life.augmented

STM32Trust

STM32H5 Security Secure Manager - Part 2

Security Features Overview

Presenter: Massimo Panzica

Agenda

I Introduction

II STM32H5 Security Features

III STiRoT

IV Resources

life.augmented

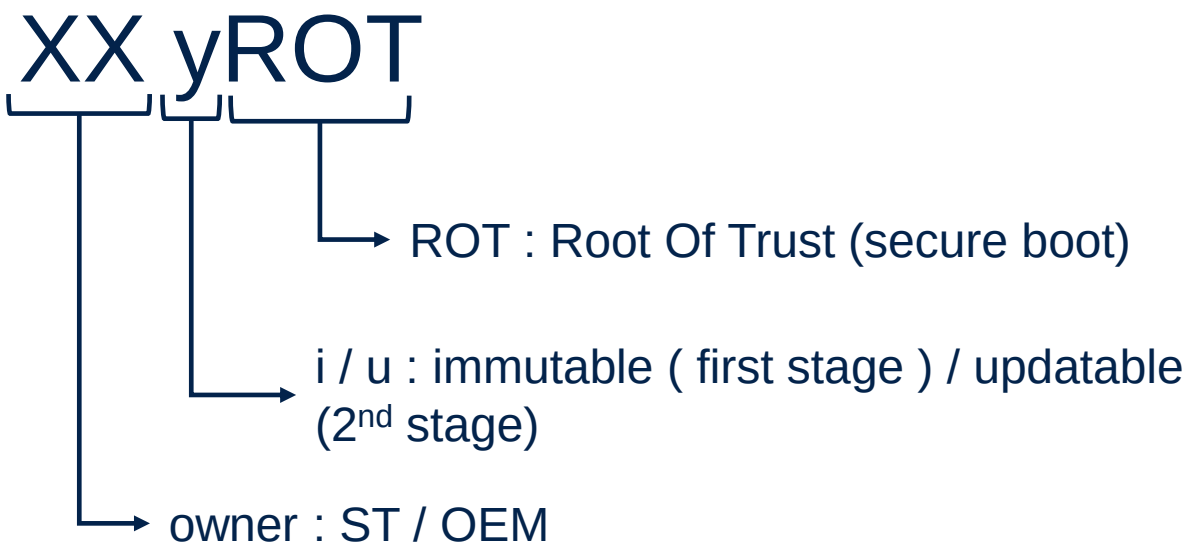
Introduction

Introduction

- STM32H5 security is the latest evolution of STM32 family
- It is based on STM32U5 and goes one step further
- The STM32U5 introduced the Secure AES with HUK and the keyed RDP
- The STM32H5 introduces
  - A new temporal isolation level
  - A secure storage coupled with temporal isolation
  - New product life cycle
  - The Debug Authentication
  - An embedded secure boot called STiROT
- You can use and combine those mechanism to build your security !
- STM32H573 security features are covered in this workshop

life.augmented

Naming convention



- STiROT
- STuROT
- OEMiROT
- OEMuROT

Security Features Overview

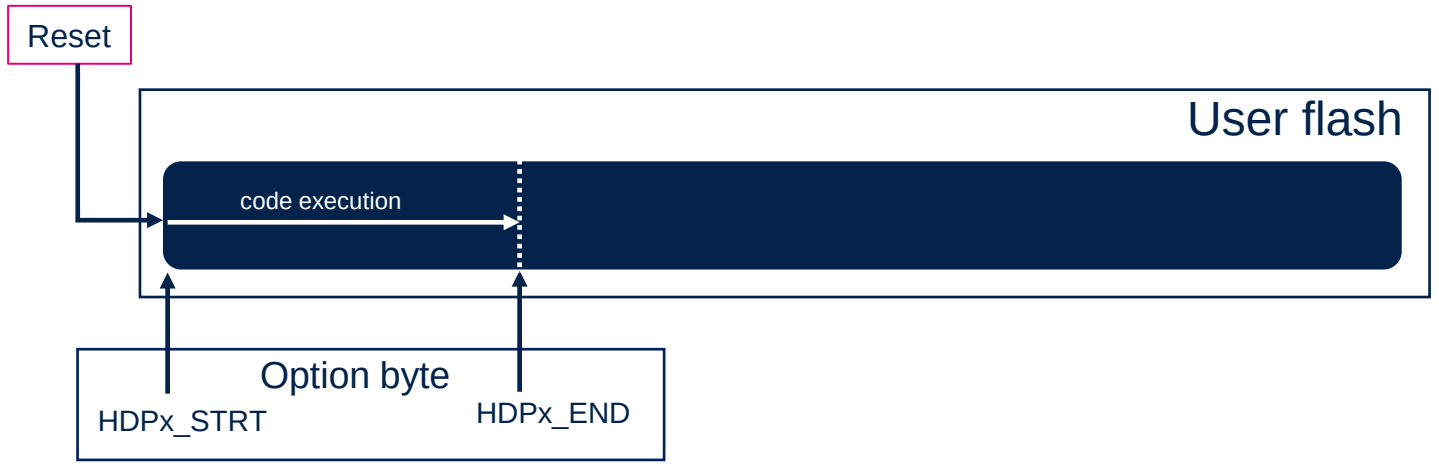
life.augmented

What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset

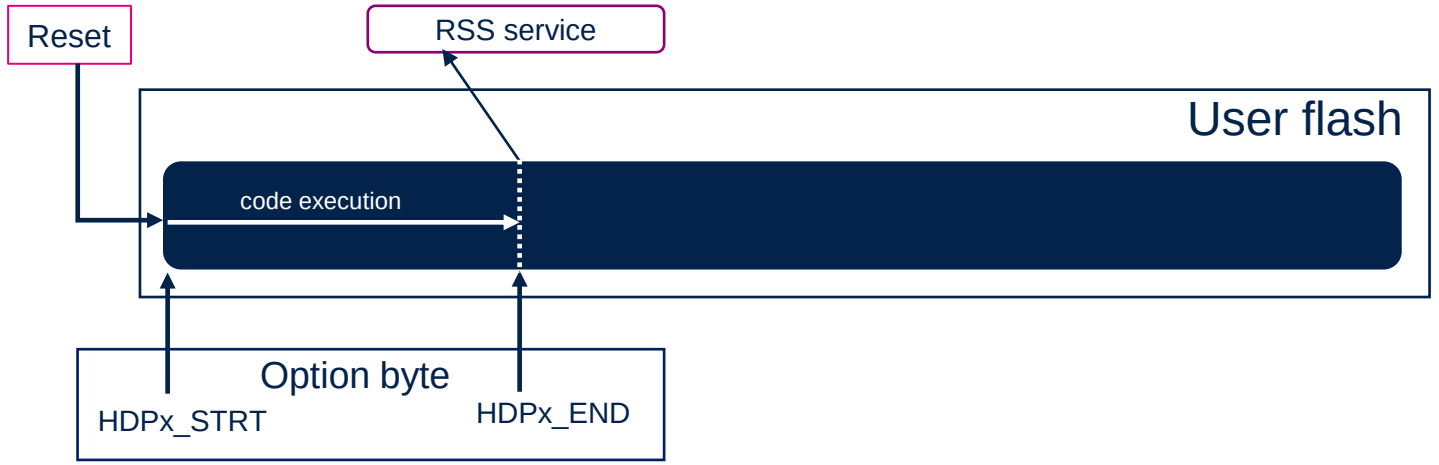
What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



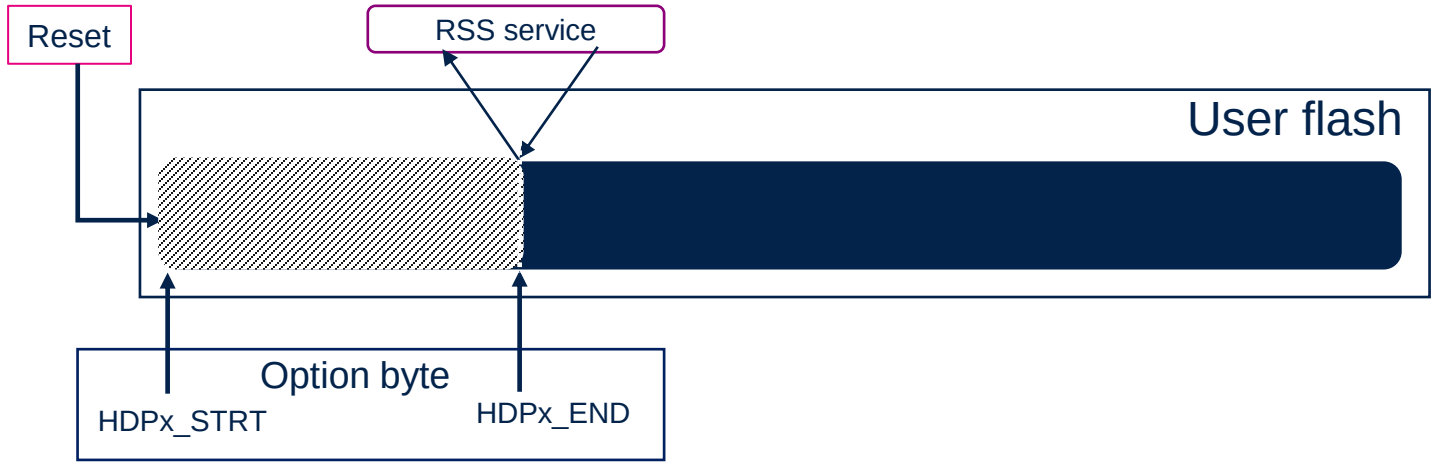
What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



