VECTOR

MICROSAR 4

Product Information

For Projects Using Infineon Microcontrollers

Version 1.00.05

Authors	Hannes Haas
Status	Released

Contents

1 Introduction

This document includes details to the offered items in the context of the specific microcontroller stated below and applies in addition to the general Product Information MICROSAR 4 (ProductInformation_2_MICROSAR4.pdf) and the program-specific Product Information (ProductInformation_2_MICROSAR4_<OEM>_<program>.pdf).

2 Modules and Options

Note
This chapter contains important information, constraints and limitations of MICROSAR modules and options for a specific microcontroller that may have been offered or delivered.

2.1 vHsm (Infineon TriCore)

Note
This chapter applies to vHsm in combination with the following microcontrollers:

> Infineon TC2x (excluded: TC23x)
> Infineon TC3x

vHsm (Infineon TriCore) is executed on the hardware security module (HSM) of the microcontroller. It will be delivered as a dedicated HSM SIP.

To access vHsm from the host controller the MICROSAR SIP and/or the Vector Flash Bootloader must be extended with respective options:

> MICROSAR 4: Crypto (vHsm)

> Vector Flash Bootloader: Secure Boot (HW) Vector vHSM Integration

The vHsm implementation must be compatible with the above host controller software implementations. If existing deliveries shall be reused, compatibility must be clarified with Vector in advance. Updates of the Flash Bootloader and MICROSAR stack may be required.

2.1.1 Supported Crypto Algorithms

The following crypto algorithms are supported:

Algorithm / Function	Standard	vHsm	Csm 4.3 Service	Csm 4.3 Interface
SHA-2 (SHA-256)	FIPS 180-4	x	Hash Functions	Hash Interface
SHA-2 (SHA-512)	FIPS 180-4	x		
Pseudo random number generation based on AES	FIPS-186-2	x	Random Numbers	Random Interface
CTR-DRBG based on AES-128 with DF and without DF	NIST SP 800-90A	x		
HMAC based on SHA-1	FIPS 198-1	x	Message Authentication Code (MAC) Generation and Verification	MAC Interface
HMAC based on SHA-2-256	FIPS 198-1	x		
AES-CMAC (based on AES 128)	IETF RFC4493	x		
Poly1305	IETF RFC7539	x		
SipHash		x		
AES-256	FIPS-197	x		Cipher Interface (Symmetric)

Algorithm / Function	Standard	vHsm	Csm 4.3 Service	Csm 4.3 Interface
AES-128 in the modes ECB/CBC	FIPS-197	x	Symmetric Encryption and Decryption	
AEAD: AES-GCM	NIST 800-38D	x		
ChaCha20	IETF RFC7539	x		
Asymmetric encryption and decryption based on RSA with key length of 512-4096 bit	PKCS #1 V1.5	x[1]	Asymmetric Encryption and Decryption	Cipher Interface (Asymmetric)
		x	Key Handling	Key Setting Interface
		x		Key Extraction Interface
		x		Key Copying Interface
		x		Key Generation Interface
KDF in Counter Mode, KDF in Counter Mode with Appendix, concatenation KDF (NIST 800-56A)	NIST SP 800-56A	x		Key Derivation Interface
Key exchange using the Elliptic Curve Diffie-Hellman protocol EC-DHE with ANSIp256r1, SECp256r1 and X25519	ANSI X9.63	x[1]		Key Exchange Interface
Digital Signatures based on RSA: RSA PKCS #1V1.5 Prehashing variants: SHA-1, SHA-256	PKCS #1 V1.5	x[1]	Signature Generation and Verification	Signature Interface
Digital Signatures based on RSA: RSA CRT DSA Verification Prehashing variants: SHA-1, SHA-256	PKCS #1 V1.5	x[1]		
Digital Signatures based on RSA: PSS Prehashing variants: SHA-1, SHA-256	PKCS #1 V2.2	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA Ed25519 PreHashing: None, SHA-1	ANSI X9.62-2005 RFC8032	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA ANSI P256 R1 PreHashing: None, SHA-1, SHA-256	ANSI X9.62-2005	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA NIST P256 R1 PreHashing: None, SHA-1, SHA-256	ANSI X9.62-2005	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA NIST P384 R1 PreHashing: None, SHA-1, SHA-256	ANSI X9.62-2005	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA SEC P256 R1 PreHashing: None, SHA-1, SHA-256	ANSI X9.62-2005	x[1]		
Digital signatures based on the Elliptic Curves: ECDSA SEC P384 R1 PreHashing: None, SHA-1, SHA-256	ANSI X9.62-2005	x[1]		

Algorithm / Function	Standard	vHsm	Csm 4.3 Service	Csm 4.3 Interface
Certificate installation and update according to ISO15118	ISO15118	x		
Secure Boot Protocol	SHE1.1 + additional features	x		
Symmetric Key Update Protocol	SHE1.1	x		

[1] vHsm Add-On Asymmetric Crypto required

Table 2-1 Supported crypto algorithms vHsm

2.1.1 Supported Hardware Accelerators

The following hardware accelerators and modes are supported by vHsm:

- TRNG,
- AES-128 (Modes: ECB, CBC),
- CMAC (AES-128),
- SHA256.

2.1.2 Platform-Specific Information

vHsm (Infineon TriCore) uses a Fee/Fls module to store data to flash. The Fee/Fls must be licensed by the customer from Infineon and provided to Vector.

To make the Infineon Fee/Fls usable on the HSM core of the Infineon TriCore, adaptations are required. The adaptations which are performed by Vector include:

- Modifications of registers

Note
The Infineon Fee/Fls are not developed according to the quality measures and/or processes of Vector and, therefore, Vector is not liable or responsible for any errors or defects in the Infineon Fee and/or Fls.

Note
The customer must ensure that Infineon grants the customer the right to

- Modify the TriCore Fee/Fls;
- Use the Fee/Fls also on the HSM core (that means it is not limited to the TriCore);
- Use the Fee/Fls in multiple instances on the TriCore (TriCore and HSM core); and
- Have the foregoing rights exercised by Vector for the purpose of performing the required adaptions described above.

2.1.3 Export Control

Caution
The HSM software (vHsm) is classified as dual-use item according to 5D002C of Annex I to Council Regulation (EC) No 428/2009 as amended by Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017.

Fulfillment of the contract by Vector is subject to the provision that contract fulfillment does not violate any legal regulations and/or government directives related to export control and/or foreign trade law.

2.2 vOtaDl (all versions) with Infineon TriCore

The synchronization of different flash users for the internal flash has to be realized by the application and is not provided by vOtaDl (all versions). Reasons are vendor specific extensions of the Infineon Fee/Fls API.

3 Contact

Visit our website for more information on

- News
- Products
- Demo software
- Support
- Training data
- Addresses

www.vector.com