life.augmented

UM2238
用户手册

STM32 Trusted Package Creator工具软件说明

引言

STM32 Trusted Package Creator是STM32CubeProgrammer工具集（STM32CUBEPROG）的一部分，能够生成安全固件和模块，用于STM32安全编程解决方案，它们是：

- 安全固件安装（SFI）：SFI是一种安全机制，通过使用AES-GCM密钥对整个固件进行加密，可以在不受信任的产品环境中安全地安装OEM固件。
- 安全模块安装（SMI）：SMI旨在通过使用AES-GCM密钥加密此部分来保护该部分固件（ELF文件的一部分）。

  SFI-SMI组合映像是包含一个或多个模块区域的SFI映像。
- 安全固件升级（SFU）：SFU是一种允许以安全方式升级STM32微控制器内置程序的解决方案。有关SFU的更多信息，请参阅http://www.st.com上的X-CUBE-SBSFU软件包以获取更多信息。

本用户手册详细介绍了软件环境先决条件以及STM32 Trusted Package Creator工具软件的可用功能。

STM32 CubeProgrammer

目录

表格索引

图片索引

1 系统要求

支持的操作系统和架构为：

- Linux® 32位和64位（已在Ubuntu 14.04上测试）
- Windows® 10-7-8 32位和64位
- macOS®（最小版本OS X® Yosemite）

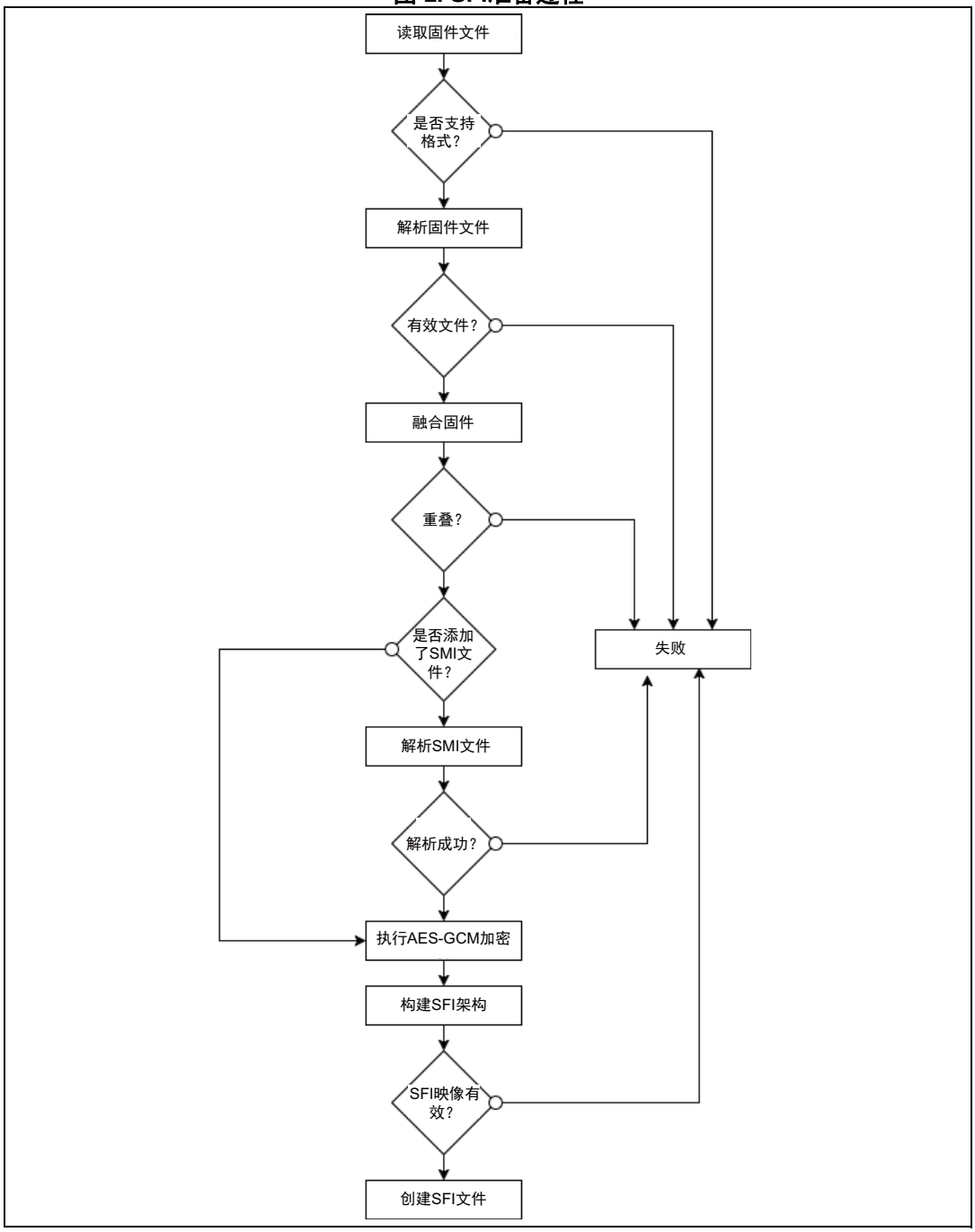
STM32CubeProgrammer和STM32 Trusted Package Creator可支持基于Arm® Cortex®-M处理器的STM32 32位器件。

2 准备过程

2.1 SFI准备过程

SFI（安全固件安装）映像是由意法半导体创建的格式，包含已使用AES-GCM算法加密和验证的固件。*图 1*中描述了SFI准备过程。

图 1. SFI准备过程



在执行AES-GCM加密一个区域之前，该工具将初始化向量（IV）计算为：

IV = nonce + Area Index。

其中nonce是一个数字，在AES-GCM算法中作为迭代过程的起始值只使用一次，以将不同的密文发送给相同的数据块。

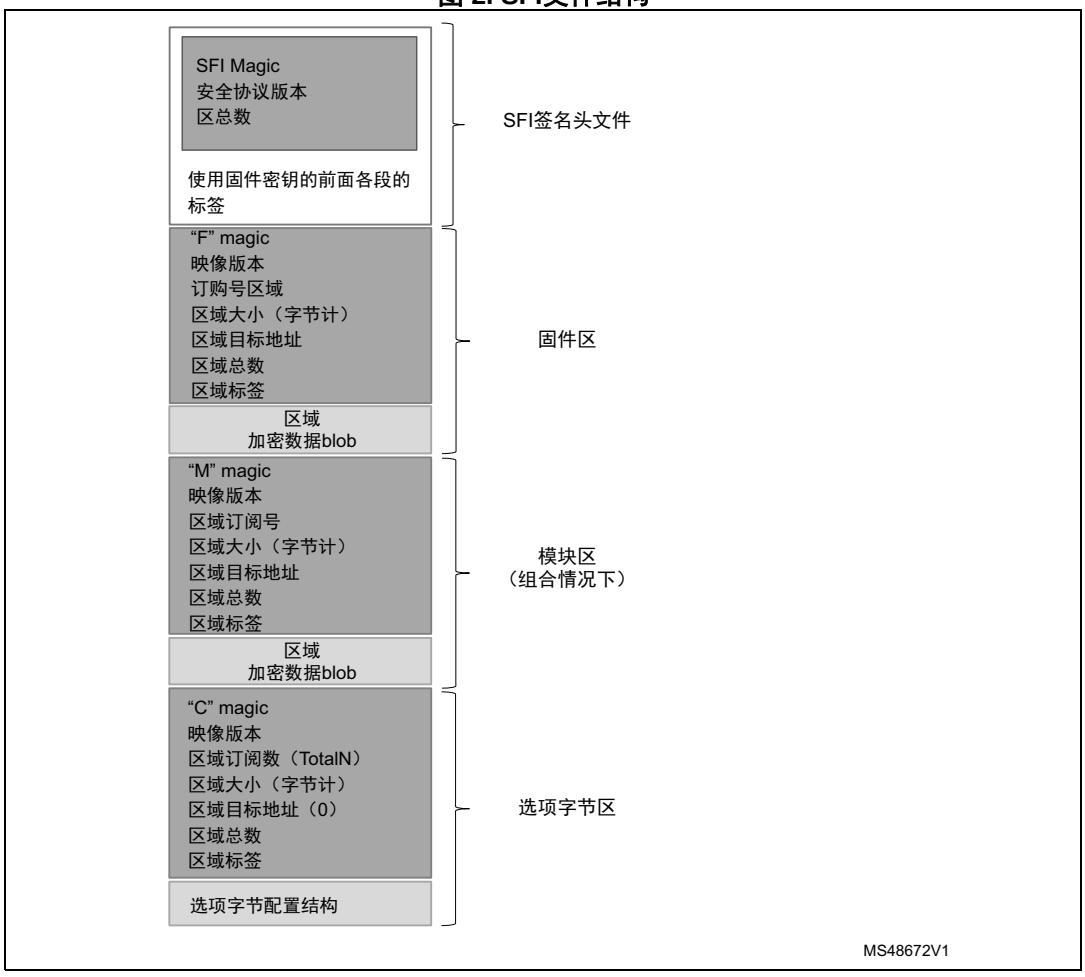
然后，它将区域描述符（从magic开始到区域总数）作为附加认证数据（AAD）来传递。

- 输入固件中的每个段都会构成SFI文件中的一个固件（F）区域。
- 每个SMI文件（组合情况）共同构成一个模块（M）区域。
- 选项字节配置构成配置（C）区域。

为了生成头文件标签，该工具使用SFI头文件作为AAD以及nonce作为IV，执行仅经过验证的AES-GCM加密（不含纯文本或密文）。

*图 2*中描述了SFI文件的结构。

图 2. SFI文件结构



要从多个固件文件准备SFI映像，您必须确保其各段之间没有重叠，否则会收到错误消息：*“段之间重叠，无法合并固件文件”*。

而且，在SFI-SMI组合映像的情况下，还会在各区域之间进行重叠检查（如果固件和模块区域之间存在重叠）。如果检查失败，将显示一条错误消息：*“SFI区域之间重叠”*。

