
STM32 Trusted Package Creator tool software description

Introduction

STM32 Trusted Package Creator is part of the STM32CubeProgrammer tool set (STM32CubeProg), and allows the generation of secure firmware and modules to be used for STM32 secure programming solutions which are:

- Secure firmware install (SFI): SFI is a secure mechanism that allows secure installation of OEM firmware in untrusted production environments by having the whole firmware encrypted with an AES-GCM key.
- Secure module install (SMI): SMI is intended to protect a part of the firmware (a section of an ELF file) by also encrypting this section using an AES-GCM key.
A combined SFI-SMI image is an SFI image that contains one or more module areas.
- Secure firmware upgrade (SFU): SFU is a solution to allow the upgrade of the STM32 microcontroller built-in program in a secure way. For more information about SFU, please refer to the X-CUBE-SBSFU package on <http://www.st.com> for further information.

This user manual details the software environment prerequisites, as well as the available features of the STM32 Trusted Package Creator tool software.

Contents

1	System requirements	6
2	Preparation processes	7
2.1	SFI preparation process	7
2.2	SMI preparation process	9
2.3	SFU preparation process	11
2.4	HSM preparation process	13
2.4.1	Why we need an HSM	13
2.4.2	HSM programming	14
2.4.3	Reading HSM information	16
3	STM32 Trusted Package Creator tool commands	17
3.1	Command line interface (CLI)	17
3.2	HSM provisioning command	19
3.3	SFI generation command	21
3.4	SMI generation command	23
3.5	SFU generation command	24
3.6	STM32WB firmware signing	26
4	STM32 Trusted Package Creator tool graphical user interface (GUI)	27
4.1	SFI generation	29
4.2	SMI generation	32
4.3	SFU generation	34
5	Option bytes file	37
6	Log dialog	38
7	Settings	39

8	SFI/SMI checking	40
9	Reference documents	41
10	Revision history	42

List of tables

Table 1. Document references 41

Table 2. Document revision history 42



List of figures

Figure 1.	SFI preparation process	7
Figure 2.	SFI file structure	8
Figure 3.	SMI preparation process	9
Figure 4.	SMI file structure	10
Figure 5.	SFU preparation process	11
Figure 6.	SFU file structure	12
Figure 7.	HSM programming tab	15
Figure 8.	Reading HSM information	16
Figure 9.	STM32 Trusted Package Creator tool's available commands (part 1)	17
Figure 10.	STM32 Trusted Package Creator tool's available commands (part 2)	18
Figure 11.	Get HSM information in CLI mode	20
Figure 12.	SFI generation with an ELF file	22
Figure 13.	SFI generation with a binary file	22
Figure 14.	Combined SFI-SMI generation	23
Figure 15.	SMI generation	24
Figure 16.	SFU generation	25
Figure 17.	STM32 Trusted Package Creator tool GUI SFI tab	27
Figure 18.	STM32 Trusted Package Creator tool GUI SMI tab	28
Figure 19.	STM32 Trusted Package Creator tool GUI SFU tab	29
Figure 20.	Firmware file addition	30
Figure 21.	Successful SFI generation	31
Figure 22.	ELF file selection	32
Figure 23.	Successful SMI generation	34
Figure 24.	Firmware file selection	35
Figure 25.	Successful SFU generation	36
Figure 26.	Example of an option bytes file	37
Figure 27.	Example of a log dialog	38
Figure 28.	Settings dialog	39
Figure 29.	SFI checking	40

1 System requirements

Supported operating systems and architectures:

- Linux® 64-bit
- Windows® 7/8/10 32-bit and 64-bit
- macOS® (minimum version OS X® Yosemite)

STM32CubeProgrammer and STM32 Trusted Package Creator support STM32 32-bit devices based on Arm®^(a) Cortex®-M processors.

