

PSOC™ Edge security introduction

Customer training workshop (CTW)

July 2026

Public

Prerequisites

Recommended training prerequisites

- Introduction to PSOC™ Edge and ModusToolbox™
  - For an introduction to PSOC™ MCUs, go to: https://www.infineon.com/product-information/psocdeveloper
  - For PSOC™ Edge trainings, go to: PSOC™ Edge E84 Training Collection

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 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 Cryptography basics 4

2 Introduction to security 10

3 PSOC™ Edge architecture 13

4 Security features 16

5 Introduction to Edge Protect Tools 31

6 Lab 33

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1	**Cryptography basics**	**4**
2	Introduction to security	10
3	PSOC™ Edge architecture	13
4	Security features	16
5	Introduction to Edge Protect Tools	31
6	Lab	33

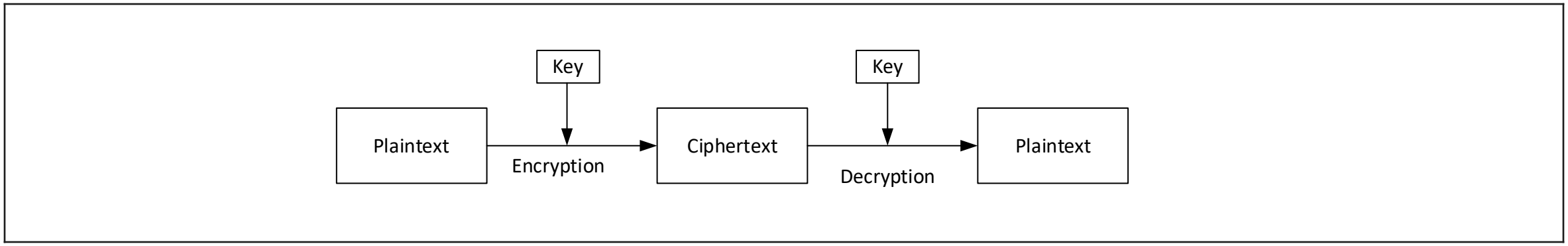
Copyright © Infineon Technologies AG 2026. All rights reserved.

Cryptography basics

- Cryptography is a technique of securing communication by converting plain text into unintelligible ciphertext. It involves various algorithms and protocols to ensure data confidentiality, integrity, authentication, and non-repudiation

- Encryption – The sender's message, or the plaintext, is converted into an unreadable form using a Key. The resultant text obtained is called the **ciphertext**

- Decryption – On the receiver side, the Ciphertext is converted into the plaintext using the same Key, so that the receiver can read it. This process is known as decryption



Copyright © Infineon Technologies AG 2026. All rights reserved.

Types of cryptography

Symmetric-key cryptography

- This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication
- For example,
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

Asymmetric-key cryptography

- Asymmetric-key cryptography, also known as public key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept confidential by the owner
- For example,
  - Rivest–Shamir–Adleman (RSA)
  - Elliptic Curve Cryptography (ECC)
    - Elliptic Curve Digital Signature Algorithm (ECDSA)

Copyright © Infineon Technologies AG 2026. All rights reserved.

Cryptography basics (1/3)

Cryptographic hash

- An irreversible, one-way mathematical function used to convert messages/data into fixed-length strings of characters. This actual message cannot be derived from the hash of the message. The hash is used to verify that the message has not been manipulated
- For example,
  - Message Digest (MD)
  - Secure Hash Function (SHA)
    - SHA 256

Copyright © Infineon Technologies AG 2026. All rights reserved.

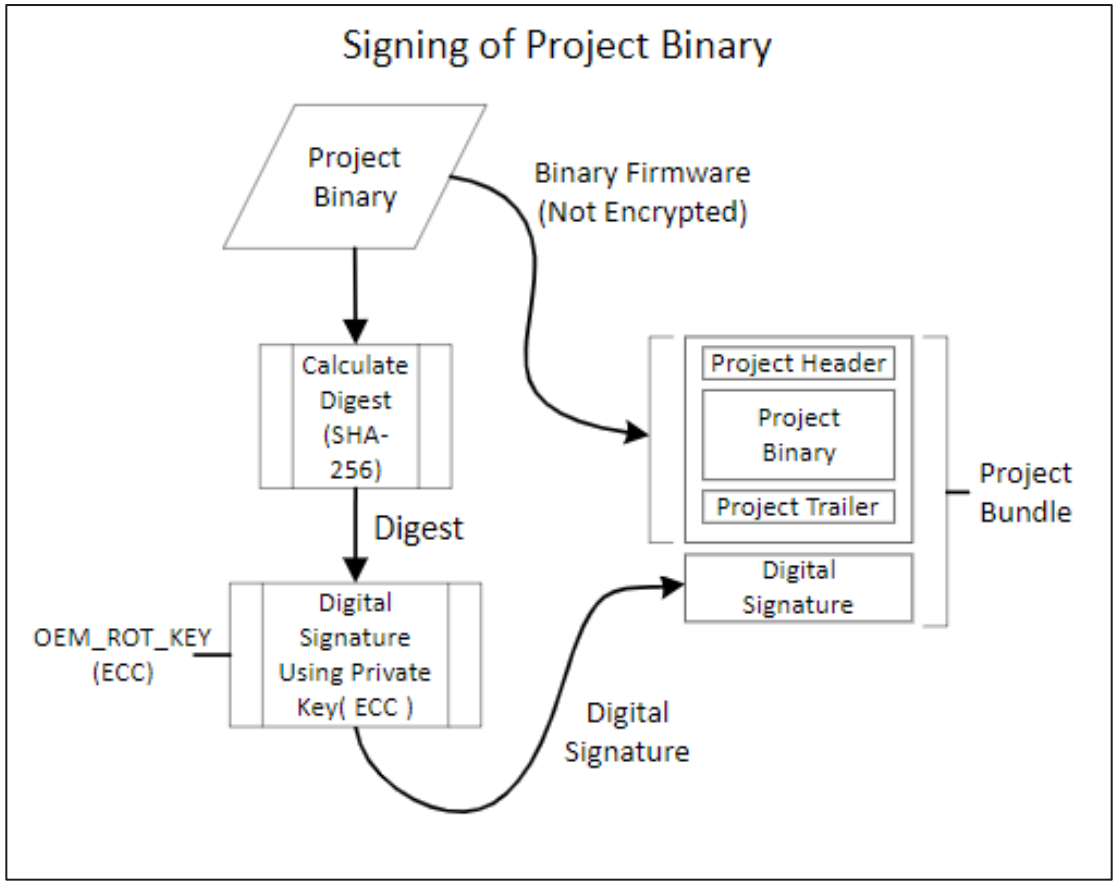
Cryptography basics (2/3)