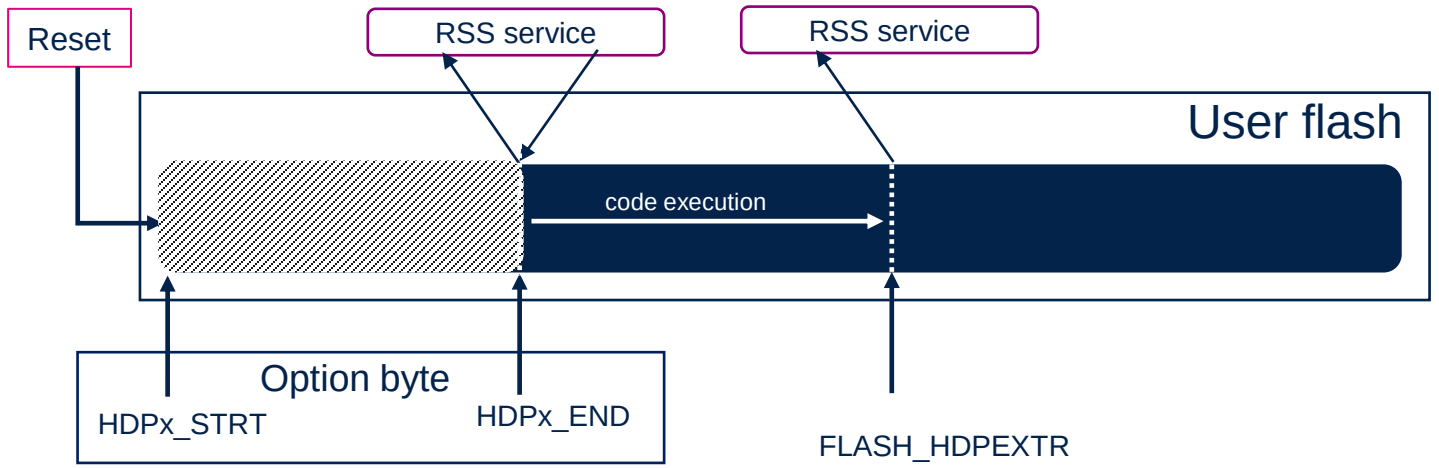
What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



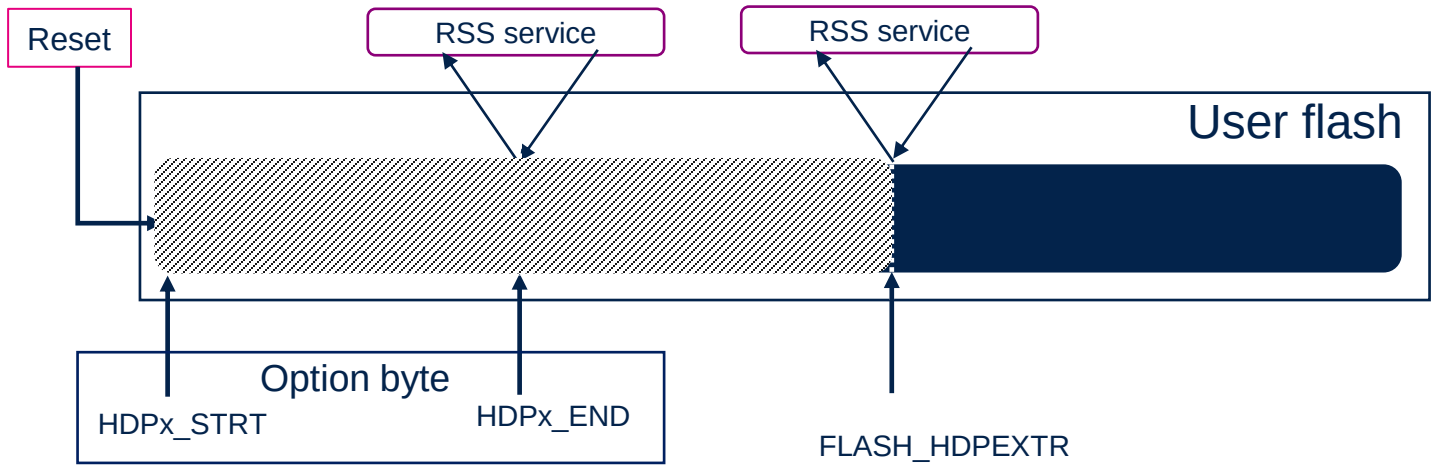
What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



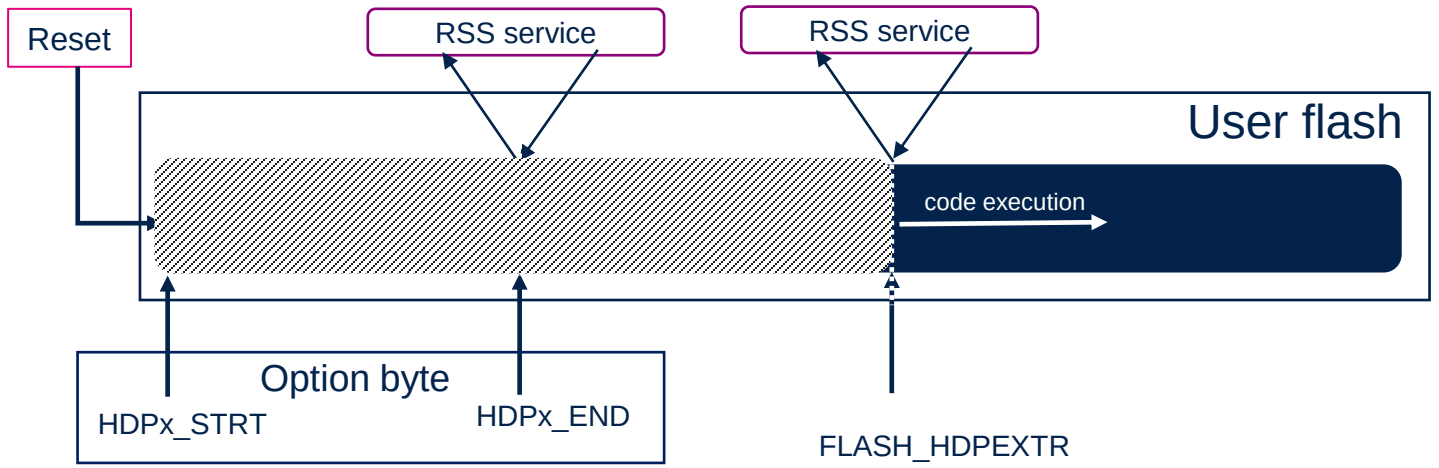
What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



What is temporal isolation ?

- Protection that evolves during the code execution at boot
- It has significantly evolved in STM32H5 (HDP – Hide Protection)
- 2 different portions of user flash can be hidden until the next reset



Secure Storage

- The Secure Storage is a specific area that allows to store data securely
  - data can be provisioned securely
  - data are isolated and can be access only by authorized part of the system
- STM32H5 provide 5 secure storage areas named OB Keys
- Data within secure storage area is
  - Temporarily isolated through the HDP
  - Optionally encrypted through mechanism based on a Hardware Unique Key (HUK) and an antirollback monotonic counter (EPOCH)

Secure Storage

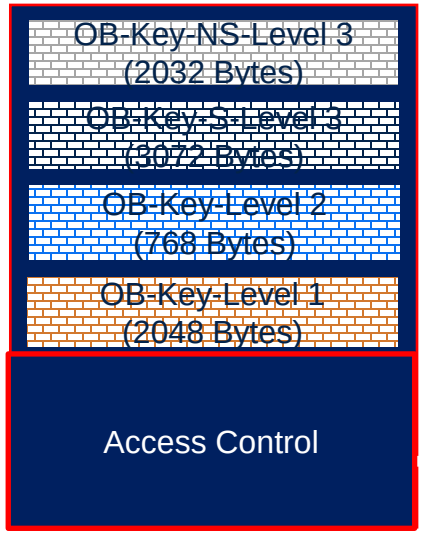
- OBK (option-byte keys) is a specific storage in system flash
- Total storage size is 8KB
- Split in 5 predefined areas corresponding to HDPL0, L1, L2, L3s, L3ns

HDPL = 0

Secure Storage

- OBK (option-byte keys) is a specific storage in system flash
- Total storage size is 8KB
- Split in 5 predefined areas corresponding to HDPL0, L1, L2, L3s, L3ns

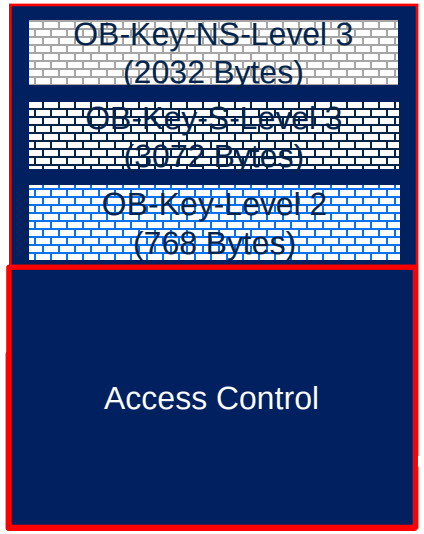
HDPL = 1



Secure Storage

- OBK (option-byte keys) is a specific storage in system flash
- Total storage size is 8KB
- Split in 5 predefined areas corresponding to HDPL0, L1, L2, L3s, L3ns