arm

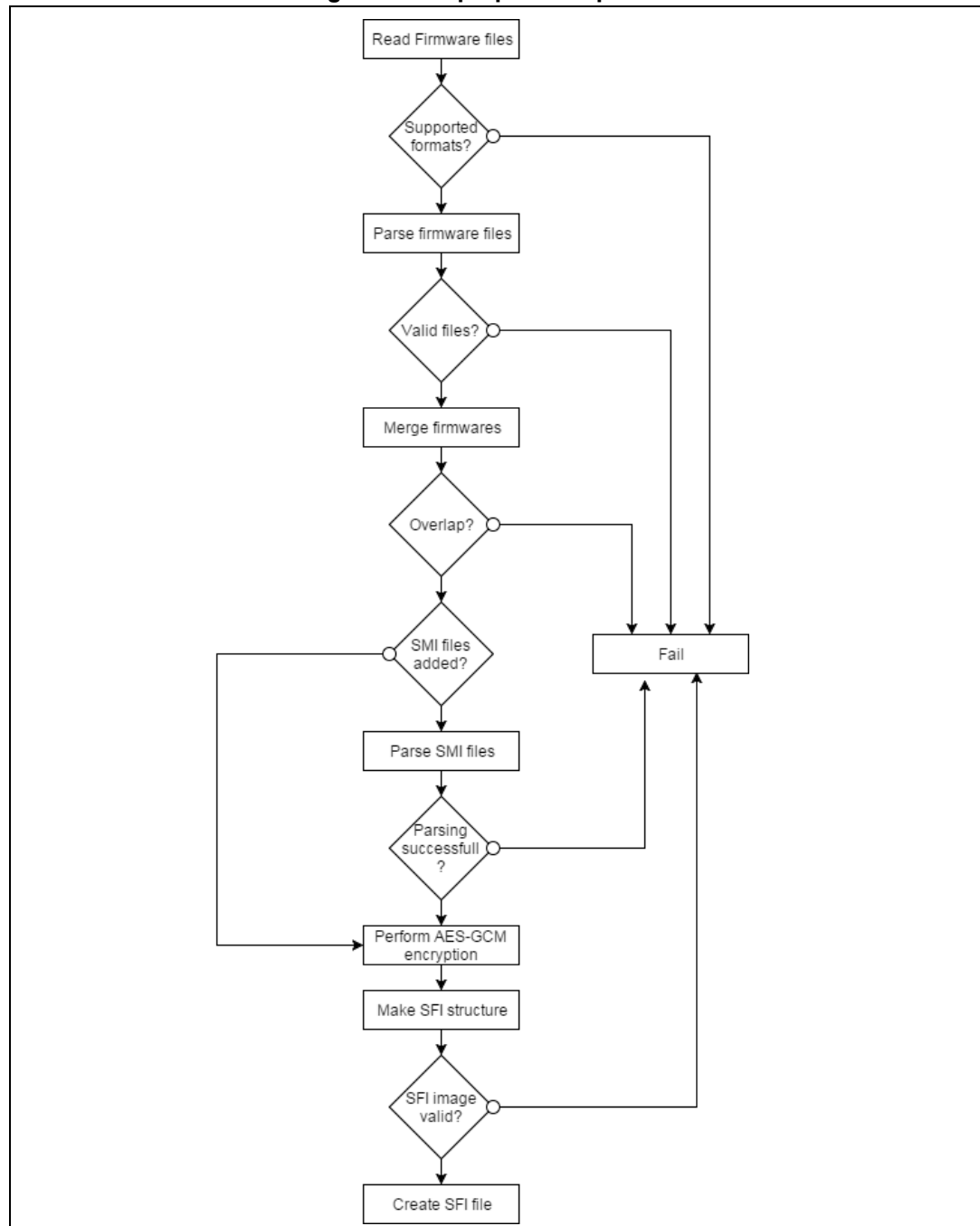
a. Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and or elsewhere.

2 Preparation processes

2.1 SFI preparation process

An SFI (Secure firmware install) image is a format created by STMicroelectronics that contains an encrypted and authenticated piece of firmware using an AES-GCM algorithm. The SFI preparation process is described in [Figure 1](#).

Figure 1. SFI preparation process



Before performing AES-GCM to encrypt an area, the tool calculates the Initialization Vector (IV) as:

$$IV = \text{nonce} + \text{Area Index}$$

Where nonce is a number used only once as a start of an iterated process in the AES-GCM algorithm to give different cipher texts to same blocks of data.