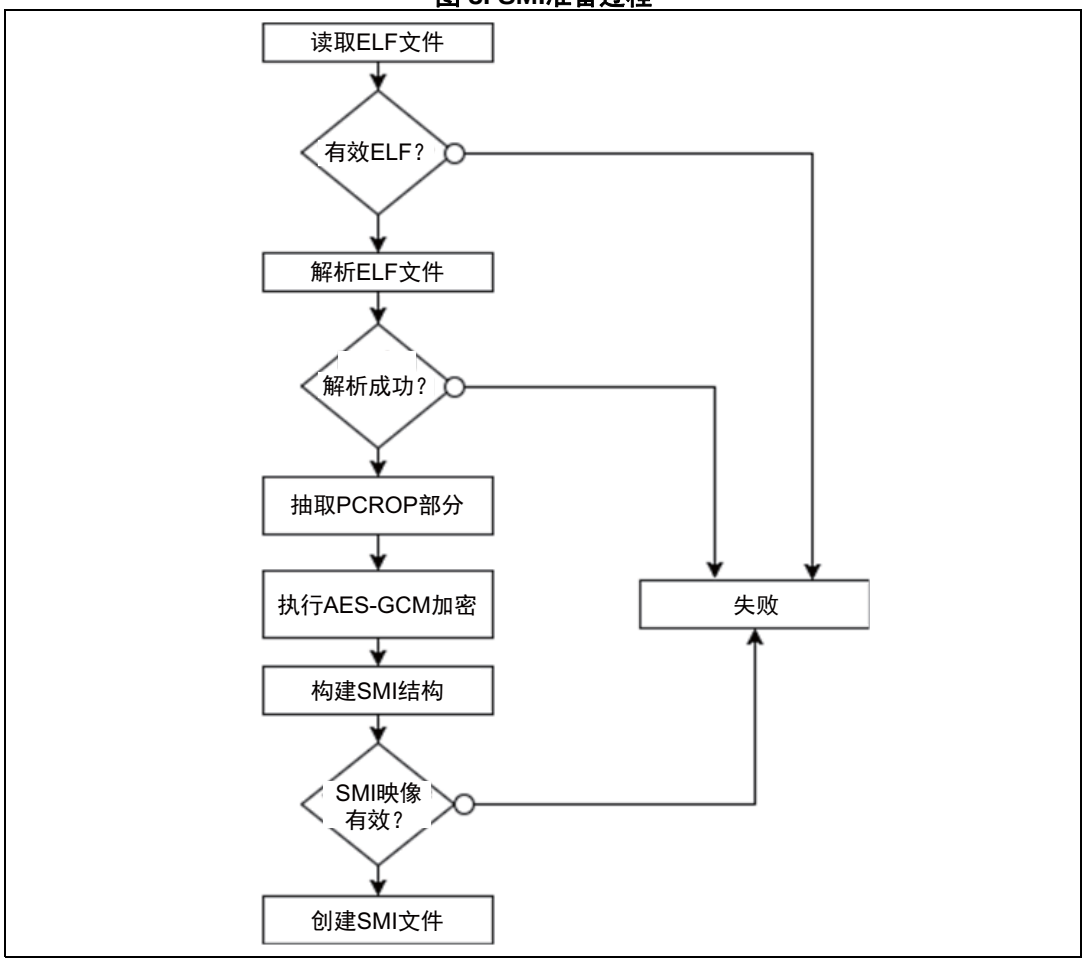
此外，所有SFI区域都必须位于flash中，否则生成将失败，并给出错误消息：*“一个或多个SFI区域不在flash中”*。

2.2 SMI准备过程

一个SMI映像（安全模块安装）仅保护固件内的一个模块。

*图 3*中描述了SMI准备过程。

图 3. SMI准备过程



使用以下输入来执行AES-GCM加密：

- 作为初始化向量（IV）的Nonce
- 作为附加认证数据（AAD）的安全版本

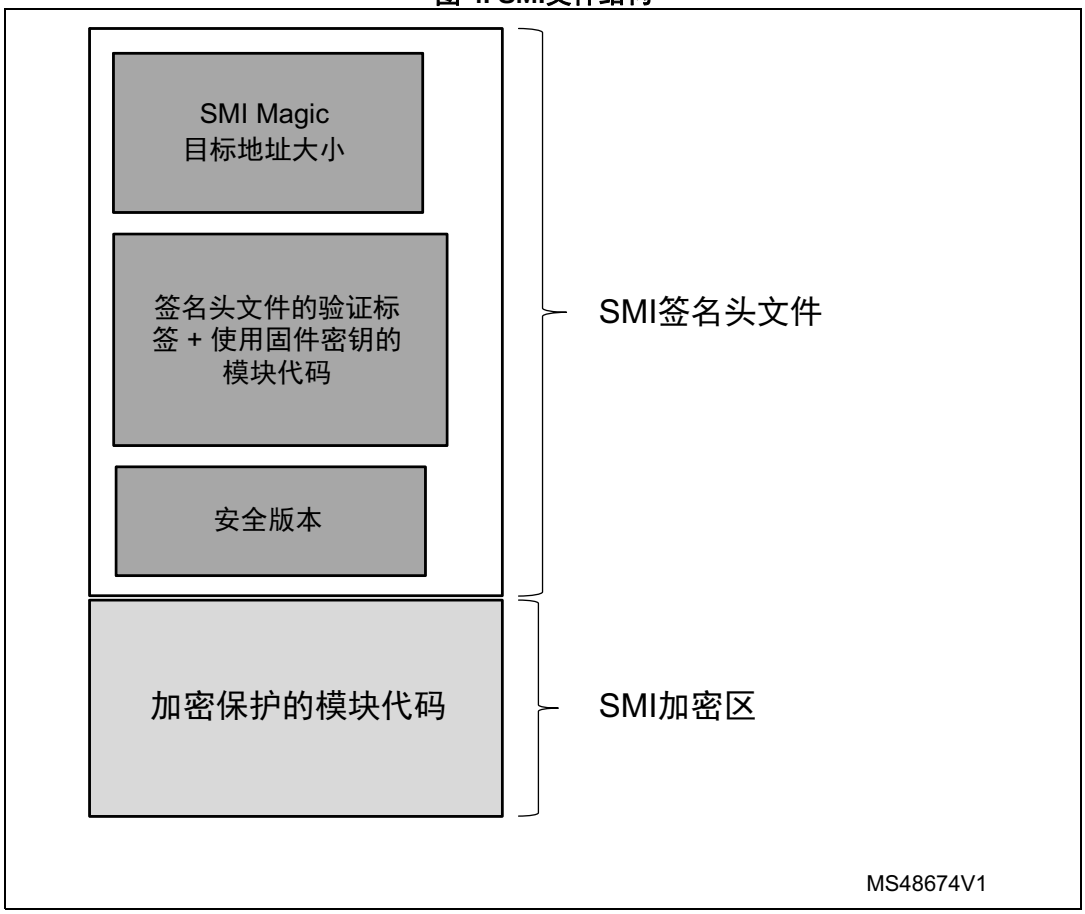
SMI准备之前，执行以下检查：

- 专有代码读出保护（PCROP）区必须与闪存字（256位）对齐，否则会显示警告
- 该区大小必须至少为2个闪存字（512位），否则会显示警告
- 该区必须以Flash字边界（256位的字）结束，否则会显示警告
- 如果该区紧接着PCROP区域并在PCROP区的最后一个Flash字处开始，则生成失败并显示错误消息。