Digital signature

– Digital signatures are used for authentication, to see whether data has been tampered with, and to provide non-repudiation

Signature generation steps

– Cryptographic hash calculation over the message.
– The sender encrypts this hash with their private key, creating the digital signature
– The digital signature is attached to the message, and both are sent to the recipient, along with the sender's public key for verification

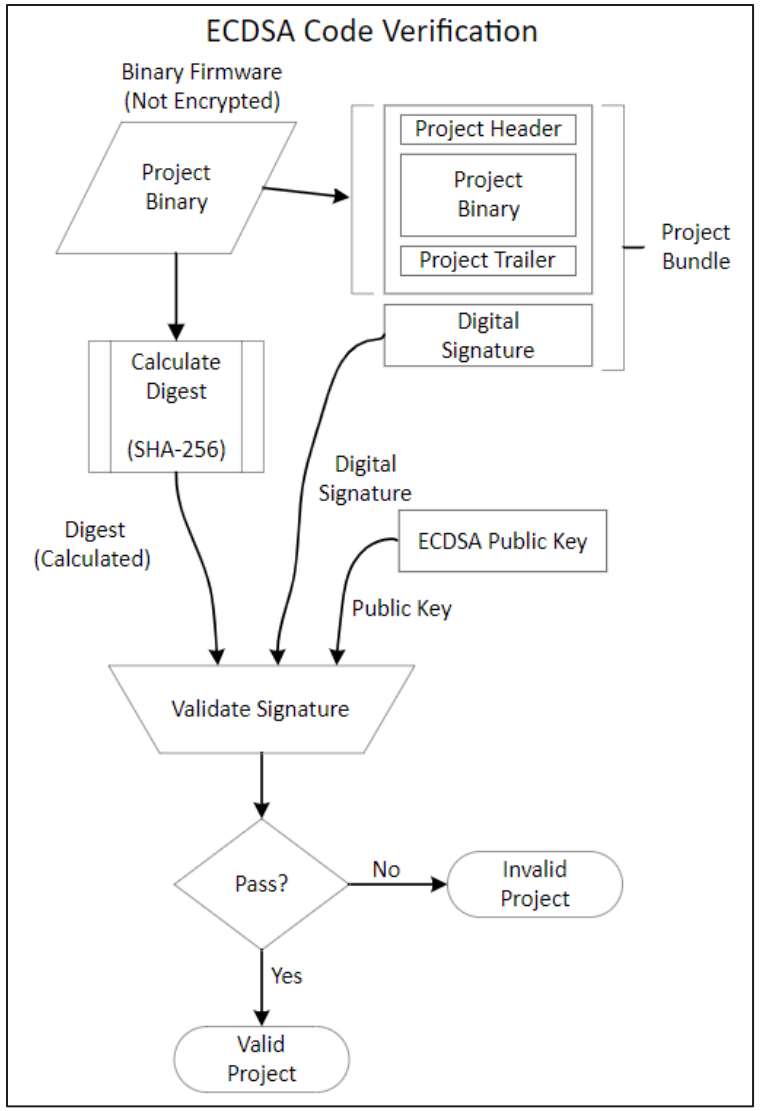


Copyright © Infineon Technologies AG 2026. All rights reserved.

Cryptography basics (3/3)

Signature verification

- The recipient uses the sender's public key to decrypt the signature, retrieving the original hash
- They also generate a hash from the received message for comparison
- If the recipient's hash matches the decrypted hash, it confirms that the message is intact and unaltered, validating the signature's authenticity



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Cryptography basics 4

2 **Introduction to security** **10**

3 PSOC™ Edge architecture 13

4 Security features 16

5 Introduction to Edge Protect Tools 31

6 Lab 33

Copyright © Infineon Technologies AG 2026. All rights reserved.

Introduction to security

The IoT devices are widely used around the world, and the addition of each new device introduces a new access point to the cloud-based network, increasing the potential for unauthorised access to confidential or safety-critical information. It is necessary to safeguard these devices from possible attacks and threats.

The value of every IoT device is built on data and how that data is managed.

