

PSOC™ Edge Protect Bootloader

Customer training workshop (CTW)

June 2026

Public

Prerequisites

Training prerequisites

- Introduction to PSOC™ Edge and ModusToolbox™
  - For an introduction to PSOC™ MCUs, including a getting started guide to ModusToolbox™, go to: https://www.infineon.com/product-information/psocdeveloper
  - For PSOC™ Edge training, from beginner tutorials to advanced training, visit: PSOC™ Edge E84 Training Collection

Development tools

- ModusToolbox™ v3.8 or later
- Eclipse IDE for ModusToolbox™ v2026.3.0
- Edge Protect Security Suite v1.6.1 or later
- ModusToolbox™ Programming Tools v1.8.1 or later
- KIT_PSE84_EVAL_EPC2 BSP v1.3.0 or later / KIT_PSE84_AI v1.3.0 or later
- Terminal Emulator

Hardware requirements

- KIT_PSE84_EVAL or KIT_PSE84_AI

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Introduction 4

2 Bootloader features 10

3 Running EPB from different memories 30

4 Lab 35

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 **Introduction** **4**

2 Bootloader features 10

3 Running EPB from different memories 30

4 Lab 35

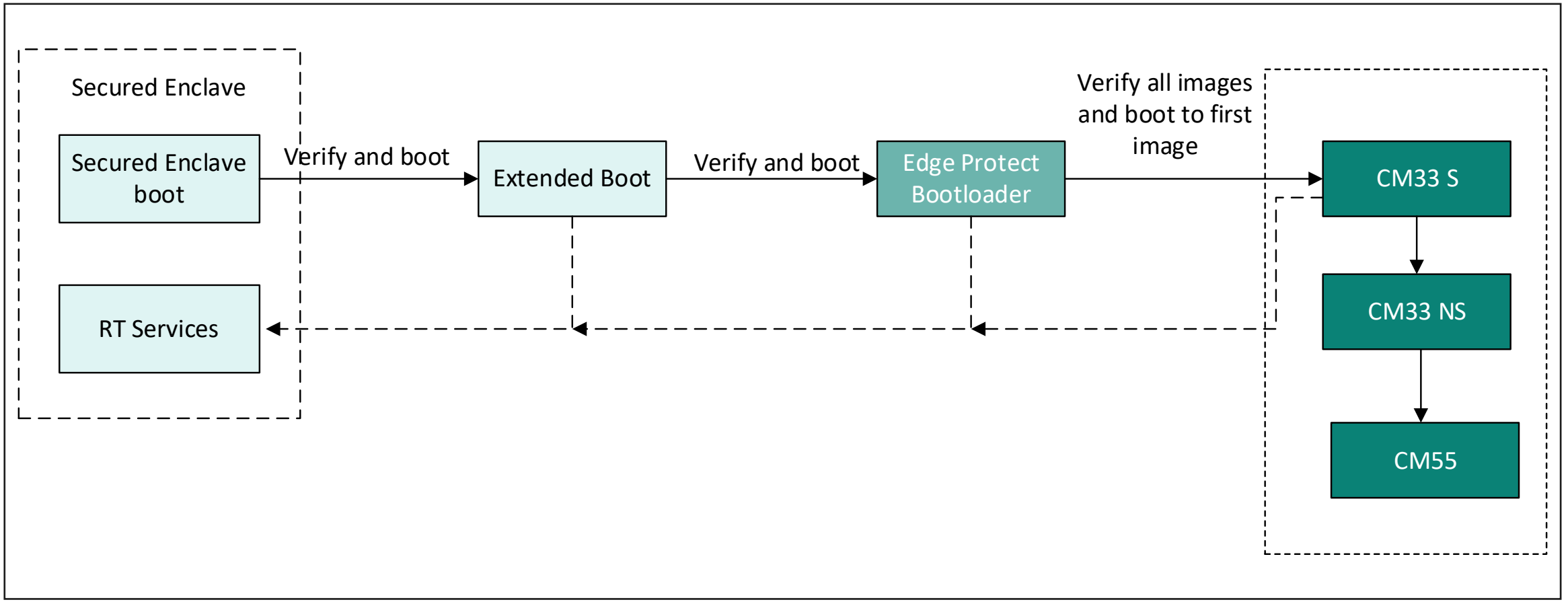
Copyright © Infineon Technologies AG 2026. All rights reserved.

Introduction to Edge Protect Bootloader (EPB)

- Edge Protect Bootloader (EPB) is an open-source MCUboot library-based bootloader for PSOC™ Edge MCU
- This is an optional bootloader stage, owned by the OEMs. This is the first OEM code that is executed when present in the boot chain
- Infineon provides the EPB as a code example along with the open-source MCUboot library
- EPB extends the chain of trust (CoT) from the extended boot to the rest of the applications in the system, i.e., the extended boot verifies and loads EPB, and the EPB verifies and loads the rest of the images
- In default configurations, the EPB can verify up to three images and launch the next image in the boot sequence
- EPB is designed to run in the secure mode of the CPU, with all resource access privileges available to it. It is hardened against physical attacks using the FIH library. This is the same fault injection hardening (FIH) library that the open-source MCUboot uses

Copyright © Infineon Technologies AG 2026. All rights reserved.

Chain of trust (CoT)



Copyright © Infineon Technologies AG 2026. All rights reserved.

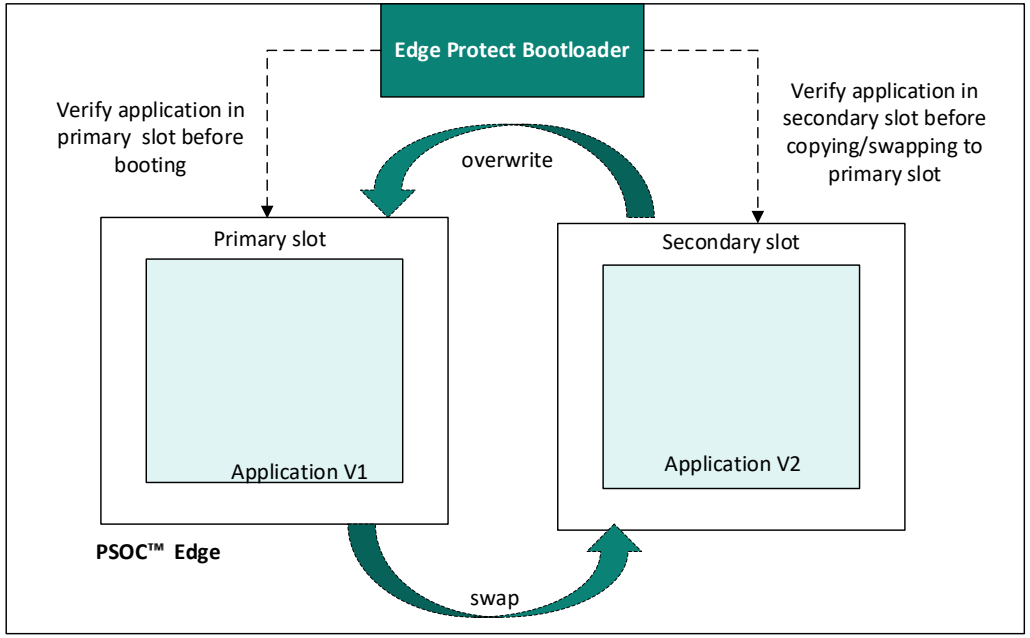
Secure boot of Edge Protect Bootloader

- For a complete CoT, it is essential that Edge Protect Bootloader is authenticated by the extended boot, before launching
- Before launching, the extended boot authenticates the Edge Protect Bootloader using ECDSA P256. It uses OEM_ROT_KEY (public) provisioned to the device for image authentication
- Edge Protect Bootloader must be signed using OEM_ROT_KEY (private)

Copyright © Infineon Technologies AG 2026. All rights reserved.

Memory map

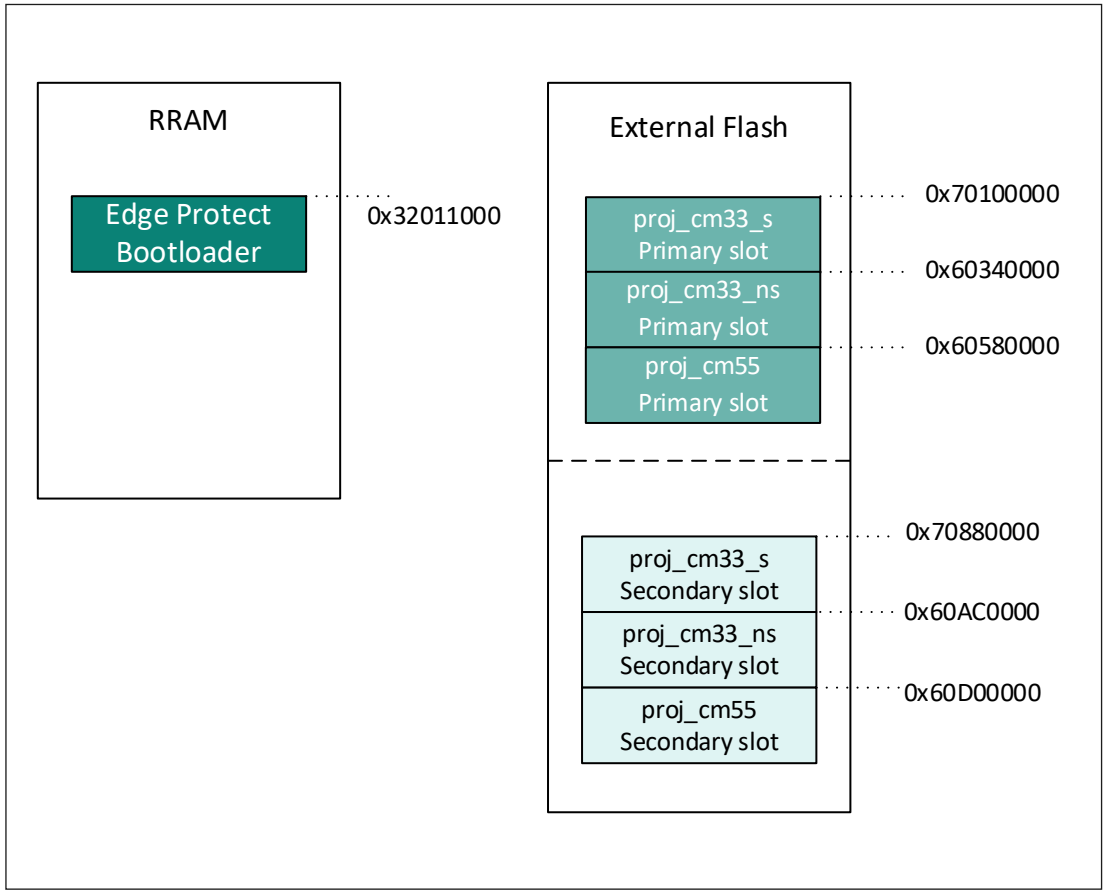
- The flash memory can be divided into multiple image areas, with each containing two image slots:
  - Primary slot
  - Secondary slot
- EPB validates and executes the application from the primary slot
- EPB validates the upgrade image in the secondary slot and copies it to the primary slot for execution



