Customer training workshop

XMC7000 Device Security

Target products

› Target product list for this training material:

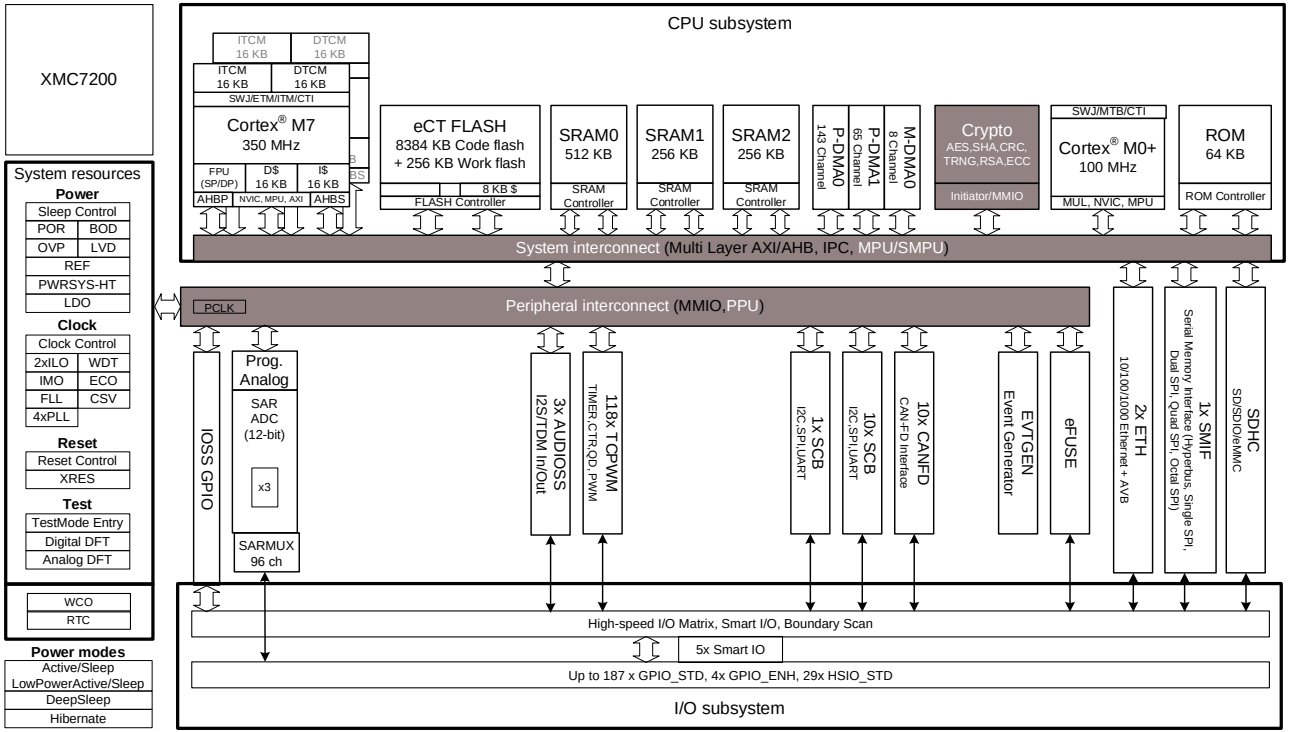
Family category	Series	Code flash memory size
XMC7200	XMC7200-8M	Up to 8384 KB
XMC7100	XMC7100-4M	Up to 4160 KB

Copyright © Infineon Technologies AG 2022. All rights reserved.

XMC7200 - 8M family

Introduction to XMC7200 - 8M

› Device security is in “CPU and Memory” and “Peripheral Interconnect”



Hint Bar

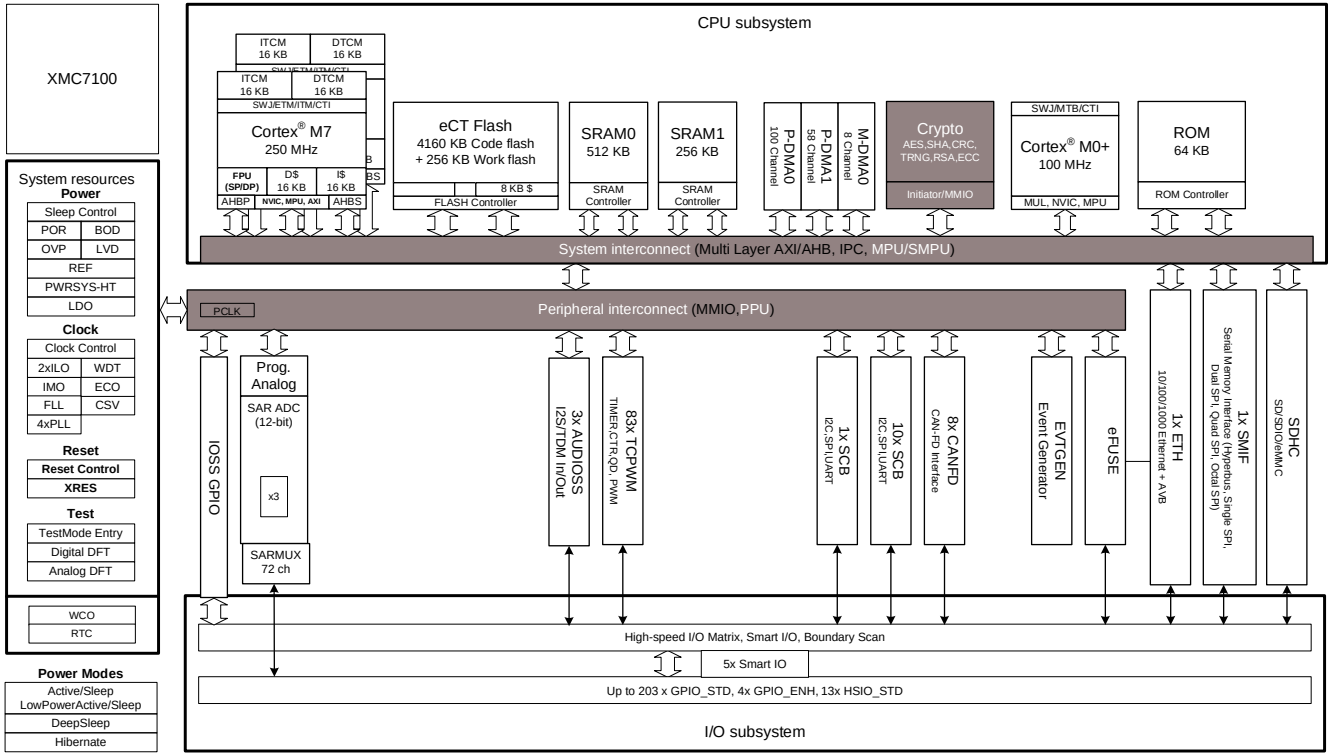
Review TRM chapters 13 and 26 for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