- Confidentiality: Data is protected from unauthorized access or viewing
- Integrity: Data is trustworthy, accurate, and not altered by unauthorized users
- Authenticity: Only a trusted source has established the current state of a data asset



Copyright © Infineon Technologies AG 2026. All rights reserved.

Security threats

Security attacks		
Logical attacks	**Physical attacks**	
Logical attacks use normal interfaces to communicate unexpectedly to the device and can be performed even remotely	A physical attack is one where the attacker has access to the device and can physically alter the hardware on the device to gain access	
Physical attacks can be either of the following:		
Observative	Semi-invasive	Manipulative



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Cryptography basics 4

2 Introduction to security 10

3 **PSOC™ Edge architecture** **13**

4 Security features 16

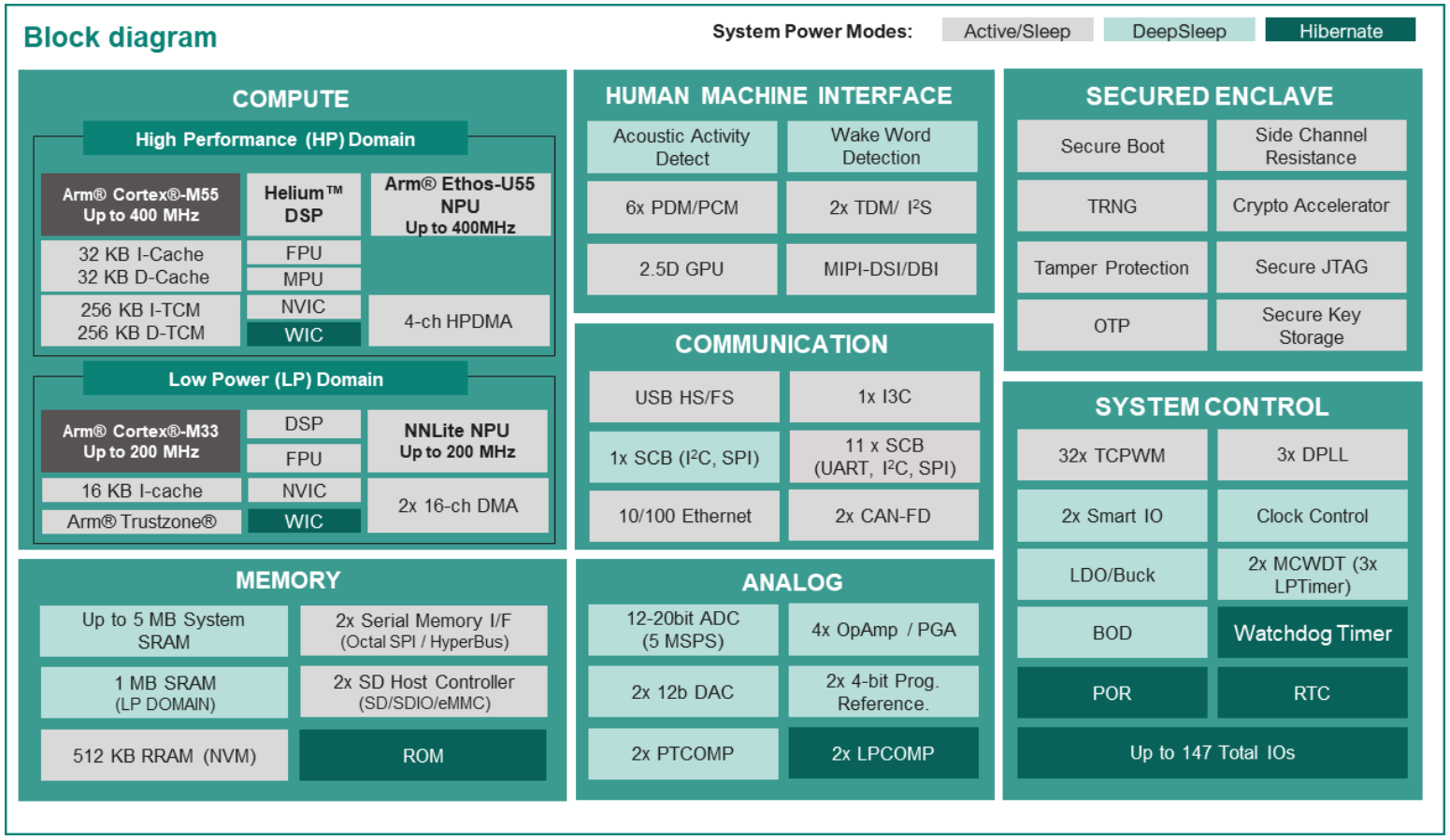
5 Introduction to Edge Protect Tools 31

6 Lab 33

Copyright © Infineon Technologies AG 2026. All rights reserved.

PSOC™ Edge architecture

The PSOC™ Edge MCU is a multicore device that contains two CPUs (Cortex®-M33 and Cortex®-M55) and a Secure Enclave



Copyright © Infineon Technologies AG 2026. All rights reserved.