Copyright © Infineon Technologies AG 2026. All rights reserved.

Memory map (contd.)

- Memory map describes allocated memory areas for different application slots and defines their start offsets and sizes
- It is defined at compile time and cannot be changed dynamically
- When the flash memory contains multiple executable images , the flash must be partitioned to allocate two slots for each image



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Introduction 4

2 **Bootloader features** **10**

3 Running EPB from different memories 30

4 Lab 35

Copyright © Infineon Technologies AG 2026. All rights reserved.

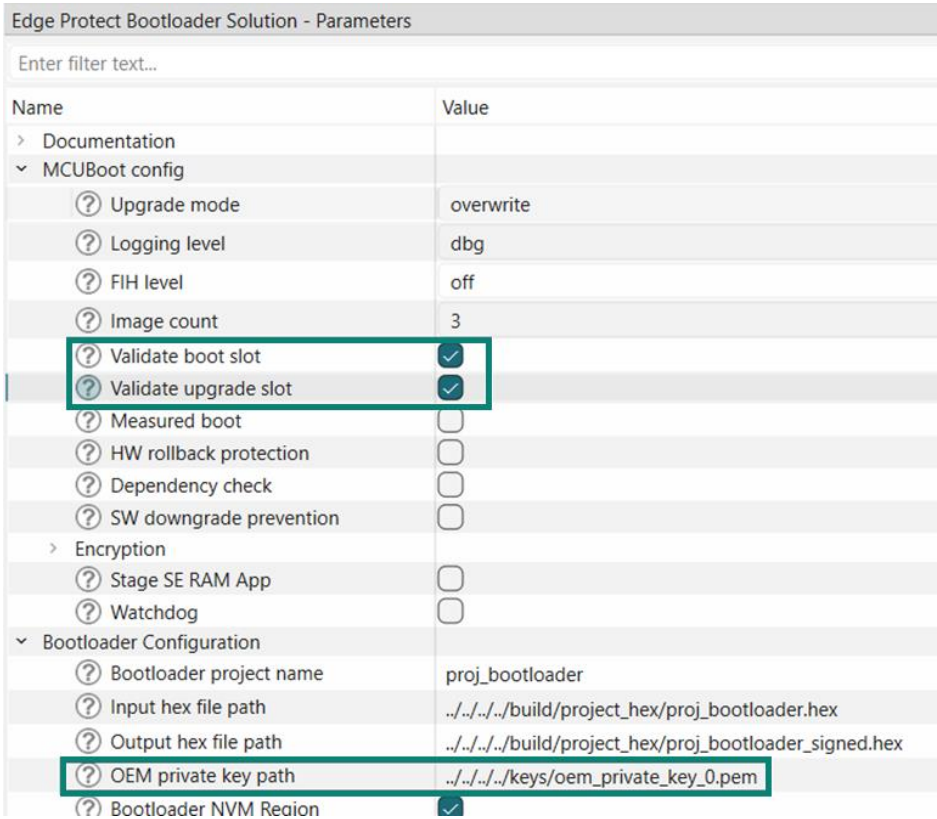
Image validation

- During the normal boot, EPB validates that the image is in the MCUboot image format
- When secure boot is enabled in the EPB, it performs additional signature verification of the images
- EPB uses the OEM_ROT_KEY provisioned in the device to verify the application images
- EPB makes use of the basic runtime (RT) services running on Secure Enclave to authenticate the application using ECDSA P256

Copyright © Infineon Technologies AG 2026. All rights reserved.

Image validation (contd.)

– Secure boot in EPB can be enabled by enabling the Validate boot slot and Validate upgrade slot options in the bootloader solution. Provide the path to the OEM private key to be used to sign the application.



Copyright © Infineon Technologies AG 2026. All rights reserved.

