

## Hardware security module for secure firmware installation



### 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.

Product status link

[STM32HSM-V2](#)

## 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 <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