PSOC™ Edge measures against security threats

- The lock-step architecture of Secure Enclave with two islands of replication provides mitigation against semi-invasive attacks inside Secure Enclave
- Software countermeasures are used for mitigation against side channel attacks (SCA)
- Secure Boot mechanism to authenticate the application at every boot
- Authenticated debug mechanism to control the debug port access using trusted firmware or a certificate
- The device integrity exam is protected against replay attacks by using a random number (nonce) value for every exam
- Ability to permanently close the system access port (SYS-AP) to prevent denial of service attacks
- The key revocation feature is supported for the OEM key in case of a security breach in the field

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Cryptography basics 4

2 Introduction to security 10

3 PSOC™ Edge architecture 13

4 **Security features** **16**

5 Introduction to Edge Protect Tools 31

6 Lab 33

Copyright © Infineon Technologies AG 2026. All rights reserved.

Security features of PSOC™ Edge

- Secure lifecycles
- Secure boot
- Secure firmware updates
- Secure debug
- Immutable internal memory for root-of-trust (RoT)
- Secure storage
- Hardware crypto accelerators
- Random Number Generators (RNG)
- Key revocation
- Tamper detection
- Side channel attack mitigation
- Device Identifier and Composition Engine (DICE) compliance. See the link for more details
- Platform Security Architecture (PSA) compliant up to PSA level 4 certification. See the link
- Common Criteria Vulnerability Analysis (AVA_VNA.4) compliant
- Trusted Firmware-M (TF- M) and MCUboot-based Edge Protect Bootloader support

psacertified™

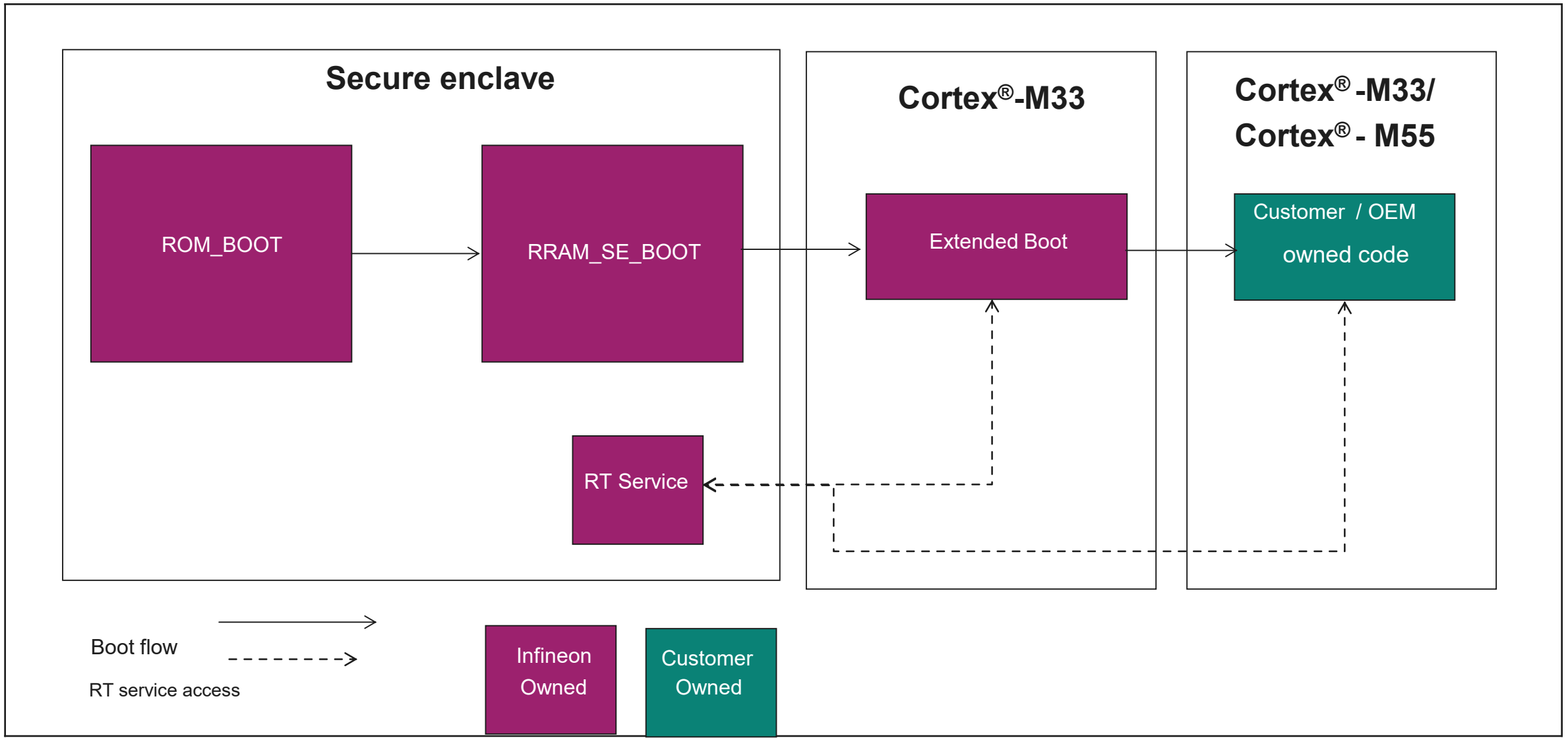
PSA L4

Common Criteria

CC AVA_VNA.4

Copyright © Infineon Technologies AG 2026. All rights reserved.

PSOC™ Edge: Basic boot flow



Copyright © Infineon Technologies AG 2026. All rights reserved.