XMC7100 - 4M family

Introduction to XMC7100 - 4M

› Device security is in “CPU and Memory” and “Peripheral Interconnect”



Hint Bar

Review TRM chapters 13 and 26 for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Device security overview

- XMC7000 provides advanced security to protect user designs from unauthorized access and copying
- Features
  - Lifecycle stage
  - Memory and peripheral protection[1]
    - Memory protection units (MPU)
    - Shared Memory Protection Unit (SMPU)
    - Peripheral Protection Units (PPU)
  - Flash Write and eFuse Read/Write Protection
    - Software Protection Units (SWPU)
  - Cryptography (Crypto) block

Hint Bar

Review the Device Security and Cryptography Block TRM chapters for additional details

[1] For details of MPU, SMPU, and PPU see the Protection Unit section

Copyright © Infineon Technologies AG 2022. All rights reserved.

Lifecycle stages

- XMC7000 has the following nonvolatile and irreversible lifecycle stages:
  - NORMAL_PROVISIONED
  - SECURE
  - SECURE_WITH_DEBUG
  - RMA
  - CORRUPTED
- ROM/Flash boot determines protection states based on the lifecycle stage
- DAP, PC1, and PCx are protected according to the protection state

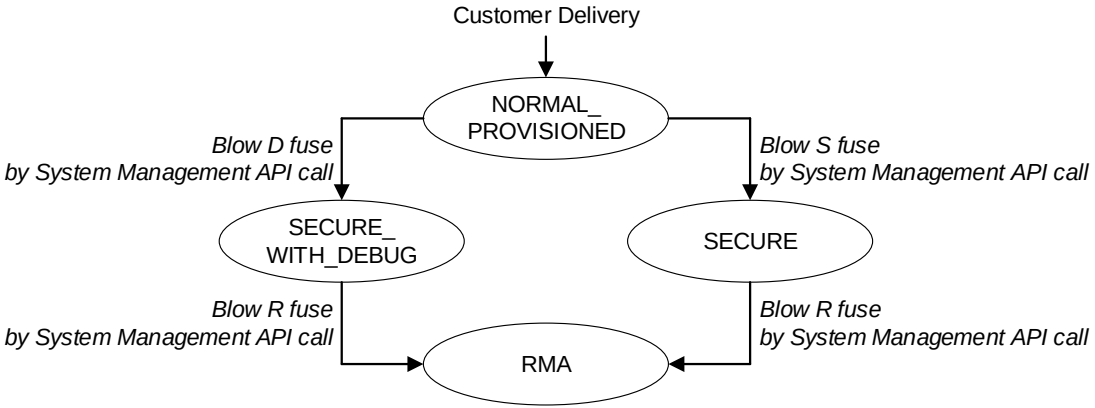
Hint Bar

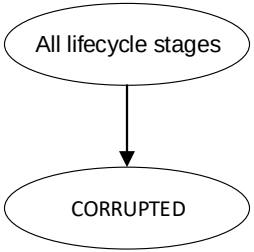
Review the Device Security TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Lifecycle stage transitions

- Lifecycle stages transition by blowing the fuse of eFuse
- eFuse cannot be changed once programmed





Hint Bar

Review the Device Security TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Lifecycle stage transitions

Lifecycle Stage	Description
NORMAL_PROVISIONED	Customers receive parts in this lifecycle stage.
SECURE	This is the lifecycle stage of a secure device. Access restrictions in SECURE mode are controlled by eFuse settings.
SECURE_WITH_DEBUG	This is similar to the SECURE lifecycle stage, except with NORMAL access restrictions applied to enable debugging, even if authentication fails. Devices that are in this stage are only used by developers and testers.
RMA	Devices can be brought into this stage so that Infineon can perform a failure analysis.
CORRUPTED	This stage is entered in case an error is detected when the boot process tries to determine the current lifecycle stage.

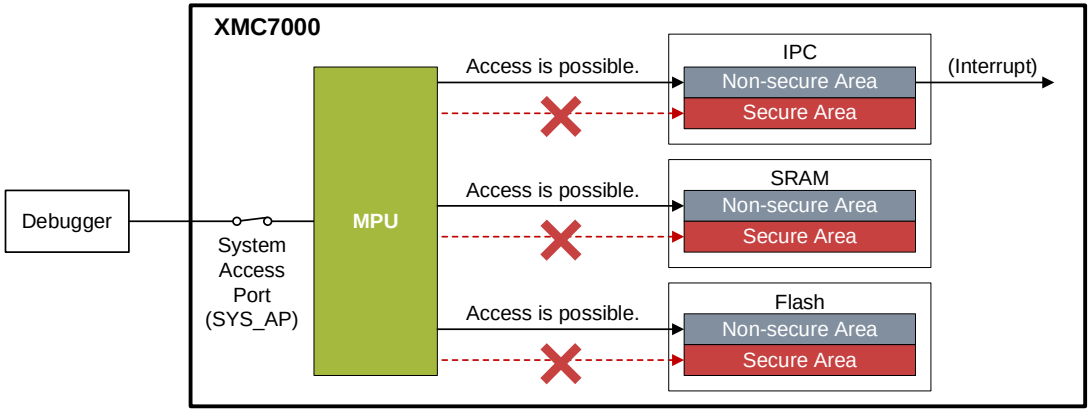
Hint Bar

Review the Device Security TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Memory and peripheral protection

- Overview
  - The MPU/SMPU/PPU restrict access to memory or peripheral address space
    - Internal attack protection
      - Prevents unauthorized code or bus masters from reading protection areas
    - External attack protection
      - Restricts access from unauthorized external equipment



