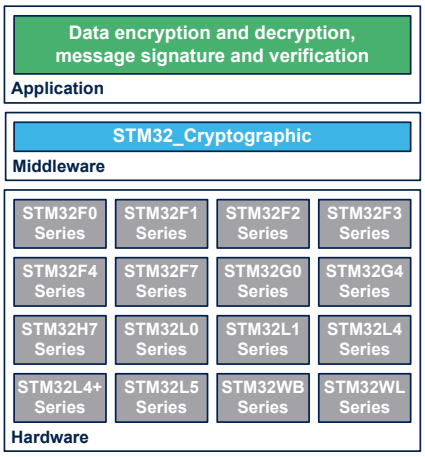
X-CUBE-CRYPTOLIB

Data brief

STM32 cryptographic library software expansion for STM32Cube



Product status link
X-CUBE-CRYPTOLIB

Features

Supported NIST CAVP certified cryptographic algorithms:

- AES-128, AES-192, AES-256 bits:
  - ECB (electronic codebook mode)
  - CBC (cipher-block chaining) with support for cipher text 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 cipher text stealing
- HASH functions with HMAC support:
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- Random engine based on DRBG-AES-128
- RSA with PKCS#1v1.5:
  - Encryption/decryption
  - Signature

  ECC (elliptic curve cryptography):
  - Key generation
  - Scalar multiplication (the base for ECDH)
  - ECDSA

Supported, but not certified, cryptographic algorithms included in the library:

- ARC4
- DES, TripleDES:
  - ECB (electronic codebook mode)
  - CBC (cipher-block chaining)
- HASH:
  - MD5
  - HKDF-SHA-512
- ChaCha20
- Poly1305
- CHaCHA20-POLY1305
- Curve25519
- ED25519

1 Description

The STM32 cryptographic library package (X-CUBE-CRYPTOLIB) includes all the major security algorithms for encryption, hashing, message authentication, and digital signing, enabling developers to satisfy application requirements for any combination of data integrity, confidentiality, identification/authentication, and non-repudiation.

The library includes firmware functions for STM32F0 Series, STM32F1 Series, STM32F2 Series, STM32F3 Series, STM32F4 Series, STM32F7 Series, STM32G0 Series, STM32G4 Series, STM32H7 Series, STM32L0 Series, STM32L1 Series, STM32L4 Series, STM32L4+ Series, STM32L5 Series, STM32WB Series and STM32WL Series. For more details refer to the *STM32 cryptographic library* user manual (UM1924) on the *www.st.com* website.

This firmware is classified ECCN 5D002.

Most of the well-used algorithms are certified according to the US cryptographic algorithm validation program (CAVP), helping customers to prove quickly and cost-effectively the security of their new products.

The certified algorithms are: AES (3971), RSA (2036), ECDSA (874), SHS (3275), DRBG (1165) and HMAC (2589). Full details are available online at the NIST CSRC algorithm validation lists website, selecting the CAVP web page.

In this package there are examples for each algorithm for popular development tools including IAR Systems® EWARM (IAR Embedded Workbench®), Keil® MDK-ARM, and GCC -based IDEs such as Ac6 SW4STM32 and STMicroelectronics STM32CubeIDE.

To benefit from STM32 cryptographic accelerators, refer to STM32Cube MCU and MPU package hardware abstraction layer (HAL) functions and examples.

2 General information

The X-CUBE-CRYPTOLIB runs on STM32 microcontrollers based on Arm® Cortex® cores.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2.1 Ordering information

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

2.2 Product information

Table 1 shows the X-CUBE-CRYPTOLIB versions available for download for each target use.