Secure Enclave (SE)

- Secure Enclave (SE) consists of two Cortex®-M0+ CPUs that operate in lock-step
- Exclusive ROM and RAM are accessible solely from Cortex®-M0+. Isolated Execution environment
- Forms the root of trust (RoT) where the immutable ROM boot executes
- Tamper detection, side channel attack (SCA) mitigation, and protection against fault injection attacks
- Basic runtime services used during device boot up (available on EPC2 / EPC4 parts).

  See the product PSOC™ Edge E8x datasheet for more details
- Secure Enclave runtime (SE RT) services for Arm® Platform Security Architecture (PSA) compliant cryptographic operations, key management, secure storage, and attestation (available on EPC4 parts).

  See the PSOC™ Edge E8x datasheet for more details

Copyright © Infineon Technologies AG 2026. All rights reserved.

Extended Boot

- Extended Boot can authenticate and launch the first user application
- Capable of booting a user application from RRAM or external flash memory
- Supports ECDSA P256 for image authentication
- Supports the authentication of a maximum of one image
- PSOC™ Edge is pre-programmed with an extended boot at the Infineon factory
- Supports the replacement of a pre-signed extended boot image by the user

Copyright © Infineon Technologies AG 2026. All rights reserved.

Secure Boot

Secure Boot of built-in Infineon code

- The Secure Enclave ensures the initial secure boot and root of trust
- Infineon provided assets (RRAM boot and Extended Boot) are always verified on every bootup
- Secure Enclave verifies the Extended boot and launches it on every bootup

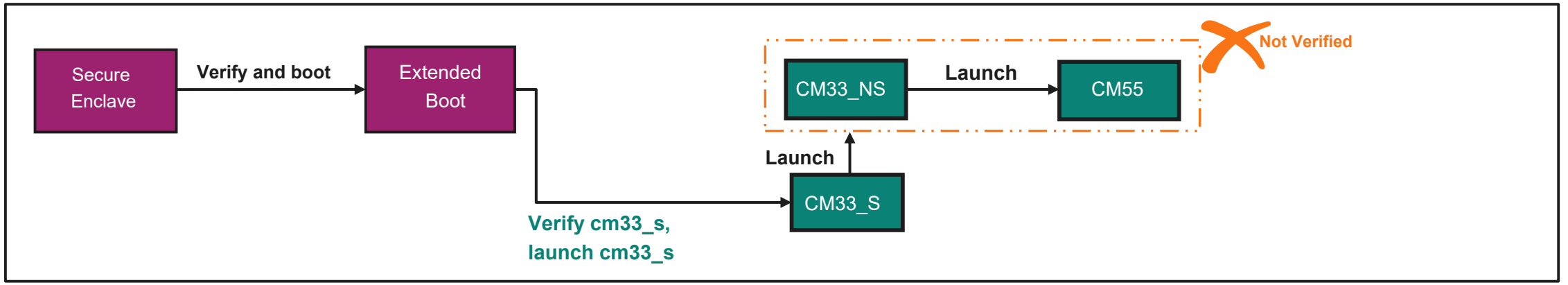
Secure Boot of OEM code

- The policy file parameter (secure_boot) determines if secure boot is extended to the first OEM code or not
- If secure_boot is enabled in the policy, extended boot authenticates the first user code before launching

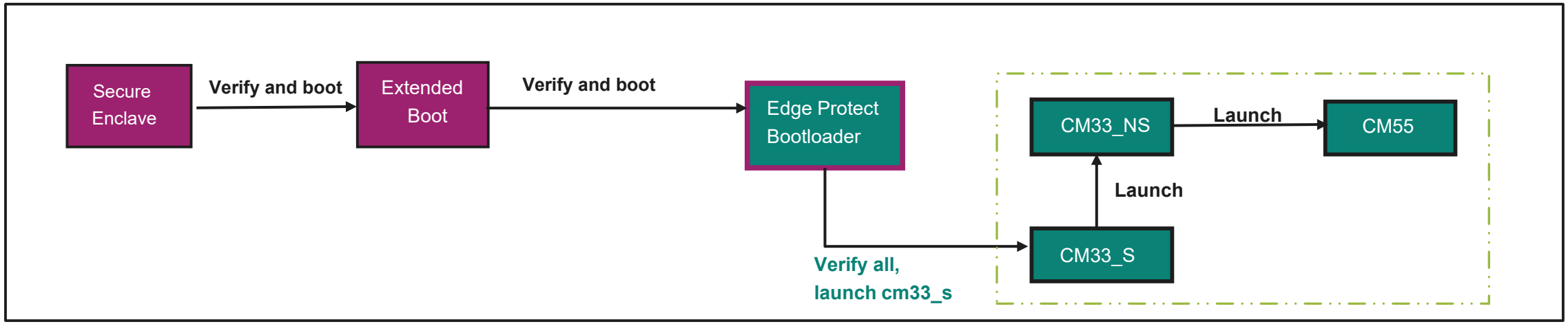
Copyright © Infineon Technologies AG 2026. All rights reserved.

Secure Boot (contd.)