在SMI准备之后，还会生成一个明文（即未加密的）ELF文件，其中包含程序数据并且只包含明文代码段。

*图 4*中显示了SMI文件的结构。

图 4. SMI文件结构

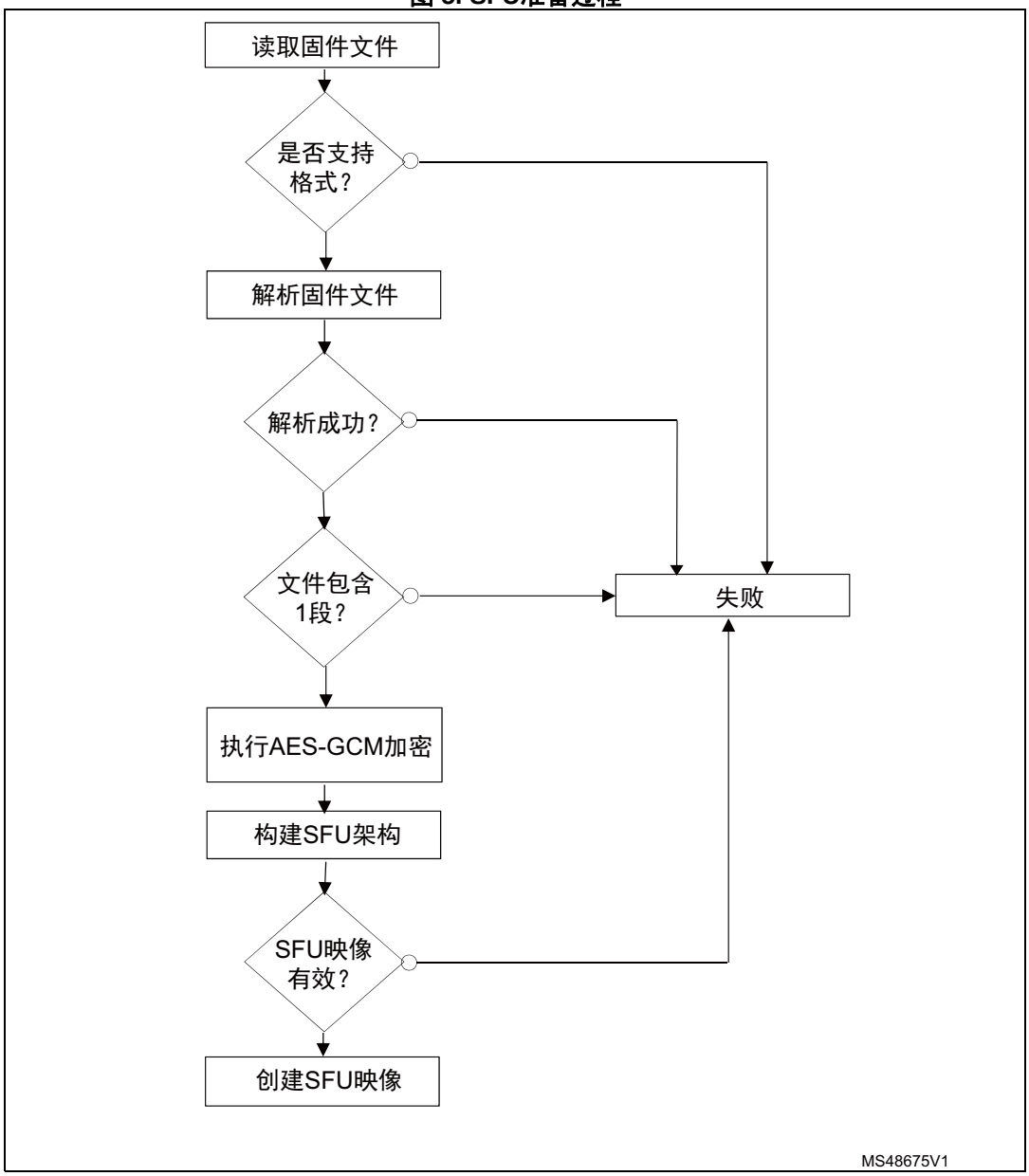


2.3 SFU准备过程

SFU映像（安全固件升级）允许以安全方式升级STM32微控制器内置程序，以防止未经授权的更新。

*图 5*中显示了SFU准备过程。

图 5. SFU准备过程



生成2个文件，SFU映像头文件和SFU加密的固件映像。

要生成头文件，使用以下输入来执行AES-GCM加密：

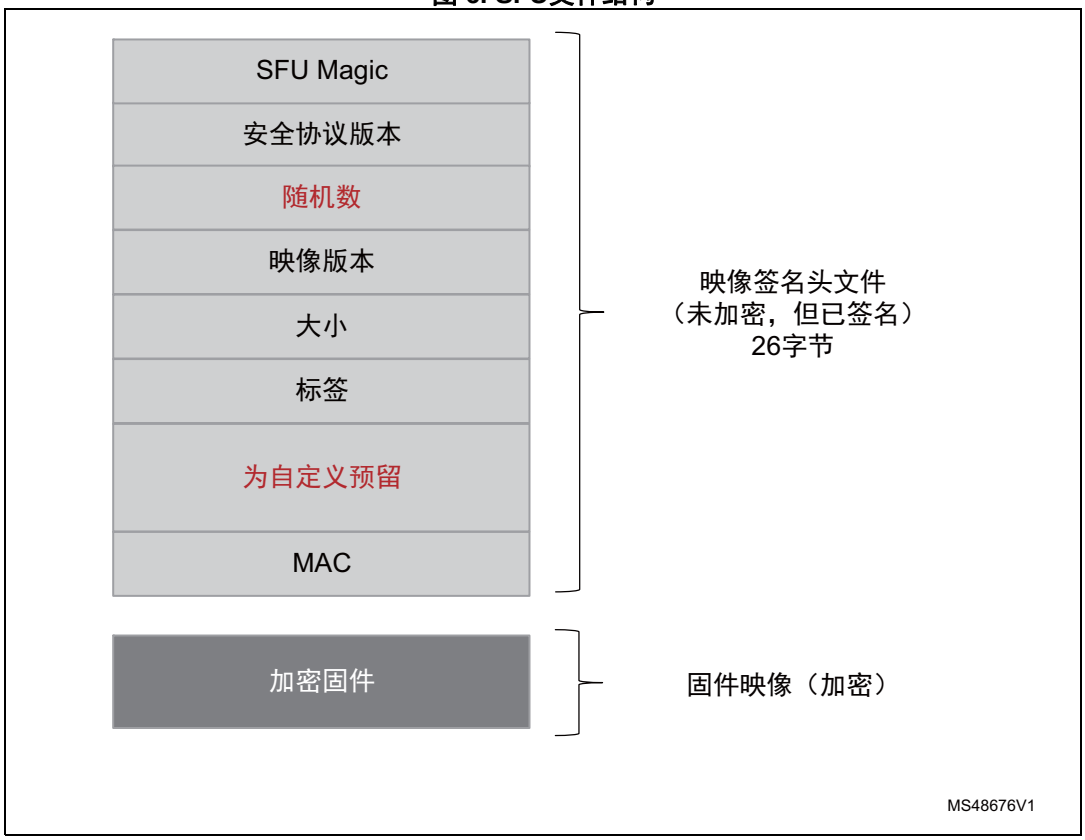
- 作为初始化向量（IV）的Nonce
- 无附加已验证数据 (AAD)

对于加密固件映像生成：

- 作为初始化向量（IV）的Nonce
- 作为附加认证数据（AAD）的头文件内容

*图 6*中显示了SFU文件的结构。

图 6. SFU文件结构



3 STM32 Trusted Package Creator工具命令

3.1 命令行界面（CLI）

以下各节介绍如何由命令行界面来使用STM32 Trusted Package Creator工具。

可用命令如*图 7* 中所示。

图 7. STM32 Trusted Package Creator工具的可用命令

3.2 SFI生成指令

-sfi, --sfi

说明：此指令生成一个SFI映像文件。

为了生成SFI映像，用户必须使用下面列出的选项提供强制输入。

-fir, --firmware

说明：添加一个输入固件文件。支持的格式是Bin、Hex、Srec和ELF。此选项可以多次使用以添加多个固件文件。

语法：-fir <Firmware_file> [<Address>]

<Firmware_file> ：固件文件。

[<Address>] ：地址（仅用于Bin文件）。

-k, --key

说明：设置AES-GCM密钥。

语法： -k <Key_file>

< Key _file> ：16字节的二进制文件。

-n, --nonce

说明：设置AES-GCM随机数。

语法： -n <Nonce_file>

<Nonce _file> ：12字节的二进制文件。

-v, --ver

说明：设置映像版本。

语法： -v <Image_version>

<Image_version> ：任何基数下在0到255之间的值。

-ob, --obfile

说明：提供选项字节文件。

语法： -ob <CSV_file>

<CSV_file>： 有9个值的csv文件。

-m, --module

说明：添加一个输入SMI文件。此选项可以多次使用以添加多个SMI文件。这是可选的（用于SFI-SMI组合）。

语法： -m <SMI_file>

<SMI_file> ：SMI文件。

[<Address>] ：仅适用于可重定位的SMI。

-o, --outfile

说明：设置要创建的SFI文件

语法： -o <out_file>

<out_file>： 要生成的SFI文件，必须有.sfi扩展名。

示例：

利用ELF文件：

STM32TrustedPackageCreator_CLI –sfi -fir ELF_firmware.axf -k test_firmware_key.bin -n nonce.bin -ob FIR_ob.csv -v 23 -o test.sfi

图 8. 使用ELF文件生成SFI

```
C:\STM32TrustedPackageCreator\bin>STM32TrustedPackageCreator_CLI.exe -sfi -fir E
LF_firmware.axf -k test_firmware_key.bin -n nonce.bin -ob FIR_ob.csv -v 23 -o te
st.sfi
SUCCES
```

利用二进制文件：

STM32TrustedPackageCreator_CLI –sfi -fir bin_firmware.bin 0x8000000 -k test_firmware_key.bin -n nonce.bin -ob FIR_ob.csv -v 23 -o test.sfi

图 9. 使用二进制文件生成SFI

```
C:\STM32TrustedPackageCreator\bin>STM32TrustedPackageCreator_CLI.exe -sfi -fir b
in_firmware.bin 0x08000000 -k test_firmware_key.bin -n nonce.bin -ob FIR_ob.csv
-v 23 -o test.sfi
SUCCES
```

SFI-SMI组合：

STM32TrustedPackageCreator_CLI –sfi -fir ELF_firmwrae.axf -fir bin_firmware.bin 0x8000000 -m FIR_pcrop.smi -k test_firmware_key.bin -n nonce.bin -ob FIR_ob.csv -v 23 -o test.sfi

图 10. SFI-SMI组合生成

```
C:\STM32TrustedPackageCreator\bin>STM32TrustedPackageCreator_CLI.exe -sfi -fir b
in_firmware.bin 0x08000000 -m FIR_pcrop.smi -k test_firmware_key.bin -n nonce.bi
n -ob FIR_ob.csv -v 23 -o test.sfi
SUCCES
```

3.3 SMI生成指令

-smi, --smi

说明：此指令生成一个SMI映像文件。

为了生成SMI映像，用户必须使用下面列出的选项提供强制输入。

-elf, --elfile

说明：添加一个输入ELF文件。

语法： -elf <ELF_file>

<ELF_file> ：ELF文件。ELF文件可以有任意扩展名：.elf，axf，.o，so，.out

-s, --sec

说明：设置要加密区的名称。

语法： -s <section_name>

<section_name>： 区名。

-k, --key

说明：设置AES-GCM密钥。

语法： -k <Key_file>

<Key _file> ：16字节的二进制文件。

-n, --nonce

说明：设置AES-GCM随机数。

语法： -n <Nonce_file>

<Nonce _file>： 12字节的二进制文件。

-sv, --sver

说明：设置安全版本文件。

语法： -sv <SV_file>

<SV_file>： 16字节文件。

-o, --outfile

说明：设置要创建的SMI文件

语法： -o <out_file>

<out_file>： 要生成的SFI文件，必须有.smi扩展名。

-c, --clear

说明：设置要创建的明文ELF文件。

语法： -c <ELF_file>

<ELF_file>： 要生成的明文ELF文件。

示例

STM32TrustedPackageCreator_CLI –smi -elf FIR_module.axf -s “ER_PCROP” -k test_firmware_key.bin -n nonce.bin -sv svFile -o test.smi -c clear.smi

图 11. SMI生成

```
C:\STM32TrustedPackageCreator\bin>STM32TrustedPackageCreator_CLI.exe -smi -elf F
IR_module.axf -s "ER_PCROP" -k test_firmware_key.bin -n nonce.bin -sv svFile -o
test.smi -c clear.axf
Warning: The section does not end on a Flash word boundary
SUCCES
```

3.4 SFU生成指令

-sfu, --sfu

说明：此指令生成一个SFU映像文件。

为了生成SFU映像，用户必须使用下面列出的选项提供强制输入。

-fir, --firmware

说明：设置输入固件文件。支持的格式是Bin、Hex、Srec和ELF。该固件文件只能包含一个段。

语法： -fir <Firmware_file> [<Address>]

< Firmware _file>： 固件文件。

[<Address>]： 地址（仅用于Bin文件格式）。

-k, --key

说明：设置AES-GCM密钥。

语法： -k <Key_file>

<Key _file>： 16字节的二进制文件

-n, --nonce

说明：设置AES-GCM随机数。

语法： -n <Nonce_file>

<Nonce _file>： 12字节的二进制文件。

-v, --ver

说明：设置映像版本。

语法： -v <Image_version>

<Image_version>： 任何基数下在0到255之间的值。

-oh, --outheader

说明：设置要创建的SFU头文件。

语法： -oh <out_file>

<out_file>： 要生成的SFU头文件，必须有.sfuh扩展名。

-os, --outsfu

说明：设置要创建的SFU文件。

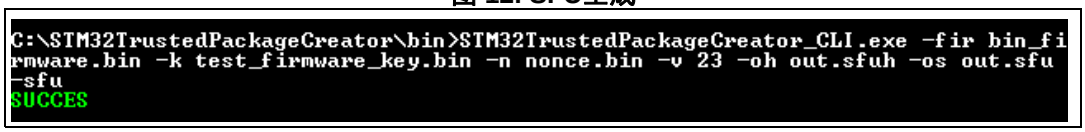
语法： -os <out_file>

<out_file>： 要生成的SFU文件，必须有.sfu扩展名。

示例：

SFMIPreparationTool_CLI –sfu -fir bin_firmware.bin -k test_firmware_key.bin -n nonce.bin -v 23 -oh out.sfuh -os out.sfu