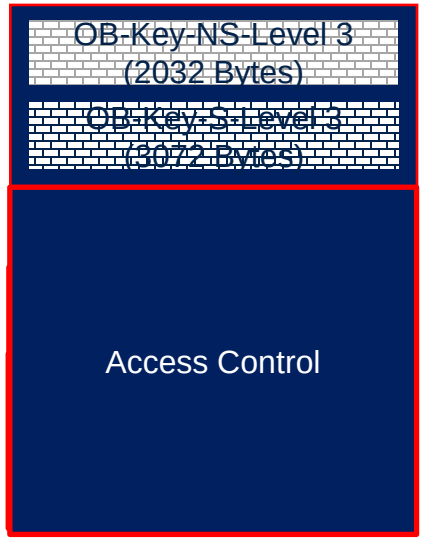
HDPL = 2



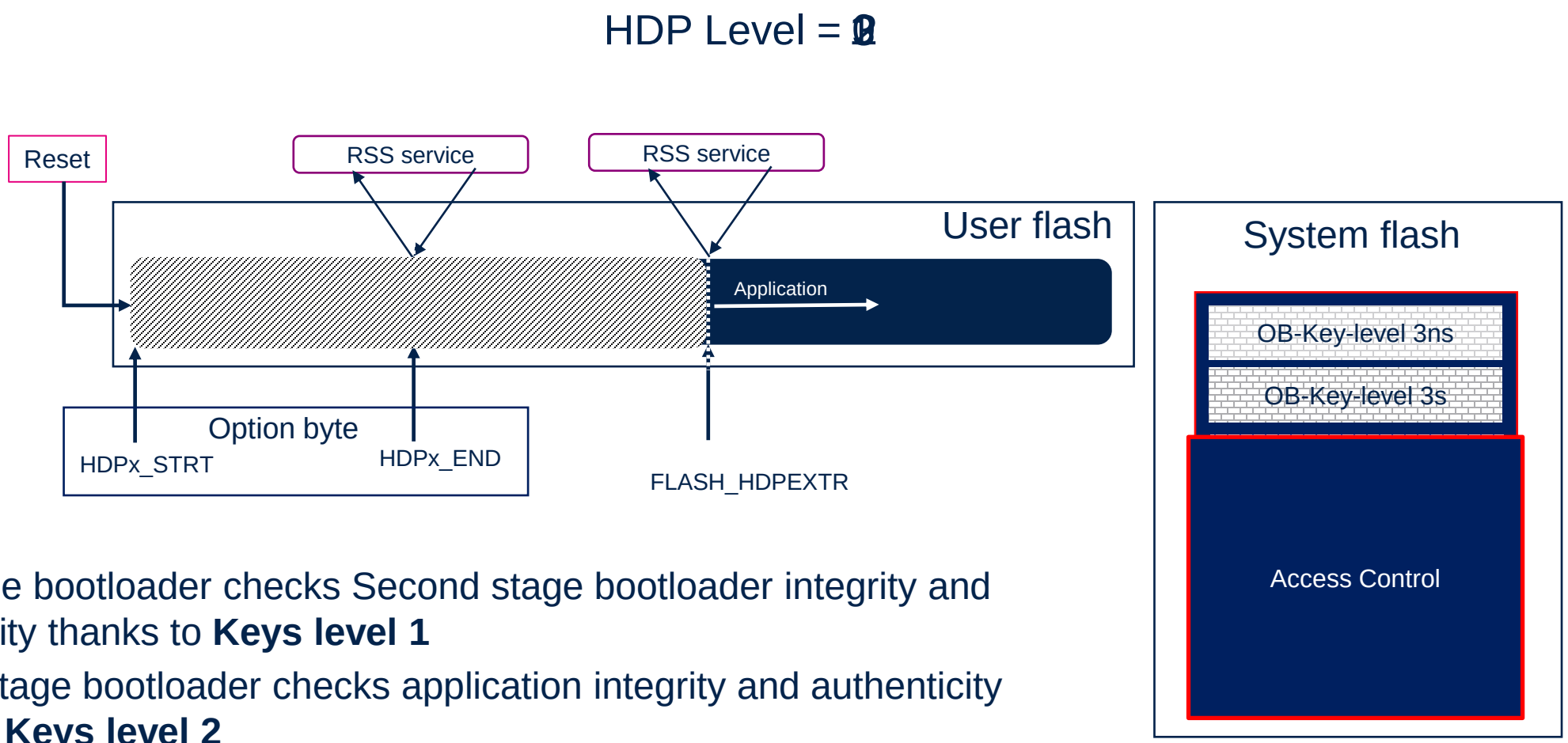
Secure Storage

- OBK (option-byte keys) is a specific storage in system flash
- Total storage size is 8KB
- Split in 5 predefined areas corresponding to HDPL0, L1, L2, L3s, L3ns

HDPL = 3



Temporal isolation and Secure storage

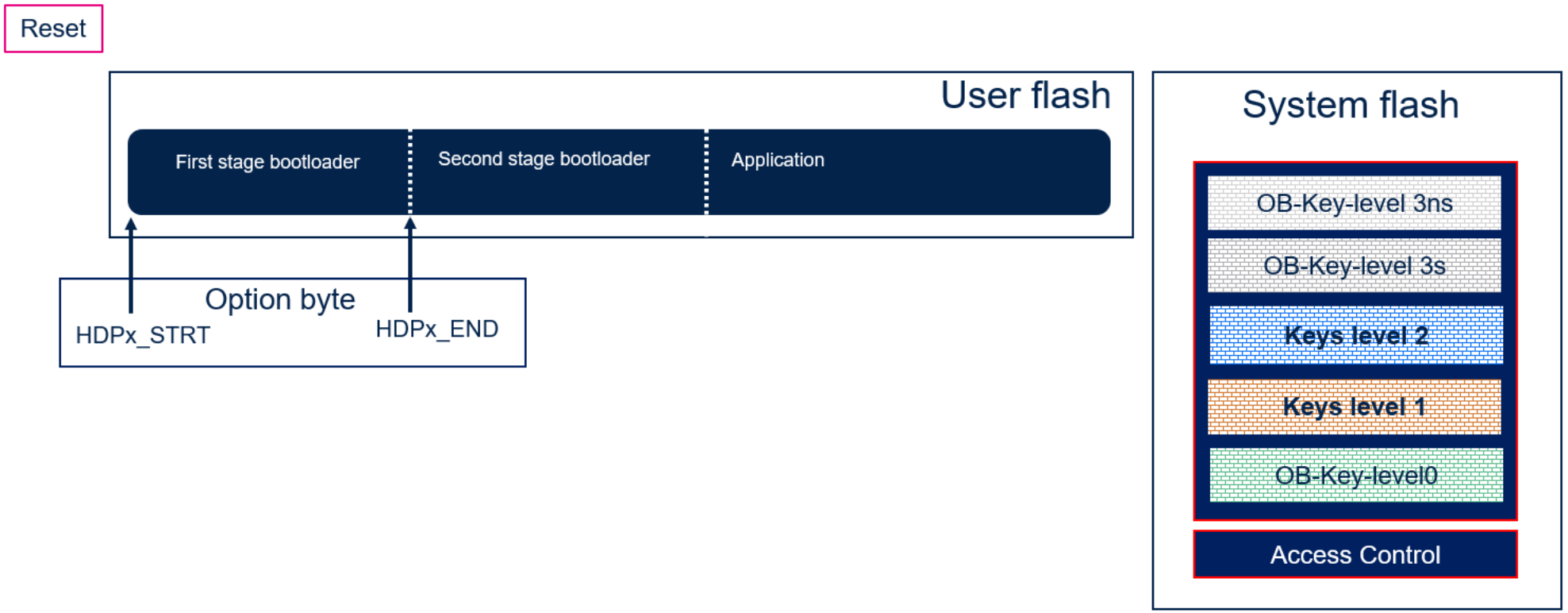


- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**
- Second stage bootloader checks application integrity and authenticity thanks to **Keys level 2**