First OEM code verified by extended boot when Secure boot enabled



First OEM code verified by extended boot, remaining OEM code verified by Edge Protect Bootloader

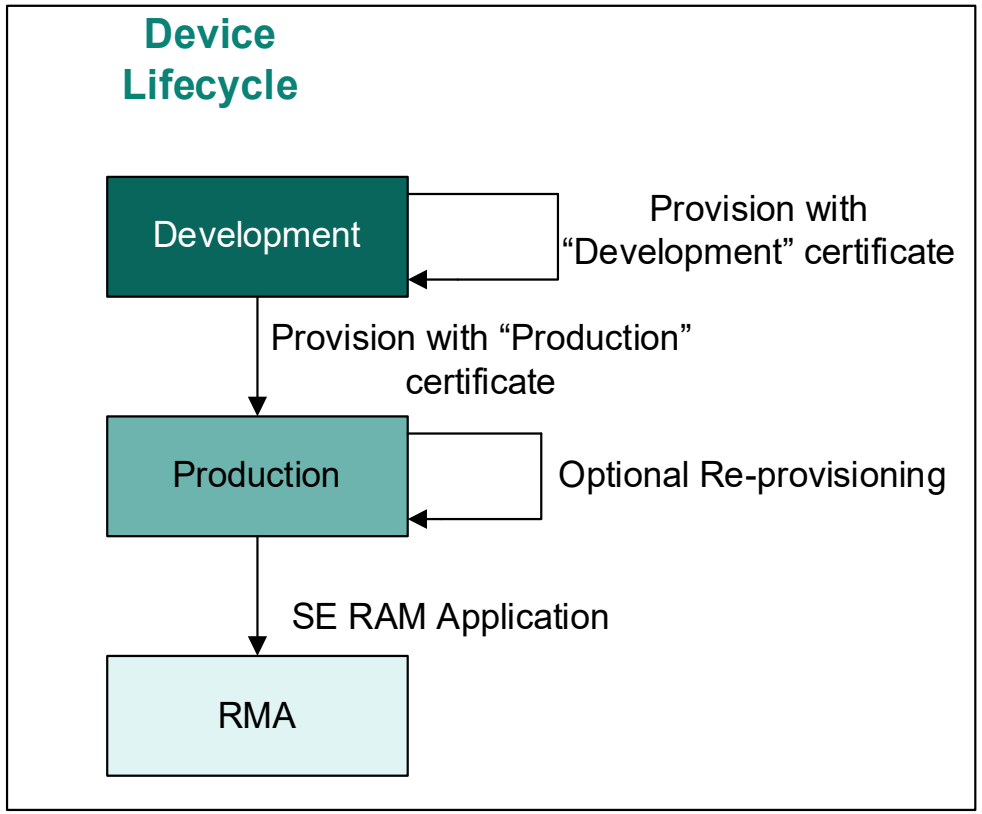


Copyright © Infineon Technologies AG 2026. All rights reserved.

Device lifecycle

Development

- The devices are shipped out of Infineon on this lifecycle. The stage (LCS) with Secure boot disabled
- The device can be provisioned, and OEM keys can be replaced as many times as required
- Can be restored to its original factory state (as shipped by Infineon)
- The device cannot be bricked in this LCS
  - Debug port (SYS-AP) is always open to recover device
- Development LCS fully emulates production LCS



Note: LCS migration is irreversible.

Copyright © Infineon Technologies AG 2026. All rights reserved.

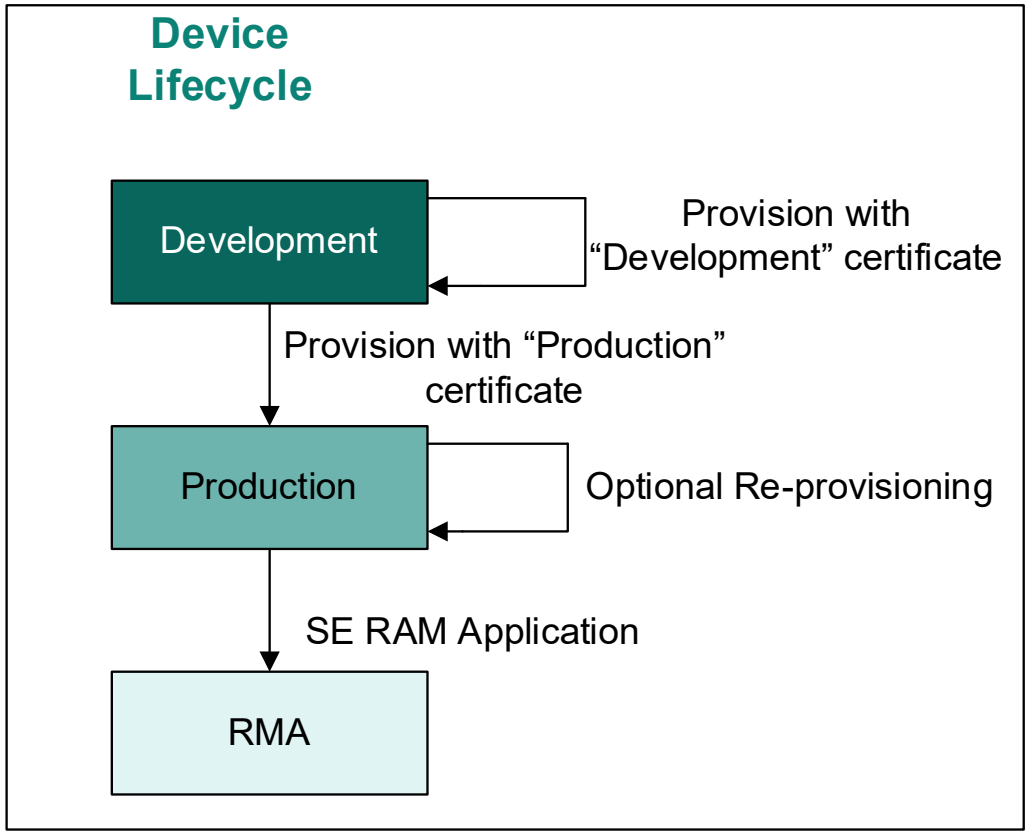
Device Lifecycle (contd.)