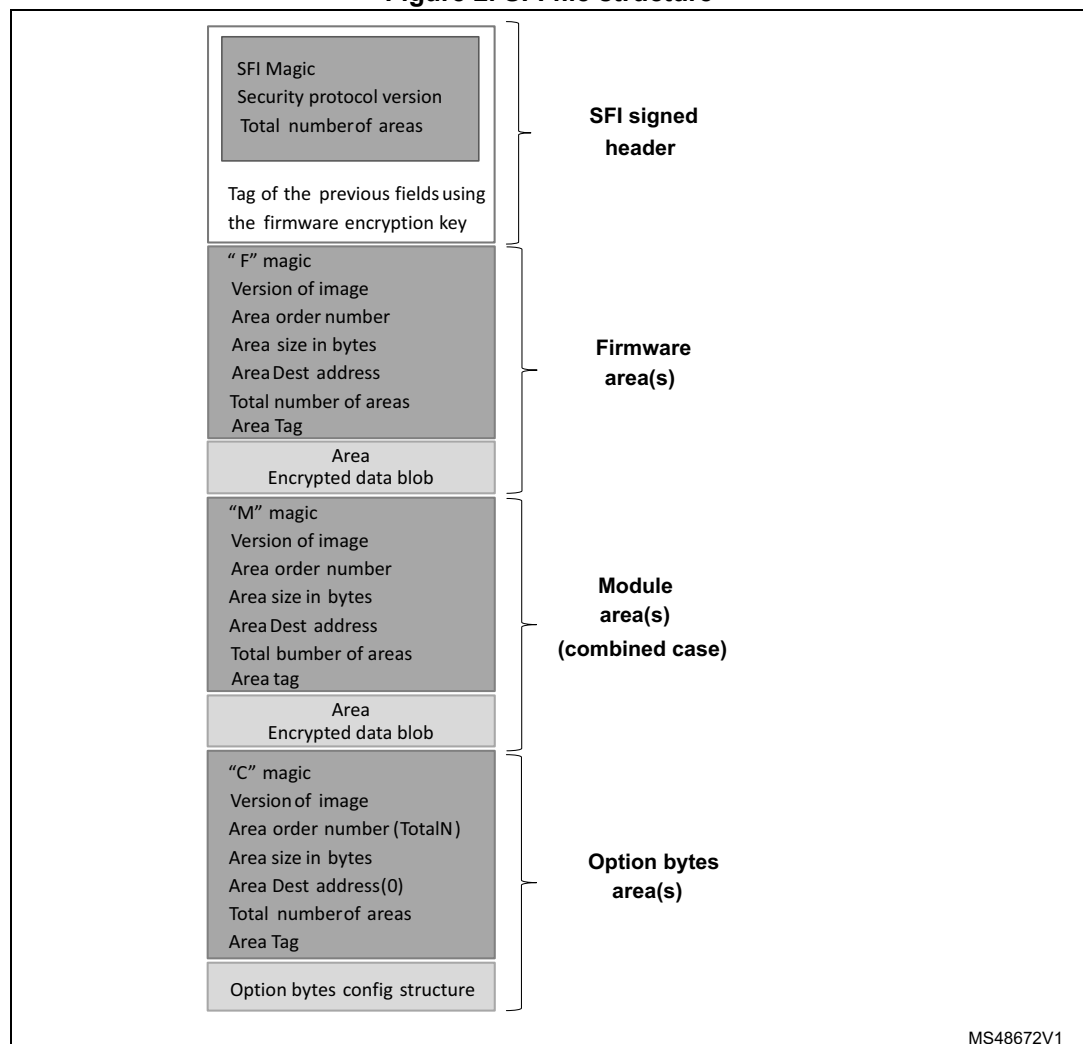
It then, it passes the area descriptor (starting from the magic to the total number of areas) as additional authenticated data (AAD).

- Each segment in the input firmwares constitutes a firmware (F) area in the SFI file.
- Each SMI file (combined case) constitutes a module (M) area.
- The option bytes configuration constitute the configuration (C) area.

To generate a header tag, the tool performs an authenticated only AES-GCM encryption (without a plain text nor a cipher text) using the SFI header as an AAD and the nonce as the IV.

