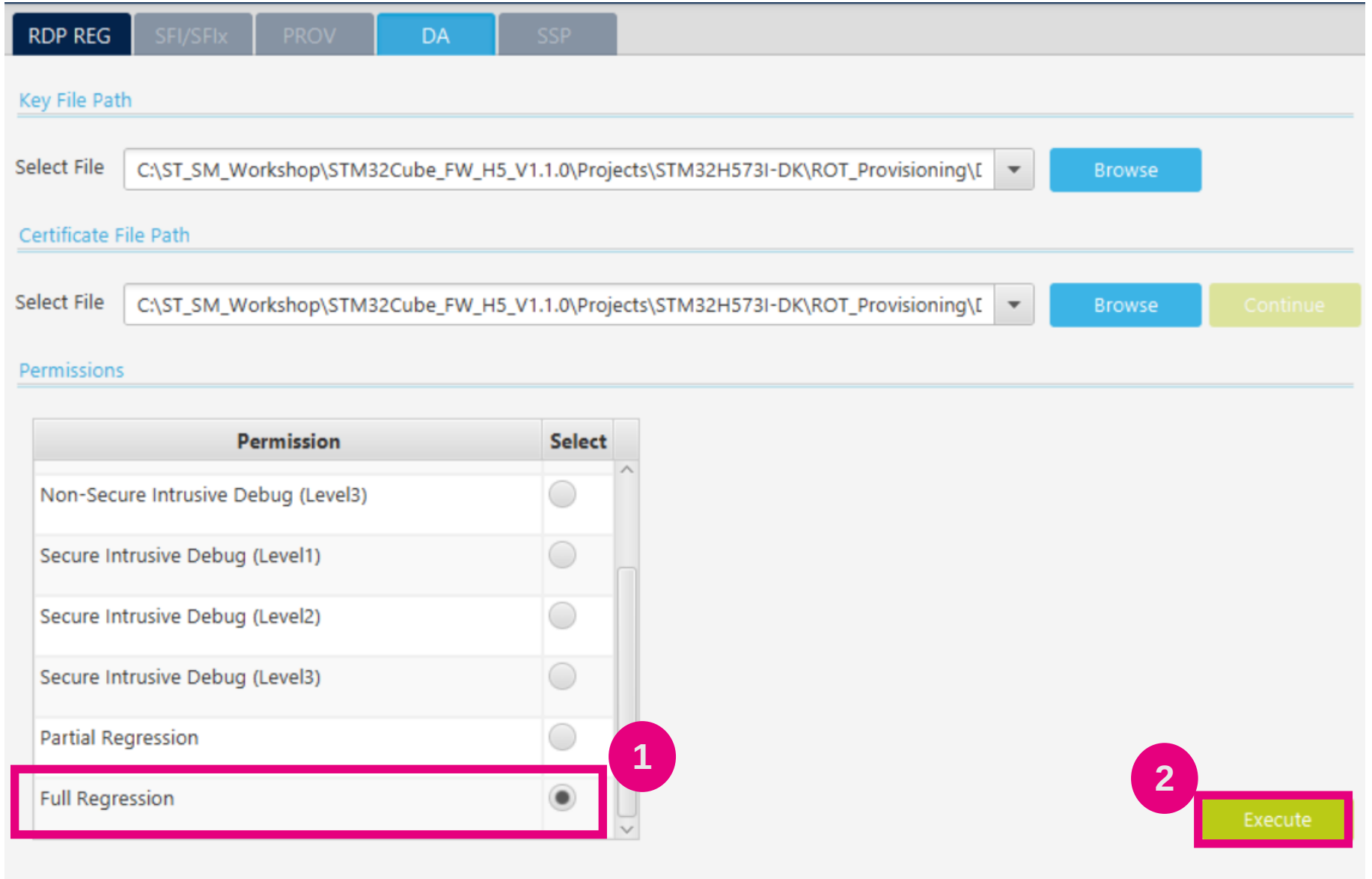


Full Regression

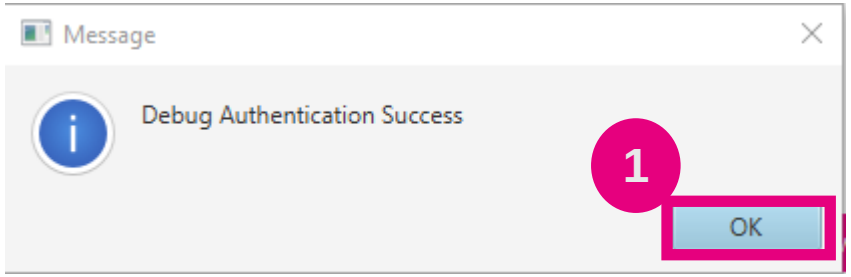


Full Regression: Keys and Certificates

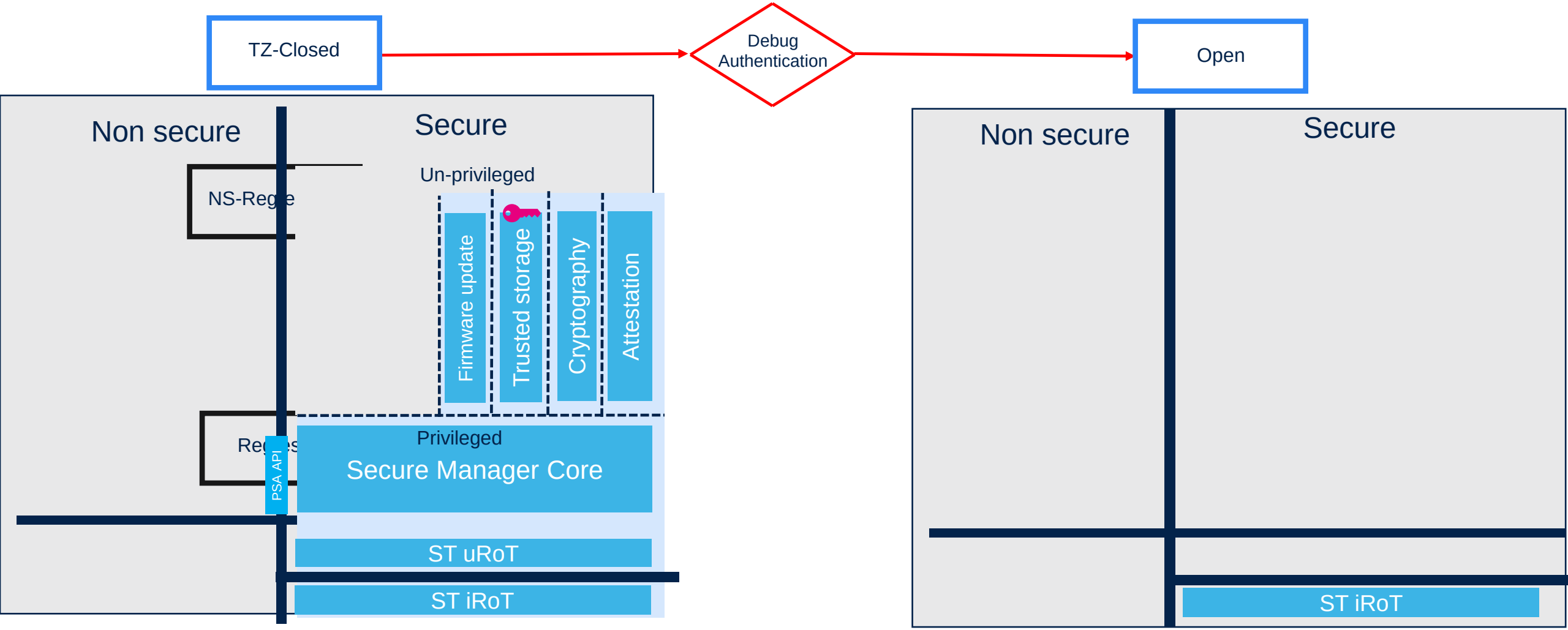
Full Regression: Permission Selection



Full Regression: Success



STM32H5 Regression (Full) Result



Review

- Debug Authentication is a new feature of STM32H5
- Certificates allow fine control on what user can do with the target
- This feature also simplifies the field return analysis

Resources

Resources

Links

- STM32Trust: Web page
- Security with STM32H5: Wiki pages
- Getting Started with STM32H5 security: Wiki pages
- Debug Authentication: How To Intro: 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