图 12. SFU生成



4 STM32 Trusted Package Creator工具图形用户界面（GUI）

本节介绍如何通过其图形用户界面来使用STM32 Trusted Package Creator工具。

STM32 Trusted Package Creator工具GUI提供三个选项卡：一个用于SFI生成（*图 13*），一个用于SMI生成（*图 14*），另一个用于SFU生成（*图 15*）。

图 13. STM32 Trusted Package Creator工具GUI SFI选项卡

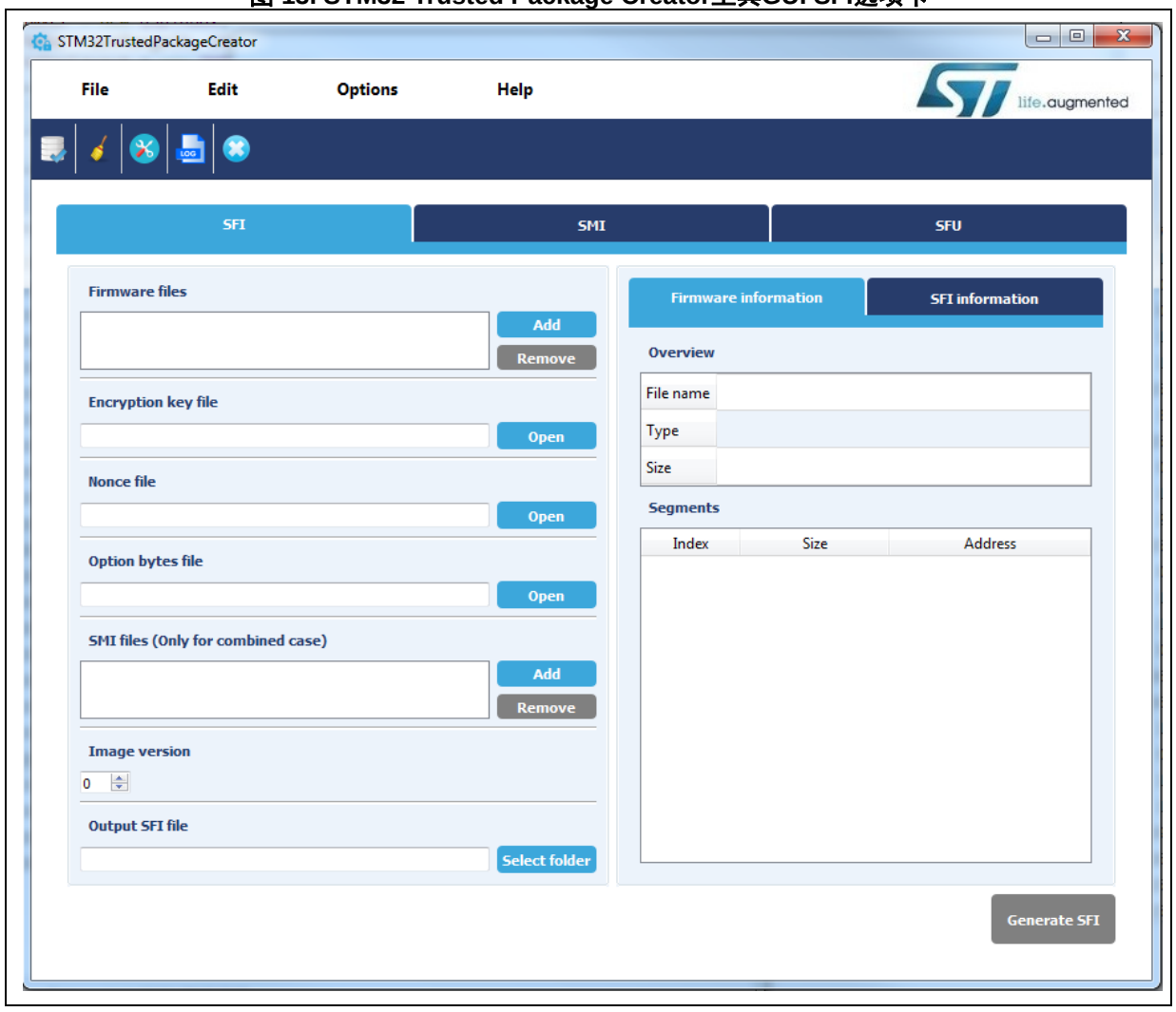


图 14. STM32 Trusted Package Creator工具GUI SMI选项卡

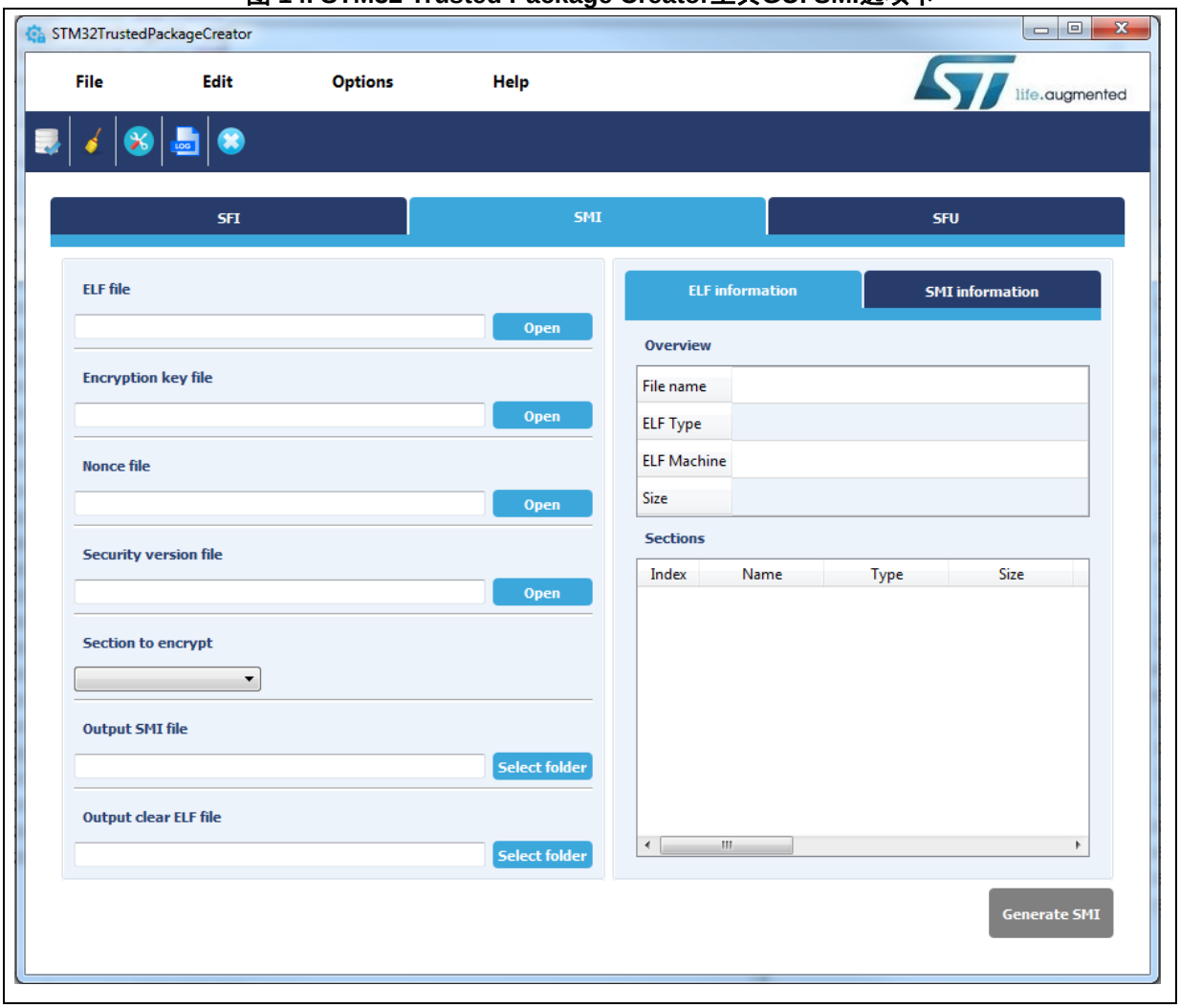
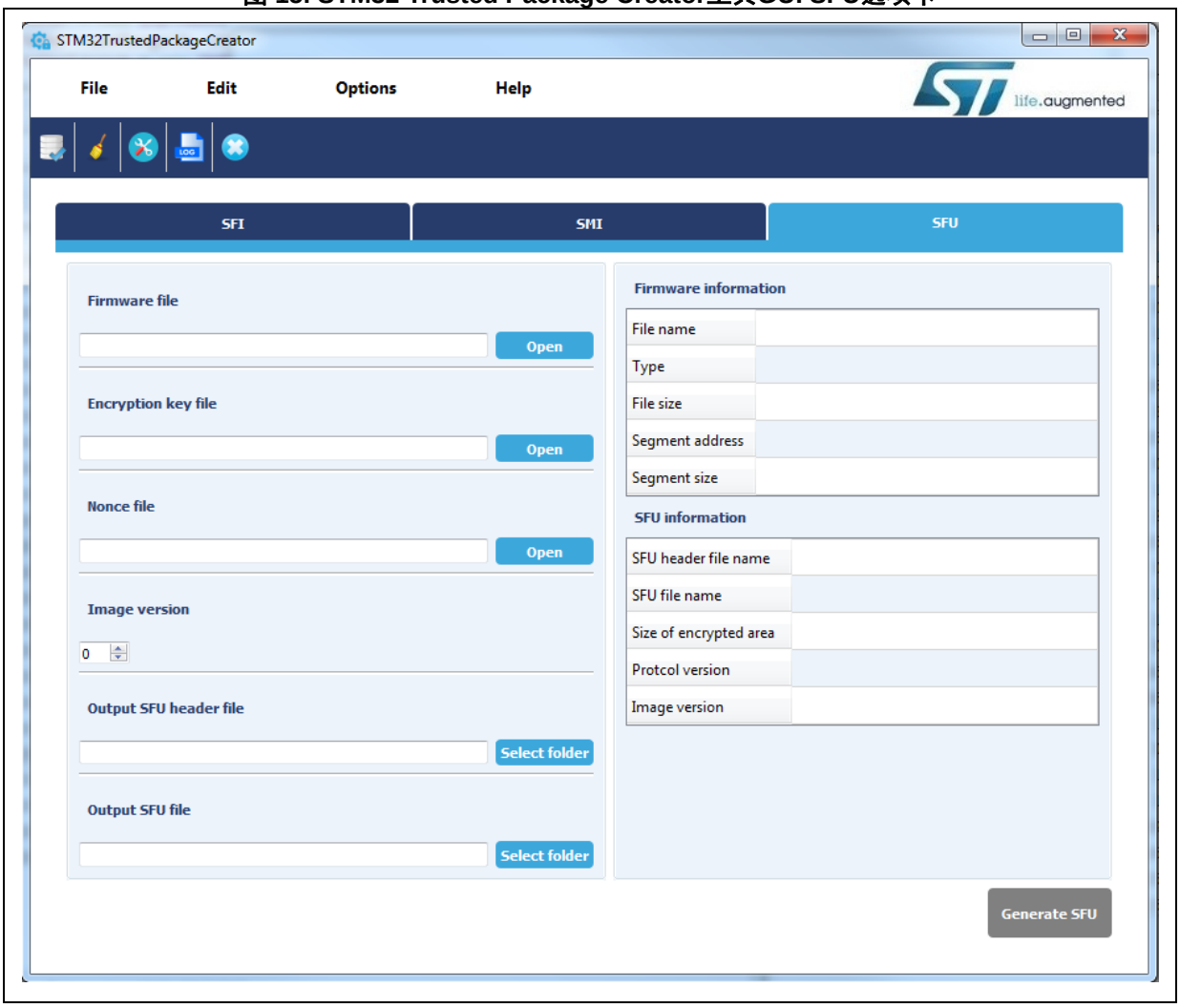