Production

- Provisioning with the “Production” certificate to move to this LCS
- Re-provisioning the device can be dictated by user-defined configuration (policy)

RMA

- Executed by the user or customer through an Infineon-signed SE RAM application
- Complete erasure of all sensitive data is possible when transitioning to RMA



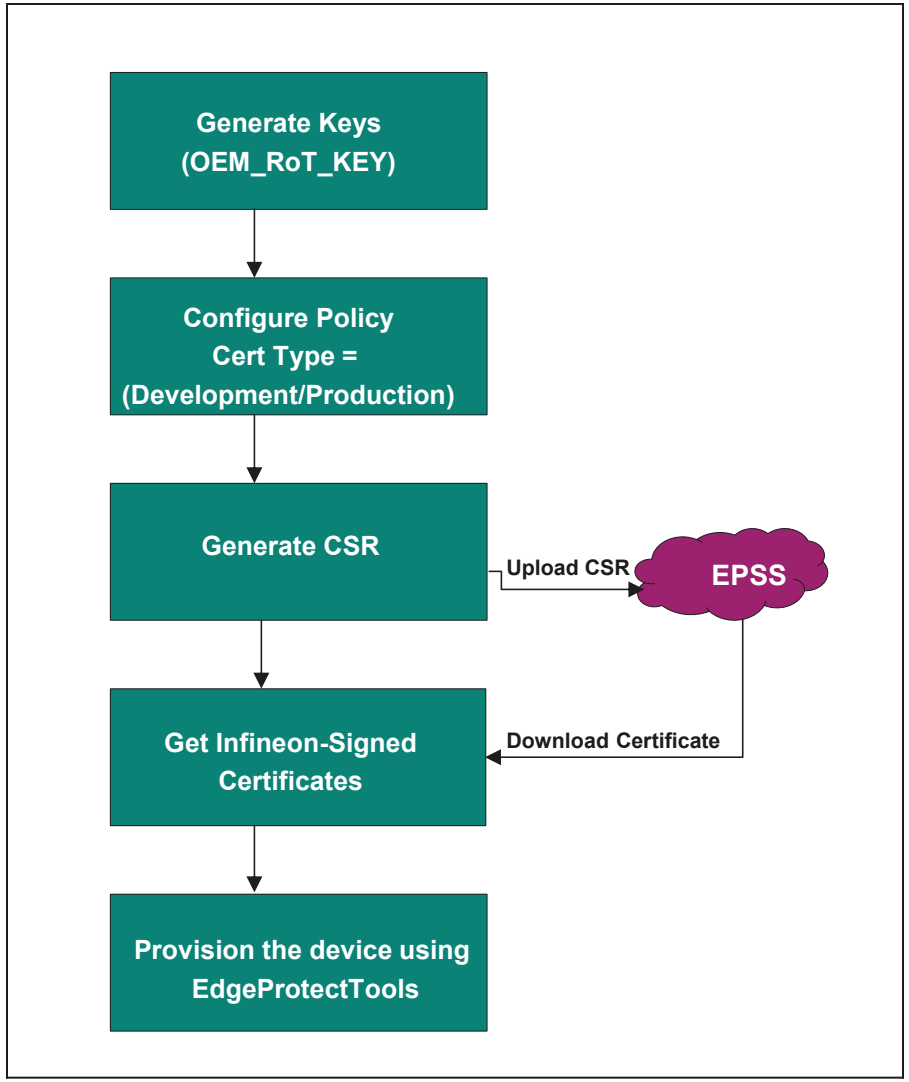
Note: LCS migration is irreversible.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Transfer of ownership

- The default owner is Infineon for the parts leaving Infineon
- Transfer ownership from Infineon to the OEM occurs through the provisioning process
- The provisioning process requires the following:
  - Asymmetric-key pair (OEM_RoT_KEY)
  - Infineon-signed OEM certificate
  - A policy file with user-defined configurations (use default policy)

Edge Protect Signing Services (**EPSS**) hosted by Infineon. Only an Infineon-approved customer/User can log in and request the signed certificates. See https://osts.infineon.com for more information.



Copyright © Infineon Technologies AG 2026. All rights reserved.

Policy file

Policy file

- Controls the boot and debug configurations applied by the boot software
- Default policy pre-installed at the Infineon factory
- This default policy file, policy_oem_provisioning.json, is available with the Edge Protect Tools package

Updating the policy

- Edit the policy fields in the policy file and provision the device with the updated policy
- Device ownership must be transferred before changing the Infineon default policy
- Edge Protect Tools provision-device command for signing the modified policy with the OEM ROT KEY and provisioning the device with the new policy

Copyright © Infineon Technologies AG 2026. All rights reserved.

Policy file (contd.)

