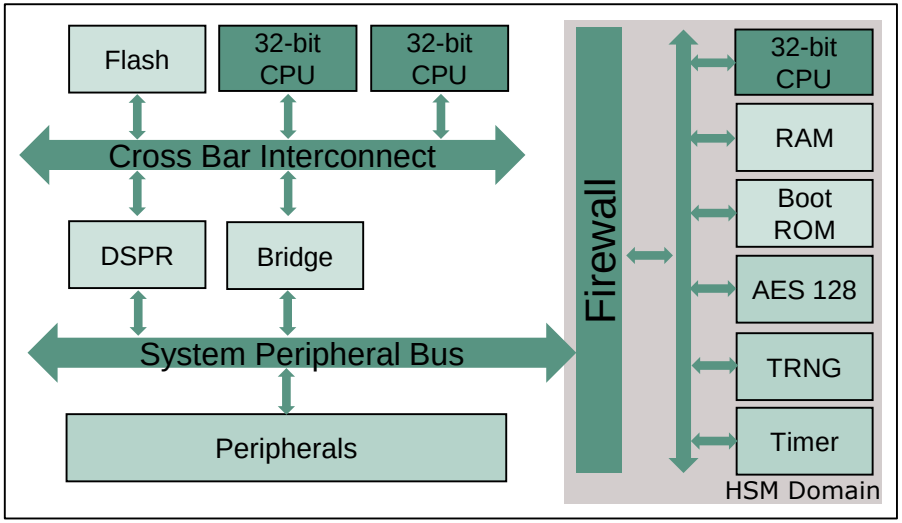
HSM

Hardware Security Module

AURIX™ Microcontroller Training
V1.0 2019-03

HSM
Hardware Security Module



Highlights

- 32 bit ARM Cortex M3 processor with up to 100 MHz CPU speed.
- MPU (Memory Protection Unit)
- Medium EVITA compliant
- True Random Number Generator

Key Features

AES128 and TRNG implemented in HW

AES CMAC with minimum rate 25 MBytes/s

Secure Key Storage in separate HSM P/DFlash portion (8 x 8 KB DF1 only in HE)

Customer Benefits

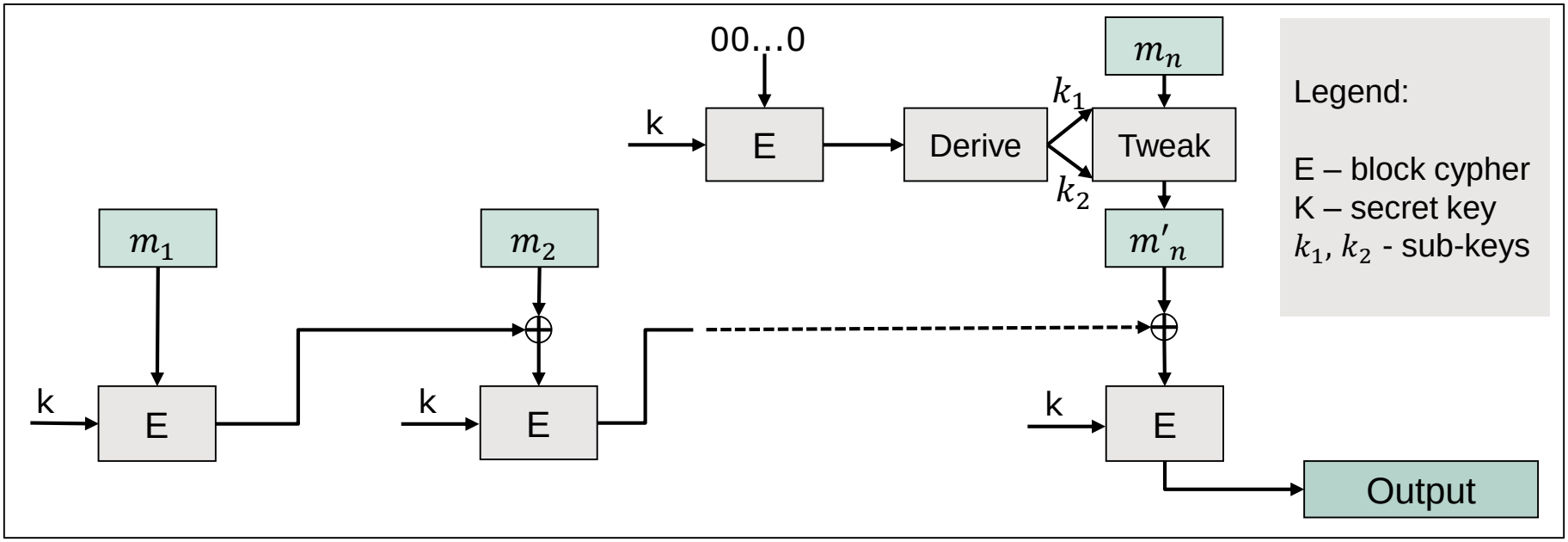
- AES-128 Hardware Accelerator for symmetric cryptography
- Protection against logical attacks, debugger protection
- Secure boot and communication, Tuning protection, Authentication, Immobilizer

