AN4023
Application note

STM32 secure firmware upgrade (SFU) overview

Introduction

One of the advantages of using a microcontroller is its flexibility and its ability to reprogram the built-in Flash memory, which provides the ability to upgrade the microcontroller remotely with new firmware versions, adding new features and correcting potential issues.

This upgrade process must be performed in a secure way in order to prevent malicious users from copying the firmware for other manufacturers. Secure download and upgrade solutions assume that the firmware binary is sent to a device in an encrypted form, and that the device can receive the encrypted binary, decrypt it, and check the version number and code authenticity/integrity before saving it in the Flash memory.

Three main actors are involved in the STM32 SFU solution (STSW-STM32099):

1. STMicroelectronics: the STM32 device manufacturer, responsible for programming the secure firmware upgrade solution, through standard programming services, provided as binary by the OEM.
2. OEM: Original equipment manufacturer: STMicroelectronics direct customer and the final product (based on STM32 devices) owner.
3. OEM-CM: OEM subcontractor: responsible for device personalization and firmware download. Its environment is considered as non-secure.

This solution is based on two main phases:

1. Device personalization: The STM32 device (where the firmware will be loaded) receives the necessary data from a hardware security module (HSM) and generates an encryption key which it saves in its internal Flash memory.

   This phase can be bypassed, removing the need for investment in an HSM. In this case, the chip must be initially personalized with an OEM key instead of an OEM master key to make it ready for secure firmware download/upgrade.
2. Device firmware secure download and upgrade: The STM32 device receives the encrypted firmware from a host station (personal computer or similar). It decrypts the received firmware, checks the version and firmware authenticity and then performs a firmware upgrade.

For more details about the complete solution, please contact your local ST sales representative.

Revision history

Table 1. Document revision history

Date	Revision	Changes
06-Mar-2012	1	Initial release.
18-Oct-2013	2	Added text ‘through standard programming services’ to STMicroelectronics definition and STSW-STM32099.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER’S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR “AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL” INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.
Information in this document supersedes and replaces all information previously supplied.
The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2013 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan -
Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com