life.augmented

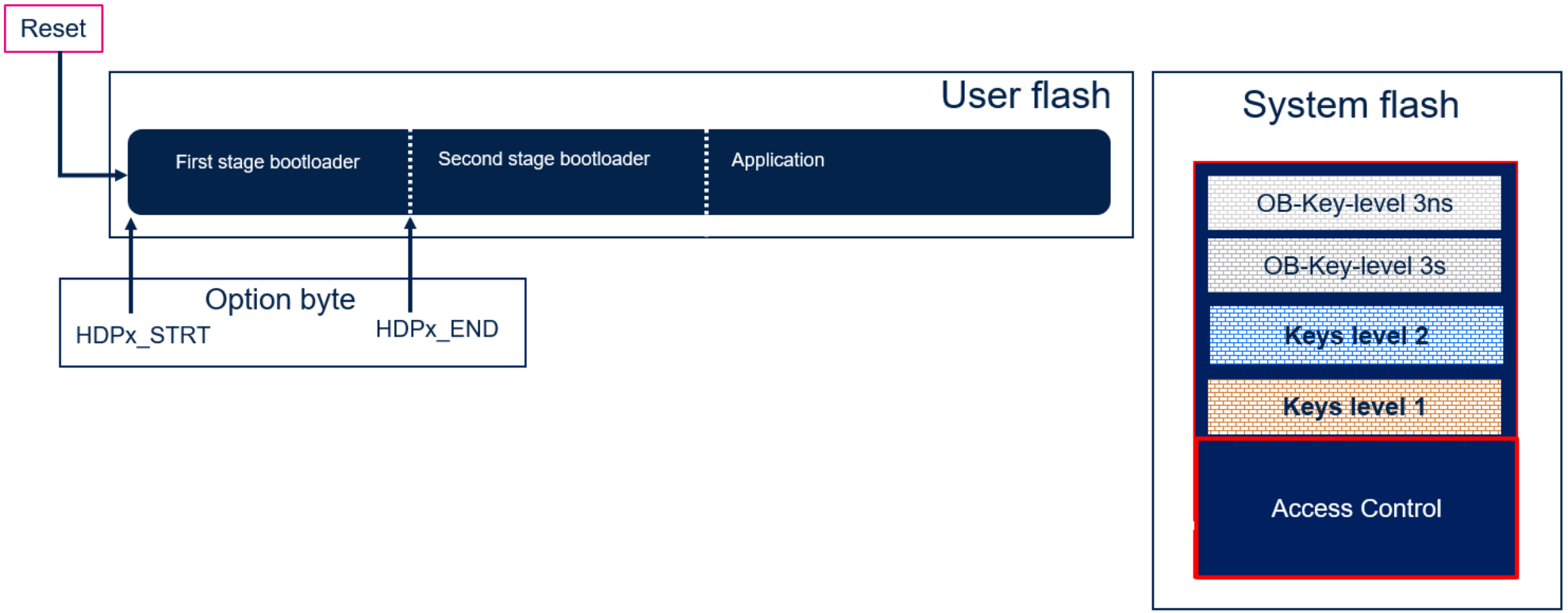
Temporal isolation and Secure storage

HDP Level = 0



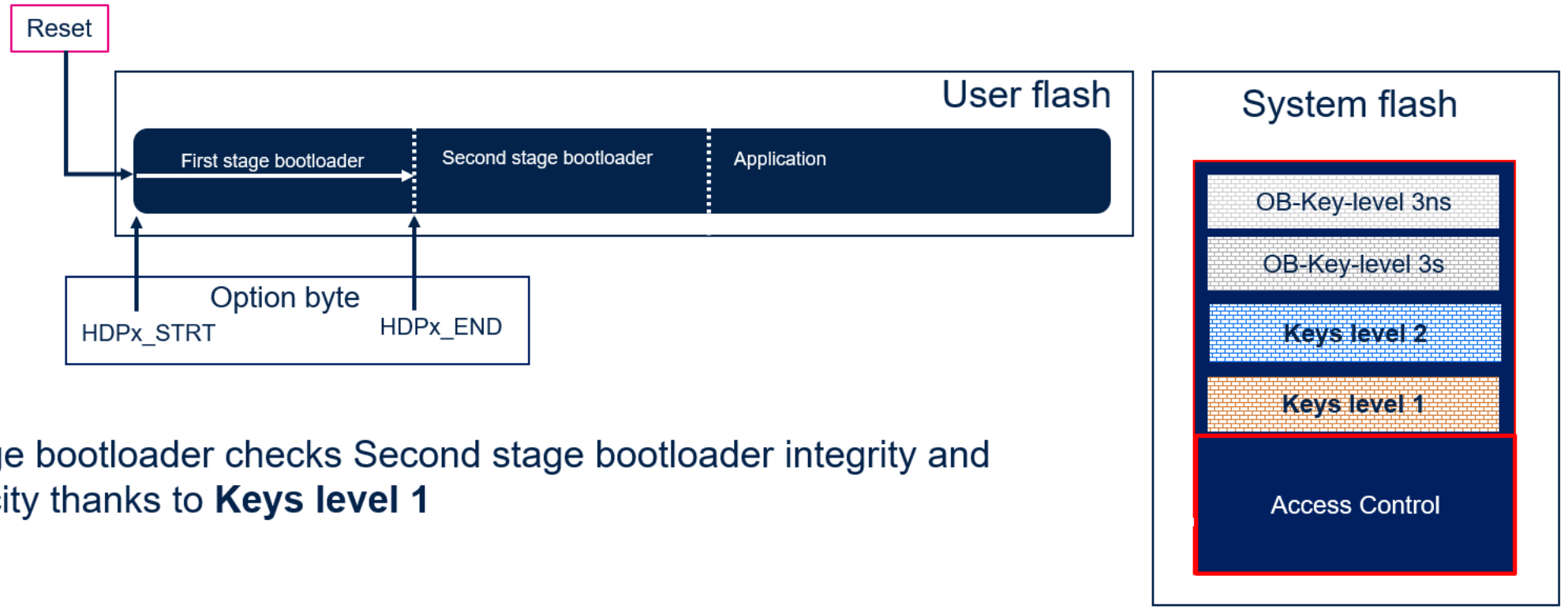
Temporal isolation and Secure storage

HDP Level = 1



Temporal isolation and Secure storage

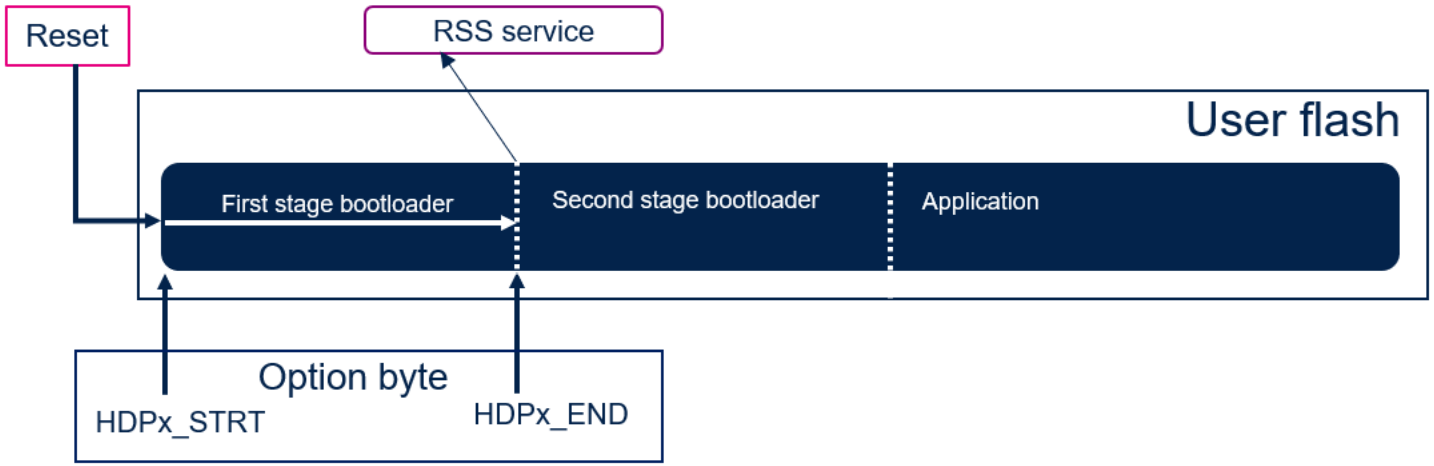
HDP Level = 1

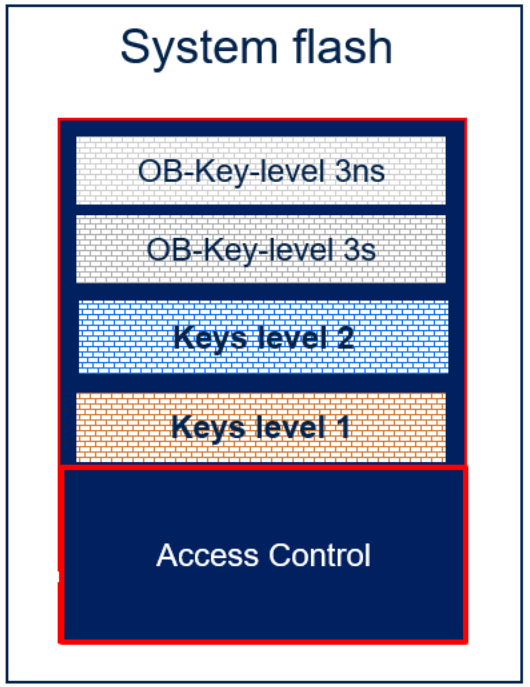


- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**

Temporal isolation and Secure storage

HDP Level = 1

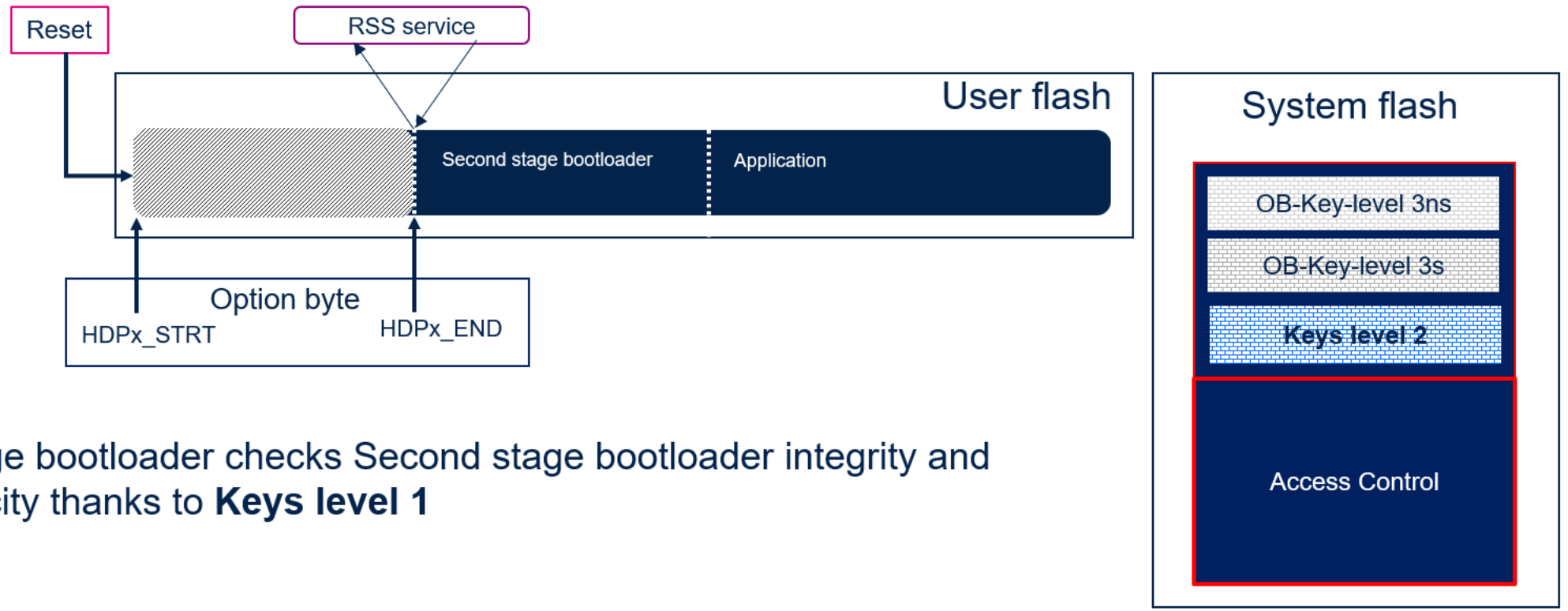




- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**

Temporal isolation and Secure storage

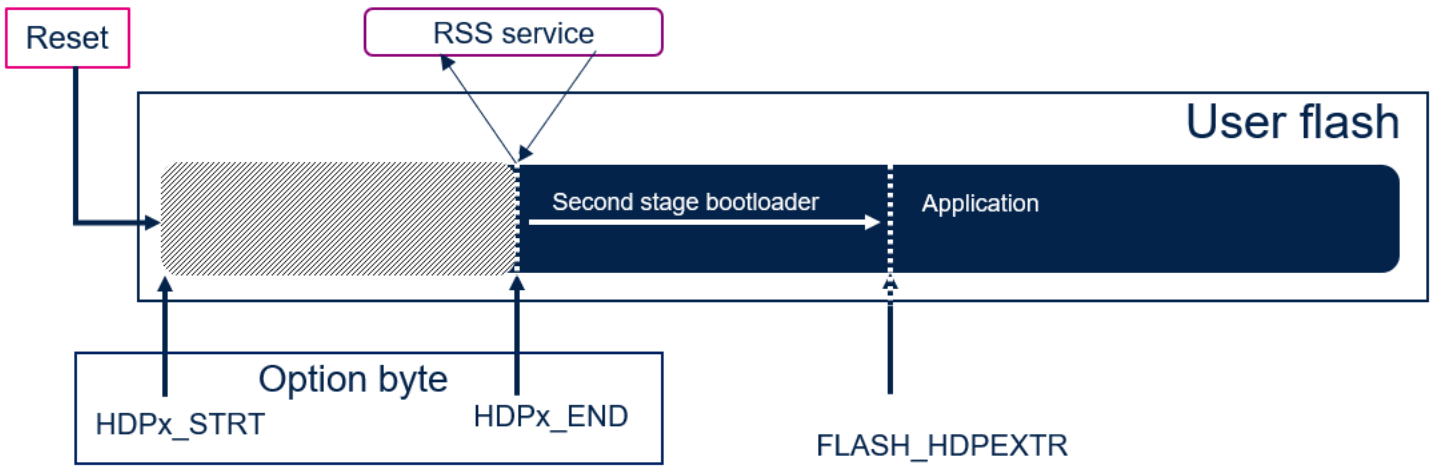
HDP Level = 2

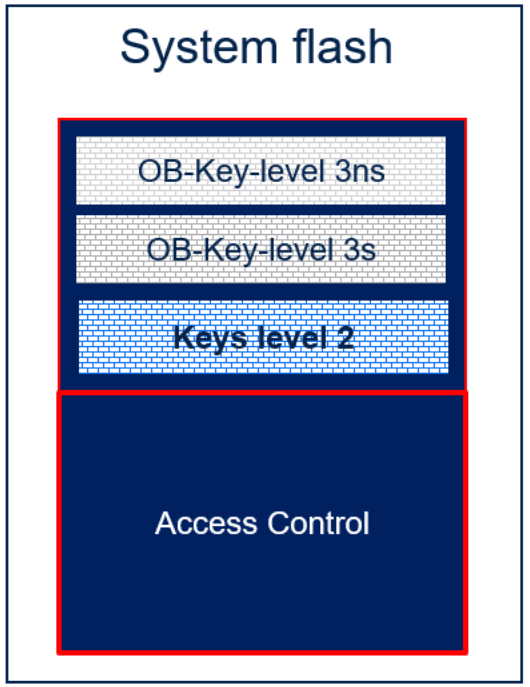


- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**

Temporal isolation and Secure storage

