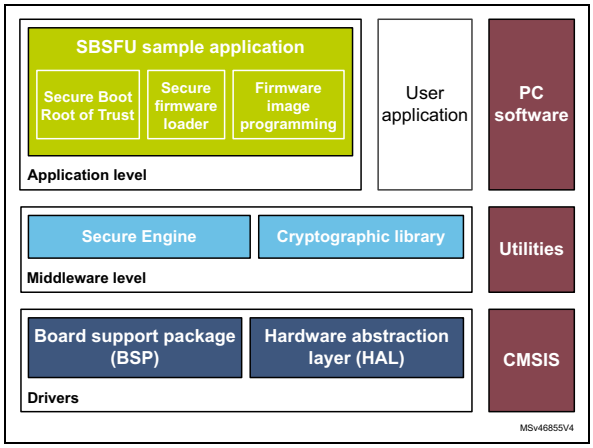
X-CUBE-SBSFU

Secure Boot and Secure Firmware Update software expansion for STM32Cube

Data brief

Features

- Secure Boot / Root of Trust:
  boot path cannot be modified. User application authenticity and integrity is checked before execution.
- Secure firmware loader:
  downloads an encrypted firmware image via UART interface / Ymodem protocol and checks its authenticity and integrity before installing it.
- Dual image support for safe firmware programing:
  - Error detection and rollback capabilities during image installation.
  - Over The Air firmware download possible from user application.
- Single image support for maximized user application size:
  - Error detection without rollback capability during installation.
  - Firmware update only possible via the SBSFU application (local loader function).
- Asymmetric and symmetric cryptographic schemes supported:
  - ECDSA asymmetric cryptography scheme for firmware verification with AES-CBC decryption.
  - ECDSA asymmetric cryptography scheme for firmware verification without decryption.
  - AES-GCM symmetric cryptography scheme for firmware verification and decryption.
- Cryptography with integrated firmware preparation scripts delivered as executable and source code for customization flexibility.



- Secure Engine services:
  protected environment managing all critical data (such as firmware decryption key), and operations (such as cryptography operations).
- STM32 security mechanisms:
  combination demonstrating the state-of-the-art use of STM32 protections.

Description

The X-CUBE-SBSFU Secure Boot and Secure Firmware Update solution allows the update of the STM32 microcontroller built-in program with new firmware versions, adding new features and correcting potential issues. The update process is performed in a secure way to prevent unauthorized updates and access to confidential on-device data.

In addition, Secure Boot (Root of Trust services) checks and activates STM32 security mechanisms, and checks the authenticity and integrity of user application code before every execution to ensure that invalid or malicious code cannot be run.

The Secure Firmware Update application receives the encrypted firmware image, checks its authenticity, decrypts it, and checks the integrity of the code before installing it.

X-CUBE-SBSFU is built on top of STM32Cube software technology, making the portability across different STM32 microcontrollers easy. It is provided as reference code to demonstrate the state-of-the-art usage of STM32 security protection.

The X-CUBE-SBSFU Expansion Package comes with examples running on the STM32L4 Series, STM32F4 Series, STM32F7 Series, and STM32G0 Series.

X-CUBE-SBSFU is classified ECCN 5D002.

Ordering information

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

License

X-CUBE-SBSFU is delivered under the *Mix Ultimate Liberty+OSS+3rd-party V1* license.

The software components provided in this package come with different license schemes as shown in *Table 1*. For more details, refer to the license agreement of each component.

Table 1. Software component license agreements

Software component	Owner	License
Board support package (BSP)	STMicroelectronics	Open source BSD
Cortex®-M CMSIS	Arm®	Open source BSD
HAL STM32 L4/F4/F7/G0	STMicroelectronics	Open source BSD
STM32_Cryptographic	STMicroelectronics	Image V2 (object release only)
STM32_Secure_Engine	STMicroelectronics	Ultimate Liberty (source and object release)
Project applications	STMicroelectronics	Ultimate Liberty (source and object release)
mbedTLS	Arm®	Apache® 2.0

The X-CUBE-SBSFU Expansion Package runs on STM32 32-bit microcontrollers based on the Arm®(a) Cortex®-M processor.

arm

Revision history

Table 2. Document revision history

Date	Revision	Changes
17-Nov-2017	1	Initial release.
13-Apr-2018	2	Added cryptographic schemes and extended to dual or single image support: – Updated *Features*. – Updated *Description*.
28-Jun-2018	3	Updated *Description*.
18-Dec-2018	4	Expanded X-CUBE-SBSFU scope to the STM32F4 Series, STM32F7 Series, and STM32G0 Series; integrated mbedTLS middleware component: – Updated *Description* – Updated *Table 1: Software component license agreements*

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