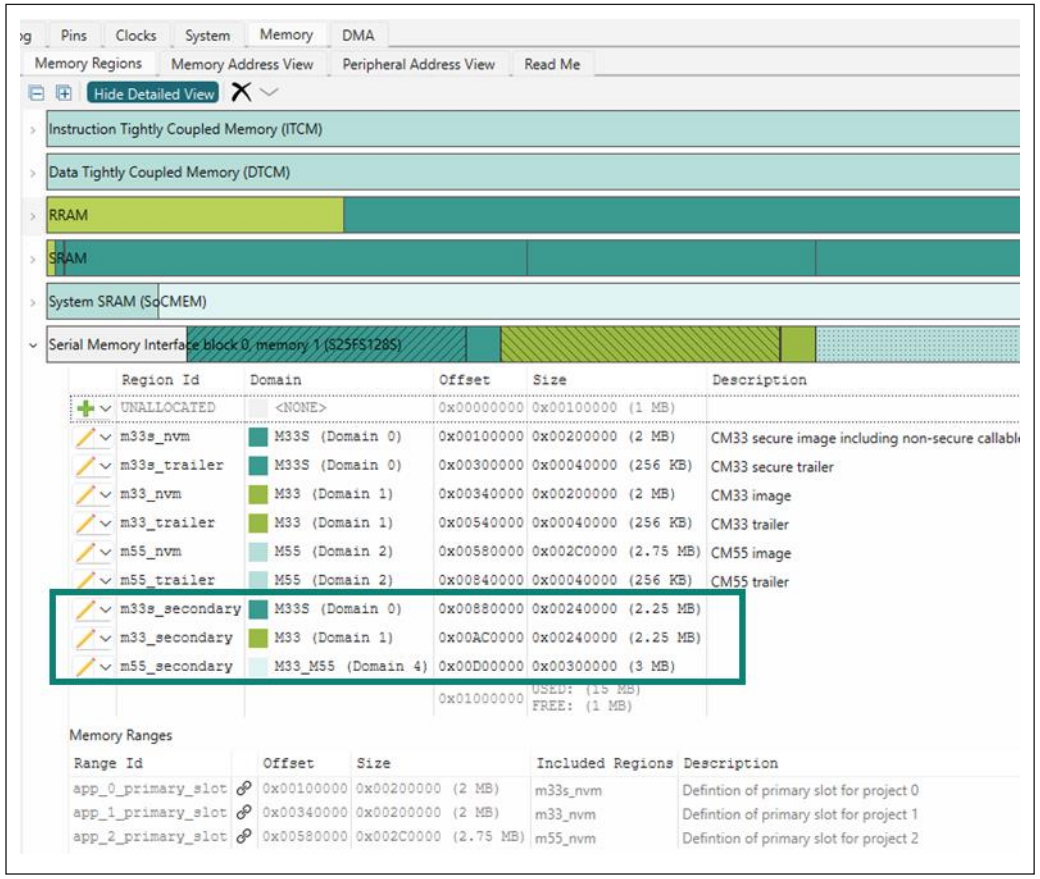
Image upgrade

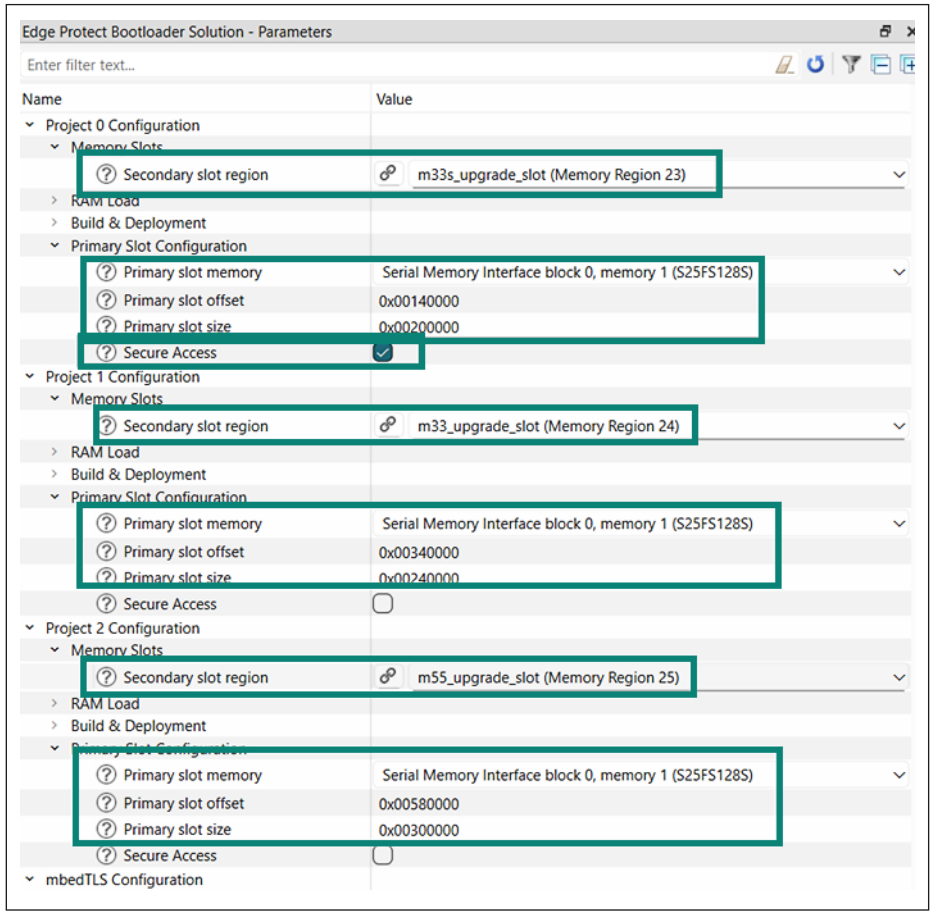
- For the firmware update use case, upgrade images are downloaded to secondary slots by the user application
- EPB detects the new image in the upgrade slot, validates it, copies it to the primary slot and launches the application
- EPB supports two different image upgrade methods:
  - Upgrade by overwrite
  - Upgrade by swap
- Either of these methods can be configured at compile time, and the compiled bootloader will only support the selected upgrade method
- The update process is a power fail-safe. If a power failure happens in the middle of an update, the Edge Protect Bootloader will perform the update on the next reset of the device

Copyright © Infineon Technologies AG 2026. All rights reserved.

Image upgrade (contd.)

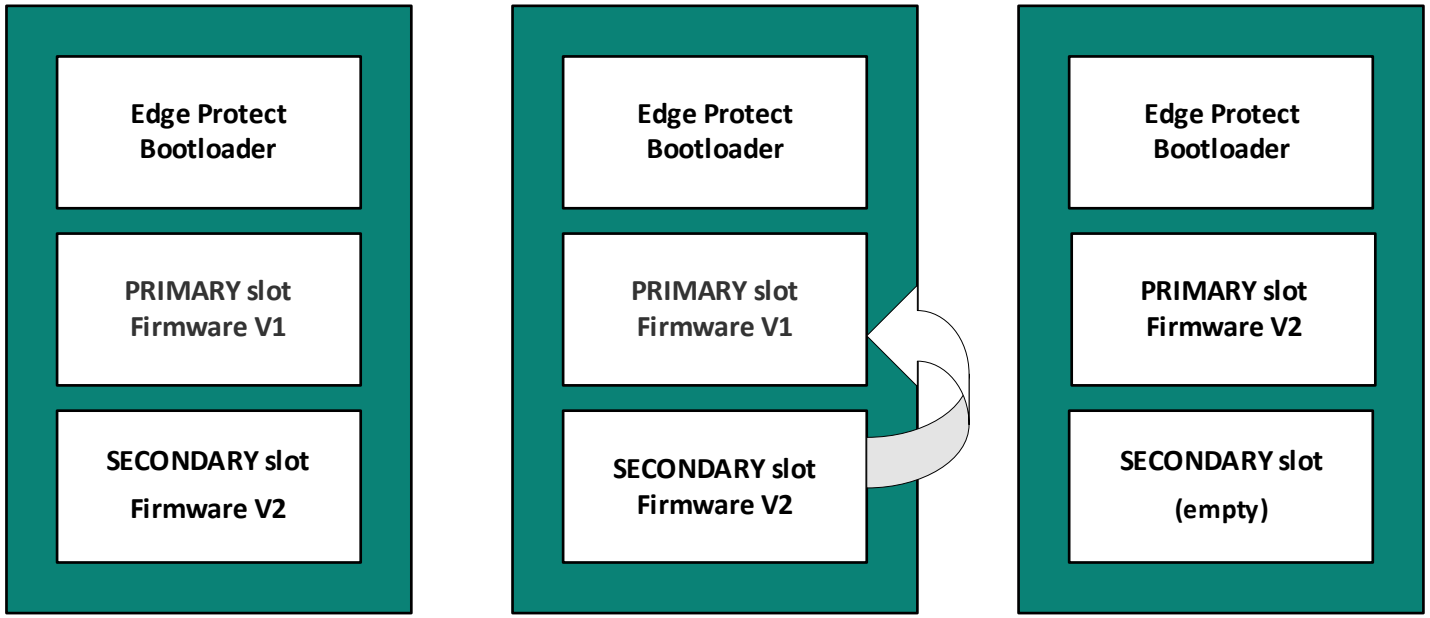
– To enable the image upgrade using the ModusToolbox™, create the upgrade slots for each image in the Memory tab of the device configurator as shown





Copyright © Infineon Technologies AG 2026. All rights reserved.

Upgrade by overwrite



Before upgrade, PRIMARY slot contains the V1 version of firmware and SECONDARY slot contains the V2 version of the firmware.

During upgrade, V2 version of the firmware will be copied from SECONDARY slot to PRIMARY slot and the V1 version will be lost

After upgrade, the PRIMARY slot contains the new version of the firmware the SECONDARY slot is erased

Copyright © Infineon Technologies AG 2026. All rights reserved.

Upgrade by overwrite (contd.)

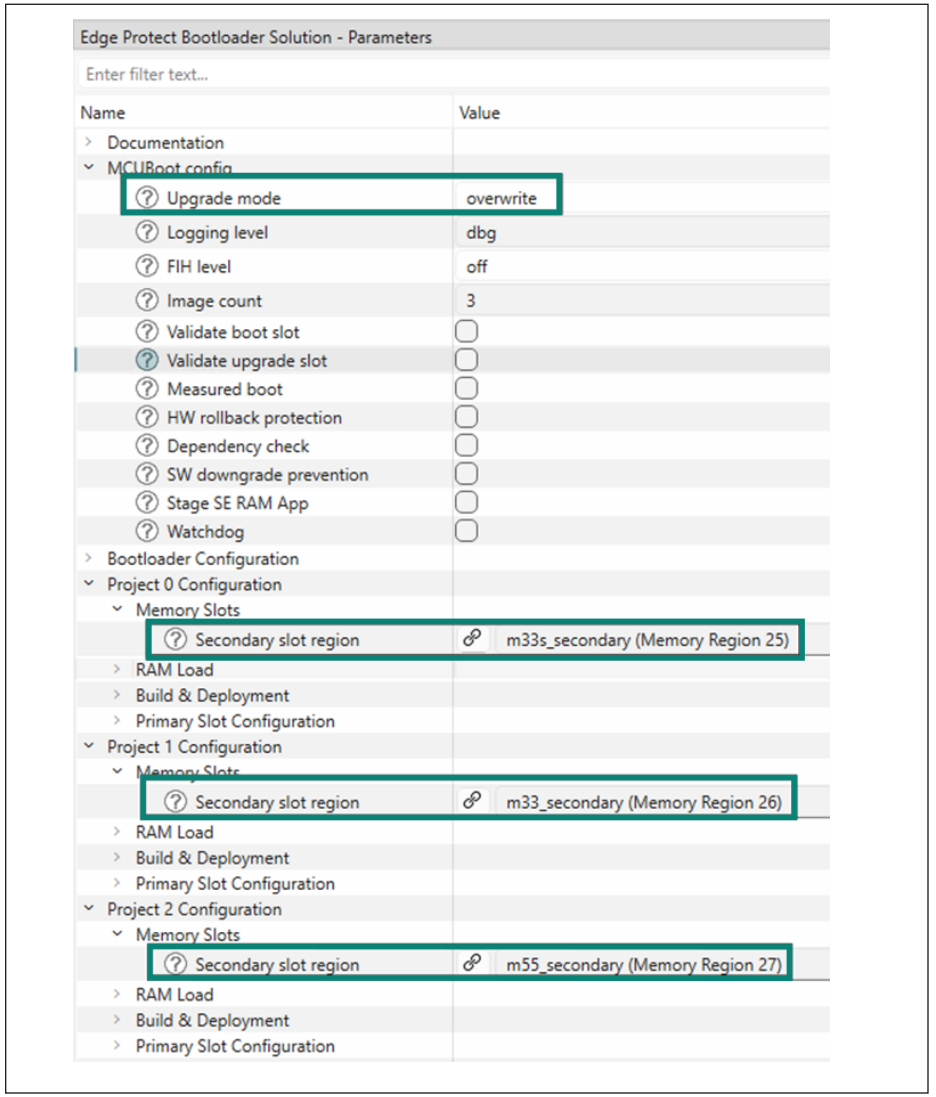
- This upgrade method can be selected in the bootloader solution personality
- The secondary slots for each image must also be allocated in the Memory tab of the device configurator and linked in the bootloader solution personality
- In the ModusToolbox™ application, common.mk file; uses the bootloader solution-generated JSON file for boot and upgrade images

- For `BOOT_IMAGE` : Combine application projects and EdgeProtect bootloder project for initial programming and booting.

```
COMBINE_SIGN_JSON?=./bsps/TARGET_$(TARGET)/config/GeneratedSource/boot_with_bldr.json
```

