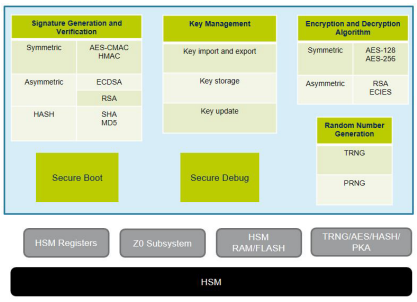
SPC58-HSM-FW

Data brief

SPC58 HSM Firmware



Product status link
SPC58-HSM-FW

Product summary	
Order code	SPC58-HSM-FW
Reference	SPC58 HSM Firmware

Features

- SHE v1.1 specification and only for SPC58-HSM-FW extension for 20NVM user Keys for AES128, AES256, RSA, ECC, HASH and HMAC
- AES-128, AES-256 bits. Supported modes are:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining) with support for ciphertext stealing
  - GCM (Galois Counter Mode)
  - CMAC
- AES256 HASH and HMCA support services (only available for SPC58-HSM-FW)
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- Elliptic Curve
- RSA
  - PKCS#1 v1.5 1024
  - PKCS#1 v1.5 2048
  - PKCS#1 v1.5 3072
- ECDSA
- ECIES
  - NIST_P_256
  - NIST_P_384
  - NIST_P_521
  - BRAINPOOL_P256R1
  - BRAINPOOL_P384R1

Description

The SPC58-HSM-FW and the SPC5 Software Cryptography Library provides an exhaustive set of software algorithms and ready-to-use examples for symmetric and asymmetric Encryption/Decryption, message authentication and Random Number Generation. The SPC58 HSM Firmware is a SW product that can be ordered at ST sales office. The SPC5 Software Cryptographic Library is an SPC5Studio Eclipse plug-in, available for free download on www.st.com. The software library can run on the whole SPC5 microcontroller family. On SPC564B/EC MCU's, AES-128 ECB/CBC Encryption/Decryption, CMAC Message Authentication, Keys access lock/unlock, secure Key loading/update and Random Number Generation are implemented by a hardware dedicated peripheral (CSE accelerator) to guarantee minimum CPU load and maximum security level (a complete set of software drivers are available as part of SPC5Studio suite www.st.com/spc5studio). SPC58 HSM Firmware exploits the embedded HSM co-processor supported and can run only in microcontroller with HSM.

1 Supported algorithms

1.1 AES algorithm

The advanced encryption standard (AES), is a symmetric cipher algorithm that can process data blocks of 128 bits, using a key with a length of 128, 192 or 256 bits.

The cryptographic library includes AES 128-bit, and 256-bit modules to perform encryption and decryption in the following modes:

- ECB (Electronic Codebook mode)
- CBC (Cipher-Block Chaining) with support for Ciphertext Stealing
- GCM (Galois Counter mode)
- CMAC

1.2 RNG algorithm

The security of cryptographic algorithms relies on the impossibility of guessing the key. The key has to be a random number, otherwise the attacker can guess it.

Random number generation (RNG) is used to generate an unpredictable series of numbers. Only for SPC5 Software Cryptography Library the random engine is implemented in software using a CTR_ DRBG based on AES-128, while a True RNG is available for SPC58 family and a dedicated API is provided by SPC58-HSM-FW.

1.3 HASH algorithm

This algorithm provides a way to guarantee the integrity of information, verify digital signatures and message authentication codes. It is based on a one-way hash function that processes a message to produce a small length / condensed message called a message digest.

The SPC5 Software Cryptography Library includes functions required to support HASH/HMAC modules to guarantee the integrity of information using the following modes:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

1.4 RSA algorithm

RSA algorithm is a public key cryptographic algorithm designed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA labs specified some public key cryptographic standards leveraging it.

The Cryptography Library includes functions required to generate and verify digital signatures and encryption / decryption using PKCS#1v1.5 standard:

- RSA PKCS#1 v1.5 1024
- RSA PKCS#1 v1.5 2048
- RSA PKCS#1 v1.5 3072

1.5 ECC algorithm

Cryptography Library supports ECC Elliptic Curve Cryptography (ECC) operations for elliptic curves defined over prime fields.

Supported functionalities includes ECC key pair generation, ECDSA (Elliptic Curve Digital Signature) and ECIES:

- NIST_P_256
- NIST_P_384
- NIST_P_521
- BRAINPOOL_P256R1
- BRAINPOOL_P384R1

Revision history

Table 1. **Document revision history**

Date	Version	Changes
17-Sep-2019	1	Initial release.

Contents