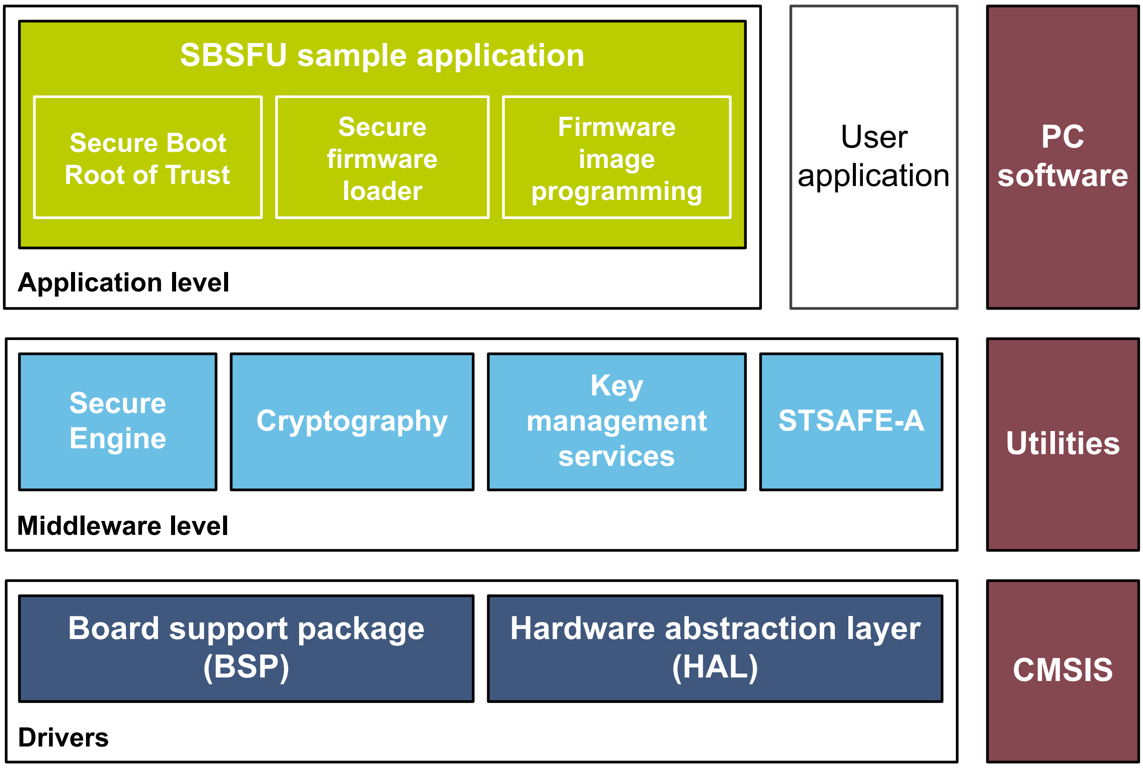
Secure Boot and Secure Firmware Update software expansion for STM32Cube



Product status link
X-CUBE-SBSFU

Features

- Secure Boot to check firmware image before execution
- Secure Firmware Update with anti-rollback and partial image update capabilities for over-the-air or local firmware image update
- Secure key management services offering cryptographic services by means of the PKCS #11 APIs
- Standalone STM32 system solution example demonstrating best use of STM32 protections to protect assets against unauthorized external or internal access
- Combined STM32 and STSAFE-A100 system solution example demonstrating hardware Secure Element protections for secure authentication services and secure data storage

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.

The Secure Boot (Root of Trust services) is an immutable code, always executed after a system reset, that checks STM32 static protections, activates STM32 runtime protections and then verifies the authenticity and integrity of user application code before every execution in order to ensure that invalid or malicious code cannot be run.

The Secure Firmware Update application receives the firmware image via a UART interface with the Ymodem protocol, checks its authenticity, and checks the integrity of the code before installing it. The firmware update is done on the complete firmware image, or only on a portion of the firmware image. Examples are provided for single firmware image configuration in order to maximize firmware image size, and for dual firmware image configurations in order to ensure safe image installation and enable over-the-air firmware update capability commonly used in IoT devices. Examples can be configured to use asymmetric or symmetric cryptographic schemes with or without firmware encryption.

The secure key management services provide cryptographic services to the user application through the PKCS #11 APIs (KEY ID-based APIs) that are executed inside a protected and isolated environment. User application keys are stored in the protected and isolated environment for their secured update: authenticity check, data decryption and data integrity check. This is available on the STM32L4 Series with example provided on the B-L475E-IOT01A board.

STSAFE-A100 is a tamper-resistant secure element (HW Common Criteria EAL5+ certified) used to host X509 certificates and keys, and perform verifications that are used for firmware image authentication during Secure Boot and Secure Firmware Update procedures. This is available on the STM32L4 Series with example provided on the B-L475E-IOT01A board.

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 best use of STM32 security protections.

The X-CUBE-SBSFU Expansion Package comes with examples running on the STM32L4 Series, STM32F4 Series, STM32F7 Series, STM32G0 Series, STM32G4 Series, STM32H7 Series, STM32L0 Series, STM32L1 Series, and STM32WB Series. An example combining STM32 microcontroller and STSAFE-A100 is also provided for the STM32L4 Series.

X-CUBE-SBSFU is classified ECCN 5D002.

1 General information

The X-CUBE-SBSFU Expansion Package runs on STM32 microcontrollers based on Arm$^{®}$ cores.

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

1.1 Ordering information

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

1.2 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 the conception to the realization, among which:
  - 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-Power (STM32CubeMonPwr), a monitoring tool to measure and help in the optimization of the power consumption of the MCU
- STM32Cube MCU & 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 the HW
  - 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 & MPU Packages with:
  - Middleware extensions and applicative layers
  - Examples running on some specific STMicroelectronics development boards

1.3 How does X-CUBE-SBSFU complement STM32Cube?

X-CUBE-SBSFU is based on STM32CubeHAL, the hardware abstraction layer for STM32 microcontrollers. The Expansion Package extends STM32Cube with a set of middleware providing secure services for a Secure Boot, for a Secure Firmware Update application, and for any other application requiring secure cryptographic services. The Expansion Package also includes a sample application useful for the developer to start experimenting with the code.

2 License

X-CUBE-SBSFU 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 1.

Table 1. Software component license agreements

Software component	Owner	License
Board Support Package (BSP)	STMicroelectronics	BSD-3-Clause
Cortex®-M CMSIS	Arm®	BSD-3-Clause or Apache License 2.0[1]
HAL STM32 F4/F7/G0/G4/H7/L0/L1/L4/WB	STMicroelectronics	BSD-3-Clause
STM32_Cryptographic	STMicroelectronics	Ultimate Liberty (object release only)
STM32_Secure_Engine	STMicroelectronics	Ultimate Liberty (source release)
STM32_Key_Management_Services	STMicroelectronics	Ultimate Liberty (source release)
STM32_WPAN	STMicroelectronics	Ultimate Liberty (source release)
Project examples	STMicroelectronics	Ultimate Liberty (source release)
mbedTLS	Arm®	Apache License 2.0
STSAFE-A middleware	STMicroelectronics	STSAFE DRIVER[2]

1. *Depends on the CMSIS version.*
2. *Refer to the “Resources” web page of STSW-STSA100 for the SLA0088 software license agreement.*

Revision history

Table 2. **Document revision history**

Date	Version	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*
22-Jul-2019	5	Added the use of STSAFE-A100 and secure key management services. Updated the entire document: • Updated Features, Description and License • Added What is STM32Cube? and How does X-CUBE-SBSFU complement STM32Cube?

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.