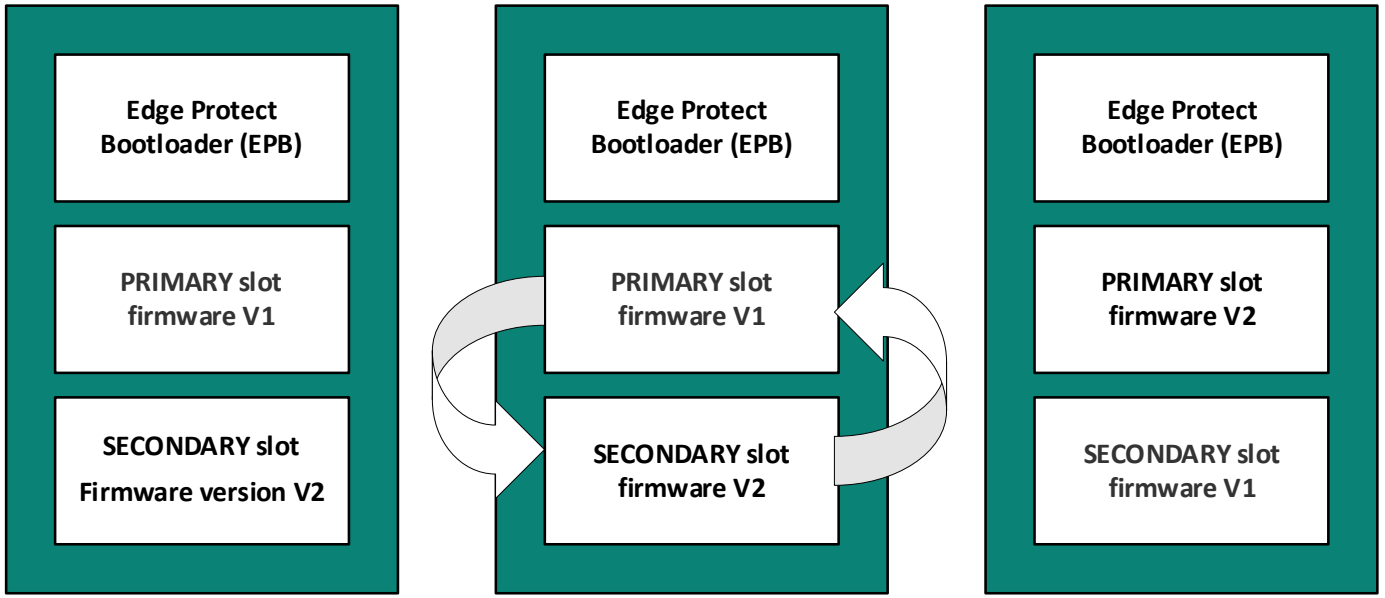
- For `UPDATE_IMAGE` : Combine only the application projects for update

```
COMBINE_SIGN_JSON?=./bsps/TARGET_$(TARGET)/config/GeneratedSource/boot_with_bldr_upgr.json
```



Copyright © Infineon Technologies AG 2026. All rights reserved.

Upgrade by swap



Before upgrade, PRIMARY slot contain the V1 version of the firmware and SECONDARY slot contains V2 version

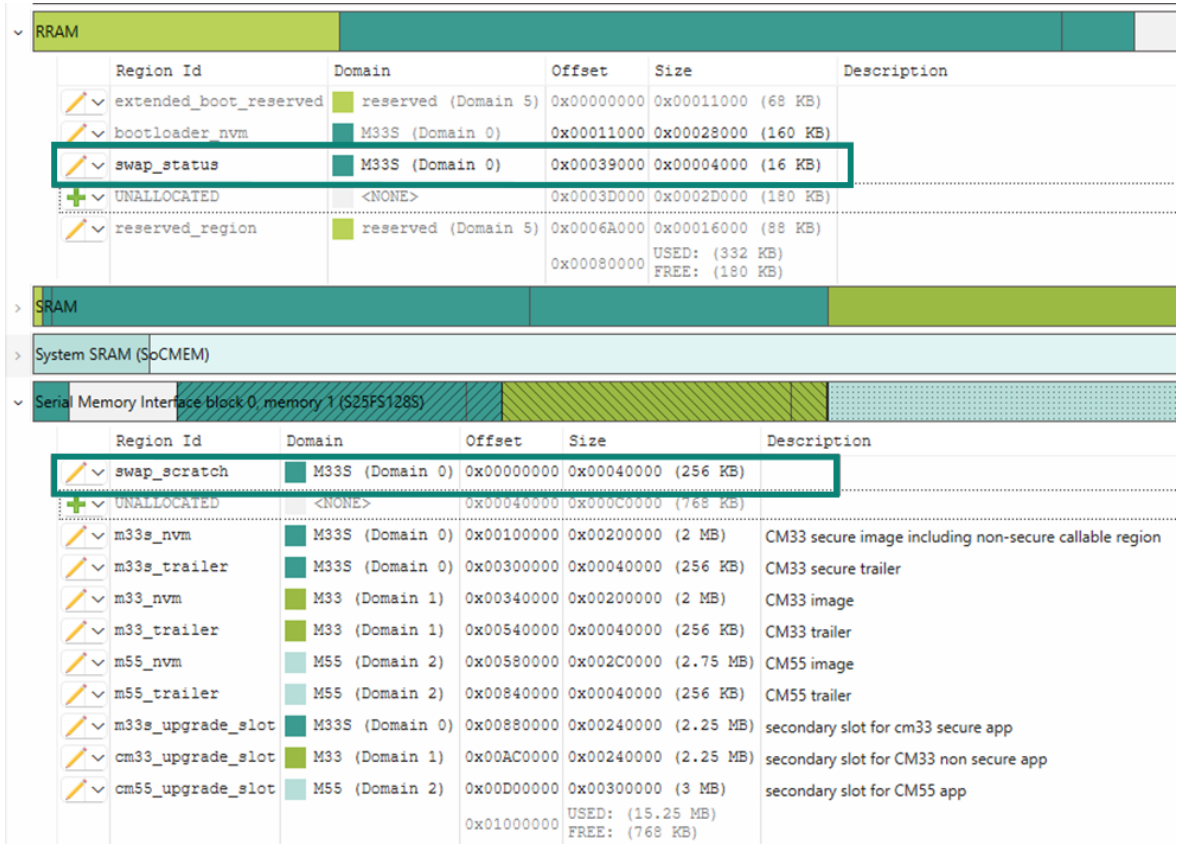
During swap upgrade, V2 version which is programmed to SECONDARY slot will be swapped with the V1 version of the firmware in PRIMARY slot

After swap upgrade, PRIMARY slot contains the V2 version , while SECONDARY slot contains the V1 version of the firmware

Copyright © Infineon Technologies AG 2026. All rights reserved.

Upgrade by swap (contd.)

– To enable swap upgrade in the ModusToolbox™ application, create new memory regions for swap_status and swap_scratch region as shown below:



Copyright © Infineon Technologies AG 2026. All rights reserved.

Upgrade by swap (contd.)

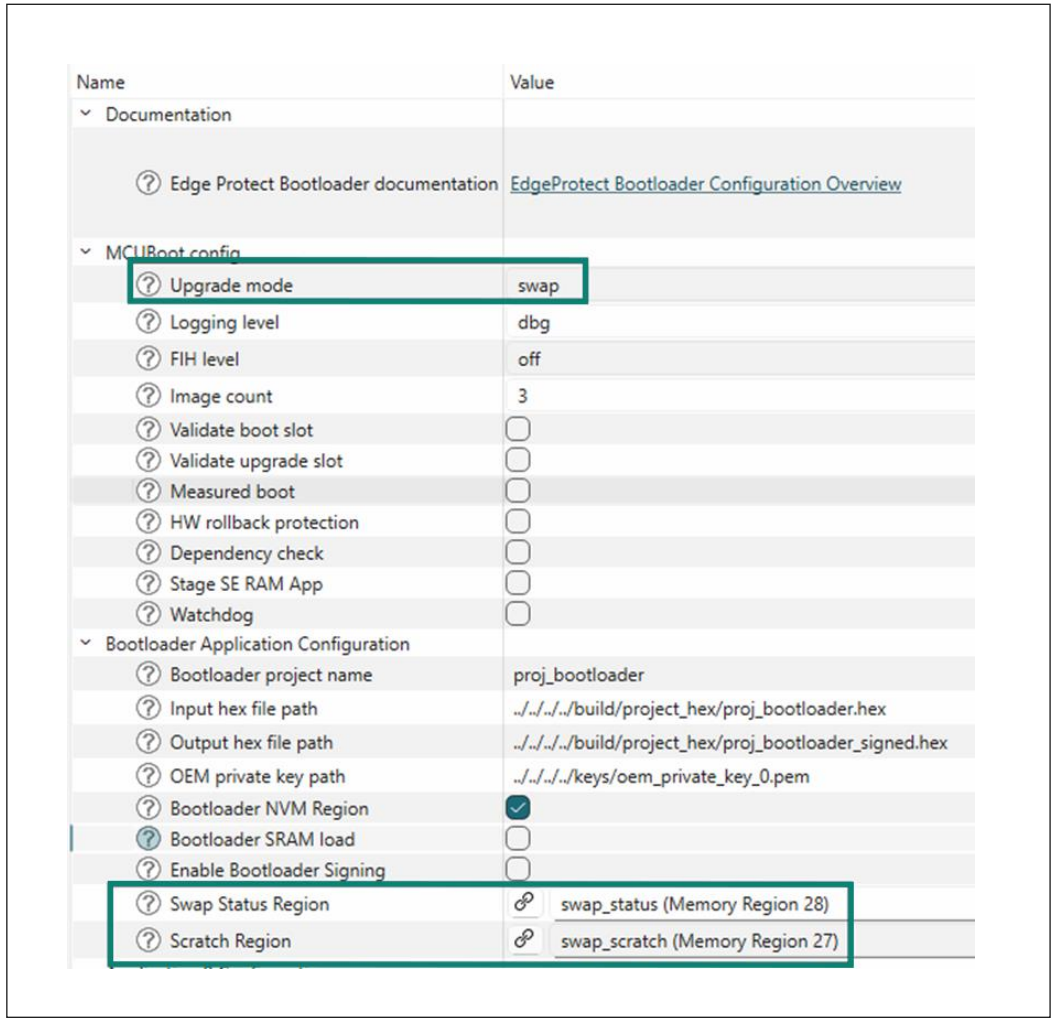
- This upgrade method can be selected in the bootloader solution personality
- The secondary slots for each image, swap status and swap scratch regions must be linked in the bootloader solution personality
- In the ModusToolbox™ application, common.mk file; use the bootloader solution-generated JSON file for boot and upgrade images

- For `BOOT_IMAGE` : Combine application projects and EdgeProtect bootloder project for initial programming and booting.

```
COMBINE_SIGN_JSON?=./bsps/TARGET_$(TARGET)/config/GeneratedSource/boot_with_bldr.json
```

- For `UPDATE_IMAGE` : Combine only the application projects for update

```
COMBINE_SIGN_JSON?=./bsps/TARGET_$(TARGET)/config/GeneratedSource/boot_with_bldr_upgr.json
```



Copyright © Infineon Technologies AG 2026. All rights reserved.

