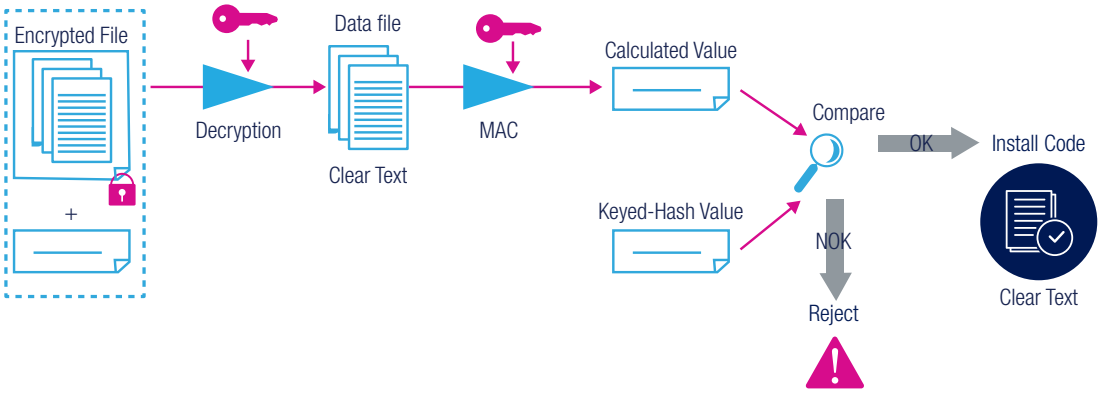
STM32Cube SW expansion
Secure boot & secure firmware

Efficient solution for secure firmware install and upgrade of embedded applications

The X-CUBE-SBSFU Secure Boot and Secure Firmware Update solution allows in the field 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.

KEY FEATURES

- 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 version (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



A SECURE BOOT AND SECURE FIRMWARE UPDATE SOFTWARE EXPANSION FOR STM32CUBE

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.

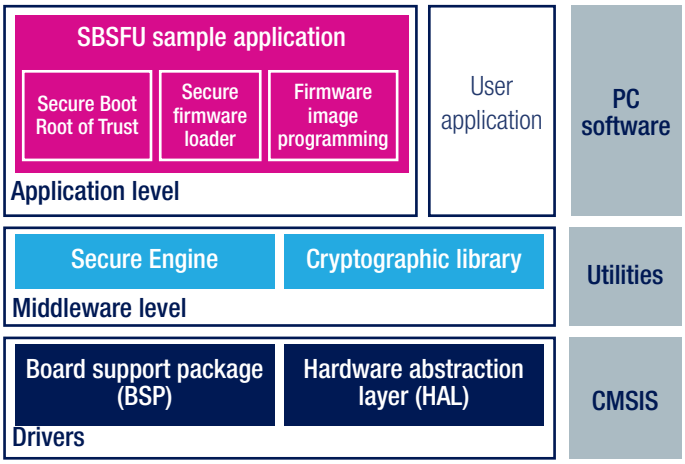
The Secure Firmware Update application receives the encrypted firmware image, checks its authenticity, decrypts it, and checks the integrity of the code before installing it.

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 STM32F4 Series, STM32F7 Series, STM32G0 Series, STM32G4 Series, STM32H7 Series, STM32L0 Series, STM32L1 Series, STM32L4 Series and STM32WB Series.

LEARN MORE

ARCHITECTURE OVERVIEW



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

Ask, learn, share, discuss, become famous and engage with the community of STM32 enthusiasts on community.st.com/stm32

life.augmented