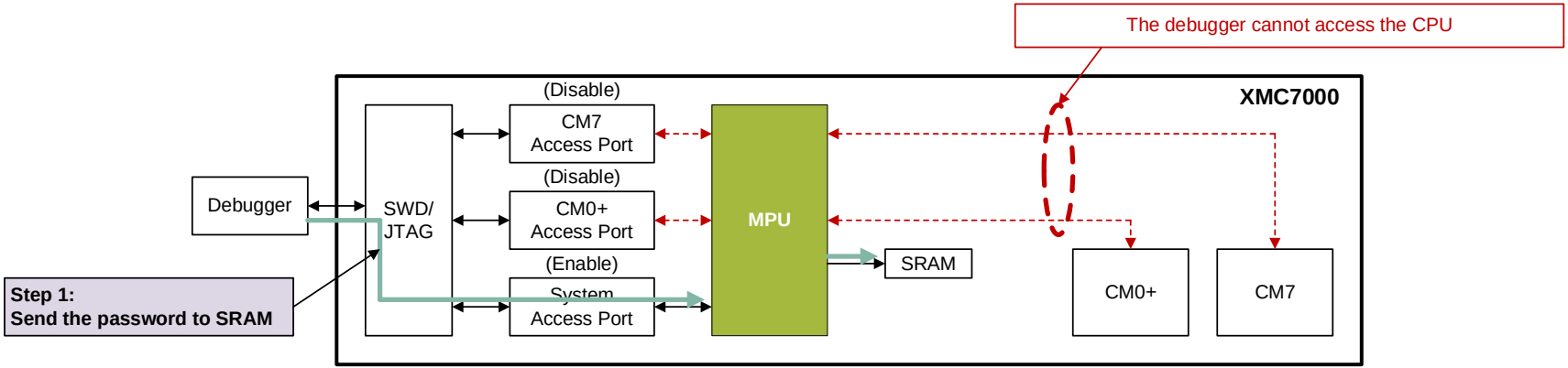
Hint Bar

Review the Device Security TRM chapter and the Program and Debug Interface TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Memory and peripheral protection

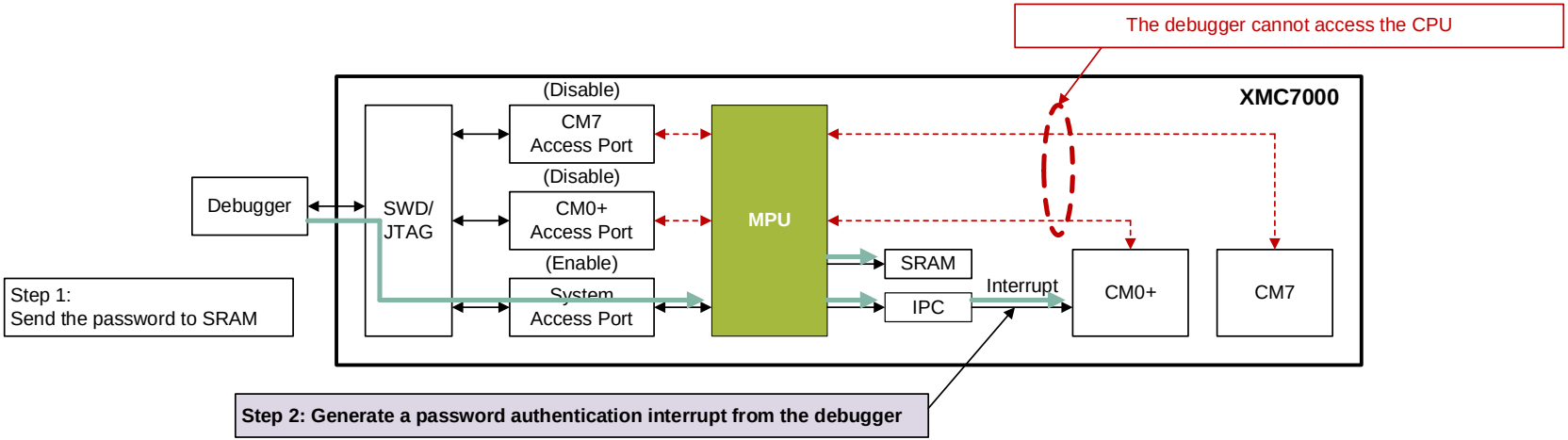
- Use case
  - Allow debugger access to the CPU after password authentication
    - **Debugger sends the password to SRAM**
    - Generate a password authentication interrupt from the debugger
    - CM0+ executes password authentication
    - Allow access to the CPU after password authentication



Copyright © Infineon Technologies AG 2022. All rights reserved.

Memory and peripheral protection

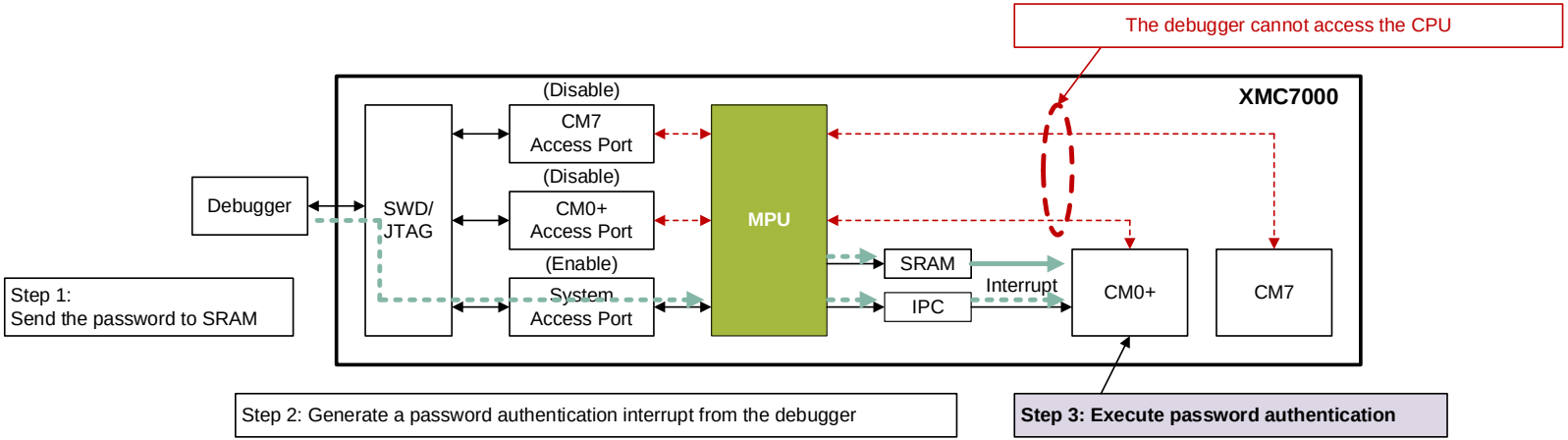
- Use case
  - Allow debugger access to the CPU after password authentication
    - Debugger sends the password to SRAM
    - **Generate a password authentication interrupt from the debugger**
    - CM0+ executes password authentication
    - Allow access to the CPU after password authentication



Copyright © Infineon Technologies AG 2022. All rights reserved.