Downgrade prevention

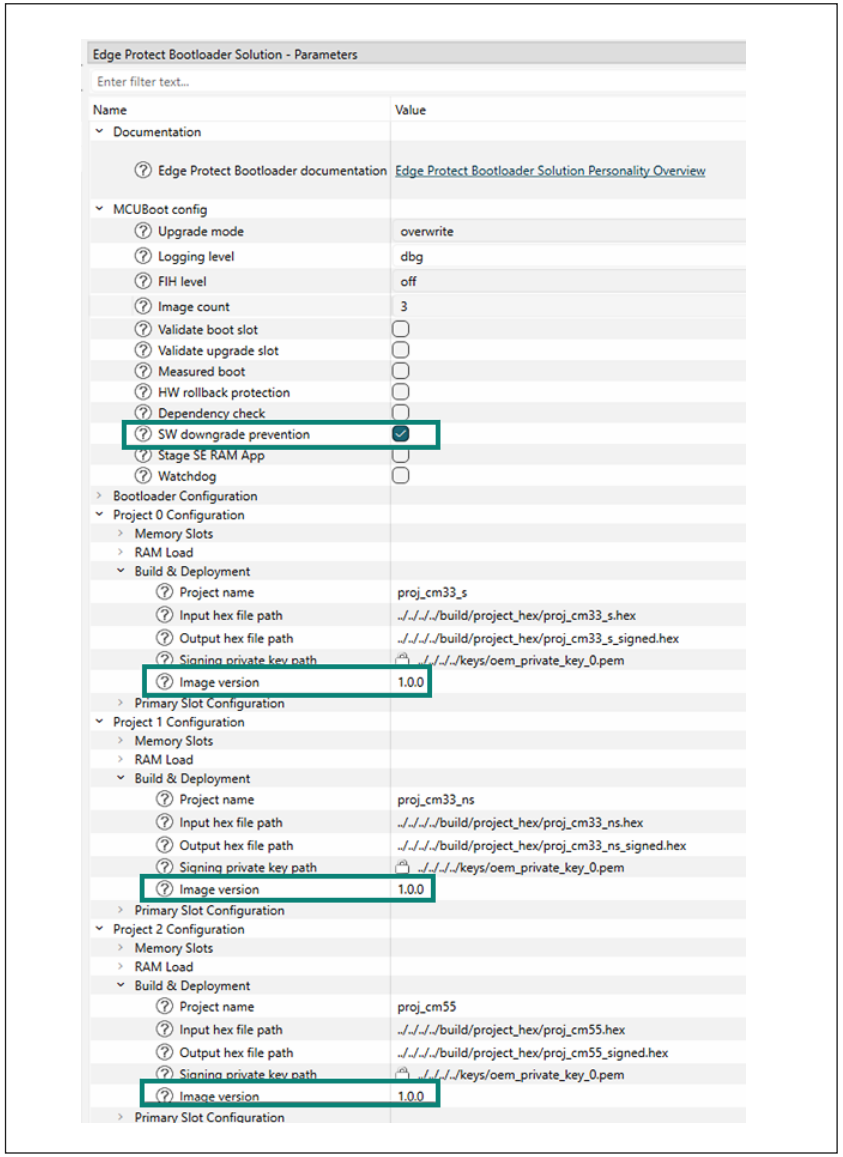
- Downgrade prevention is a feature that ensures that only firmware with a higher version or security counter can replace an existing image
- This safeguards against malicious attempts to revert the device to a potentially vulnerable older version
- There are two types of downgrade prevention
  - Software-based downgrade prevention
  - Hardware-based downgrade prevention

Copyright © Infineon Technologies AG 2026. All rights reserved.

Software-based downgrade prevention

- Software-based downgrade prevention compares image version numbers to block installations of older firmware
- This feature works exclusively with the overwrite-based image update strategy
- EPB will reject the image upgrade if the new image contains a lower major, minor, or patch version

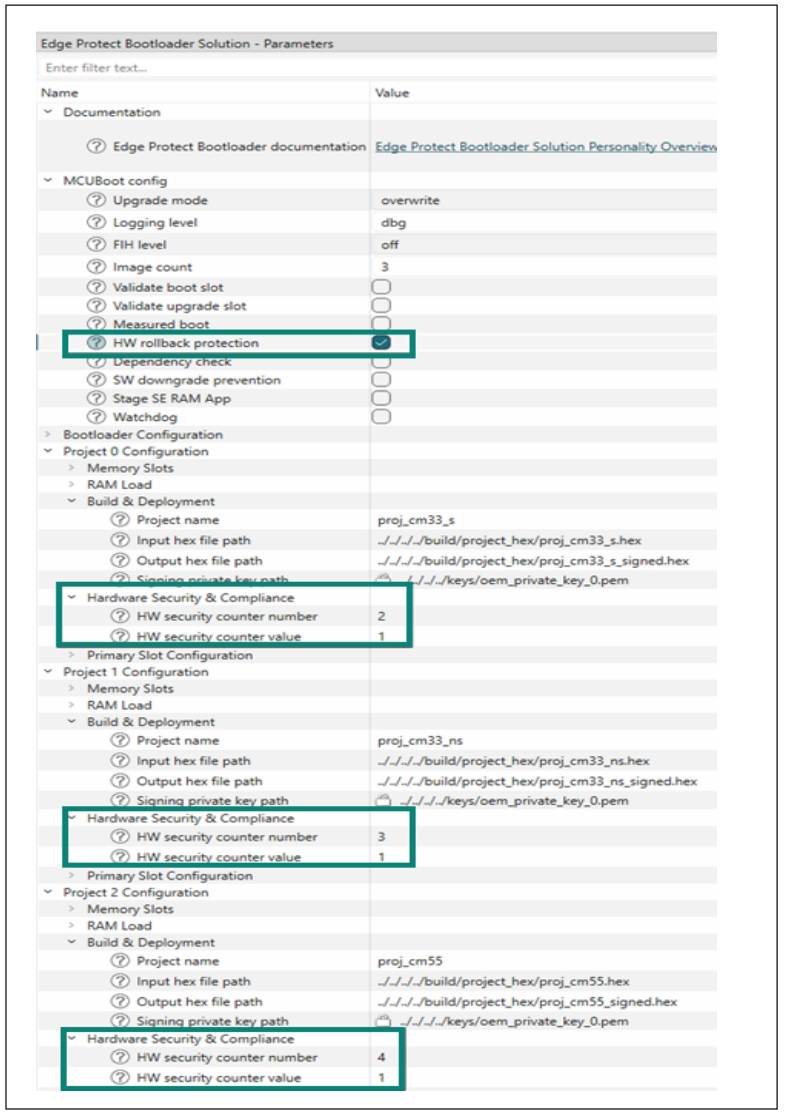
Current image version	Upgrade image version	EPB action
1.2.3	1.2.2	Upgrade rejected



Copyright © Infineon Technologies AG 2026. All rights reserved.