The structure of an SFI file is shown in [Figure 2](#).

Figure 2. SFI file structure



To prepare an SFI image from multiple firmware files you have to make sure that there is no overlap between their segments, otherwise you will get the error message: *“Overlap between segments, unable to merge firmware files”*.

Furthermore, in the case of a combined SFI-SMI image, there is also an overlap check between the areas (in case there is an overlap between firmware and module areas). If the check fails, an error message is shown: *“Overlap between SFI areas”*.

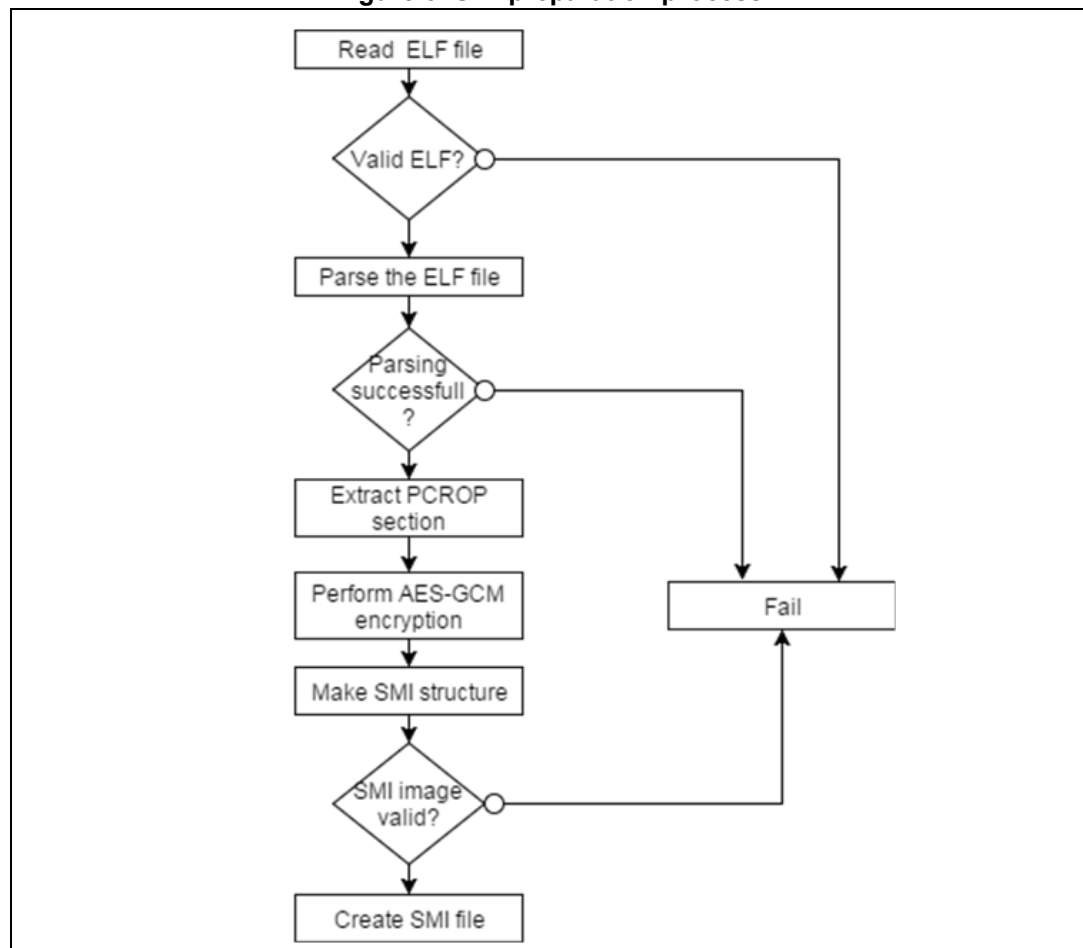
Also, all SFI areas must be located in Flash memory, otherwise the generation fails giving the error message: *“One or more SFI areas are not located in Flash memory”*.

2.2 SMI preparation process

An SMI image (Secure Module Install) protects only a module of the firmware.

The SMI preparation process is shown in [Figure 3](#).

