

PSOC™ Edge Extended Boot

Customer training workshop (CTW)

July 2026

Public

Prerequisites

Training prerequisites

- Introduction to PSOC™ Edge and ModusToolbox™
  - For an introduction to PSOC™ MCUs, including a getting started guide, go to: https://www.infineon.com/product-information/psocdeveloper
  - For PSOC™ Edge trainings, go to: PSOC™ Edge E84 Training Collection
  - Introduction to PSOC™ Edge Security: https://github.com/Infineon/mtb-training-psoc-edge-security-intro

Development tools

- ModusToolbox™ v3.8 or later
- Eclipse IDE for ModusToolbox™ v2026.3.0 or later
- 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 BSP v1.3.0
- Terminal Emulator
- KIT_PSE84_EVAL/ KIT_PSE84_AI

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 Alternate serial interface 18

6 Replacing extended boot 23

7 Lab 1: Replacing the Extended Boot 26

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 **Introduction to Extended boot** **4**

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 Alternate serial interface 18

6 Replacing extended boot 23

7 Lab 1: Replacing the Extended Boot 26

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Introduction to Extended Boot

- **Secure boot of Extended Boot**
  - First code executed on the CM33 CPU after reset
  - Secure Enclave verifies and loads the Extended Boot image from RRAM
- **Launching the next application**
  - The Extended Boot launches the next application image (in MCUboot image format)
  - If secure boot is enabled, it can also authenticate the next image
- **Serial interfaces**
  - The default version of Extended Boot supports serial interfaces: UART, I2C,SPI and USB
  - These interfaces support Infineon Device Firmware Update (DFU) middleware

Copyright © Infineon Technologies AG 2026. All rights reserved

Introduction to Extended Boot (contd..)

- **RAM loading**
  - Optionally, load an application image into SRAM and launch it from SRAM

- **Extended Boot versions**
  - Infineon-signed Extended Boot binaries are included in Edge Protect tools
    - Extended Boot with serial interface
    - Extended Boot without serial interface
  - The Extended Boot image can be replaced as long as the device is in Development LCS

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1	Introduction to Extended boot	4
2	**Secure boot**	**6**
3	Boot source	9
4	RAM Loading	15
5	Alternate serial interface	18
6	Replacing extended boot	23
7	Lab 1: Replacing the Extended Boot	26
8	Lab 2: RAM loading using Extended Boot	28

Copyright © Infineon Technologies AG 2026. All rights reserved

Secure boot

- The device is shipped in the development LCS by Infineon with secure boot disabled. Secure boot can be enabled via provisioning

- To enable secure boot, the secure_boot policy field under extended_boot_policy must be set to ‘true’

```
"extended_boot_policy": {
"secure_boot": {
  "description": "Disable/Enable secure boot option",
  "value": true
   },
 },
```

- The secure boot is enabled or disabled multiple times while the device is in development in the LCS. Edge Protect Tools provides the necessary support for provisioning the PSOC™ Edge devices

Copyright © Infineon Technologies AG 2026. All rights reserved

Secure boot (contd.)

- Once secure boot is enabled, Extended Boot verifies the signature of the next image in the boot chain and launches it on successful authentication
  - The next image can be either the bootloader or the user code

- Extended Boot supports ECDSA P256 for image authentication. The image must be signed using ECDSA private key (OEM_RoT_Private Key). The image is verified using the ECDSA public key (OEM_RoT_Public Key) provisioned to the device

- The Extended Boot can authenticate only the next image. If there are multiple images in the boot chain, it is the responsibility of the first OEM image in the boot chain to perform the authentication of the rest of the images

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 **Boot source** **9**

4 RAM Loading 15

5 Alternate serial interface 18

6 Replacing extended boot 23

7 Lab 1: Replacing the Extended Boot 26

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Boot sources (1/5)

- OEM policy defines two boot locations: oem_app_address and oem_alt_app_address. The Extended Boot can verify and launch an application from either of these locations defined by the policy

- oem_alt_app_address is valid only if oem_alt_boot is enabled in the policy

```
"oem_alt_boot": {
      "description": "Disable/Enable alternate boot",
      "value": true
    }
```

- If oem_alt_boot is disabled, the device always boots to oem_app_address

Copyright © Infineon Technologies AG 2026. All rights reserved

Boot sources (2/5)

- When oem_alt_boot is enabled, the boot location is determined based on the GPIO P17.6.

