STM32HSM-V2

Data brief

Hardware security module for secure firmware installation

Product status link
STM32HSM-V2

Product version	Maximum counter version
STM32HSM-V2XL	1 000 000
STM32HSM-V2HL	100 000
STM32HSM-V2ML	10 000
STM32HSM-V2BE	300
STM32HSM-V2AE	25

Features

- Genuine firmware identification (firmware identifier)
- Identification of STM32 products with secure firmware install (SFI) functionality
- Management of STMicroelectronics (ST) public keys associated with STM32 products
- License generation using a customer-defined firmware encryption key
- Secure counter allowing the generation of a predefined number of licenses
- Direct support of the STM32CubeProgrammer software tool (STM32CubeProg) including the STM32 Trusted Package Creator tool

Description

The STM32HSM-V2 hardware security module (HSM) is used to secure the programming of STM32 products, and to avoid product counterfeiting at contract manufacturers' premises.

The secure firmware install (SFI) feature allows secure downloading of customer firmware to STM32 products that embed a secure bootloader. For further information on this feature, refer to the AN4992 application note available from st.com.

Original equipment manufacturers (OEM) working on a specific STM32 product receive the relevant ST public key to be stored to one or more STM32HSM-V2 HSMs using the STM32CubeProgrammer and STM32 Trusted Package Creator software tools.

Using the same toolchain, after defining the firmware encryption key and encrypting its firmware, the OEM also stores the encryption key to one or more STM32HSM-V2 HSMs, and sets the number of authorized SFI operations for each HSM. Contract manufacturers must then use these STM32HSM-V2 HSMs to load encrypted firmware to the STM32 devices: each STM32HSM-V2 HSM only allows the OEM-defined number of SFI operations before irreversible deactivation.

Revision history

Table 1. Document revision history

Date	Revision	Changes
07-Jul-2020	1	Initial release.
30-Mar-2021	2	Added reference to AN4992 to Description.
25-Oct-2021	3	Added product version and corresponding maximum counter version to the product status link table on the cover page.