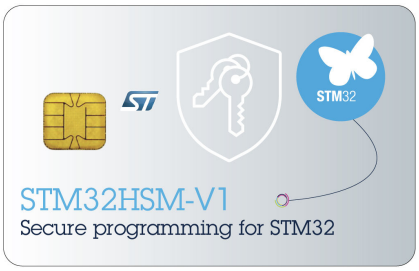
STM32HSM-V1

Data brief

Hardware security module for secure programming



Features

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

Description

The STM32HSM-V1 hardware security module (HSM) is used to secure the programming of STM32 products, and to avoid product counterfeiting at contract manufacturers' premises.

The SFI feature allows secure loading of customer firmware to STM32 products embedding a secure bootloader. For further information on this feature, refer to the AN4992 application note available from st.com.

After defining the firmware encryption key and encrypting their firmware, the original equipment manufacturer (OEM) stores the encryption key to one or more STM32HSM-V1 HSMs and sets the number of authorized SFI operations (counter value) using the STM32CubeProgrammer and STM32 Trusted Package Creator software tools. Contract manufacturers must utilize the STM32HSM-V1 HSMs to load encrypted firmware to STM32 devices: each HSM only allows the OEM-defined number of programming operations before being irreversibly deactivated.

Product status link
STM32HSM-V1

Product summary	
Product version	**Maximum counter value**
STM32HSM-V1XL	1 000 000
STM32HSM-V1ML	10 000
STM32HSM-V1BE	300
STM32HSM-V1AE	25

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
06-May-2019	1	Initial release.
10-Oct-2019	2	Updated Product summary.
30-Mar-2021	3	Added reference to AN4992 to Description.

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Programmers - Processor Based ***category:***

Click to view products by STMicroelectronics ***manufacturer:***

Other Similar products are found below :

5.05.10 TPG100004 X2S-FP-X APM32PROG ECC111429EU UMFTPD2A MIKROPROG FOR 8051 JTAG HS2 PROGRAMMING CABLE JTAG-SMT2-NC SM PROGRAMMING MODULE MIKROPROG FOR AVR MIKROPROG FOR PIC,DSPIC AND PIC32 MIKROPROG FOR STM32 MIKROPROG FOR TIVA ZL20PRG AVR-ISP500-TINY GP-ARM DFR0116 PGM-08702 ACNPROG PGM-07834 XUP USB-JTAG PROGRAMMING CABLE REVELPROG-IS FLASHPRO-2000-STD GANGPRO-ARM-1V CODEGRIP FOR ARM CODEGRIP FOR STM32 CODEGRIP FOR TIVA FLASHPRO-430-CC FLASHPRO-430-LJ FLASHPRO-430-STD FLASHPRO-ARM(X2S) FLASHPRO-ARM-1V(XS) GANGPRO-430(XS) GANGPRO-ARM-1V(XS) AVR-ISP500-ISO AVR-JTAG-USB-A 462 MIKROPROG FOR MSP432 JTAG USB CABLE PROGRAMMER FOR CMT 2548 46 VA800A-PROG CY8CKIT-005 FlashPro-CC-STD FLASHPRO-X REP430F USB-MSP430-FPA-LJ J-32 DEBUG PROBE JTAG-SMT3-NC PROGRAMMING MODULE