chanhvinh.com

life.augmented

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.

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

chanhvinh.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
06-May-2019	1	Initial release.
10-Oct-2019	2	Updated Product summary.

chanhvinh.com

chanhvinh.com

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. 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.

© 2019 STMicroelectronics – All rights reserved