HDP Level = 2



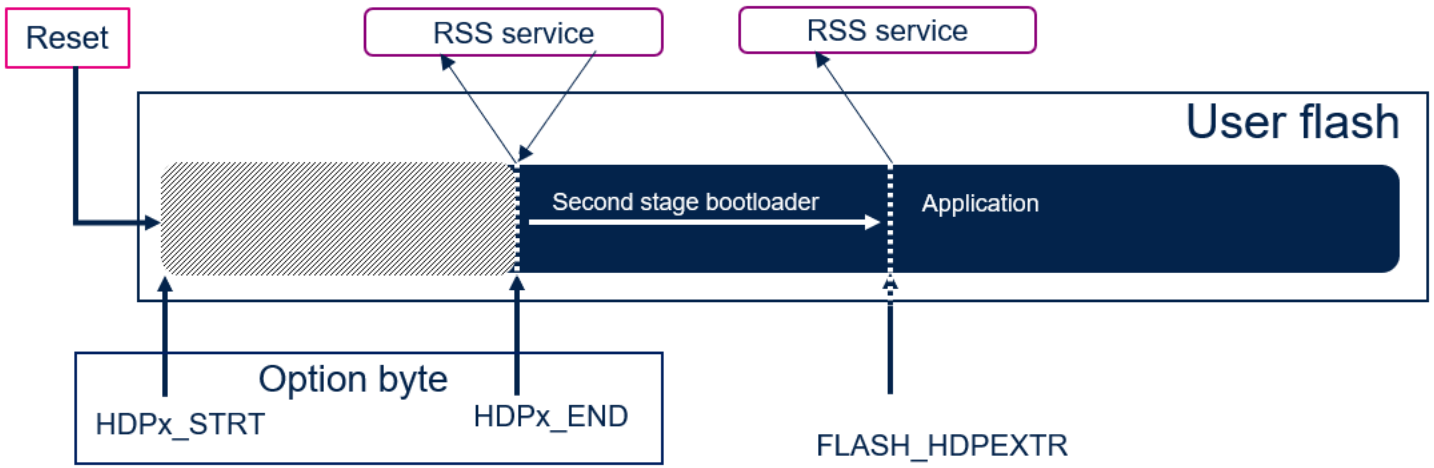


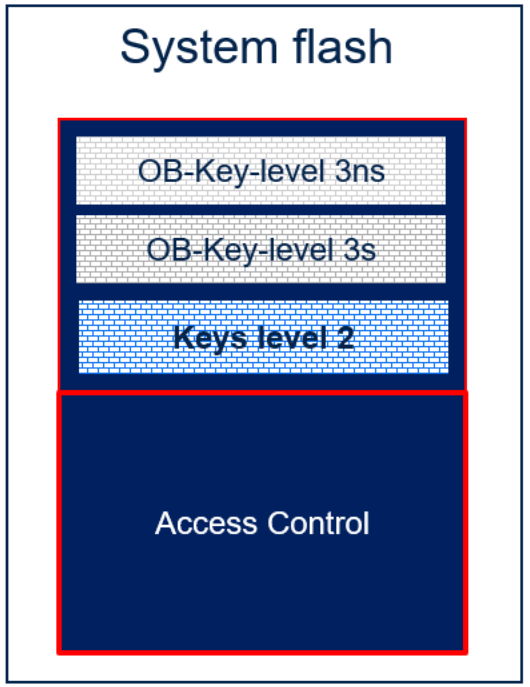
- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**
- Second stage bootloader checks application integrity and authenticity thanks to **Keys level 2**

life.augmented

Temporal isolation and Secure storage

HDP Level = 2

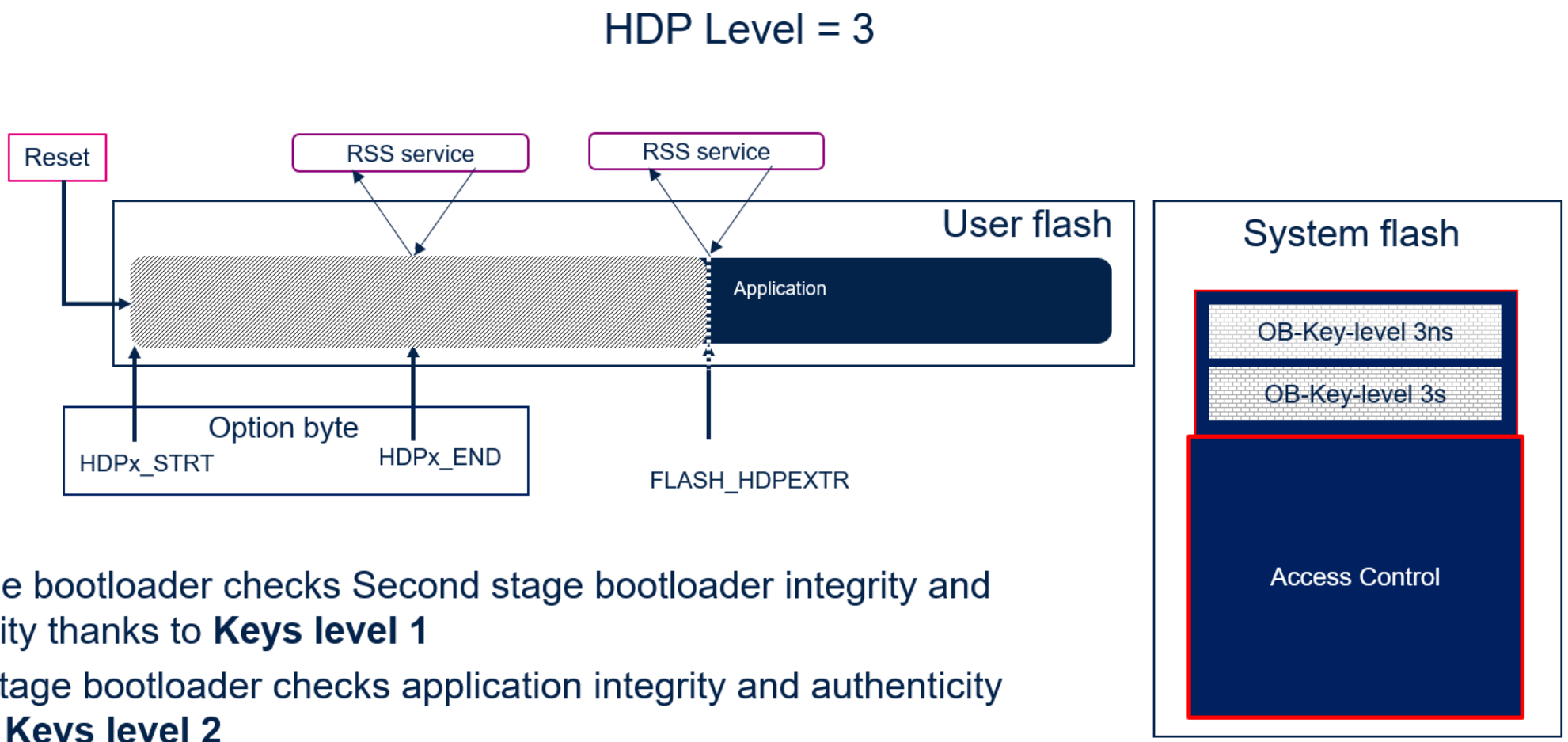




- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**
- Second stage bootloader checks application integrity and authenticity thanks to **Keys level 2**

life.augmented

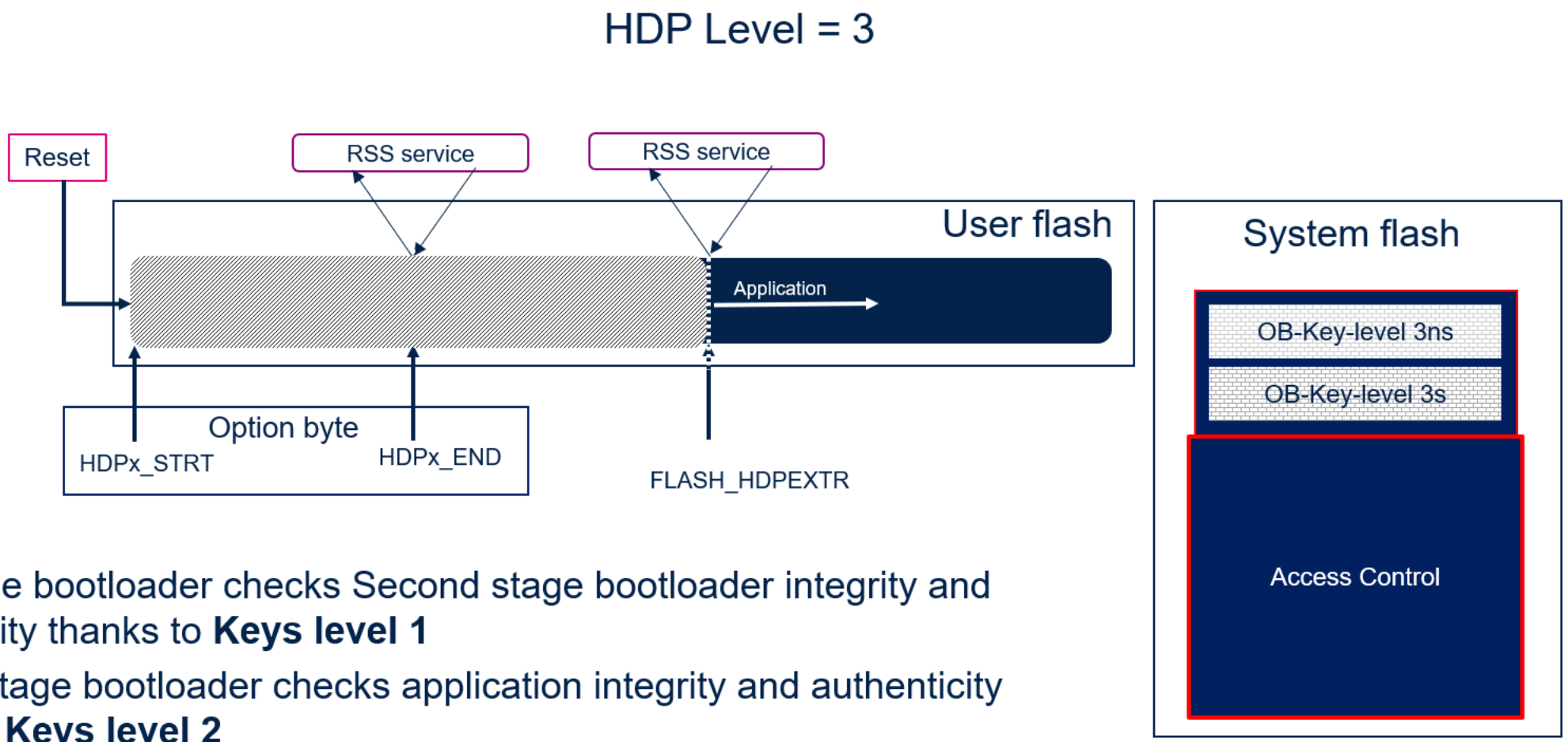
Temporal isolation and Secure storage



- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**
- Second stage bootloader checks application integrity and authenticity thanks to **Keys level 2**

