AN4023
Application note

STM32 secure firmware upgrade (SFU) overview

Introduction

One of the advantages of using a microcontroller is its flexibility and its ability to reprogram the built-in Flash memory, which provides the ability to upgrade the microcontroller remotely with new firmware versions, adding new features and correcting potential issues.

This upgrade process must be performed in a secure way in order to prevent malicious users from copying the firmware for other manufacturers. Secure download and upgrade solutions assume that the firmware binary is sent to a device in an encrypted form, and that the device can receive the encrypted binary, decrypt it, and check the version number and code authenticity/integrity before saving it in the Flash memory.

Three main actors are involved in the secure firmware upgrade solution:

1. STMicroelectronics: the STM32 device manufacturer, responsible for programming the secure firmware upgrade solution provided as binary by the OEM.
2. OEM: Original equipment manufacturer: STMicroelectronics direct customer and the final product (based on STM32 devices) owner.
3. OEM-CM: OEM subcontractor: responsible for device personalization and firmware download. Its environment is considered as non-secure.

This solution is based on two main phases:

1. Device personalization: The STM32 device (where the firmware will be loaded) receives the necessary data from a hardware security module (HSM) and generates an encryption key which it saves in its internal Flash memory.

   This phase can be bypassed, removing the need for investment in an HSM. In this case, the chip must be initially personalized with an OEM key instead of an OEM master key to make it ready for secure firmware download/upgrade.
2. Device firmware secure download and upgrade: The STM32 device receives the encrypted firmware from a host station (personal computer or similar). It decrypts the received firmware, checks the version and firmware authenticity and then performs a firmware upgrade.

For more details about the complete solution, please contact your local ST sales representative.

Revision history

Table 1. Document revision history

Date	Revision	Changes
06-Mar-2012	1	Initial release.