Figure 3. SMI preparation process



The AES-GCM encryption is performed using the following inputs:

- Nonce as the initialization vector (IV)
- The security version as additional authenticated Data (AAD)

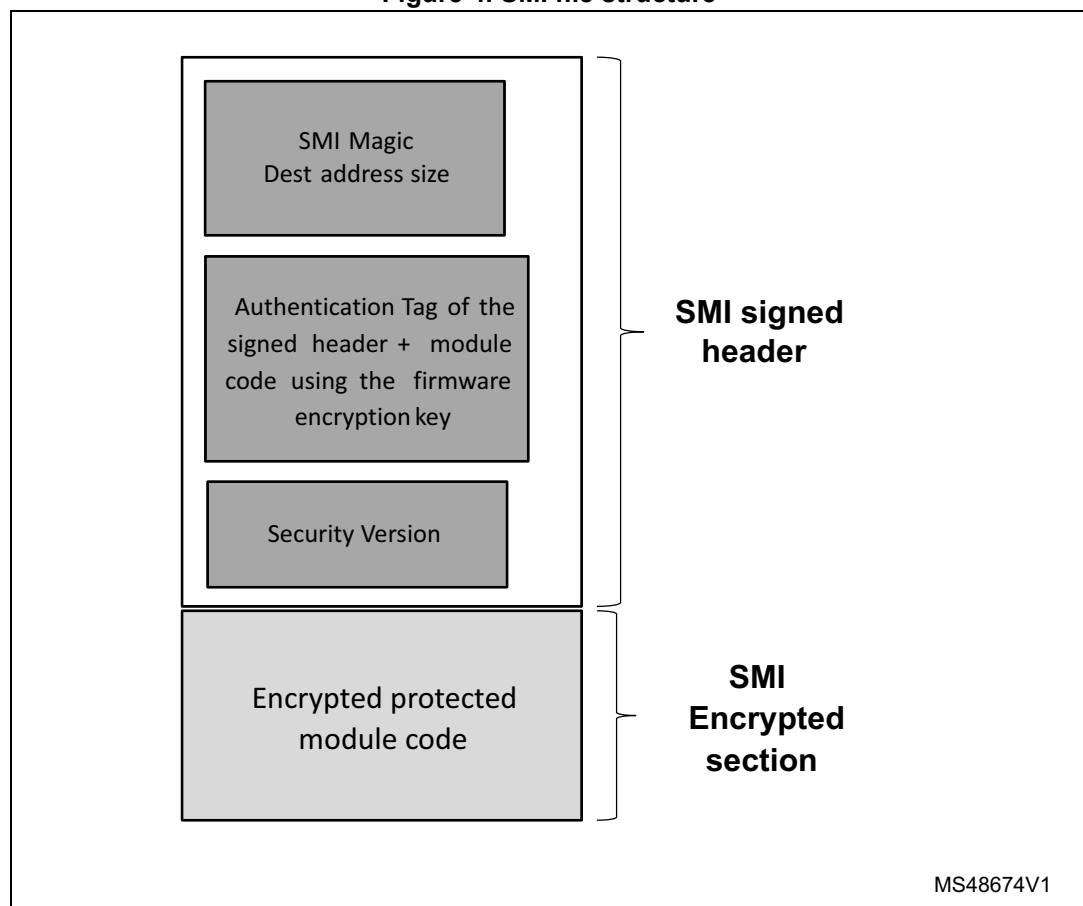
Before SMI preparation, the following checks are performed:

- A proprietary code read out protection (PCROP) section must be aligned on a Flash word (256 bits) otherwise a warning is shown
- The section's size must be at least 2 Flash words (512 bits) otherwise a warning is shown
- The section must end on a Flash word boundary (a 256 bit word) or a warning is shown
- If the section immediately following the PCROP area starts in the last Flash word of the PCROP section, the generation fails and an error message is shown.

After the SMI preparation, a clear (that is, not encrypted) ELF file is also generated containing program data and only clear sections of the code.

The structure of an SMI file is shown in [Figure 4](#).