life.augmented

Temporal isolation and Secure storage

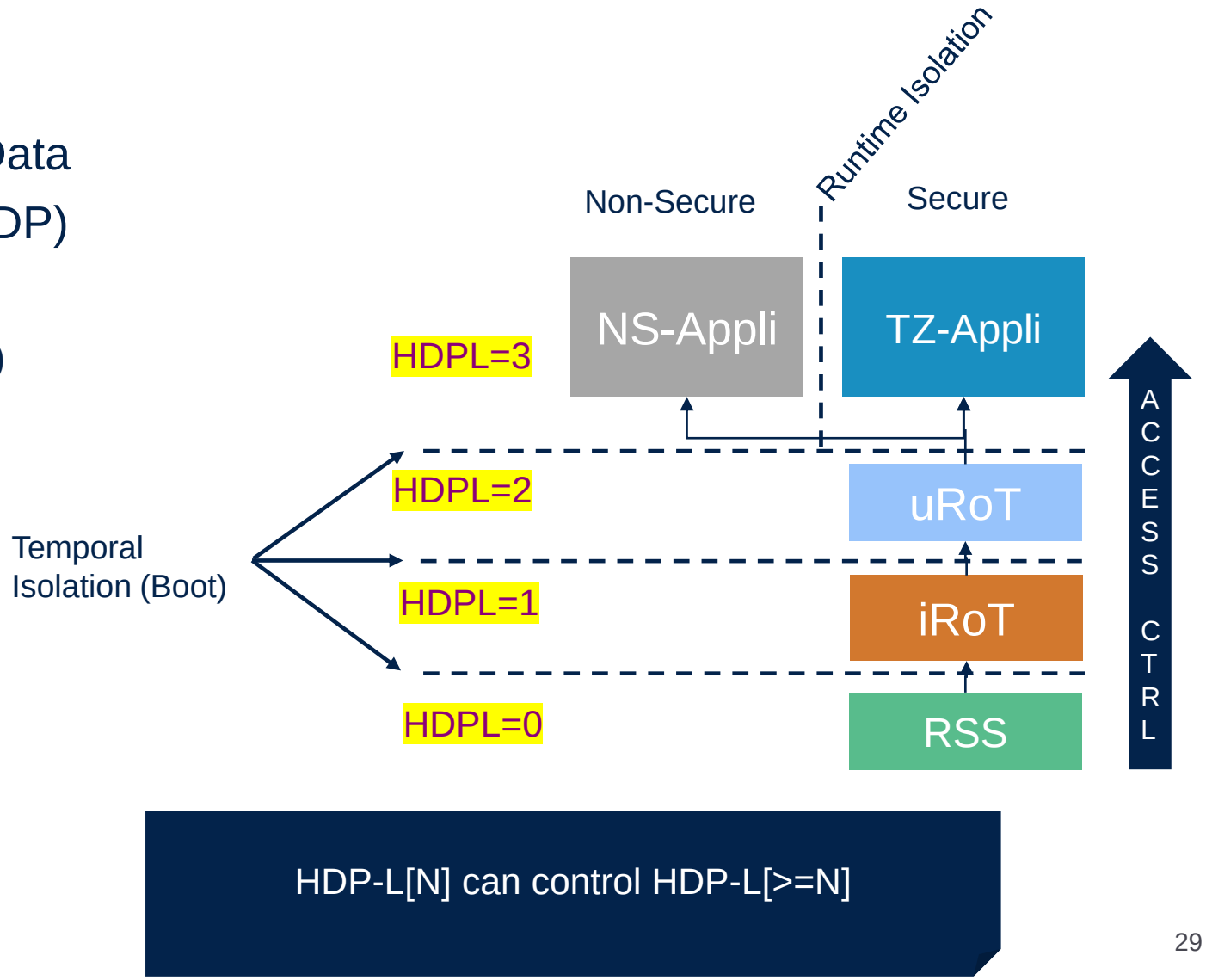


- First stage bootloader checks Second stage bootloader integrity and authenticity thanks to **Keys level 1**
- Second stage bootloader checks application integrity and authenticity thanks to **Keys level 2**

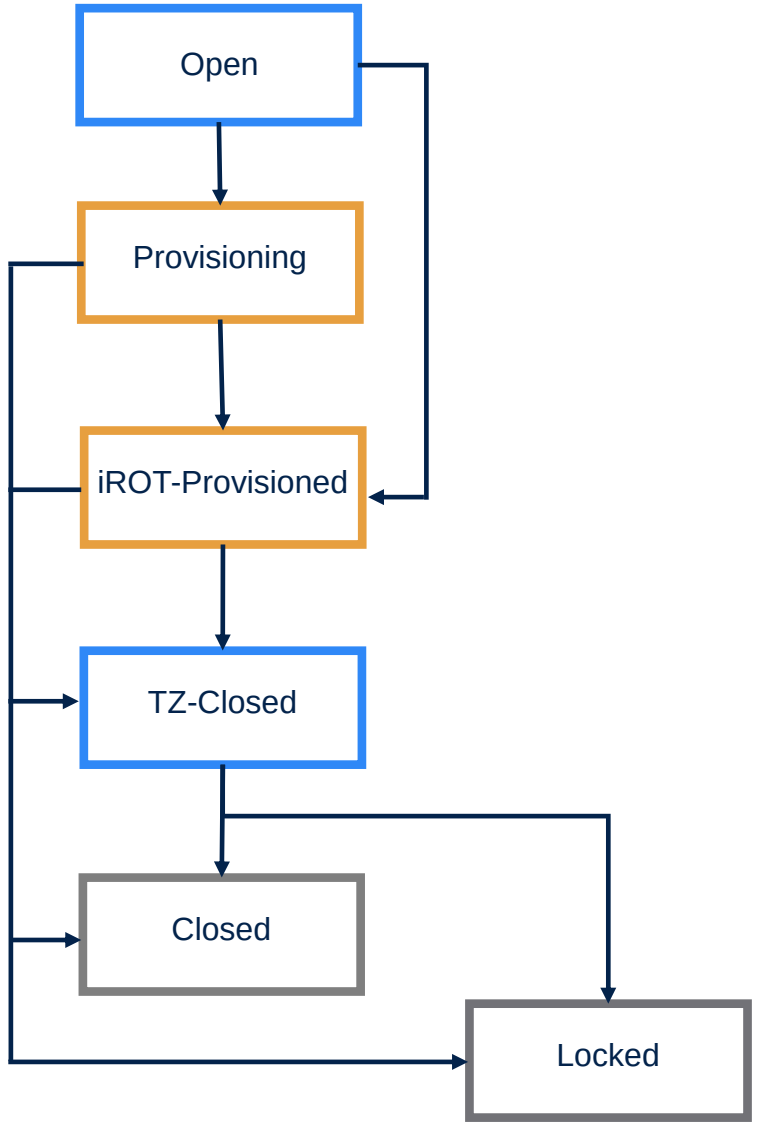
life.augmented

Temporal Isolation recap

- Temporal Isolation Levels: HDPLx
  - To manage access control on Code & Data
  - Code protected with Hide protection (HDP)
  - Data:
    - Flash OB-Keys (Physical Access Control)
      - 5 secure storage areas
        - HDPL0 ➔ST (never erased)
        - HDPL1 ➔iROT (ST-iROT or OEM-iROT)
        - HDPL2 ➔uROT
        - HDPL3 + Secure ➔Trust Zone
        - HDPL3 + NS ➔Non secure appli
    - Data can be Wrapped with DHUK
      - Based on HUK + Version counter
      - Different for each HDPLx