Hardware-based downgrade prevention

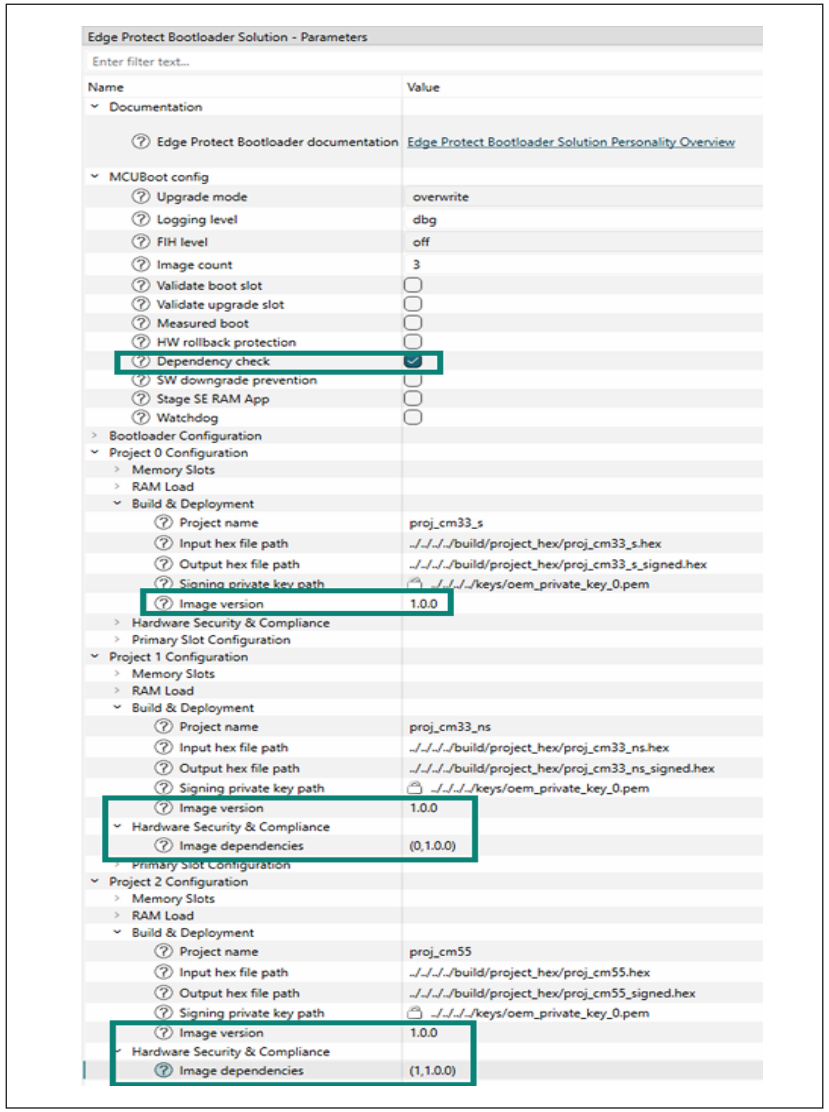
- Each signed image can contain a security counter in its protected TLV area
- During the hardware-based downgrade prevention (rollback protection). The new image's security counter value will be compared with the currently active security counter (stored in the Secure Enclave)
- HW security counter number refers to the number of the counter cell in the device. It can be set in the range of 2-7
- HW security counter value refers to the counter value that is stored in the counter. It can be set in the range of 1-63 or left unchanged



Copyright © Infineon Technologies AG 2026. All rights reserved.

Dependency check

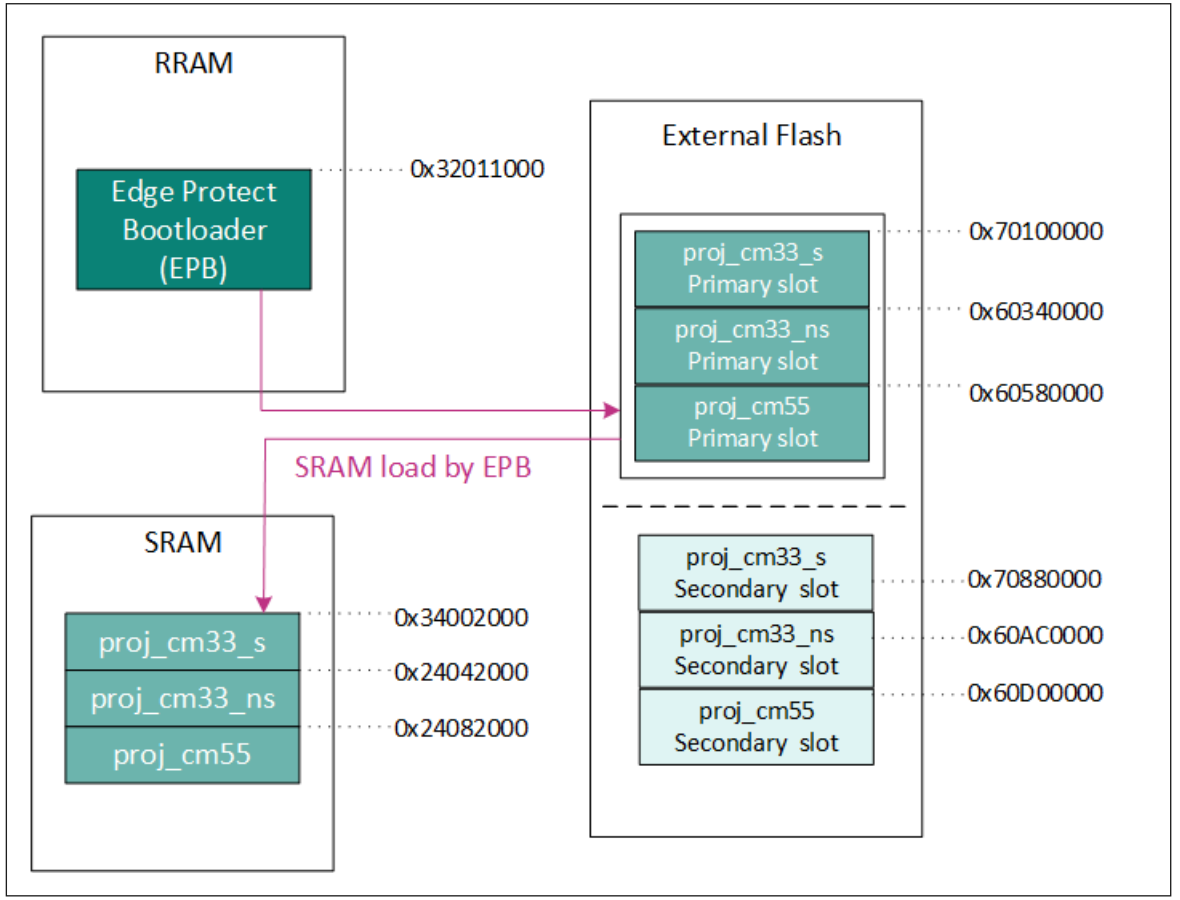
- When enabled, EPB performs dependency checks and rejects incompatible updates
- Useful feature when only one of the applications is being updated
- Set image dependencies in the format: (image_ID, image_version) where the image_ID on which this image depends. It starts from 0. image_version version on which this image depends. One image can depend on several other images, such as (1, 1.1.0), (2, 2.0.0)



Copyright © Infineon Technologies AG 2026. All rights reserved.

SRAM loading by EPB

- Execution of user application from the external flash has some drawbacks such as lower execution speed, higher power consumption etc., when compared to execution from SRAM
- Bootloader supports the RAM loading of application for execution from SRAM memory. In this case, the application images are programmed to persistent external flash memory, but copied into the internal RAM before execution
- Application should be compiled for execution from SRAM memory
- Refer to PSOC™ Edge SRAM Loading code example



Copyright © Infineon Technologies AG 2026. All rights reserved.

Encryption support

- Edge Protect Bootloader supports the encrypted firmware when EPB runs from RRAM only
- Encrypted user images must be located in the external flash memory and executed in SMIF XIP mode or loaded into SRAM for execution
- Edge Protect Bootloader supports the execution of the encrypted application in the following different methods:
  - Single-key encryption (EPC 2)
  - Multi-key encryption (EPC 2)
  - Secure encryption (EPC 4)
- For more details, check out the Encryption training module for PSOC™ Edge

Copyright © Infineon Technologies AG 2026. All rights reserved.

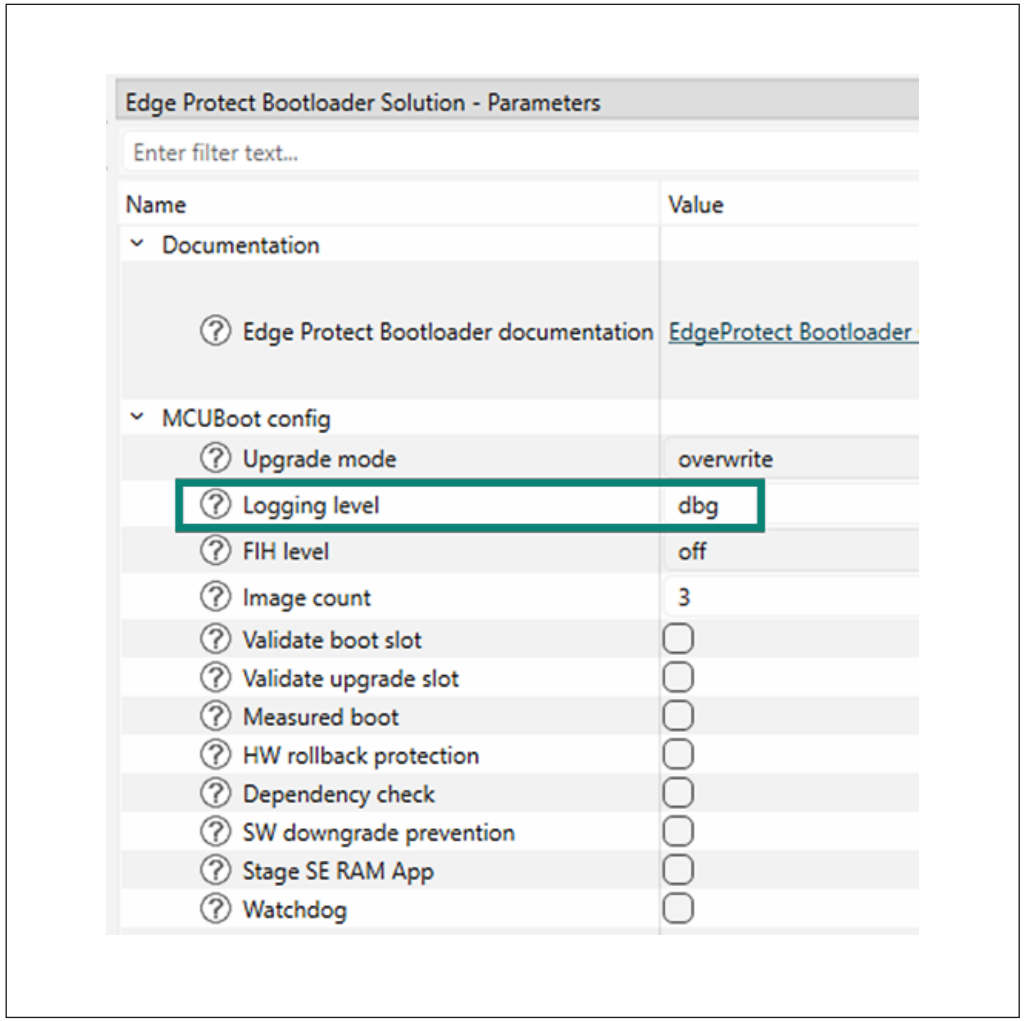
Measured boot and data sharing

- Mechanism for sharing boot status information (also known as measured boot) and an interface for sharing application-specific information with the runtime software in a shared memory region
- When enabled, adds a BOOT_RECORD TLV to the image manifest. The TLV consists of the following information about the image in CBOR encoded format
  - Software type (role of the software component)
  - Software version
  - Signer ID (identifies the signing authority)
  - Measurement value (hash of the image)
  - Measurement type (algorithm used to calculate the measurement value)
- Measured boot and data sharing feature by the bootloader is used by other components such as Trusted Firmware-M for attestation services
- Refer to the TF-M attestation code examples for EPC 2 and EPC 4 demonstration of how to use this feature along with TF-M