  In PSOC™ Edge EVK, P17.6 is connected to boot switch (SW6)

  - If the boot pin is LOW or floating, the Extended Boot verifies and boots the application from oem_app_address
  - If boot pin is HIGH, the Extended Boot verifies and boots the application from oem_alt_app_address

```
"oem_app_address": {
      "description": "Starting location of OEM application",
      "value": "0x3200F000"
    },
"oem_alt_app_address": {
      "description": "Alternate starting location of OEM application",
      "value": "0x70100000"
    },
```


Copyright © Infineon Technologies AG 2026. All rights reserved

Boot sources (3/5)

- Default policy configures the following:
  - oem_app_address in RRAM
  - oem_alt_app_address in external flash

- Addresses defined in the default policy can be changed via provisioning. Both oem_app_address and oem_alt_app_address can be set to RRAM or external flash. For example,
  - oem_app_address can be changed to a boot image from a different address in RRAM
  - oem_app_address can be set to the boot image from external flash

- Extended Boot exclusively supports SMIF Port0 (SMIF0), and it does not permit launching an application directly from SMIF1. However, an application running from RRAM can choose to configure the SMIF1 and launch the application from it, a capability not facilitated by Extended Boot

Copyright © Infineon Technologies AG 2026. All rights reserved

Boot sources (4/5)

– The default policy configures Slave Select 1 (SMIF0, SSEL1) as default external flash for Extended Boot

```
"smif_chip_select": {
        "description": "Chip select for primary external flash",
        "applicable_conf": "0, 1, 2, 3",
        "value": 1
      },
```

– You can select a different slave (for example, SSEL0) of your choice by provisioning the new policy with appropriate updates to the smif_chip_select field in the policy

– The Extended Boot can detect and work with Quad-SPI and Octal-SPI flashes (based on provision configurations)

Copyright © Infineon Technologies AG 2026. All rights reserved

Boot sources (5/5)

– On the PSOC™ Edge EVK both Quad-SPI (SMIF0, SSEL1) and Octal-SPI (SMIF0, SSEL0) are available. Extended Boot can boot from either of these memories

– Default policy configures Quad-SPI. For Octal-SPI support, the smif_data_width should be set to '8'

```
    "smif_data_width": {
            "description": "Select data width used to interface the external flash",
            "applicable_conf": "4, 8",
            "value": 4
        },
```


Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1	Introduction to Extended boot	4
2	Secure boot	6
3	Boot source	9
4	**RAM Loading**	**15**
5	Alternate serial interface	18
6	Replacing extended boot	23
7	Lab 1: Replacing the Extended Boot	26
8	Lab 2: RAM loading using Extended Boot	28

Copyright © Infineon Technologies AG 2026. All rights reserved

RAM loading

- The Extended Boot can copy an application to internal volatile memory like SRAM and System RAM (SoCMEM)
- Load address (RAM/System RAM address) where the image is copied to and is stored in the image header
  - Edge Protect Tools provides --load-addr command, which embeds the load address in the image header
- The project must be compiled to run from the designated location (RAM or SystemRAM), to which Extended Boot copies the images
- Once the image is copied, the Extended Boot validates it and launches from the copied location

Copyright © Infineon Technologies AG 2026. All rights reserved

RAM loading (contd.)

- Extended Boot can load only one image into the RAM, with the entire image being copied to the target location. Partial loading of images is not supported
- RAM loading is useful when you want to place the image in an external non-volatile memory but want to copy the entire image to internal memory, like RAM, for execution
- Benefits of executing the code from internal memory include lower power consumption, improved execution performance, and enhanced security
- This feature will be demonstrated in the Lab module

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 **Alternate serial interface** **18**

6 Replacing extended boot 23

7 Lab 1: Replacing the Extended Boot 26

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Alternate serial interface (ASF)

- Extended Boot facilitates communication with the external world through UART, I2C, and SPI interfaces. These interfaces, termed as alternate serial interfaces (ASF), offer an alternative method for programming devices aside from Serial wire debug (SWD)

- Supported serial interface configurations:
  - UART (115.2 Kbaud)
  - SPI (up to 12 Mbps)
  - I2C (400 Kbps)

- The default version of the Extended Boot is programmed on the device, and the default OEM policy enables the ASF

```
"enable_alt_serial": {
    "description": "Disable/Enable Alternate serial interface",
    "value": true
  },
```


Copyright © Infineon Technologies AG 2026. All rights reserved

Selecting ASF boot mode

- For Extended Boot to activate the ASF mode, user needs to configure GPIO P20.1
- During bootup, Extended Boot checks GPIO P20.1
  - If this pin is pulled-low or pulled-high, ASF mode is enabled
  - If the pin is tristate, ASF mode is disabled
- If ASF mode is enabled, Extended Boot inspects the GPIO P20.2 pin to determine the serial interface to be used