Memory and peripheral protection

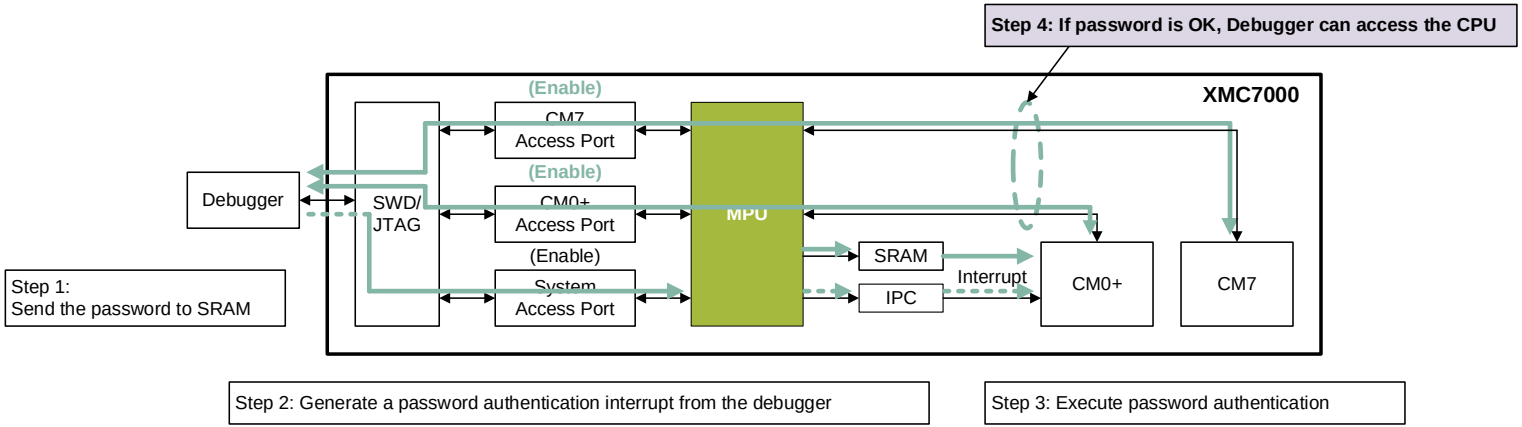
- Use case
  - Allow debugger access to the CPU after password authentication
    - Debugger sends the password to SRAM
    - Generate a password authentication interrupt from the debugger
    - **CM0+ executes password authentication**
    - Allow access to the CPU after password authentication



Copyright © Infineon Technologies AG 2022. All rights reserved.

Memory and peripheral protection

- Use case
  - Allow debugger access to the CPU after password authentication
    - Debugger sends the password to SRAM
    - Generate a password authentication interrupt from the debugger
    - CM0+ executes password authentication
    - **Allow access to the CPU after password authentication**



(Note: The password authentication process is implemented by the user in software)

Copyright © Infineon Technologies AG 2022. All rights reserved.

Flash Write and eFuse Read/Write protection

- Overview
  - XMC7000 has software protection units (SWPUs)[1] that support:
    - Permissions for flash writing and erasing
    - Permissions for eFuse reading and writing
- Advantages
  - Prevents malicious or inadvertent modification of flash or eFuse
  - Prevents reading of eFuse protection data

Hint Bar

Review the Device Security TRM chapter for additional details

[1] SWPUs are stored in Supervisory Flash (SWPU details will be updated in a later revision)

Copyright © Infineon Technologies AG 2022. All rights reserved.

Crypto overview

- Crypto provides hardware implementation and acceleration of cryptographic functions
- Features
  - Cryptography function:
    - Symmetric key ciphers
    - Hashing
    - Asymmetric key ciphers
    - Pseudo-Random Number Generator (PRNG)
    - True Random Number Generator (TRNG)
    - Cyclic Redundancy Check (CRC)
  - Secure Hardware Extension (SHE)[1]
  - Hardware Security Module (HSM)[1]