Copyright © Infineon Technologies AG 2026. All rights reserved.

Serial logging

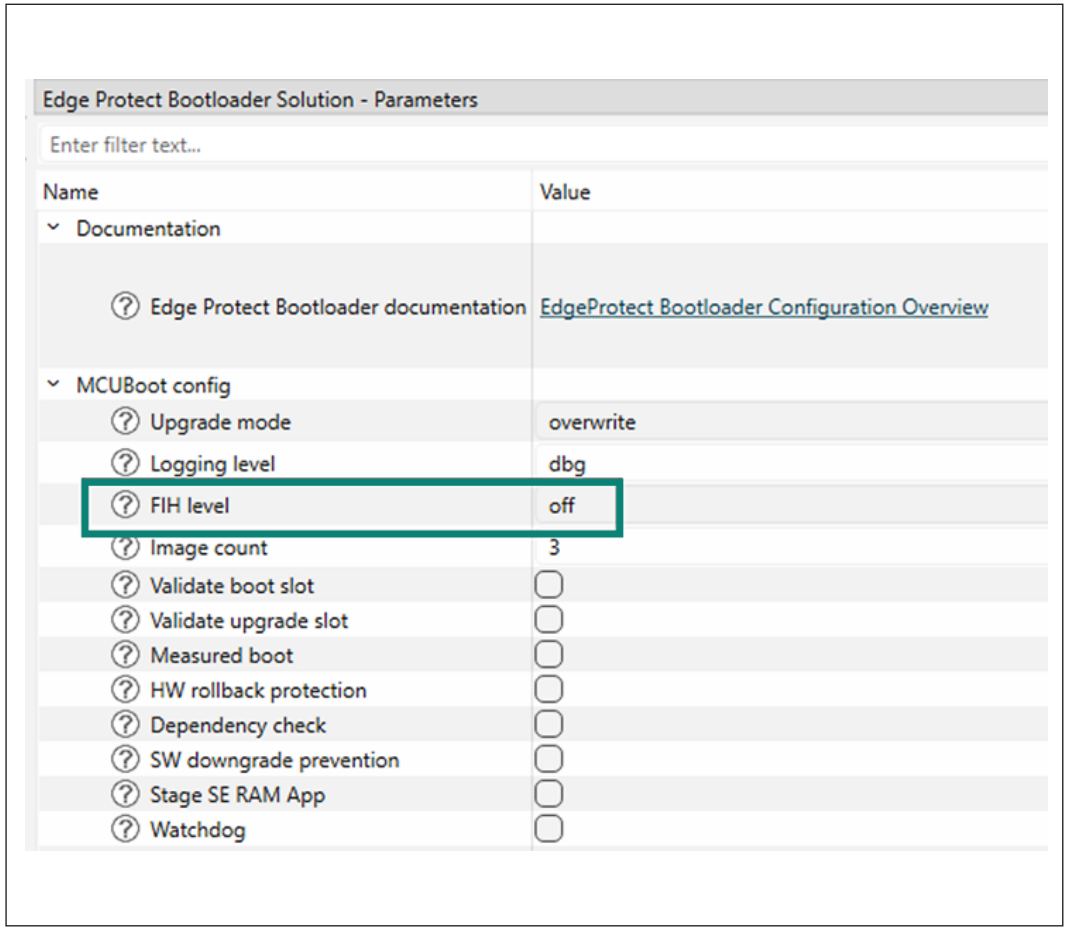
- The bootloader logs the status and reports over the serial port during the boot and upgrade process.
- The logs are printed over a UART port and are determined based on the minimum logging level that is set during compile time
- Five logging levels are supported:
  - MCUBOOT_LOG_LEVEL_OFF (0)
  - MCUBOOT_LOG_LEVEL_ERROR (1)
  - MCUBOOT_LOG_LEVEL_WARNING (2)
  - MCUBOOT_LOG_LEVEL_INFO (3)
  - MCUBOOT_LOG_LEVEL_DEBUG (4)



Copyright © Infineon Technologies AG 2026. All rights reserved.

Fault Injection Hardening (FIH)

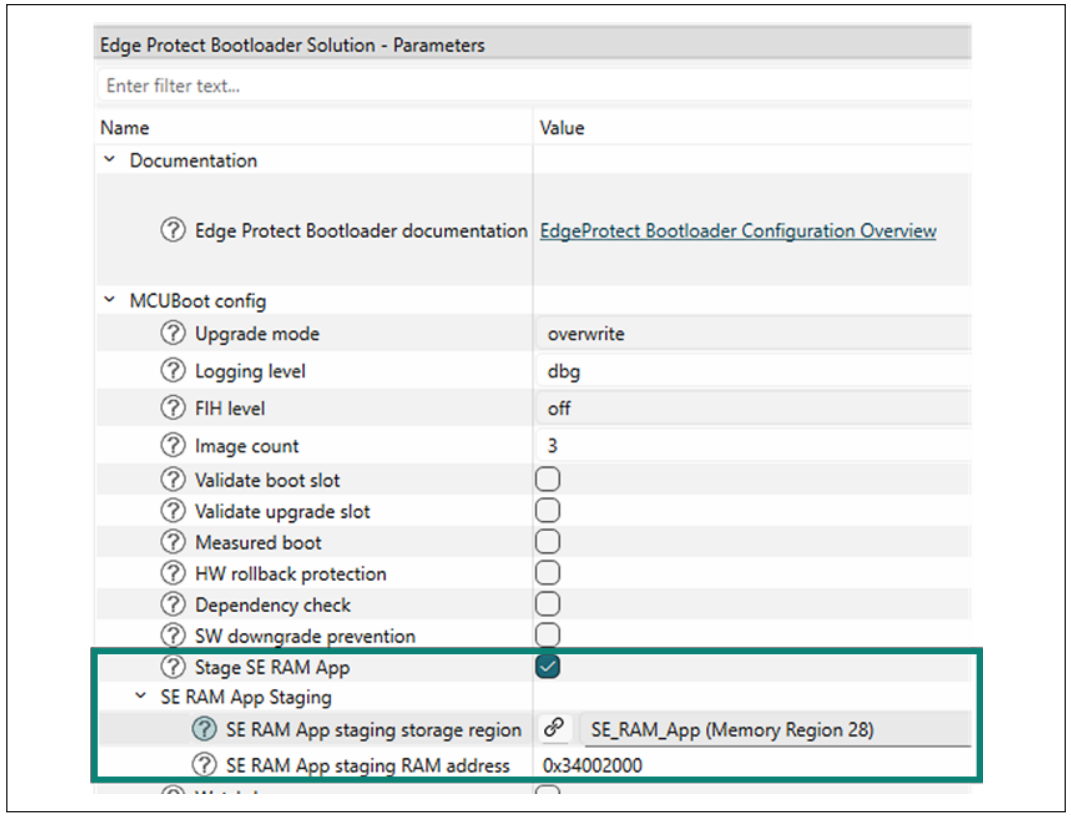
- To mitigate hardware-based fault injection attacks (for example, power glitching, EM pulses) aimed at executing unauthorised code, MCUboot incorporates software countermeasures
- Their activation is controlled by the MCUBOOT_FIH_PROFILE_* macros, offering four protection levels: none, moderate, medium, and maximum
- The fault injection mitigation library has support for different measures, which can either be enabled/disabled separately or by defining one of the MCUBOOT_FIH_PROFILE



Copyright © Infineon Technologies AG 2026. All rights reserved.

SE RT services update

- In EPC 4 devices, the Secure Enclave runtime services (SE RT) library may be updated using the SE RAM App staging feature of EPB
- This feature allows users to use the EPB to stage the SE RT services update RAM application from a persistent storage region and indicate to the ROM Boot to execute it
- The SE RAM app must be placed in a storage region (using OTA or other mechanism)



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Introduction 4

2 Bootloader features 10

3 **Running EPB from different memories** **30**

4 Lab 35

Copyright © Infineon Technologies AG 2026. All rights reserved.

Running Edge Protect bootloader on RRAM

- Edge Protect Bootloader running on RRAM
  - Edge Protect Bootloader programmed to RRAM
  - Launched by extended boot on RRAM
  - Execute in-place (XIP) from RRAM
- This is the default configuration of Edge Protect Bootloader
- Advantages
  - Better resilience against attacks
  - Low-power
  - Faster boot to first OEM-owned code
- Disadvantages
  - Limited size of RRAM

Copyright © Infineon Technologies AG 2026. All rights reserved.