Serial port configuration			
	P20.1 = Tristate	**P20.1 = Vss**	**P20.1 = Vdd**
P20.2 = Tristate	Serial Disable	SPI	UART
P20.2 = Vss	Serial Disable	SPI	UART
P20.2 = Vdd	Serial Disable	I2C	UART

- ASF can be left enabled after the OEM has shipped the product or deactivated. It is recommended to disable the ASF before shipping the devices to field from OEMs

Copyright © Infineon Technologies AG 2026. All rights reserved

Using the alternate serial interfaces

- The Extended Boot allows users to provision and program the devices using ASF
- CM33 RAMAPP (CM33 project) can be downloaded to the device SRAM, verified and launched by the Extended Boot
- The download protocol used by Extended Boot is the same as Infineon DFU
- CM33 RAMApp is owned by OEMs and can be customised according to use case requirements. Infineon only provides a reference code example that demonstrates the concept

Copyright © Infineon Technologies AG 2026. All rights reserved

Using the alternate serial interfaces (contd.)

– Default policy configurations allow Extended Boot to download the image to 0x34008000 as defined by the cm33_ram_app policy field

```
"cm33_ram_app": {
          "enable": {
            "description": "Disable/Enable CM33 OEM RAM applications",
            "value": true
          },
          "address": {
            "description": "Start address of the CM33 OEM RAM application",
            "value": "0x34008000"
          },
    },
```

– This functionality of the Extended Boot allows for the factory programming of the device, utilizing the serial interfaces

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 Alternate serial interface 18

6 **Replacing extended boot** **23**

7 Lab 1: Replacing the Extended Boot 26

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Replacing the Extended Boot

- Two versions of the Extended Boot provided in <application directory>/packets/apps/extended_boot path. This directory gets populated once the Edge Protect tools is initialized

- Alternate version saves about 27 KB of RRAM. You can provision the device with Extended Boot version with reduced size. This version of the Extended Boot does not offer the serial interface capabilities

Extended Boot binary

Binary	Description
`extended-boot-no-serial.cbor`	This version of the Extended Boot does not include support for the serial interface. It saves around 27 KB of RRAM memory that can be used by the OEM user application. With this version of the Extended Boot, user application in RRAM can start from 0x3200B000.
`extended-boot-serial.cbor`	This version of the Extended Boot includes support for the serial interface (UART, I2C, and SPI). This is the default version on your device out of the box. With this version of the Extended Boot, user application from RRAM can start from 0x32011000.

Copyright © Infineon Technologies AG 2026. All rights reserved

Replacing the Extended Boot (contd.)

- Before replacing the Extended Boot, follow the steps described in AN237849 - Getting started with PSOC™ Edge security
- Update the policy to provide the absolute location of the Extended Boot image and provision the device with the new policy

```
"extended_boot_image":
{
    "description": "Image of Extended Boot in CBOR format, signed by Infineon"
    "value": "<pathto>/packets/apps/prov_oem/Extended Boot-no-serial.bin"
}
```

- To use the extra 27 KB in the first CM33 code, update the oem_app_address in the policy, and modify the linker file of the corresponding project
- The Extended Boot can be replaced as long as the device is in development LCS. Once devices transition to production LCS, the Extended Boot is locked and can not be updated

Copyright © Infineon Technologies AG 2026. All rights reserved

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 Alternate serial interface 18

6 Replacing extended boot 23

7 **Lab 1: Replacing the Extended Boot** **26**

8 Lab 2: RAM loading using Extended Boot 28

Copyright © Infineon Technologies AG 2026. All rights reserved

Lab 1: Replacing the Extended Boot

What will you learn?

- How to find the version of Extended Boot on the device
- How to modify the policy to select the Extended Boot images
- How to replace the boot image via provisioning

Table of contents

1 Introduction to Extended boot 4

2 Secure boot 6

3 Boot source 9

4 RAM Loading 15

5 Alternate serial interface 18

6 Replacing extended boot 23

7 Lab 1: Replacing the Extended Boot 26

8 **Lab 2: RAM loading using Extended Boot** **28**

Copyright © Infineon Technologies AG 2026. All rights reserved

Lab 2: RAM loading using Extended Boot

What will you learn?

- To configure a project to run from SRAM
- To indicate Extended Boot to copy the image to SRAM (from external flash) and launch it in SRAM

Revision history

Document revision	Date	Description of change
**	2025-12-10	Initial release.
*A	2026-03-03	Updates speaker notes. Updated version of tools.
*B	2026-05-25	Added KIT_PSE84_AI support in hands-on labs.
*C	2026-07-16	No updates are required for the training presentation. All the new EPT updates have been incorporated into the training manual.

Copyright © Infineon Technologies AG 2026. All rights reserved


Infineon