图 15. STM32 Trusted Package Creator工具GUI SFU选项卡



4.1 SFI生成

要验证SFI生成请求，用户必须使用有效值来填充输入字段：

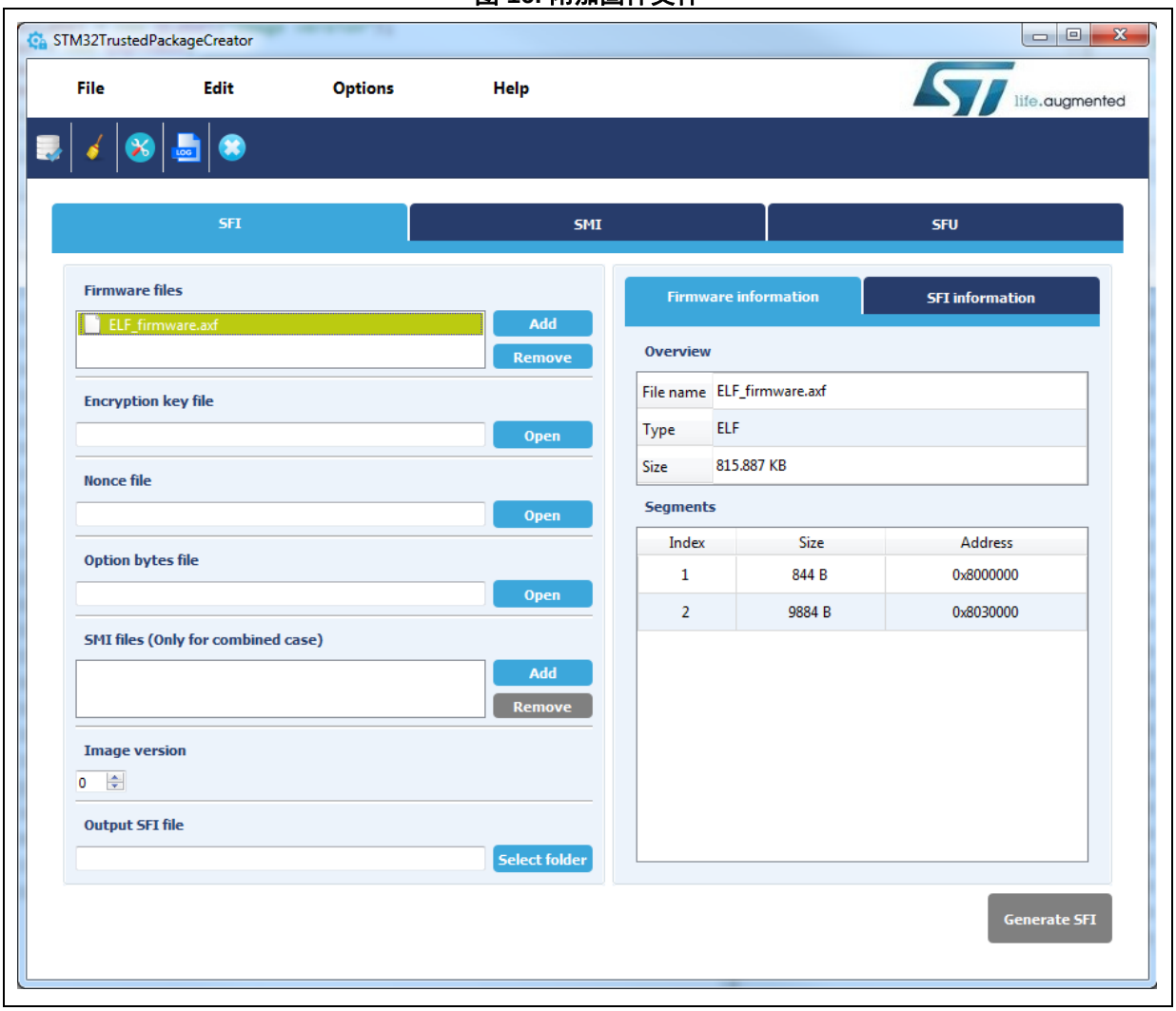
固件文件：

用户必须使用**add**按钮来添加输入固件文件。

注： *如果该文件有效，则将其添加到固件文件列表中。选择它，会在固件信息部分（图 16）中出现几条相关信息，否则会显示一条错误消息框，指出文件无法打开或文件无效。*

*如果文件是二进制格式，则会出现一个对话框，要求提供一个地址。使用**remove**按钮可以删除一个文件。*

图 16. 附加固件文件



密钥和随机数文件：

密钥和随机数文件可以通过输入其路径（绝对或相对）或通过选择**open**按钮来选择。请注意，其大小必须符合规定（密钥为16个字节，随机数为12个字节）。

选项字节文件：

选项字节文件可以同样的方式来选择。仅支持csv文件。

SMI文件：

SMI文件可以采用跟固件文件同样的方式来添加。选择文件后会在固件信息部分显示几条相关信息。

映像版本：

映像版本值为[0...255]。

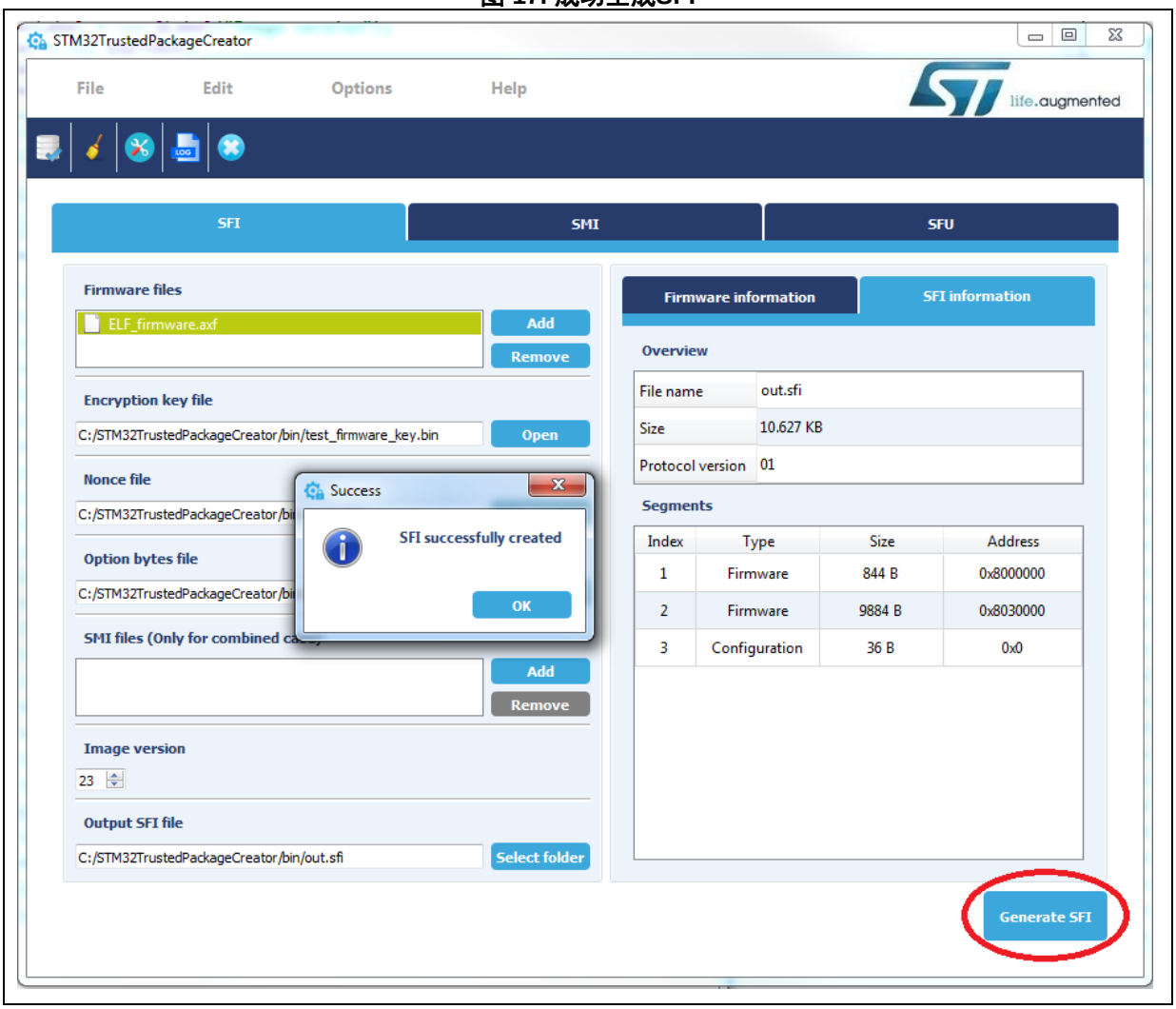
输出文件：

输出文件可以通过输入其路径（绝对或相对）或使用**select folder**按钮来选择，请注意，使用后一种方式时，建议使用名称*out.sfi*，您可以将其保留或对其进行更改

