X-CUBE-CRYPTOLIB

STM32 crypto library software expansion for STM32Cube

Data brief

Features

Crypto algorithms supported are:

- AES-128, AES-192, AES-256 bits:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining) with support for ciphertext stealing
  - CTR (Counter Mode)
  - CFB (Cipher Feedback)
  - OFB (Output Feedback)
  - CCM (Counter with CBC-MAC)
  - GCM (Galois Counter Mode)
  - CMAC
  - KEY WRAP
  - XTS (XEX-based tweaked-codebook mode with ciphertext stealing)
- ARC4
- DES, TripleDES:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining)
- HASH functions with HMAC support:
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- ChaCha20
- Poly1305
- CHACHA20-POLY1305
- Random engine based on DRBG-AES-128
- RSA signature functions with PKCS#1v1.5
- RSA encryption/decryption functions with PKCS#1v1.5
- ECC (Elliptic Curve Cryptography):
  - Key generation
  - Scalar multiplication (the base for ECDH)
  - ECDSA
- ED25519
- Curve25519

Description

STM32 crypto library package (X-CUBE-CRYPTOLIB) is based on STM32Cube architecture package and includes a set of crypto algorithms based on firmware implementation ready to use in all STM32 microcontrollers. This software is classified ECCN 5D002.

For dedicated devices some algorithms are supported with hardware acceleration, to optimize the performance and the footprint usage.

Up to 31 examples are provided in this package, covering all the available algorithms with template projects for the most common development tools, such as: Keil® MDK-ARM™, IAR EWARM (IAR Embedded Workbench®), GCC-based IDEs (free AC6: SW4STM32, Atollic® TrueSTUDIO®,...). Even without the appropriate hardware evaluation board, this layer allows the user to quickly get started with a new STM32 cryptographic firmware library brand.

1 Ordering information

X-CUBE-CRYPTOLIB is available for free download from the *www.st.com* website.

This software is classified ECCN 5D002.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
01-Sep-2015	1	Initial release.
09-Dec-2015	2	Updated *Features* and *Description* to introduce a new cryptographic firmware version.
15-Dec-2015	3	Updated *Description* and *Section 1: Ordering information*.