Protecting the policy

- Policy is stored in device NVM (RRAM) in Concise Binary Object Representation (CBOR) format
- It is protected from access by the Secure Enclave and the Extended boot
- The policy is verified on every bootup to determine the integrity of the policy

A sample policy JSON contents

```
"extended_boot_policy": {
  "secure_boot": {
    "description": "Disable/Enable secure boot option",
    "value": false
  },
  "clock": {
    "description": "Defines default core clock speed in MHz",
    "applicable_conf": "200, 100, 50, 5",
    "value": 200
  },
  "listen_window": {
    "description": "Defines listen window timeout in ms",
    "value": 100
  },
  "enable_alt_serial": {
    "description": "Disable/Enable Alternate serial interface",
    "value": true
  },
  "cm33_ram_app": {
    "enable": {
      "description": "Disable/Enable CM33 OEM RAM applications",
      "value": true
    },
```


Copyright © Infineon Technologies AG 2026. All rights reserved.

Important parameters in the policy

```
"secure_boot": {
     "description": "Disable/Enable secure boot option by setting
    the value to false/true",
     "value": false
   },
```

```
 "debug": {
    "cm33": {
      "cpu": {
        "description": "CPU access port debug restriction",
        "applicable_conf": "Disabled, Enabled, Allowed",
        "value": "Enabled"
},
```

```
      "oem_app_address": {
        "description": "Starting location of OEM application",
        "value": "0x32011000"
      },
```

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


Copyright © Infineon Technologies AG 2026. All rights reserved.

Important parameters in the policy (contd.)

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

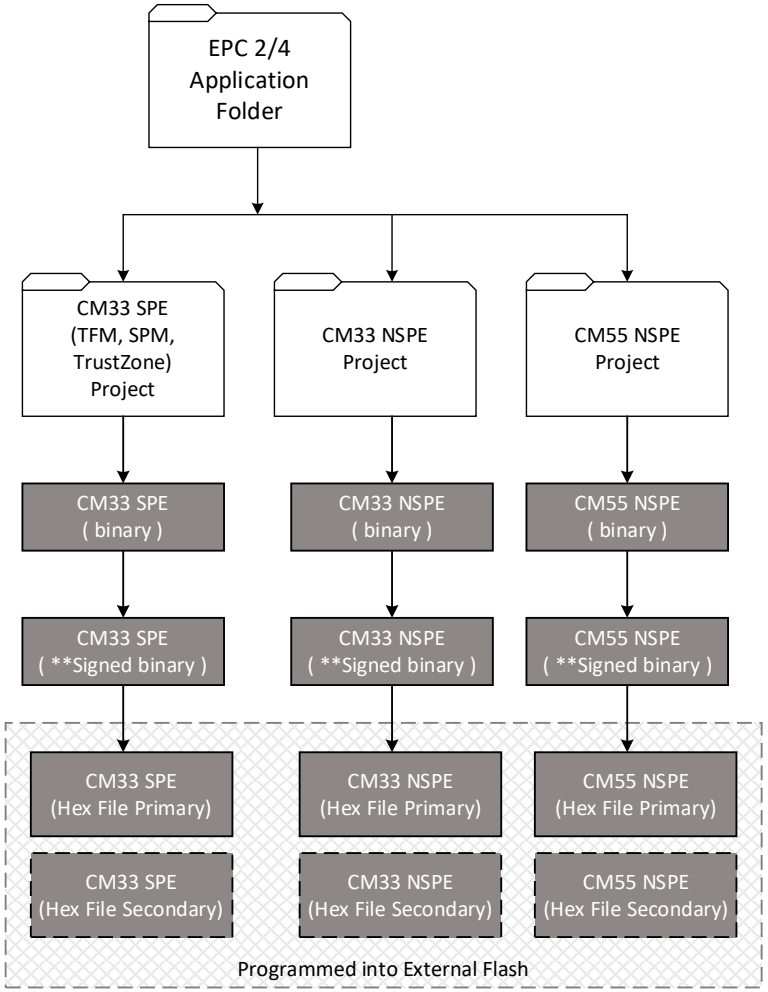
```
" smif_data_width": {
   "description": "Select data width used to interface the external
 flash",
   "applicable_conf": "4, 8",
    "value": 4
}
```

```
  "oem_alt_boot": {
   "description": "Disable/Enable alternate boot by setting the
  value to false/true",
   "value": true
 },
```

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


Copyright © Infineon Technologies AG 2026. All rights reserved.

Typical application structure



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Cryptography basics 4

2 Introduction to security 10

3 PSOC™ Edge architecture 13

4 Security features 16

5 **Introduction to Edge Protect Tools** **31**

6 Lab 33

Copyright © Infineon Technologies AG 2026. All rights reserved.

Edge Protect tools

- Edge Protect tools are pre-installed with ModusToolbox™ Edge Protect Security Suite

- Capabilities
  - Key generation
  - Image signing and encryption
  - Provisioning the device
  - Factory reset
  - Device integrity check

- Communicates with the target device over serial or SWD interfaces
- Infineon-signed SE RAM applications and Extended Boot are bundled in the Edge Protect Tools package

Note: See AN238041 for more information on Edge Protect Tools.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Cryptography basics 4

2 Introduction to security 10

3 PSOC™ Edge architecture 13

4 Security features 16

5 Introduction to Edge Protect Tools 31

6 **Lab** **33**

Copyright © Infineon Technologies AG 2026. All rights reserved.

Lab: Getting started with Basic Secure App

What will we learn?

- Using the Edge Protect Tools
- Provisioning the device
- Ownership transfer
- Enabling Secure boot
- Image signing

Revision history

Document revision	Date	Description of change
**	2025-11-20	Initial release.
*A	2026-02-16	Updated speaker notes.
*B	2026-06-04	Added KIT_PSE84_AI support in hands-on labs.
*C	2026-07-15	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