所有字段都正确填入时，**Generate SFI**按钮激活。用户可以通过点击它来生成SFI文件。

如果一切顺利，将出现一个指示成功生成的消息框（*图 17*），并在SFI信息区显示有关生成的SFI文件信息。

图 17. 成功生成SFI



4.2 SMI生成

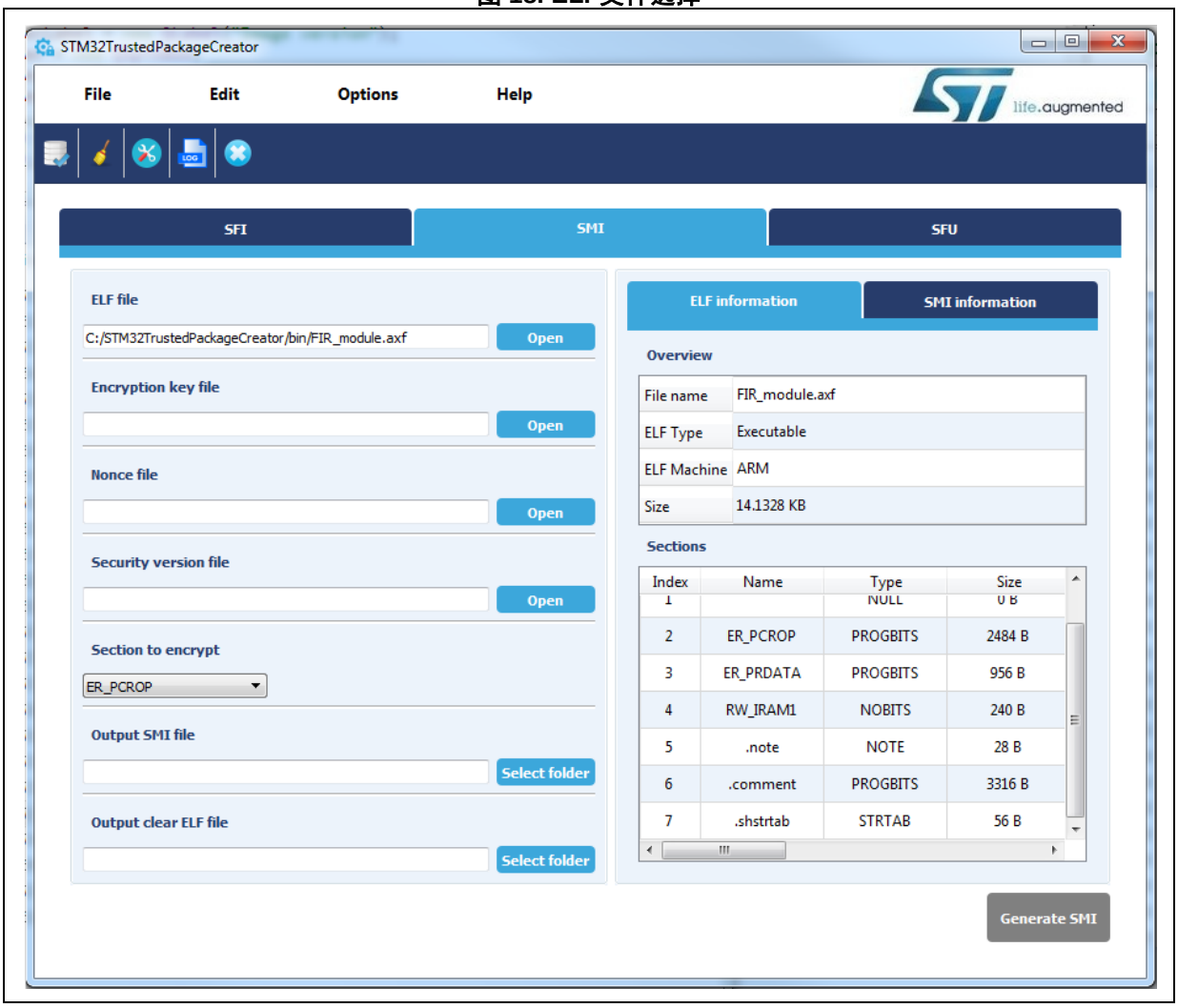
对于SFI生成，用户必须提供输入信息。

Elf文件：

这种情况下，输入文件只能是elf文件。

如果该文件有效，会在*"ELF information"*选项卡（*图 18*）中显示信息，否则会显示一条错误消息框，指出文件无法打开或文件无效。

图 18. ELF文件选择



密钥和随机数文件：

类似SFI，可以按照与固件文件相同的方式选择密钥和随机数文件。请注意，其大小必须符合规定（密钥为16个字节，随机数为12个字节）。

安全版本文件：

安全版本文件大小必须为16字节。

安全版本文件位于*Security_Version*文件夹下。

加密段：

这是一个段列表，可以选择哪个段被加密。

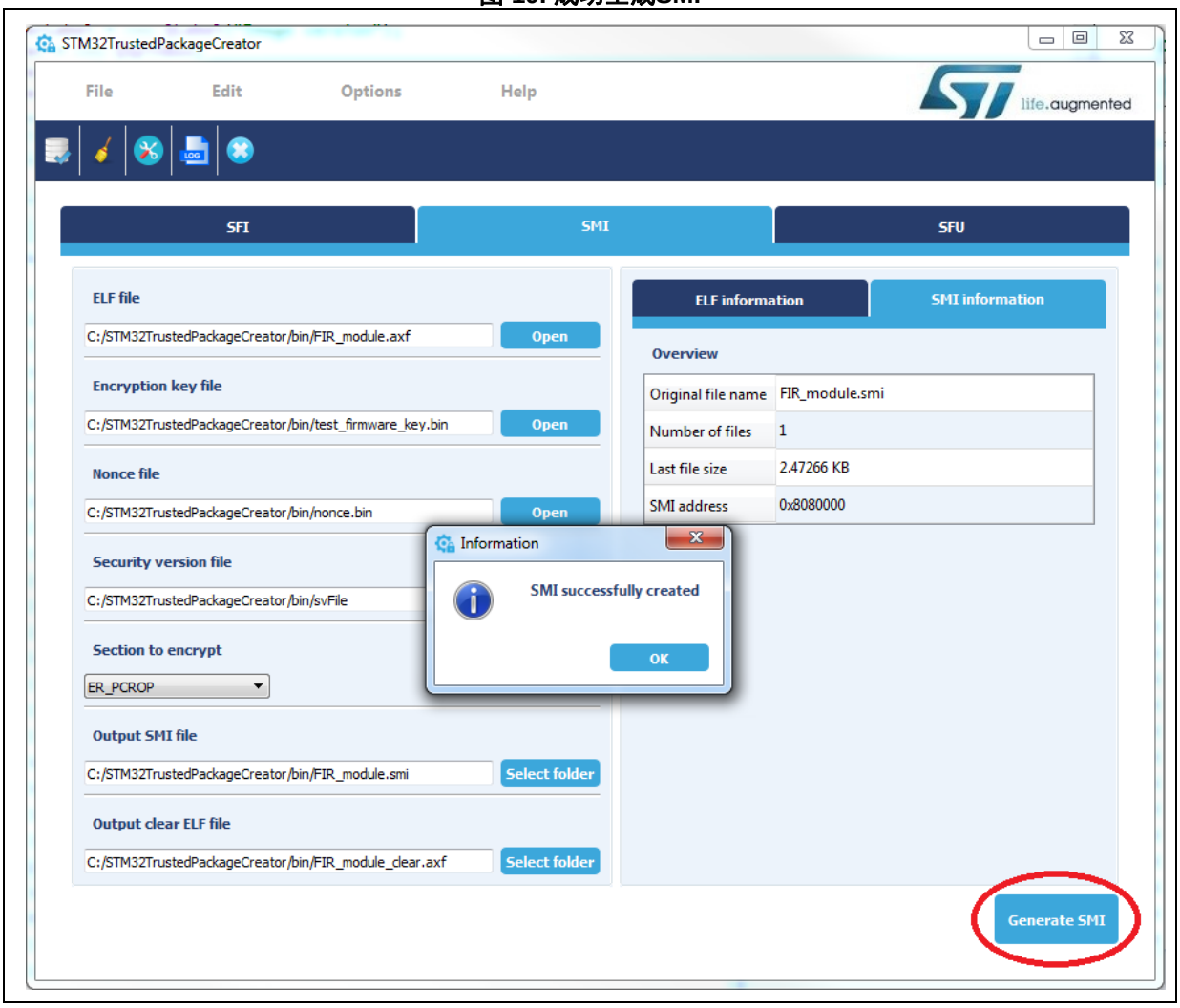
输出文件：

输出文件可以通过输入其路径（绝对或相对）或使用**Select folder**按钮来选择，请注意，使用后一种方式时，文中建议了一个名称，您可以将其保留或对其进行更改。