STM32H5 Product Life Cycle



RDP level 0

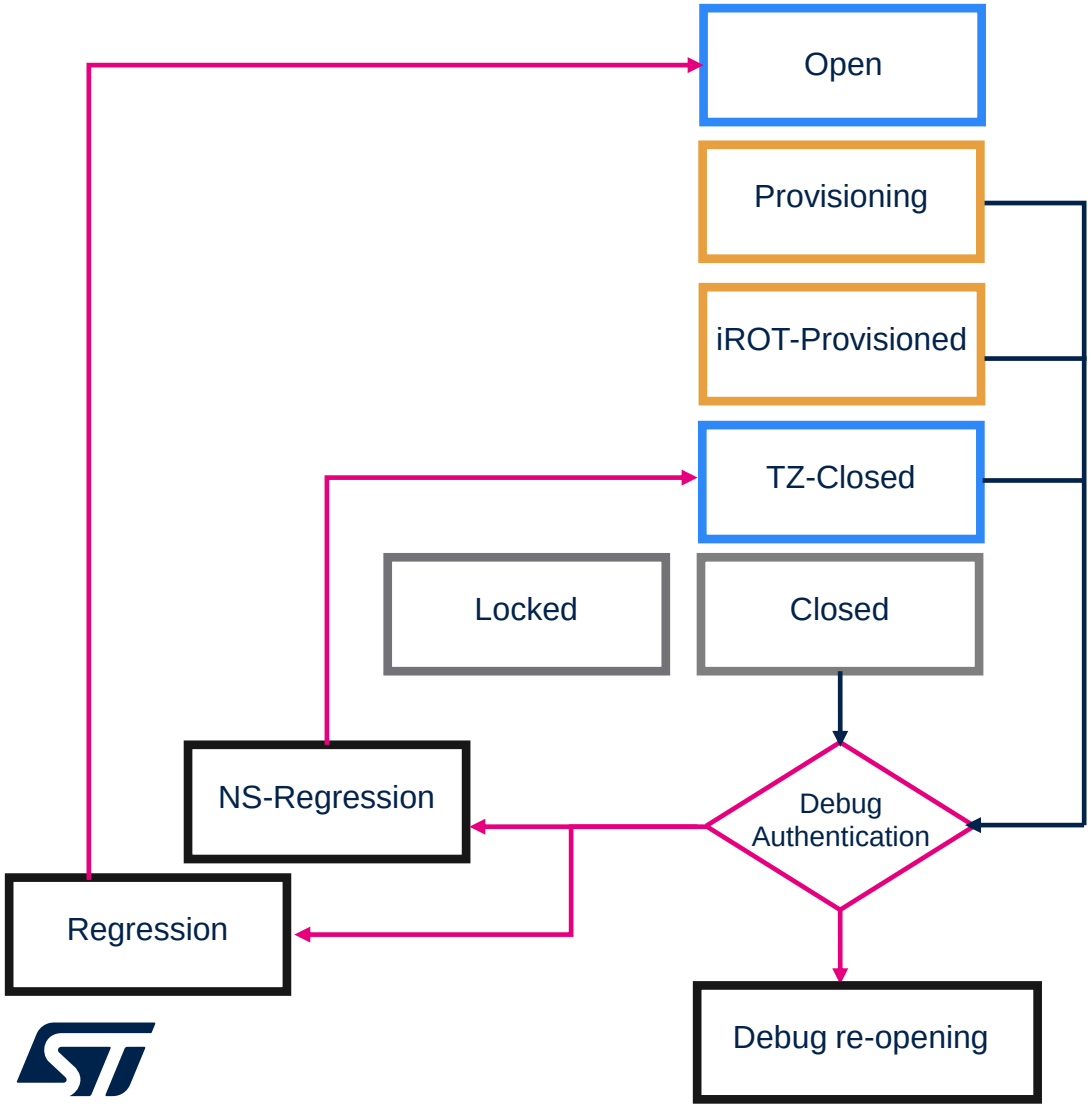
RDP level 0.5

Keyed RDP level 2

RDP level 2

life.augmented

Debug Authentication



NS-Regression

- NS flash code is erased
- OBK HDPL3NS are erased
- EPOCH_NS incremented
- Similar to RDP1 to RDP0.5 regression

Regression

- All the user flash code is erased
- OBK HDPL1,2,3S, 3NS are erased
- EPOCH_S and EPOCH_NS are incremented
- Similar to RDP1 to RDP0 regression

life.augmented

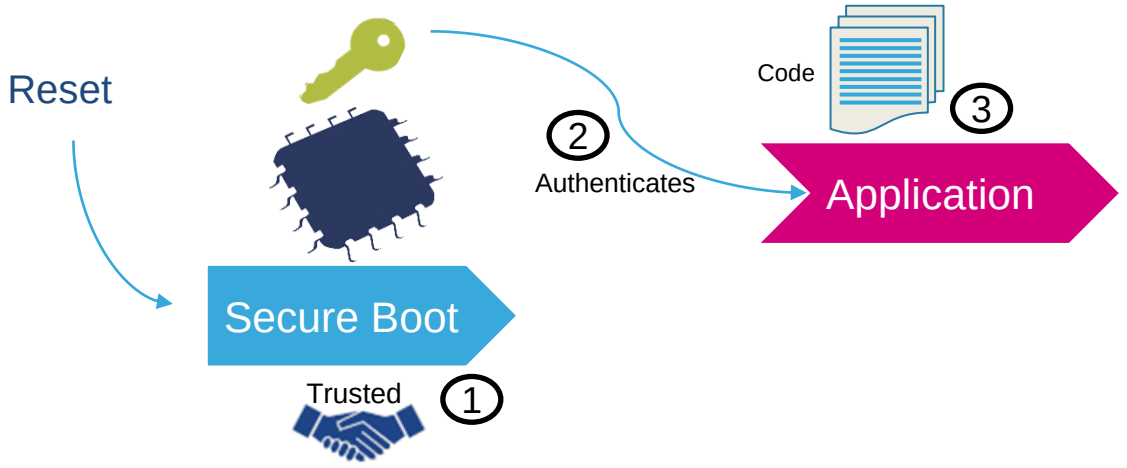
STiRoT

- STiRoT
  - stands for ST immutable (unchangeable) Root Of Trust and acts as a first boot stage.
  - is embedded in an immutable area of the system and provides two services:
    - Secure Boot (root of trust services)
    - Secure Firmware Update

- STiRoT selected configuration is:
  - ECDSA-256 asymmetric cryptography for image authenticity verification,
  - AES-CTR-128 symmetric cryptography with key ECIES-P256 encrypted for image confidentiality,
  - SHA 256 for image integrity check.
  - Keys dedicated to authentication and confidentiality are OEM assets and can be customized by OEM during the provisioning process.

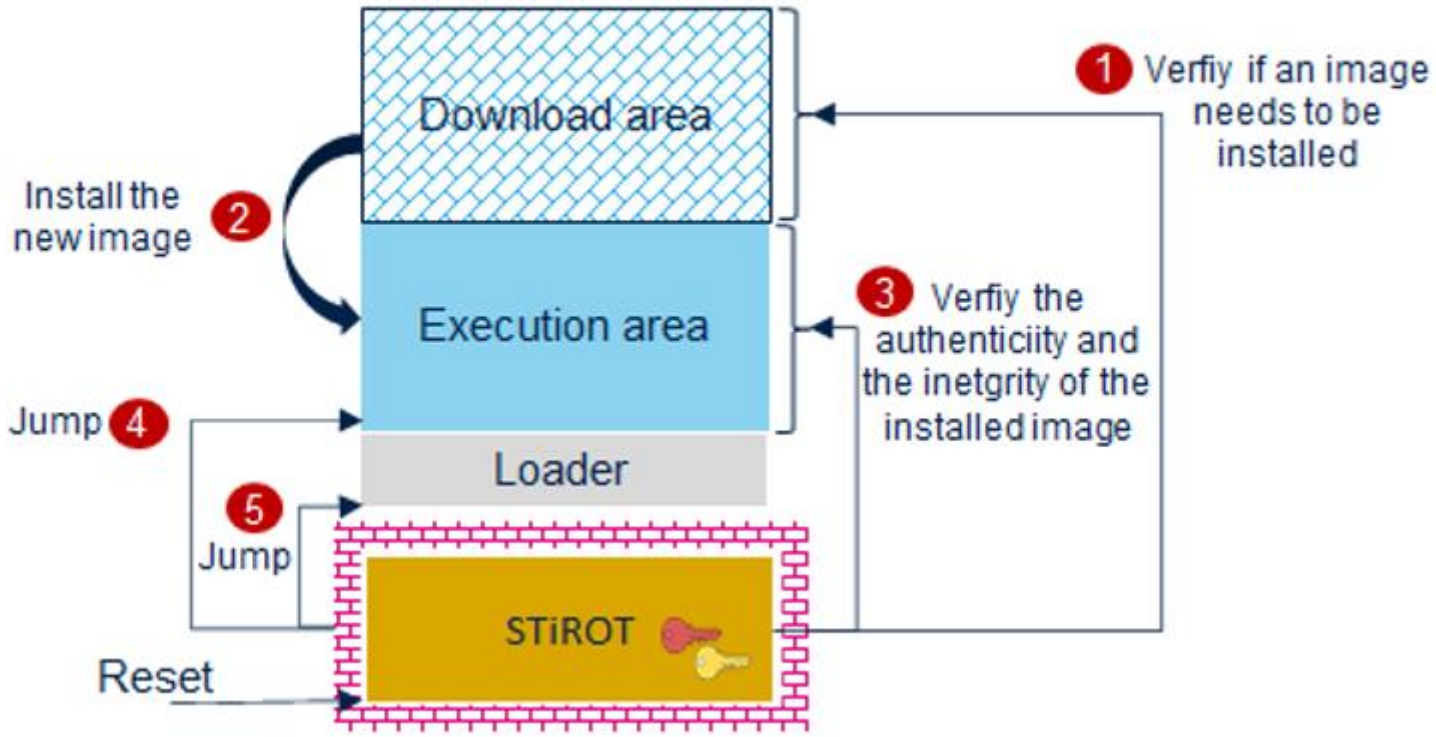
STiRoT: Secure Boot

- The Secure Boot (root of trust service) is an immutable code, which is always executed after a system reset (1). It activates STM32 runtime protections and then, it verifies the authenticity and integrity of the Application (2) code before every execution (3).



