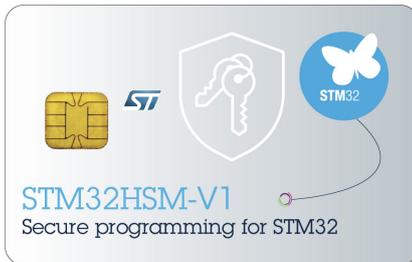


## Hardware security module for secure programming



### 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](http://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	
<a href="#">STM32HSM-V1</a>	
Product summary	
Product version	Maximum counter value
<b>STM32HSM-V1XL</b>	1 000 000
<b>STM32HSM-V1ML</b>	10 000
<b>STM32HSM-V1BE</b>	300
<b>STM32HSM-V1AE</b>	25

## Revision history

**Table 1. Document revision history**

Date	Revision	Changes
06-May-2019	1	Initial release.
10-Oct-2019	2	Updated <a href="#">Product summary</a> .
30-Mar-2021	3	Added reference to AN4992 to <a href="#">Description</a> .

**IMPORTANT NOTICE – PLEASE READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to [www.st.com/trademarks](http://www.st.com/trademarks). All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2021 STMicroelectronics – All rights reserved

## X-ON Electronics

Largest Supplier of Electrical and Electronic Components

*Click to view similar products for* [Programmiers - 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](#)