Figure 4. SMI file structure

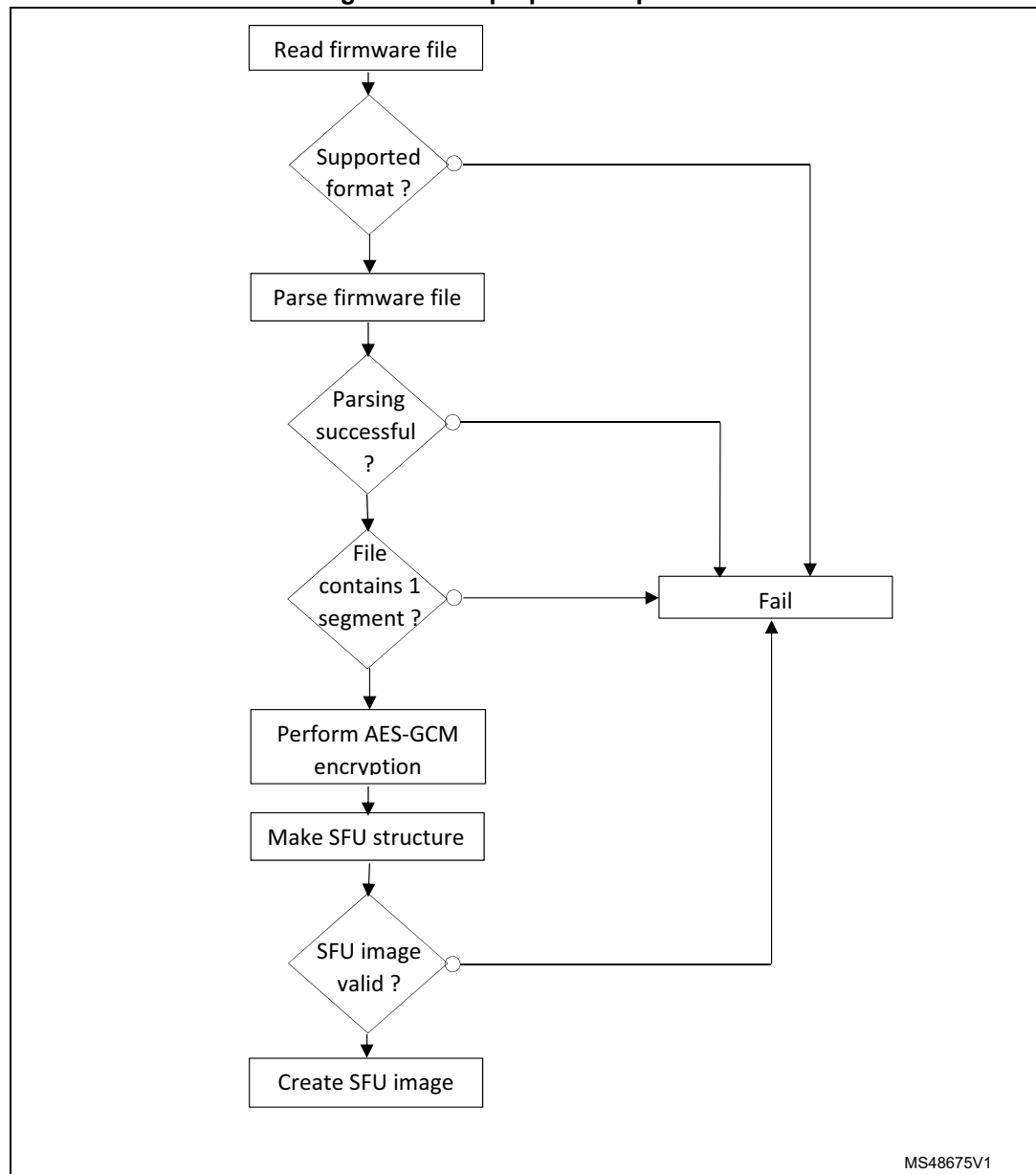


2.3 SFU preparation process

An SFU image (Secure Firmware Upgrade) allows the upgrade of the STM32 microcontroller built-in program in a secure way to prevent unauthorized updates.

The SFU preparation process is shown in [Figure 5](#).

Figure 5. SFU preparation process



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/598116125043006073>