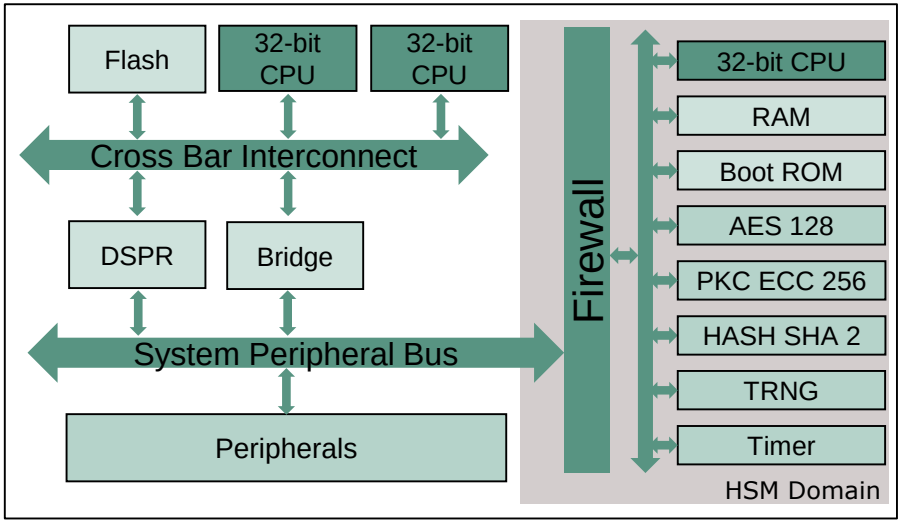
HSM

Hardware Security Module

AURIX™ TC3xx Microcontroller Training
V1.0 2020-09

HSM
Hardware Security Module



Highlights

- 32 bit ARM Cortex M3 processor with up to 100 MHz CPU speed
- MPU (Memory Protection Unit)
- PKC ECC 256 and SHA224/256 Hardware Accelerators
- True Random Number Generator

Key Features

AES128 and TRNG implemented in HW

HW implemented PKC and HASH SHA-224/SHA-256

Secure key storage in separate HSM DFlash portion

Customer Benefits

- AES-128 Hardware Accelerator and TRNG for cryptography
- Fast signature generation, verification and generic data integrity check
- Secured 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
AES128 and TRNG implemented in HW

- True Random Number Generator (TRNG) is used to generate Random Numbers for:
  - Keys for cryptographic algorithms
  - Support protocols (challenges,..)

- High “entropy” is required
  - Uncertainty associated with a random variable
  - The lower the entropy, the more predictable the bit values
  - Post processing implemented to increase the entropy

- The Quality (min. entropy req.) is defined by:
  - AIS-31 publication by German BSI
- The time needed to generate a random number is not constant:
  - Depends on the “entropy” level of the source
  - For a clock frequency of 100MHz the typical throughput is approximately Rtyp = 360kb/s

HSM
HW implemented PKC and HASH SHA-224/SHA-256

- The hash module is capable of executing MD-5, SHA-1 or SHA-224/SHA-256 functions using a common internal engine
- The module supports multi-tasking environments
- Less than 2 µs latency for a 512 bit block
- The timer required to process one 512-bit input data block depends on the selected algorithm

Hash Algorithms and Performance

Algorithm	Clock cycles per 512-bit Data Block	Notes
MD-5	65	-
SHA-1	81	-
SHA-224	65	Special software handling needed
SHA-256	65	

Note: 65 cycles corresponds to theoretical reachable 98 Mbyte/s SHA256 module performance.

HSM
HW implemented PKC and HASH SHA-224/SHA-256

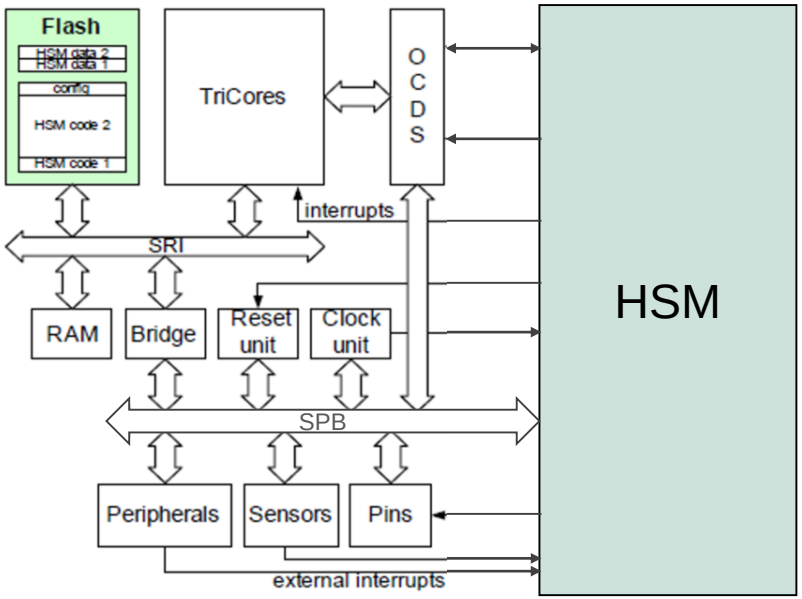
- The Public Key Cryptography (PKC) module is a hardware module that supports fast signature generation and verification with ECDSA.
  In particular, it enables modular and non-modular operations on integers and binary polynomials up to 256 bit length:
  - Multiplication
  - Modular addition, subtraction, multiplication, division and inversion
- It enables also complex algorithms on all common elliptic curves of bit length up to 256:
  - Addition of two points in affine coordinates
  - Doubling of a point in affine coordinates
  - Scalar multiplication
- The supported curves are all curves defined over finite fields of the type F_p and $GF(2^d) = F_2[X]/f$ of bit length up to 256 bit length:
  - This includes the **NIST curves** P-192, P-224, P-256, K-163, B-163, K-233, B-233, as well as the **Brainpool curves** brainpoolP160r1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1
  - Additionally support for operations on Curve25519 and Ed25519 is included
- Furthermore, the PKC module supports the following features:
  - Storage for 32 values (integers or binary polynomials) of up to 256 bit length
  - **Generation of 200 ECDSA-signature/s @100MHz for elliptic curves of key-length 256**
  - **Verification of 100 ECDSA-signature/s @100MHz for elliptic curves of key-length 256**

HSM
Secure key storage in separate HSM DFlash portion

- Secured key storage, secured data and counters can be saved in a dedicated Data Flash area
- 128 KB of DFlash (DF1) reserved for HSM
- Data Flash content is refreshed in Round Robin via FEE drivers
- The segregation of the sensible information inside the HSM P/DFlash 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 secured non-volatile information in DF1

HSM
System integration

- HSM is connected with the device via the SPB (System 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

Revision history

Revision	Description of change
V1.0	Initial version

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

Edition 2020-09
Published by
Infineon Technologies AG
81726 Munich, Germany

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

Document reference
AURIX_Training_2_
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.