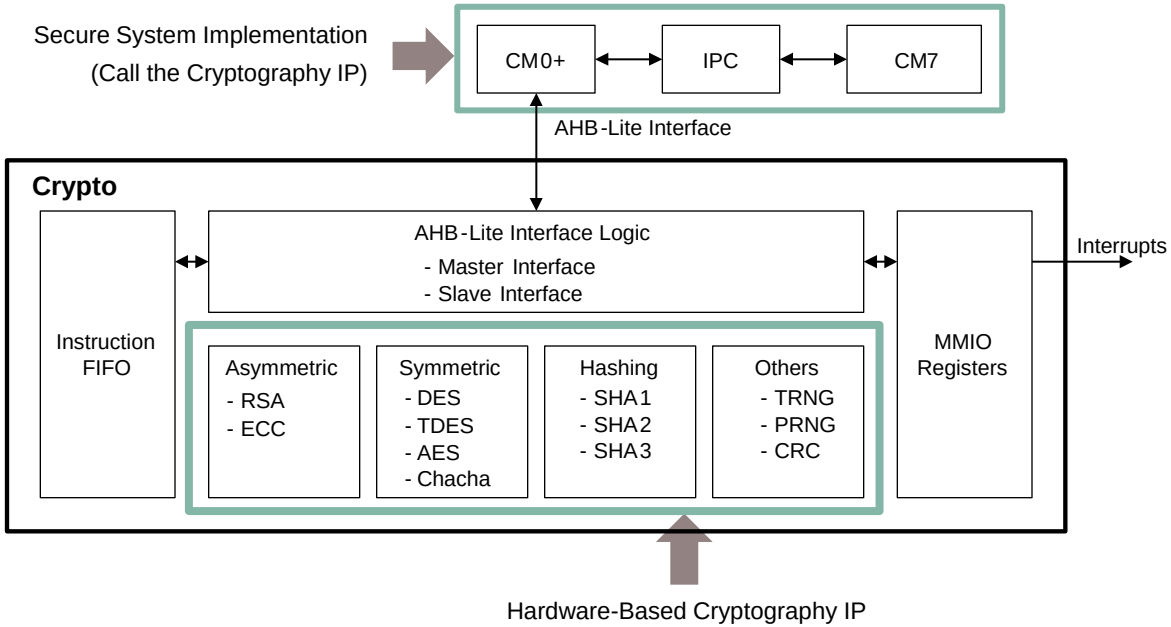
Hint Bar

Review the Cryptography Block TRM chapter for additional details

[1] The SHE and HSM solutions are provided by a third party

Copyright © Infineon Technologies AG 2022. All rights reserved.

Crypto block diagram



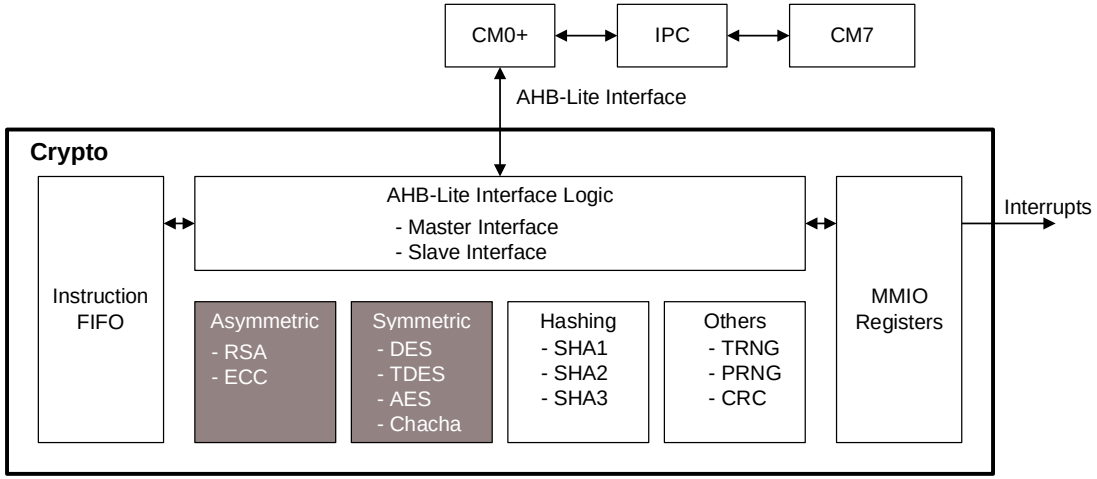
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Hardware-based cryptography IP

- Asymmetric key ciphers
  - RSA and ECC
- Symmetric key ciphers
  - TDES: 64-bit length using a 64-bit key
  - AES: 128-bit length and programmable key length (128/192/256-bit key)
  - Chacha20: 512 random-looking bits



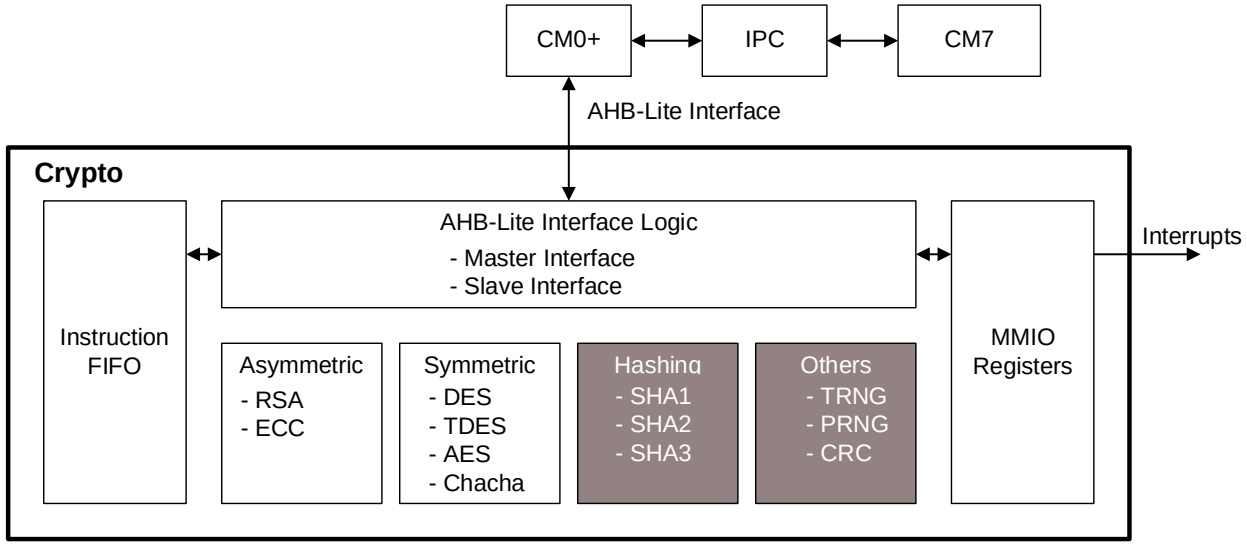
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Hardware-based cryptography IP

- Hashing: SHA1, SHA2, and SHA3 hashes
- PRNG: Generate in a fixed range using three LFSRs
- TRNG: Generate using ring oscillators
- CRC: Programmable polynomial of up to 32 bits