当所有字段都正确填入后，用户可以通过点击**Generate SMI**（该按钮变为激活状态）按钮来生成SMI文件。

除了有关所生成SMI文件的信息外，还会出现一个消息框，通知用户文件成功生成（*图 19*），否则会显示错误。

图 19. 成功生成SMI



4.3 SFU生成

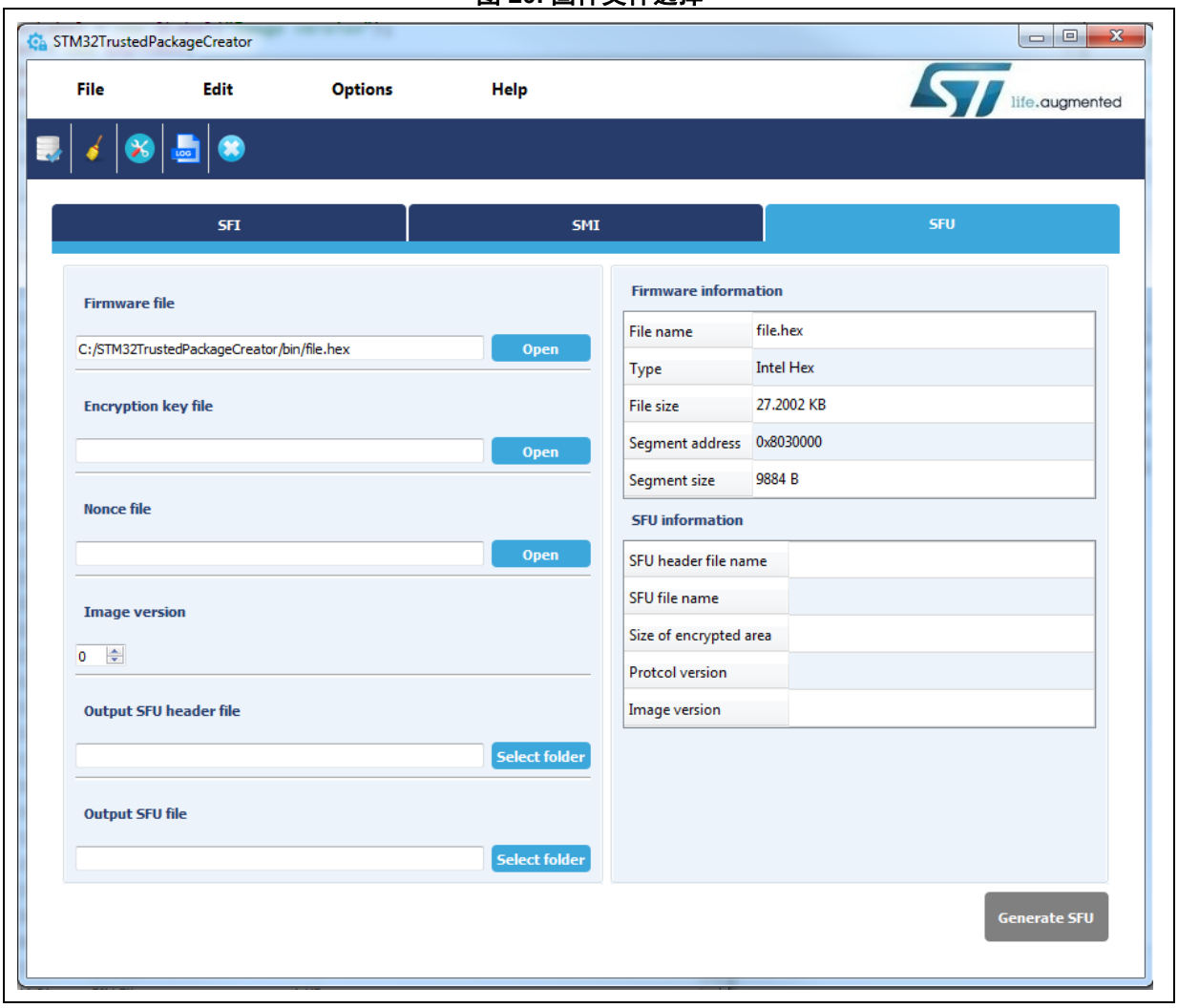
这种情况下的输入字段与SFI生成用例的输入字段类似。

固件文件：

用户需要导入固件文件。

如果该文件有效，则在固件信息区（*图 20*）中会显示几条相关信息，否则会显示错误消息框。注意，该固件文件只能包含一个段。

图 20. 固件文件选择



密钥和随机数文件：

与SFI和SMI用例类似。

映像版本：

映像版本值为[0...255]。

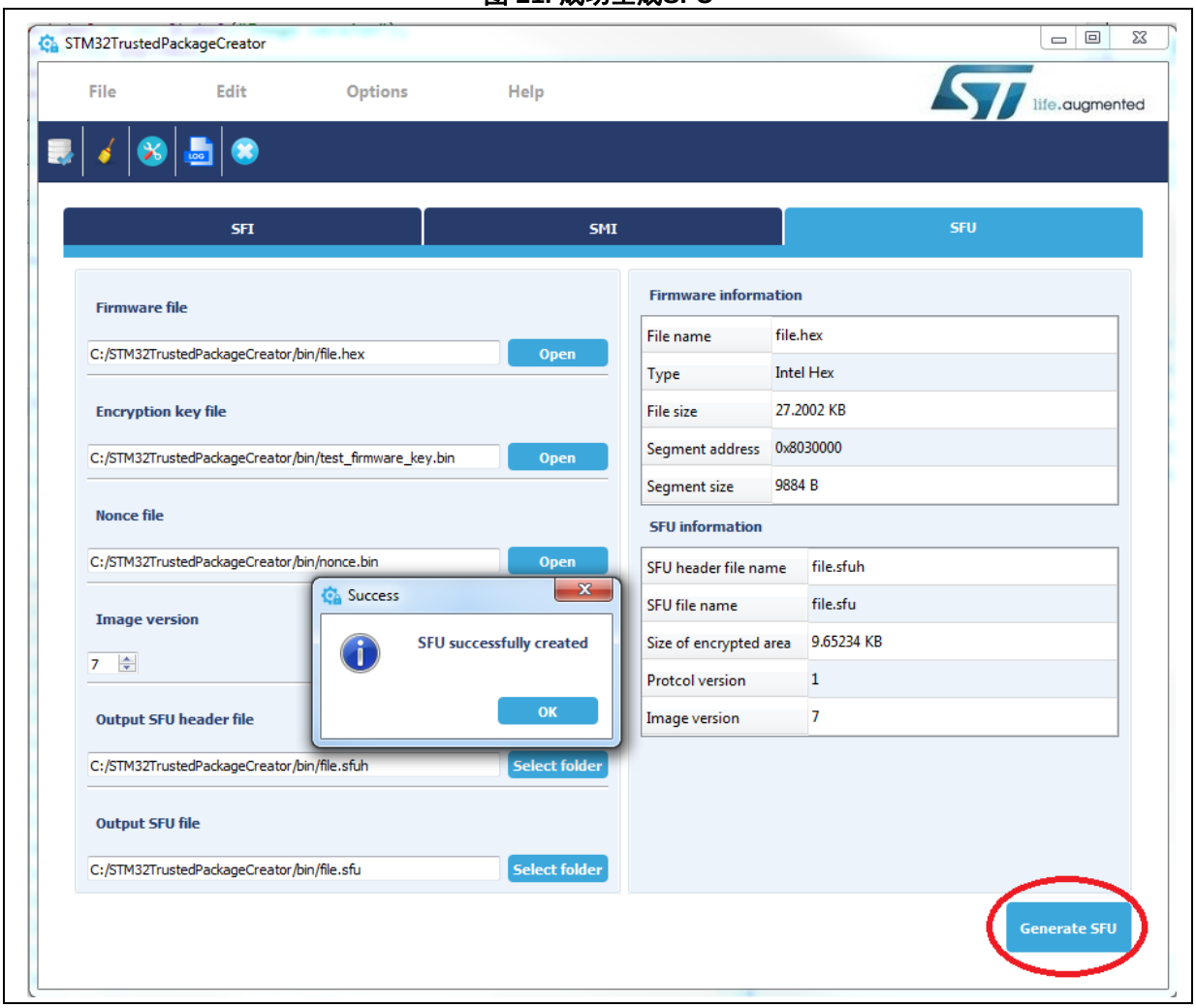
输出文件：

输出文件可以通过输入其路径（绝对或相对）或使用**select folder**按钮来选择，请注意，使用后一种方式时，文中建议了一个名称，您可以将其保留或对其进行更改。

所有字段都正确填入时，**Generate SFU**按钮激活。用户可以通过点击它来生成SFU文件。

如果一切顺利，将出现一个通知成功生成的消息框（*图 21*），并在SFU信息区显示有关生成的SFU文件信息。

图 21. 成功生成SFU


STM32TrustedPackageCreator
File
Edit
Options
Help
life.augmented
SFI
SMI
SFU
Firmware file
C:/STM32TrustedPackageCreator/bin/file.hex
Open
Encryption key file
C:/STM32TrustedPackageCreator/bin/test_firmware_key.bin
Open
Nonce file
C:/STM32TrustedPackageCreator/bin/nonce.bin
Open
Image version
7
Output SFU header file
C:/STM32TrustedPackageCreator/bin/file.sfuh
Select folder
Output SFU file
C:/STM32TrustedPackageCreator/bin/file.sfu
Select folder
Success
SFU successfully created
OK
Firmware information
File name file.hex
Type Intel Hex
File size 27.2002 KB
Segment address 0x8030000
Segment size 9884 B
SFU information
SFU header file name file.sfuh
SFU file name file.sfu
Size of encrypted area 9.65234 KB
Protcol version 1
Image version 7
Generate SFU

5 选项字节文件

选项字节文件字段仅对SFI应用程序是必需的，它允许在安全固件安装期间对选项字节进行编程。

这类文件只支持CSV（逗号分隔值）格式，该格式由两个向量组成：寄存器名和其值。

所有9个选项字节寄存器都必须进行配置（在csv文件中共有9行）。

图 22. 选项字节文件示例

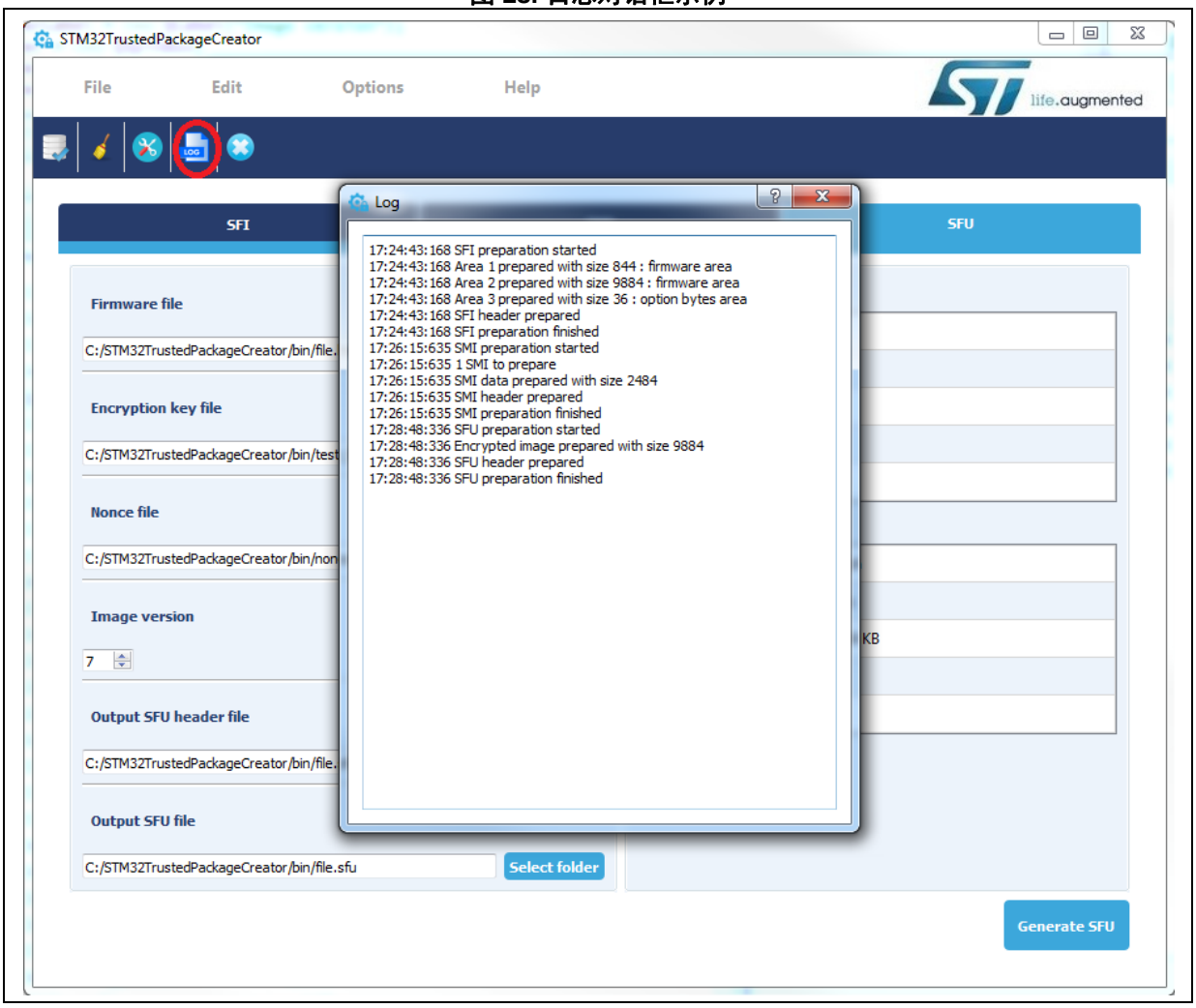
FIR_ob.csv

```
1  FOPTSR_PRG,0x13FE00F8
2  FPRAR_PRG_A,0x88060800
3  FPRAR_PRG_B,0x80000FFF
4  FSCAR_PRG_A,0x80000FFF
5  FSCAR_PRG_B,0x80000FFF
6  FWPSN_PRG_A,0x000000FF
7  FWPSN_PRG_B,0x000000FF
8  FBOOT7_PRG,0x1FF10800
9  RFU,0x10000810
```