Table 1. X-CUBE-CRYPTOLIB versions

Target use	Version
STM32F0 Series	V3.1.5 (patch for version V3.1.0)
STM32F1 Series	V3.1.0
STM32F2 Series	V3.1.0
STM32F3 Series	V3.1.0
STM32F4 Series	V3.1.0
STM32F7 Series	V3.1.0
STM32G0 Series	V3.1.5 (patch for version V3.1.3)
STM32G4 Series	V3.1.3
STM32H7 Series(1)	V3.1.2 (patch for version V3.1.0)
STM32H7A3xx and STM32H7B3xx	V3.1.3
STM32L0 Series	V3.1.5 (patch for version V3.1.0)
STM32L1 Series	V3.1.0
STM32L4 Series	V3.1.0
STM32L4+ Series	V3.1.0
STM32L5 Series	V3.1.5
STM32WB Series	V3.1.3
STM32WL Series	V3.1.5 (patch for version V3.1.4)

1. *Except for STM32H7A3xx and STM32H7B3xx microcontrollers.*

2.3 What is STM32Cube?

STM32Cube is an STMicroelectronics original initiative to significantly improve designer's productivity by reducing development effort, time, and cost. STM32Cube covers the whole STM32 portfolio.

STM32Cube includes:

- A set of user-friendly software development tools to cover project development from conception to realization, among which are:
  - STM32CubeMX, a graphical software configuration tool that allows the automatic generation of C initialization code using graphical wizards
  - STM32CubeIDE, an all-in-one development tool with peripheral configuration, code generation, code compilation, and debug features
  - STM32CubeProgrammer (STM32CubeProg), a programming tool available in graphical and command-line versions
  - STM32CubeMonitor (STM32CubeMonitor, STM32CubeMonPwr, STM32CubeMonRF, STM32CubeMonUCPD) powerful monitoring tools to fine-tune the behavior and performance of STM32 applications in real-time
- STM32Cube MCU and MPU Packages, comprehensive embedded-software platforms specific to each microcontroller and microprocessor series (such as STM32CubeL4 for the STM32L4 Series), which include:
  - STM32Cube hardware abstraction layer (HAL), ensuring maximized portability across the STM32 portfolio
  - STM32Cube low-layer APIs, ensuring the best performance and footprints with a high degree of user control over hardware
  - A consistent set of middleware components such as FAT file system, RTOS, USB Host and Device, TCP/IP, Touch library, and Graphics
  - All embedded software utilities with full sets of peripheral and applicative examples
- STM32Cube Expansion Packages, which contain embedded software components that complement the functionalities of the STM32Cube MCU and MPU Packages with:
  - Middleware extensions and applicative layers
  - Examples running on some specific STMicroelectronics development boards

3 License

X-CUBE-CRYPTOLIB is delivered under the *Mix Ultimate Liberty+OSS+3rd-party V1* software license agreement (SLA0048).

The software components provided in this package come with different license schemes as shown in Table 2.

Table 2. Software component license agreements

Software component	Copyright	License
STM32_Cryptographic middleware	STMicroelectronics	Proprietary
Board support package (BSP)	STMicroelectronics	BSD-3-Clause
Cortex®-M CMSIS	Arm Limited	BSD-3-Clause or Apache License 2.0(1)
HAL/LL STM32F0, STM32F1, STM32F2, STM32F3, STM32F4, STM32F7, STM32G0, STM32G4, STM32H7, STM32L0, STM32L1, STM32L4, STM32L4+, STM32L5, STM32WB and STM32WL	STMicroelectronics	BSD-3-Clause
Project examples	STMicroelectronics	BSD-3-Clause

1. *Depends on the CMSIS version.*

Revision history

Table 3. Document revision history

Date	Revision	Changes
1-Sep-2015	1	Initial release.
9-Dec-2015	2	Updated *Features* and *Description* to introduce a new cryptographic firmware version.
15-Dec-2015	3	Updated *Description* and *Section 2: Ordering information*.
7-Jul-2016	4	Updated *Features* and *Description* to introduce the list of certified algorithms.
20-Nov-2020	5	Extended the document scope to the STM32WL Series. Added the *Product information* and *License* sections and the cover picture. Updated *Description*.
12-Jan-2021	6	Updated the document title. Updated in Product information the versions for the STM32F0 Series, STM32G0 Series, STM32L0 Series, STM32L5 Series and STM32WL Series.