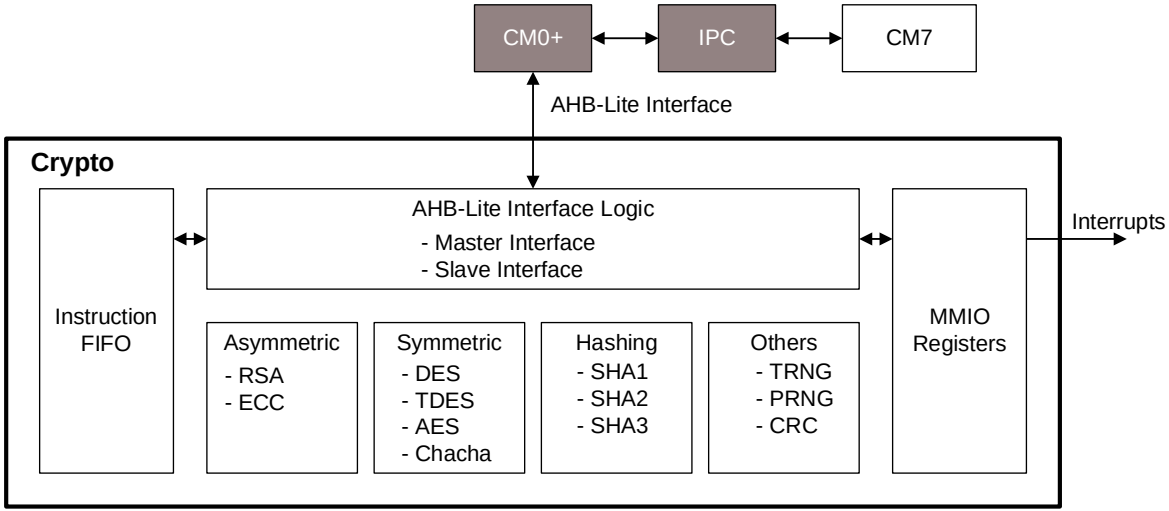
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Secure system implementation

- The cryptography IP can be accessed only by the secure master (CM0+)
- Requests to CM0+ must be made via system calls using IPC from CM7



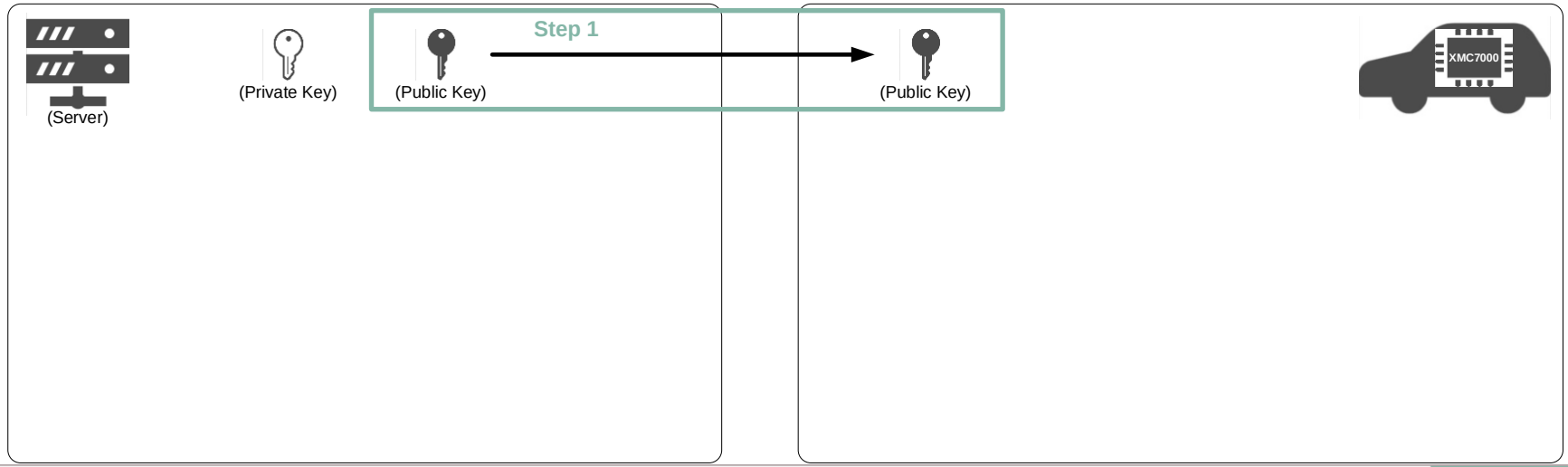
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Digital signature verification with asymmetric key ciphers

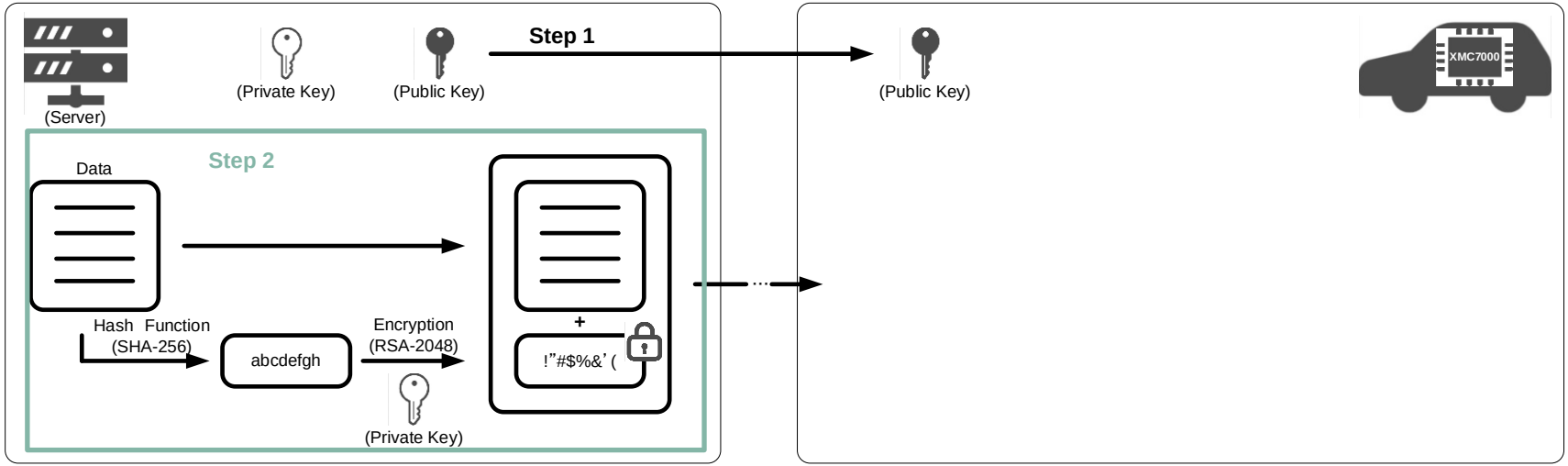
- Use case
  - XMC7000 can support digital signatures by controlling the hardware IP with software
    - Step 1: Distribute the public key



Copyright © Infineon Technologies AG 2022. All rights reserved.

