STM32Cube SW expansion

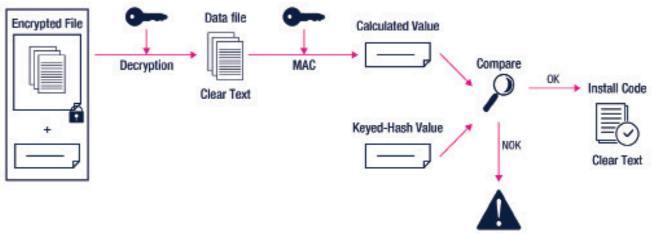
life.augmented

Secure boot & secure firmware update

Efficient solution for secure firmware install and upgrade of embedded applications

The X-CUBE-SBSFU allows to start the root of trust chain thanks to a Secure Boot mechanism verifying the firmware identity loaded into the MCU, and to perform Secure updates once in the field. These 2 functions will prevent unauthorized software and their updates to run no the platform. A Secure Engine module is also presents to execute cryptography and secure key storage.

Secure Firmware Update mechanism



KEY FEATURES & BENEFITS

- Secure Boot module
  - Execution with Root of trust service
  - Application authentication and Integrity check before execution
- Secure Firmware Update module
  - Detect new FW version to install
  - Manage FW updates (check unauthorized updates or unauthorized installation)
- Secure Engine module
  - Code isolated from main Firmware Secure execution
  - Dedicated to executing cryptographic algorithms
  - Manage secure key storage

www.st.com/x-cube-sbsfu

A secure boot and secure firmware update software expansion for STM32Cube

Secure Boot (Root of Trust services) checks and activates STM32 security mechanisms, by verifying 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.

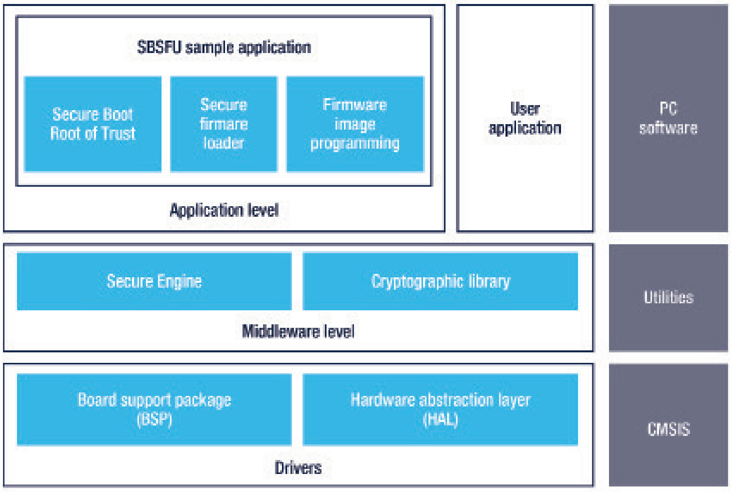
It is provided as reference code to demonstrate the state-of-the-art usage of STM32 security protection.

The X-CUBE-SBSFU Expansion Package comes with examples running on the STM32F4 Series, STM32F7 Series, STM32G0 Series, STM32G4 Series, STM32H7 Series, STM32L0 Series, STM32L1 Series, STM32L4 Series, STM32L5 Series and STM32WB Series.

LEARN MORE

www.st.com

Architecture overview


SBSFU sample application

Secure Boot Root of Trust

Secure firmare loader

Firmware image programming

Application level

User application

PC software

Secure Engine

Cryptographic library

Middleware level

Utilities

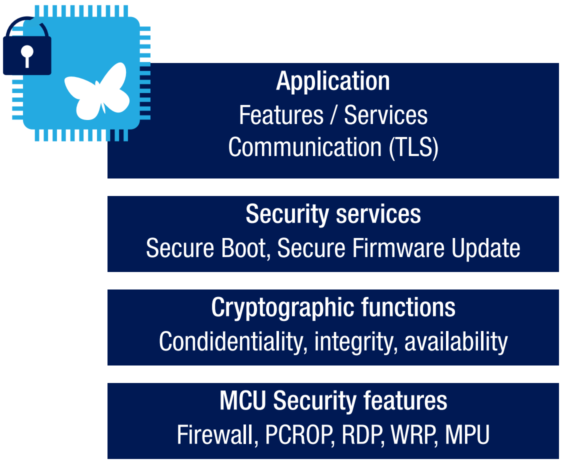
Board support package (BSP)

Hardware abstraction layer (HAL)

Drivers

CMSIS

Security layering


Application
Features / Services
Communication (TLS)

Security services
Secure Boot, Secure Firmware Update

Cryptographic functions
Condidentiality, integrity, availability

MCU Security features
Firewall, PCROP, RDP, WRP, MPU

Roadmap on STM32

X-CUBE-SBSFU Expansion software for STM32Cube	STM32F4	STM32F7	STM32H7 dual/single	STM32L0	STM32L1	STM32L4 STM32L4+	STM32G0	STM32G4	STM32WB
	High-performance MCUs			Ultra-low-power MCUs			Mainstream MCUs		Wireless MCUs
Secure boot	✓	✓	✓	✓	✓	✓	✓	✓	✓ (M4)
Secure FW update	✓	✓	✓	✓	✓	✓	✓	✓	✓ (M4)
Secure engine	✓	✓		✓	✓	✓			
Secure key storage						✓			✓ (Sec-M0)

ST COMMUNITY
community.st.com/stm32

life.augmented

Order code: FLXCUBESBSFU0121

For more information on ST products and solutions, visit www.st.com