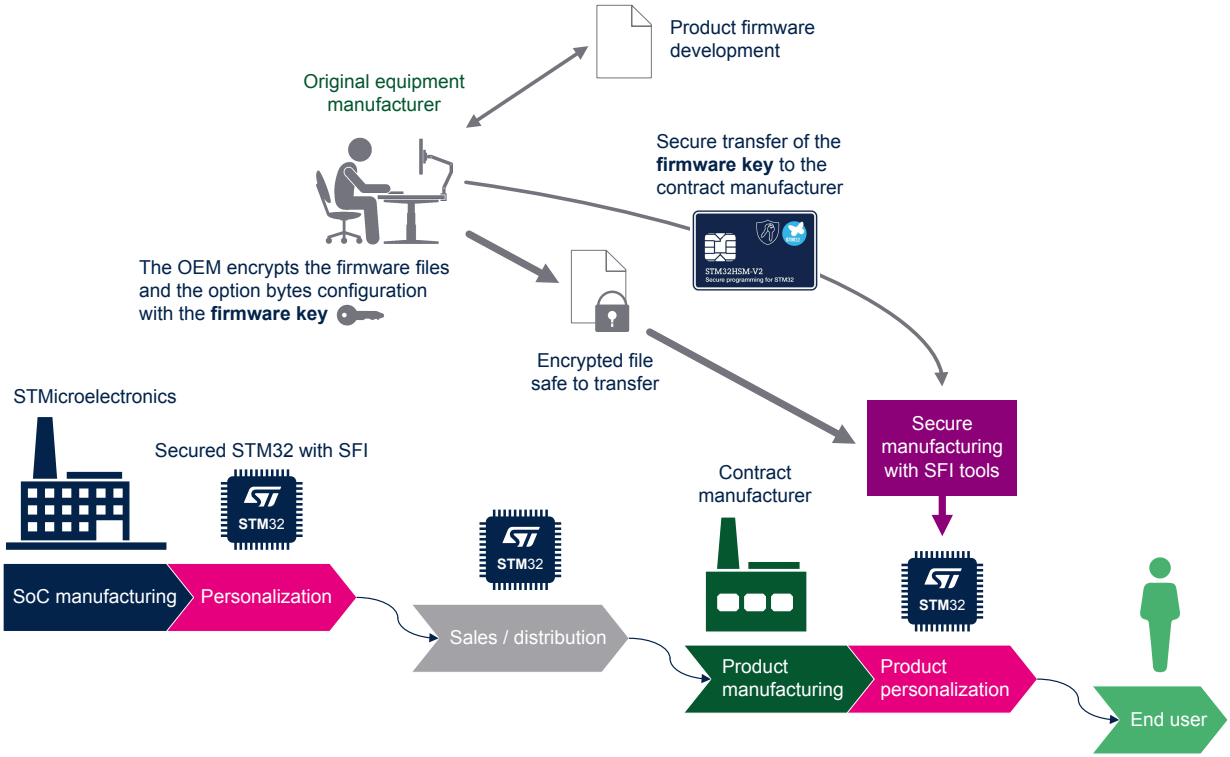
Secure firmware install (SFI) software expansion for STM32Cube



Product status link
X-CUBE-SFI

Features

- SFI: secure firmware install in the internal flash memory
  - Encrypted OEM firmware and option bytes secure installation in the internal flash memory
  - Counted installation of the OEM firmware with the HSM (hardware security module)
- SFIx: secure firmware install in the external flash memory.
  Supports the same features as SFI with additionally:
  - Random key generation in the internal flash memory (can be used for external flash memory encryption)
  - Encrypted OEM firmware secure installation in the external flash memory
- SMI: secure module install
  - Encrypted OEM module firmware secure installation in the internal flash memory
  - Counted installation of OEM module firmware with the HSM

Description

The X-CUBE-SFI STM32Cube Expansion Package shows how to go through the secure firmware install (SFI) process for STM32 microcontrollers. It illustrates how to protect an original equipment manufacturer (OEM) firmware during the product manufacturing stage at the contract manufacturer (CM).

The product manufacturing outsourcing enables the OEMs to reduce their direct costs and concentrate on high added-value activities such as research and development, sales, and marketing. However, contract manufacturing puts an OEM's proprietary assets at risk: The CM manipulates the OEM's intellectual property (IP), which can be disclosed to other customers, or appropriated.

STMicroelectronics proposes the SFI security concept to meet the new market security requests and protect its customers against any leakage of their IPs. The SFI enables the programming of an OEM firmware into the STM32 flash memory. The programming is done in a secure way with confidentiality, authentication, and integrity checks. The OEMs must check the availability of the SFI with their CMs.

Several STM32 microcontrollers support protection mechanisms against unexpected access for critical operations (such as cryptography algorithms) and critical data (such as secret keys). The SFI solution provides a protection when these microcontrollers are being programmed for the first time. For more details, visit the *SFI overview* page of the STM32 MCU wiki at wiki.st.com/stm32mcu. For the list of the supported STM32 microcontrollers, refer to the application note *STM32 MCUs secure firmware install (SFI) overview* (AN4992).

The SFI offers a complete toolset: the STM32 Trusted Package Creator to encrypt OEM binaries, the STM32CubeProgrammer (STM32CubeProg) to program the STM32 securely, and the STM32HSM-V2 hardware security module to transfer the OEM credentials to the programming partner.

1 General information

X-CUBE-SFI runs on STM32 microcontrollers based on the Arm® Cortex®-M processor.

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

1.1 What is STM32Cube?

STM32Cube is an STMicroelectronics original initiative to improve designer productivity significantly 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 STM32CubeU5 for the STM32U5 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 ThreadX, FileX / LevelX, NetX Duo, USBX, USB-PD, touch library, network library, mbed-crypto, TFM, and OpenBL
  - 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

2 License

X-CUBE-SFI is delivered under the SLA0048 software license agreement and its Additional License Terms.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
4-May-2022	1	Initial release.