Running Edge Protect bootloader on RRAM (contd.)

- Extended boot can launch the Edge Protect Bootloader from RRAM if BOOT SW (GPIO P17.6) EVK is set to LOW/OFF and the policy supports booting from external flash memory

Note: "bootloader_nvm" region must start at 0x00011000 offset to be successfully launched by the Extended Boot. If you want to place your first application in offsets other than 0x00011000, then you must provision the device with an updated OEM policy file.

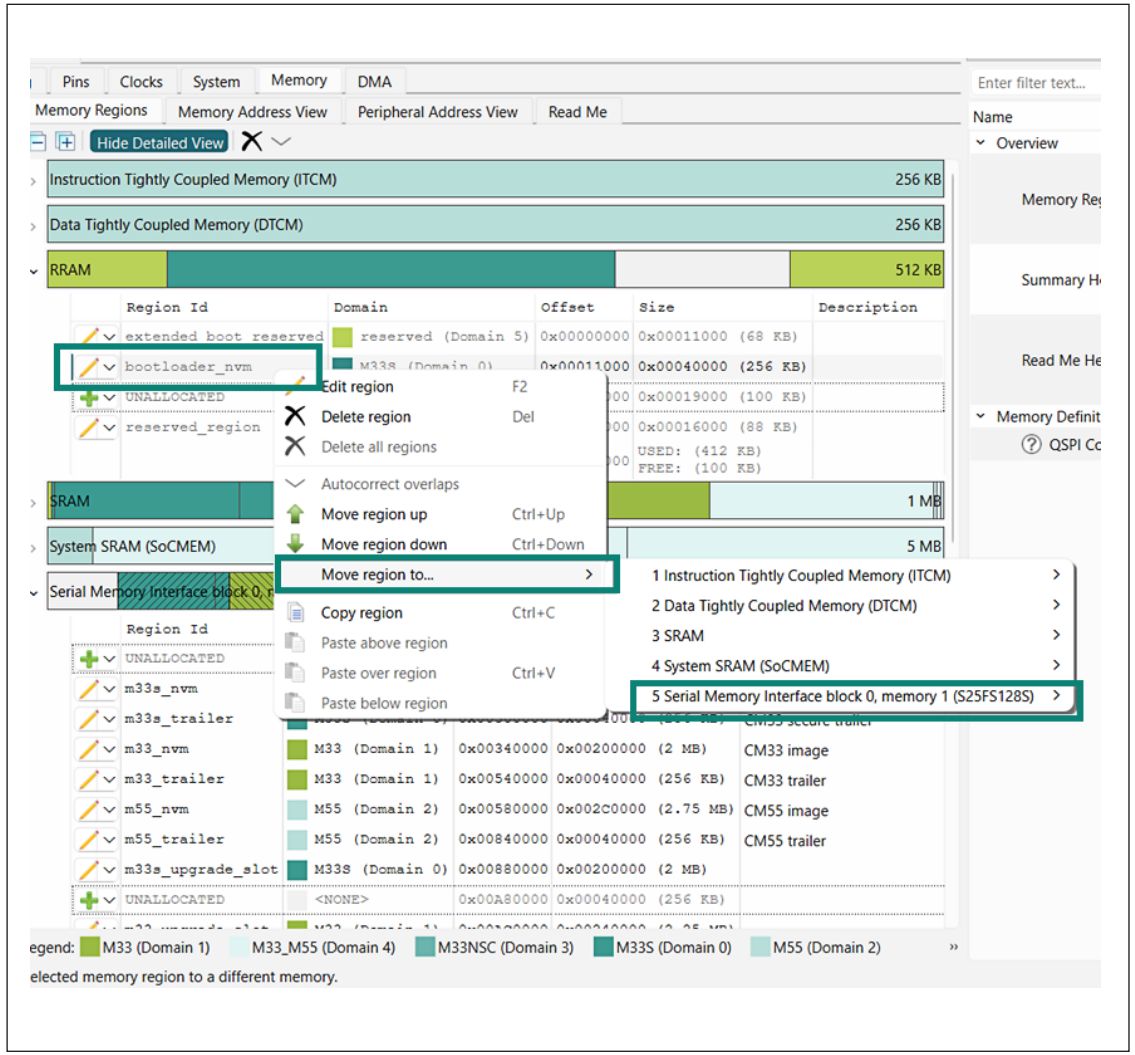
Copyright © Infineon Technologies AG 2026. All rights reserved.

Running Edge Protect Bootloader on external flash

- Edge Protect Bootloader running on external flash
  - Edge Protect Bootloader programmed to external flash
  - Launched by Extended boot on external flash
  - Execute in-place (XIP) from external flash

- BOOT SW pin (GPIO P17.6) on the EVK must be in the ON/HIGH position

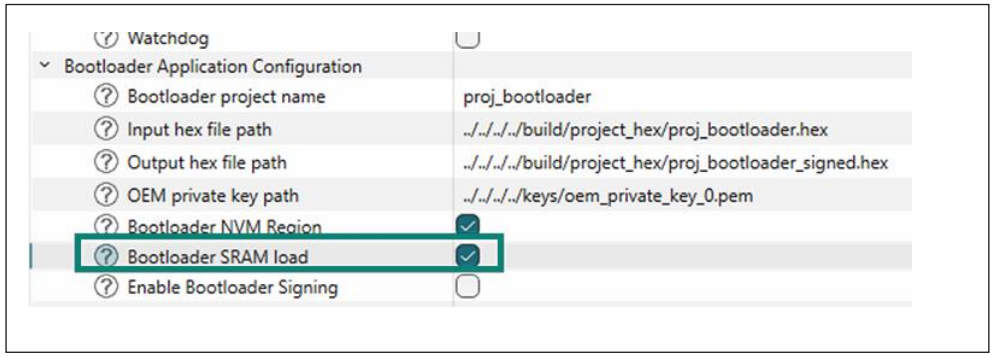
- **Note:** "bootloader_nvm" region must start at 0x00100000 offset to be successfully launched by the Extended Boot. If you want to place your first application in offsets other than 0x00100000, then you must provision the device with updated OEM policy file

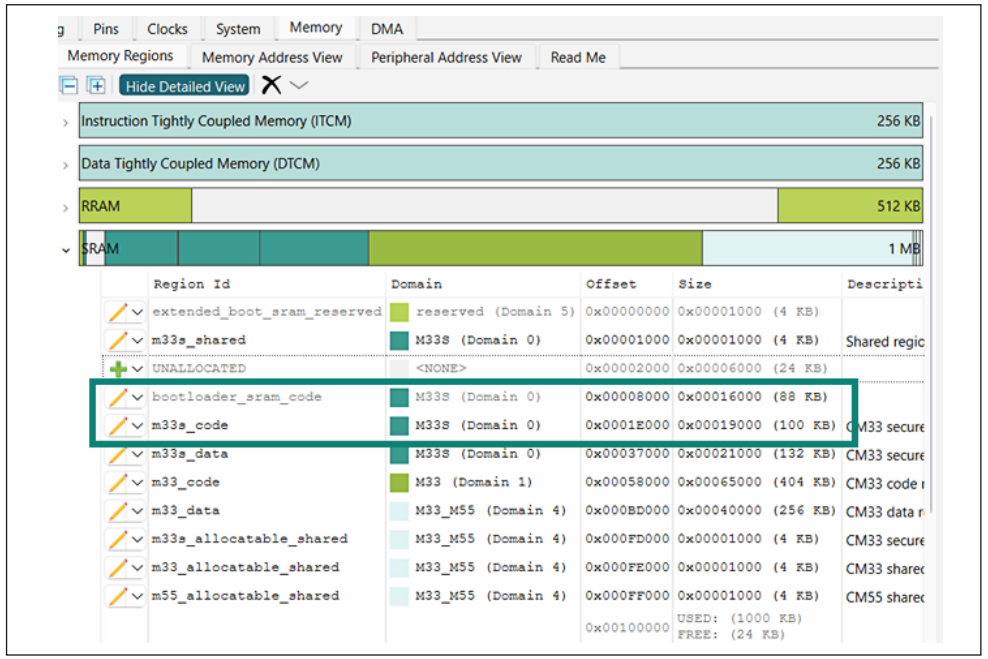


Copyright © Infineon Technologies AG 2026. All rights reserved.

Running Edge Protect Bootloader on SRAM

- Edge Protect Bootloader running on SRAM
  - Edge Protect Bootloader programmed to external flash
  - Copied to SRAM (and authenticated in SRAM, if Secure boot is enabled) by extended boot
  - Execute from SRAM
- Advantages
  - Reduced security risks compared to running code from external flash
  - Saves ~160 KB of internal RRAM for the user application, without compromising on security
- Disadvantages
  - Consumes a large chunk of the SRAM region for code and data
  - Application may reuse the SRAM region, provided that a secure application (such as TF-M) applies the modified security settings associated with the allocated region





Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Introduction 4

2 Bootloader features 10

3 Running EPB from different memories 30

4 **Lab** **35**

Copyright © Infineon Technologies AG 2026. All rights reserved.

Lab: Secure Boot with Edge Protect Bootloader

- Set up the Basic Secure App to function alongside the Edge Protect Bootloader
- Enable secure boot in Edge Protect Bootloader

Revision history

Document revision	Date	Description of change
**	2025-12-11	Initial release.
*A	2026-05-08	Updated speaker notes. Updated images to align with brand guidelines.
*B	2026-07-09	Added KIT_PSE84_AI support.

Copyright © Infineon Technologies AG 2026. All rights reserved.


Infineon