6 日志对话框

可以通过单击工具栏或菜单栏中的**log**按钮来查看日志：选项 - >日志。

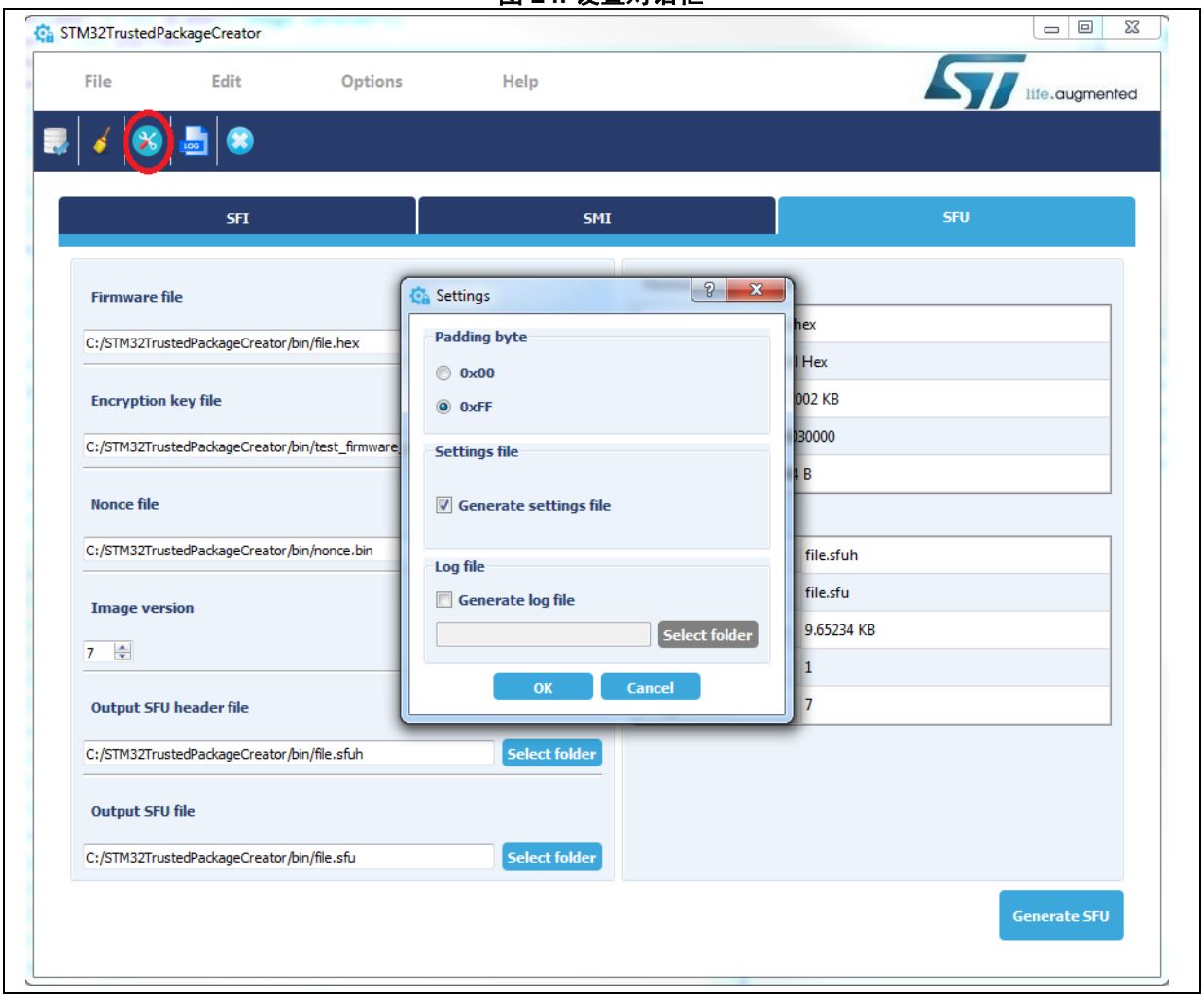
图 23. 日志对话框示例



7 设置

可以通过单击工具栏或菜单栏中的**settings**按钮来访问设置对话框：选项 - >设置。

图 24. 设置对话框



填充字节：

在解析文件时，可以添加填充字节来填补由16个或更少字节所分隔的各段之间的空隙，以将其合并并减少段数。用户可以选择0xFF（默认值）或0x00。

设置文件：

选中后，将在可执行文件夹中生成*settings.ini*文件。它保存了应用程序状态：窗口大小和字段内容。

日志文件：

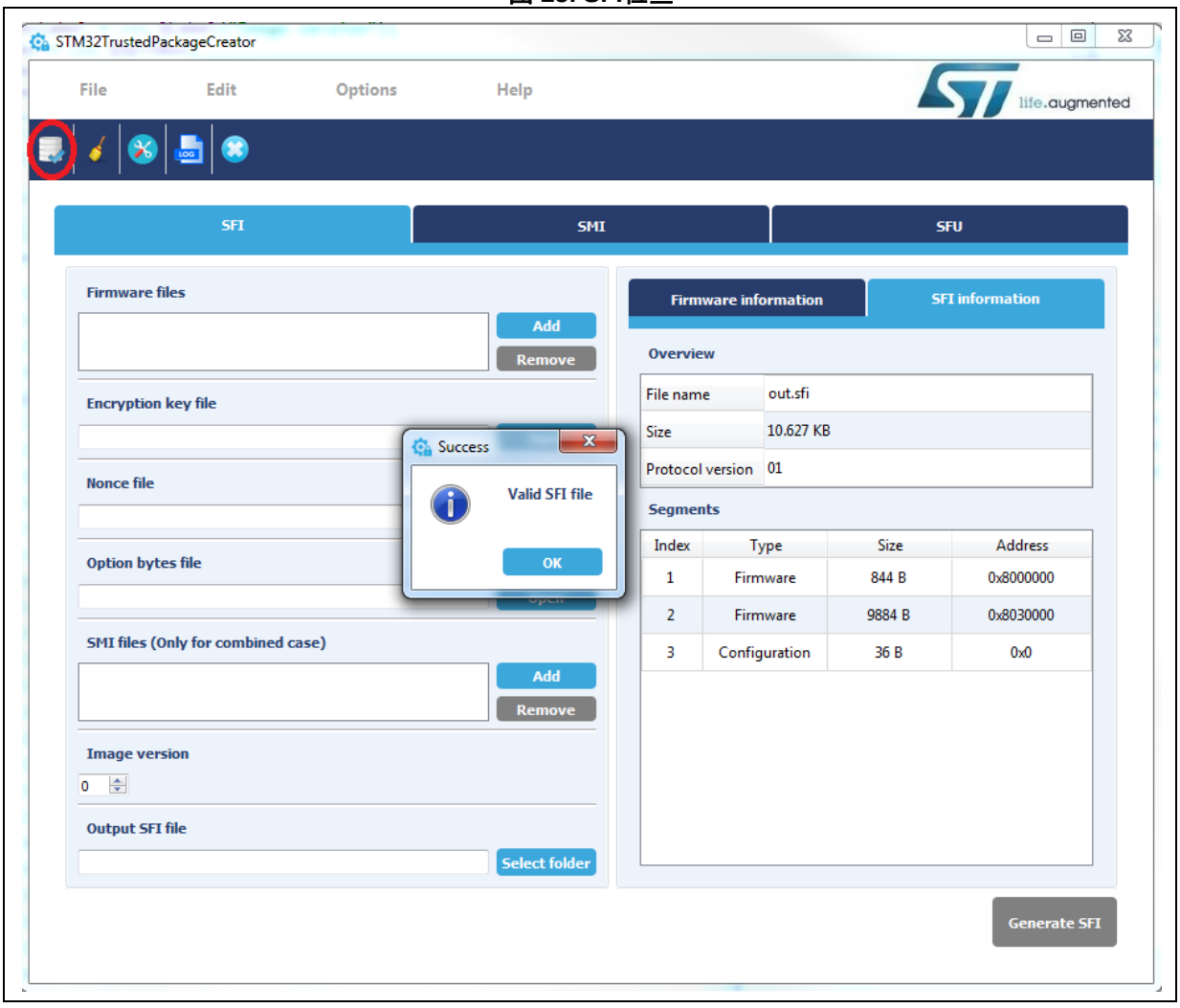
选中后，将在所选路径下生成一个日志文件。

8 SFI/SMI检查

可以通过单击工具栏或菜单栏中的**Check SFI/SMI**按钮来访问SFI/SMI检查：文件 - >检查SFI/SMI。

这样可以检查SFI或SMI文件的有效性，并显示其相关信息。

图 25. SFI检查



9 版本历史

表1. 文档版本历史

日期	版本	变更
2017年12月20日	1	初始版本。

表2. 中文文档版本历史

日期	版本	变更
2018年8月10日	1	中文初始版本。

重要通知 - 请仔细阅读

意法半导体公司及其子公司 （“ST”）保留随时对 ST 产品和 / 或本文档进行变更、更正、增强、修改和改进的权利，恕不另行通知。买方在订货之前应获取关于 ST 产品的最新信息。 ST 产品的销售依照订单确认时的相关 ST 销售条款。

买方自行负责对 ST 产品的选择和使用， ST 概不承担与应用协助或买方产品设计相关的任何责任。

ST 不对任何知识产权进行任何明示或默示的授权或许可。

转售的 ST 产品如有不同于此处提供的信息的规定，将导致 ST 针对该产品授予的任何保证失效。

ST 和 ST 徽标是 ST 的商标。所有其他产品或服务名称均为其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。本文档的中文版本为英文版本的翻译件，仅供参考之用；若中文版本与英文版本有任何冲突或不一致，则以英文版本为准。