HSM
AES128 and TRNG implemented in HW

- The AES module is a fast hardware device that supports encryption and decryption via a 128-bit key AES (Advanced Encryption System)
- It enables plain/simple encryption and decryption of a single 128-bit data (i.e., plain text or cipher text) block as well as encryption or decryption of a multitude of data blocks of 128 bits each. For these, several so called modes of operation are implemented
  - ECB (electronic code book mode)
  - CBC (cipher block chaining mode)
  - CTR (32-bit counter mode)
  - OFB (output feedback mode)
  - CFB (cipher feedback mode)
- This enables also the additional modes
  - GCM (Galois counter mode)
  - XTS (XEX-based Tweaked Code Book mode (TCB) with Cipher Text Stealing (CTS))
- TRNG generates Random Numbers:
  - Keys for cryptographic algorithm
  - Support Protocols (Challenges, blinding values, padding bytes, etc.)
  - Fully compliant to the AIS 20/31 standard

HSM
AES CMAC with minimum rate 25 MBytes/s

- CMAC (Cipher-based Message Authentification Code) is widely used for authentication
- It is based on symmetrical encryption like the CBC-MAC algorithm
- Secure boot uses the CMAC for tampering detection and prevention
- A fast calculation of a CMAC is desired to speed up the boot process time

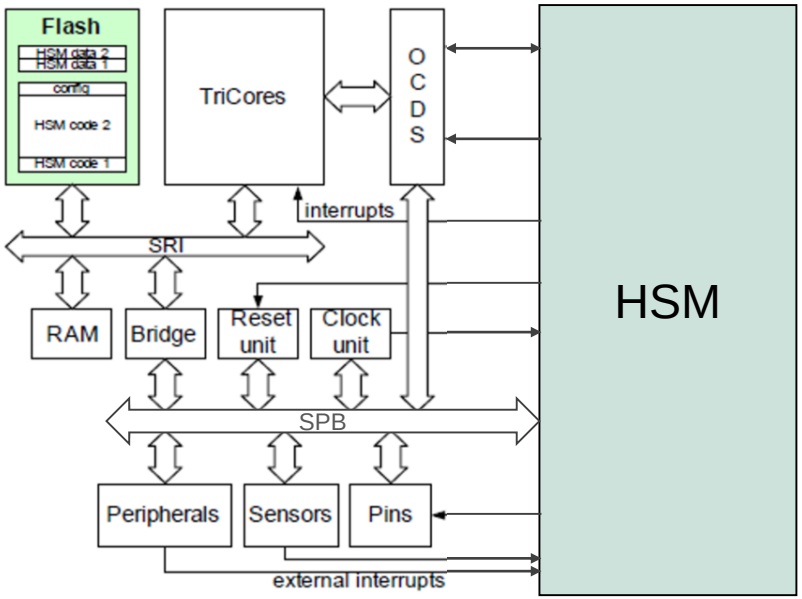


HSM
Secure key storage in separate HSM P/DFlash portion

- Secure key storage, secure data and counters can be saved in a dedicated Data Flash area
- 8 x 8 KB = 64 KB of DFlash (DF1) reserved for HSM (only in AURIX™ TC27x/TC29x devices)
- Data Flash content is refreshed in Round Robin via FEE drivers
- The segregation of the sensible information inside the HSM Data Flash can be enforced using the feature „exclusive access“, which allows the read and write access only to the HSM core
- A dedicated HSM Data Flash allows that the execution of the TriCore™ application can fetch and read code or data from Program Flash while updating secure non-volatile information

HSM
System integration

- HSM is connected with the device via the SPB (Serial Peripheral bus)
- The Bridge module acts as a „firewall“ so the HSM internal resources are protected from accesses by other masters
- P/DFlash of the HSM are shared with the device but can be protected via an „exclusive access“ from TriCore™ and other masters accesses
- HSM, as a system on chip, is a bus master on the SPB



Application example
Chip tuning protection

Overview

- Challenge Response Authentication
- Closed Debugger Interface
- IP Protection
- Tuning Protection

Advantages

- Memory protection plus the option to close the debug interfaces protects against unauthorized read and write access
- An exchange of the micro can be prevented by means of challenge-response authentication

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2019-03
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Email: erratum@infineon.com

Document reference
AURIX_Training_1_
Hardware_Security_Module

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (www.infineon.com).

WARNINGS
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.