Digital signature verification with asymmetric key ciphers

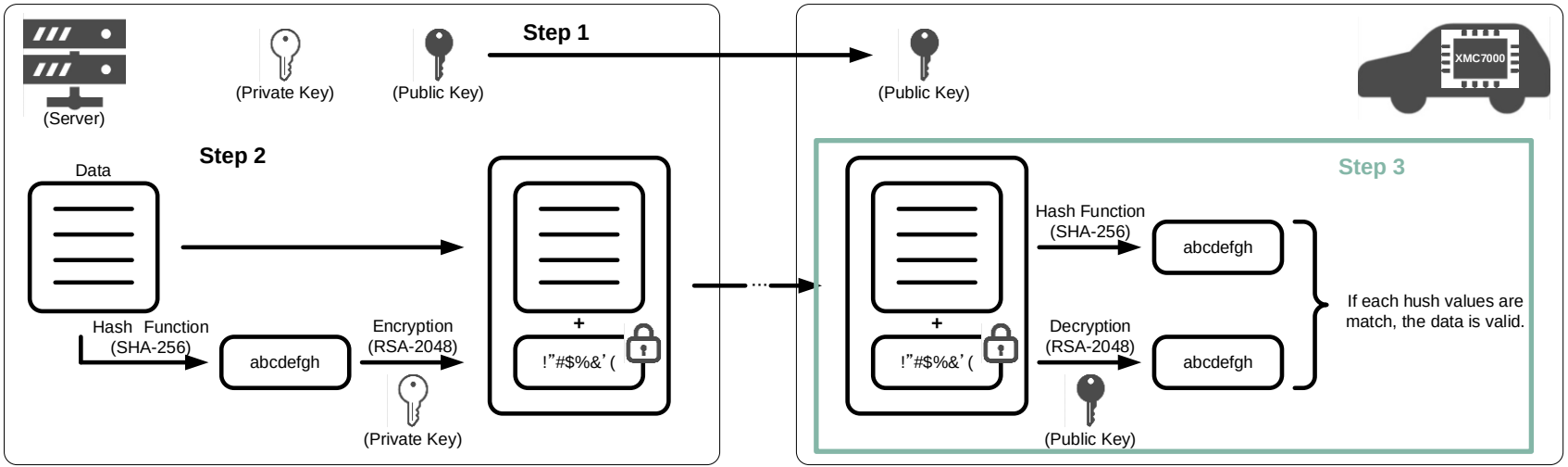
- Use case
  - Step 2:
    - First, using the hash function, calculate the hash value of the data.
    - Next, encrypt the hash value using the private key.
    - Finally, add the encrypted hash value as "signature" to the created data and send it.



Copyright © Infineon Technologies AG 2022. All rights reserved.

Digital signature verification with asymmetric key ciphers

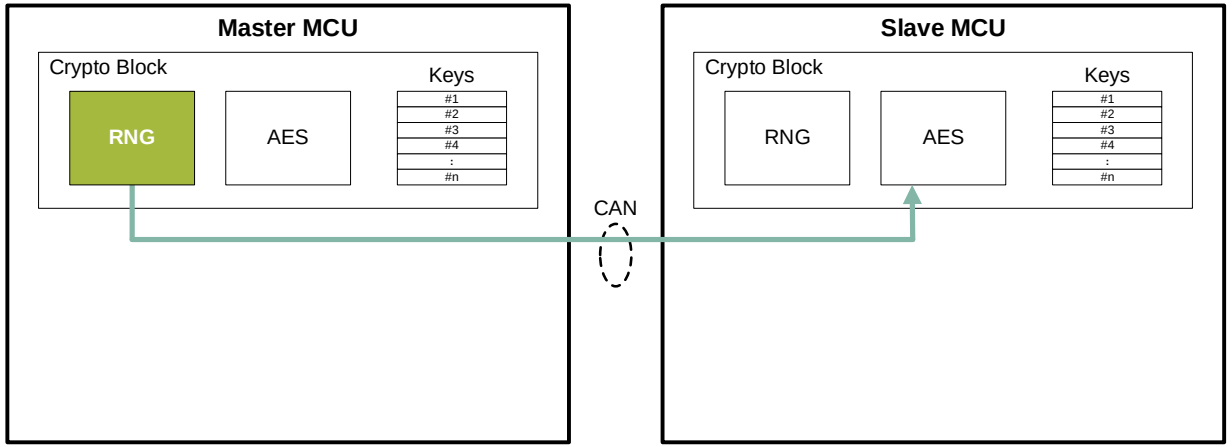
- Use case
  - Step 3:
    - First, decrypt the encrypted hash value using the public key.
    - Next, calculate the hash value of the received data using the same hash function as the sender.
    - Finally, compare the decrypted hash value with the calculated hash value. If they match, the data is correct.



Copyright © Infineon Technologies AG 2022. All rights reserved.

Authentication of communication partner

- Use case
  - Random numbers and encryption are used to authenticate the CAN communication partner
    - Step 1: Master ECU transmits the generated random number