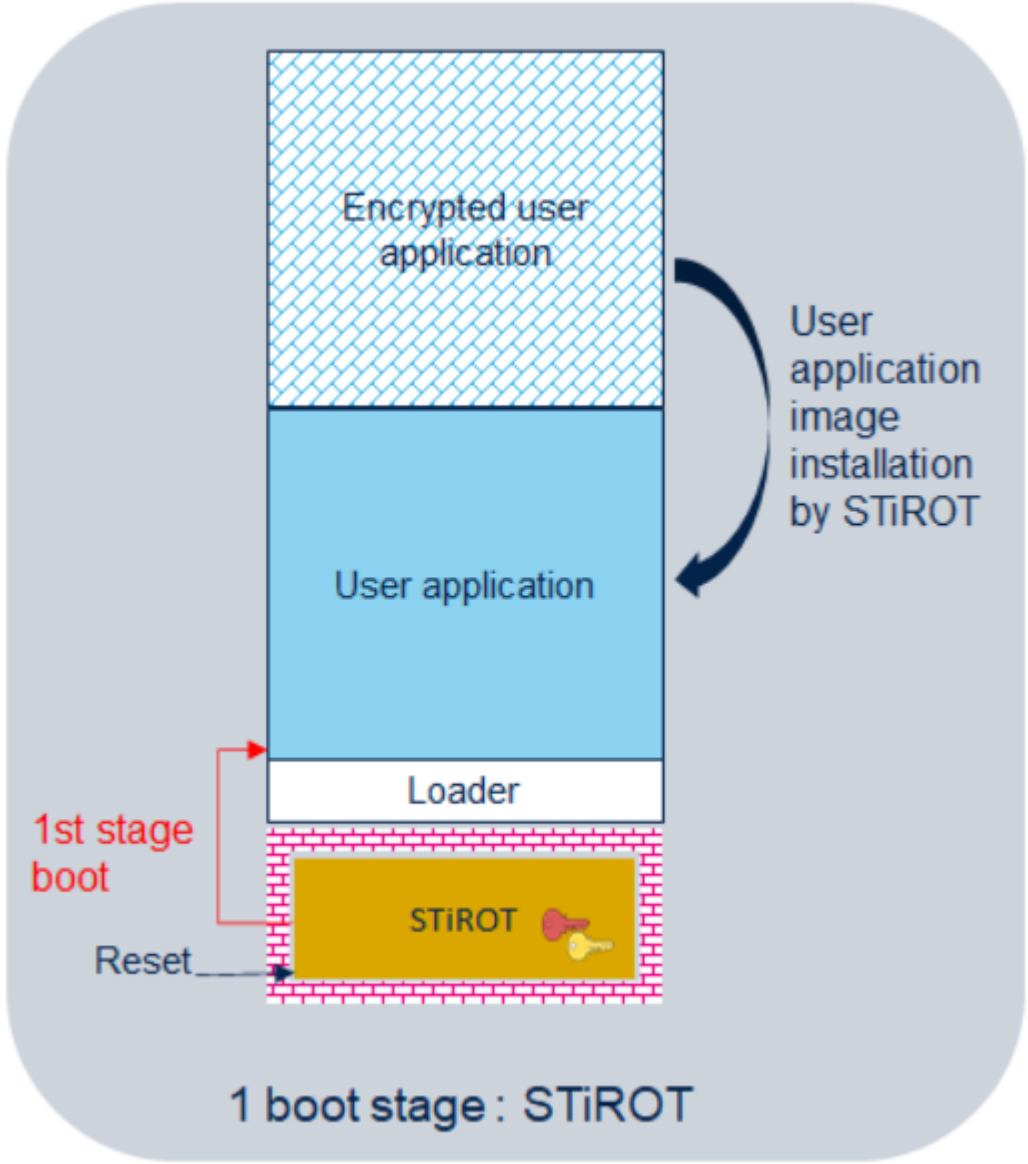
STiRoT: Startup sequence

- Option bytes should be configured to force the boot on STiROT.
- At reset, the following sequence will be executed



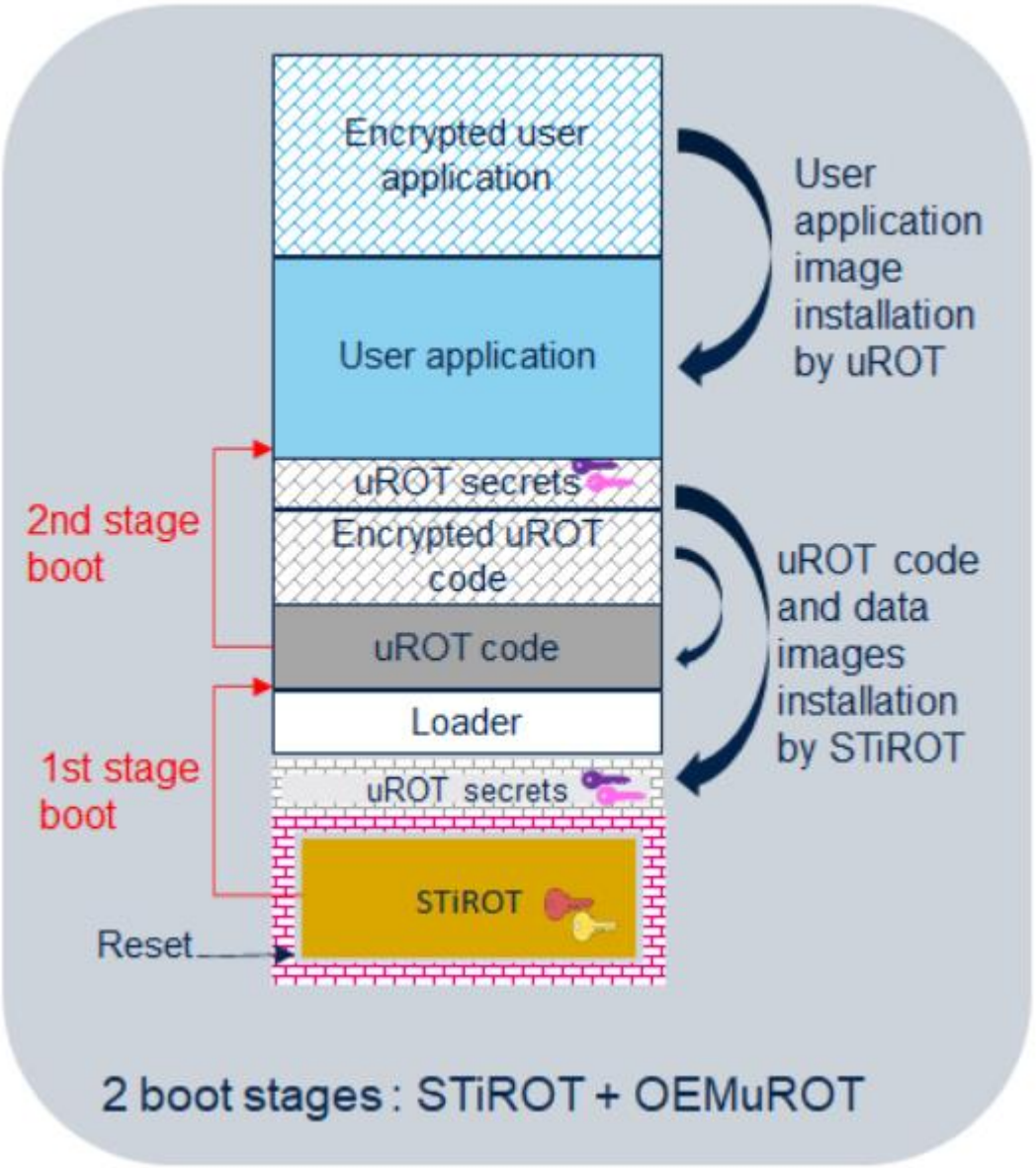
STiRoT: Use Cases 1/2

- 1 boot stage: Immutable ROT:
  - In this use case, most of the time STiRoT is configured to manage only one image: the user application



STiRoT: Use Cases 2/2

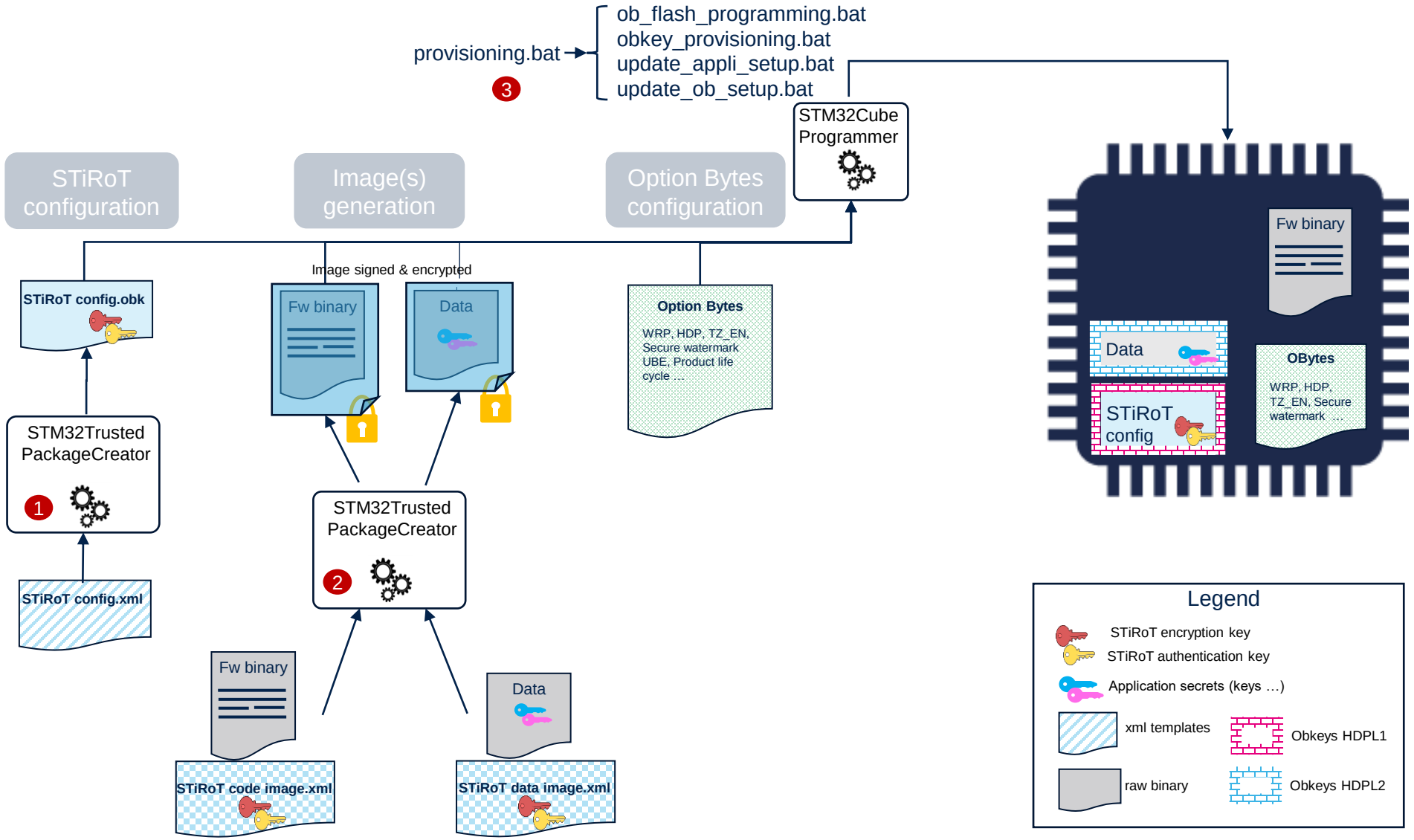
- 2 boot stages: Immutable and Updatable ROT
  - STiRoT is configured to manage two images, the uROT code and its associated secret data, such as authentication and encryption keys



life.augmented

STiRoT: Provisioning

- The product provisioning to activate the STiRoT booth path follows the steps below:



Recap

- The STM32H5 introduces
  - A new temporal isolation level
  - A secure storage coupled with temporal isolation
  - New device life cycle
  - The Debug Authentication
  - An embedded secure boot called STiROT
- Other available security features
  - Resource isolation using TrustZone
  - Hardware unique Key (HUK)
  - 2x AES 256, one with SCA resistance
  - AES and PKA, side attack resistant by HW.
  - ECC up to 640 bits and RSA up to 4160 bits
  - HASH: SHA-1, SHA-2 (up to 512)
  - TRNG
  - On The Fly Decryption on External OctoSPI Flash
  - Active tamper detections

life.augmented

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 & takeways

life.augmented

Our technology starts with You

Find out more at www.st.com

life.augmented