Step 1: Transmit the random number to the Slave MCU

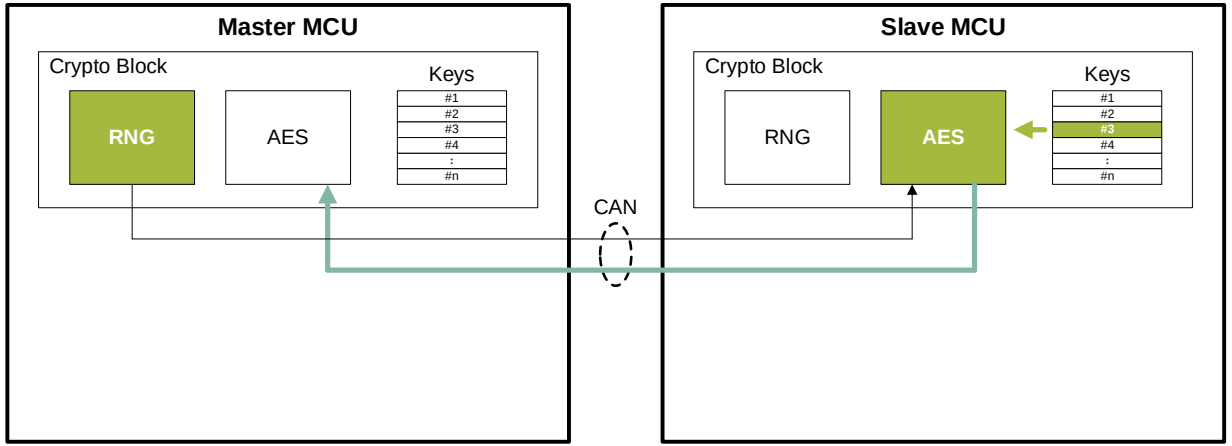
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Authentication of communication partner

- Use case
  - Step 2: The slave ECU encrypts the received random number with Key#3 and sends it to the master ECU



Step 1: Transmit the random number to the Slave MCU

Step 2:
Encrypt the received random number with key #3 and send it to the Master MCU

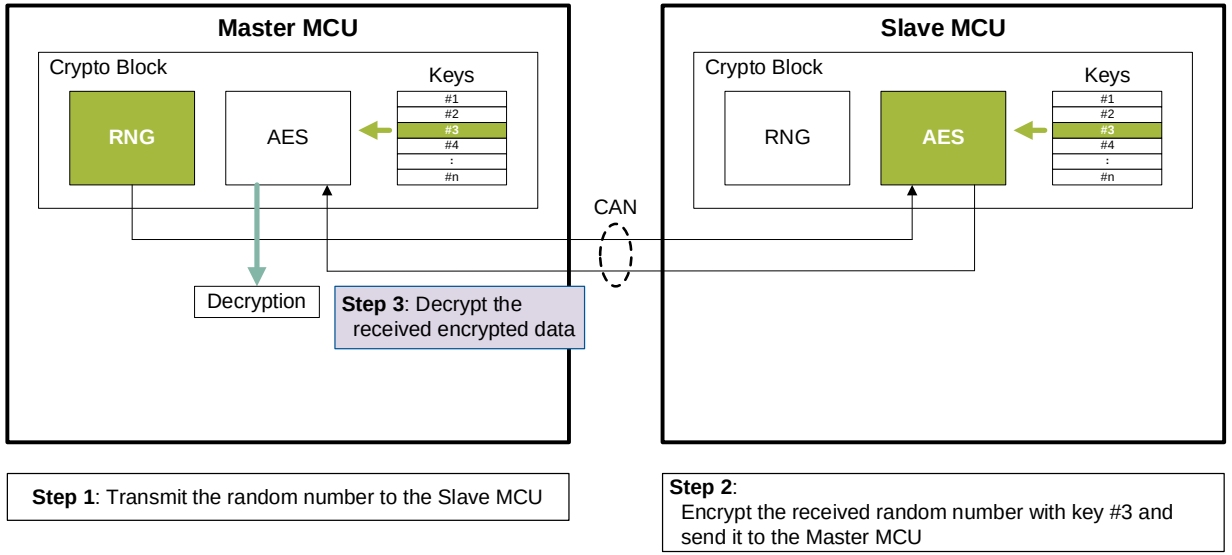
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Authentication of communication partner

- Use case
  - Step 3: The master ECU decrypts the received encrypted data with Key#3



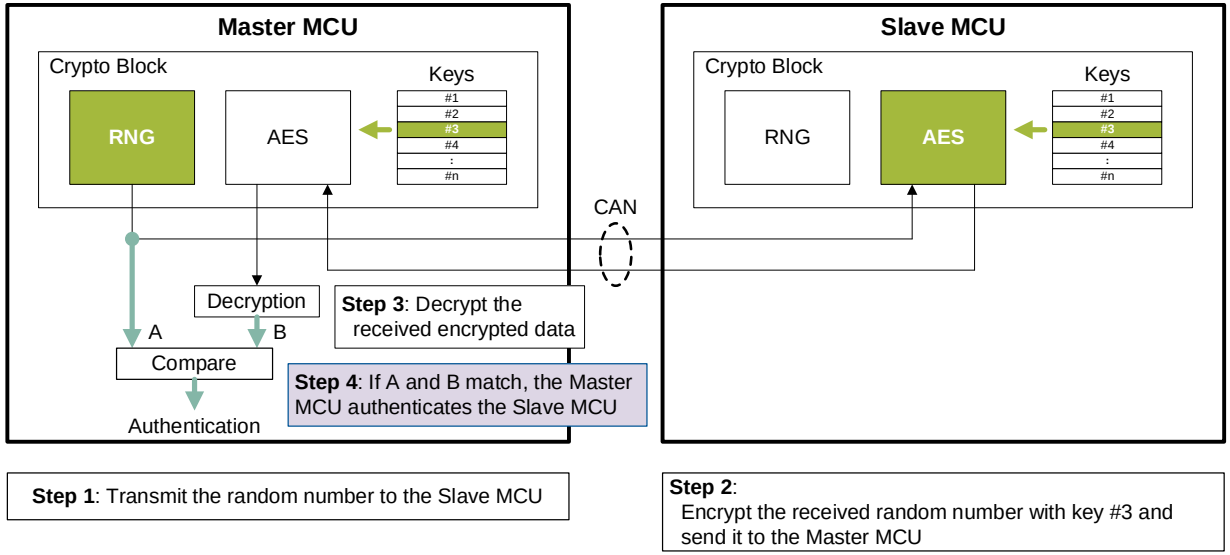
Hint Bar

Review the Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.

Authentication of communication partner

- Use case
  - Step 4: The master ECU checks whether the decrypted data and the transmitted RNG are the same, and authenticates the communication partner if they are the same



Hint Bar

Review Cryptography Block TRM chapter for additional details

Copyright © Infineon Technologies AG 2022. All rights reserved.



Part of your life. Part of tomorrow.

Revision History

Revision	ECN	Submission Data	Description of Change
**	7826963	2022-10-19	Initial release

Copyright © Infineon Technologies AG 2022. All rights reserved.