

## 一步一步使用 STM32 安全启动与固件更新

### 前言

STM32 X-CUBE-SBSFU 软件包已经发布，提供了安全启动 (Secure Boot) 和安全固件更新 (Secure Firmware Update) 功能。安全启动和安全固件更新使用了 STM32 内建的各种软硬件安全技术，构建了从启动开始的根信任链，可以用来防止固件克隆、恶意软件下载以及固件破坏。本文则是带领读者一步一步来体验 STM32 安全启动与安全固件更新。

### 硬件

- STM32 NUCLEO-L476RG 开发板
- Mini USB 连接线

### X-CUBE-SBSFU 1.0.0

从 [http://www.st.com/content/st\\_com/en/products/embedded-software/mcus-embedded-software/stm32-embedded-software/stm32cube-expansion-packages/x-cube-sbsfu.html](http://www.st.com/content/st_com/en/products/embedded-software/mcus-embedded-software/stm32-embedded-software/stm32cube-expansion-packages/x-cube-sbsfu.html) 可以下载 X-CUBE-SBSFU 1.0.0 安全启动以及安全更新组件。因为是安全相关的组件，下载需要发送请求并且需要得到批准。读者需要注册成为 my.st.com 用户。

### GET SOFTWARE

Part Number ▲	Software Version ▼	Marketing Status ▼	Supplier ▼	Order from ST ▼
X-CUBE-SBSFU	1.0.0	Active	ST	<a href="#">Request Software</a>

填写相关信息，就会进入等待批准的状态。

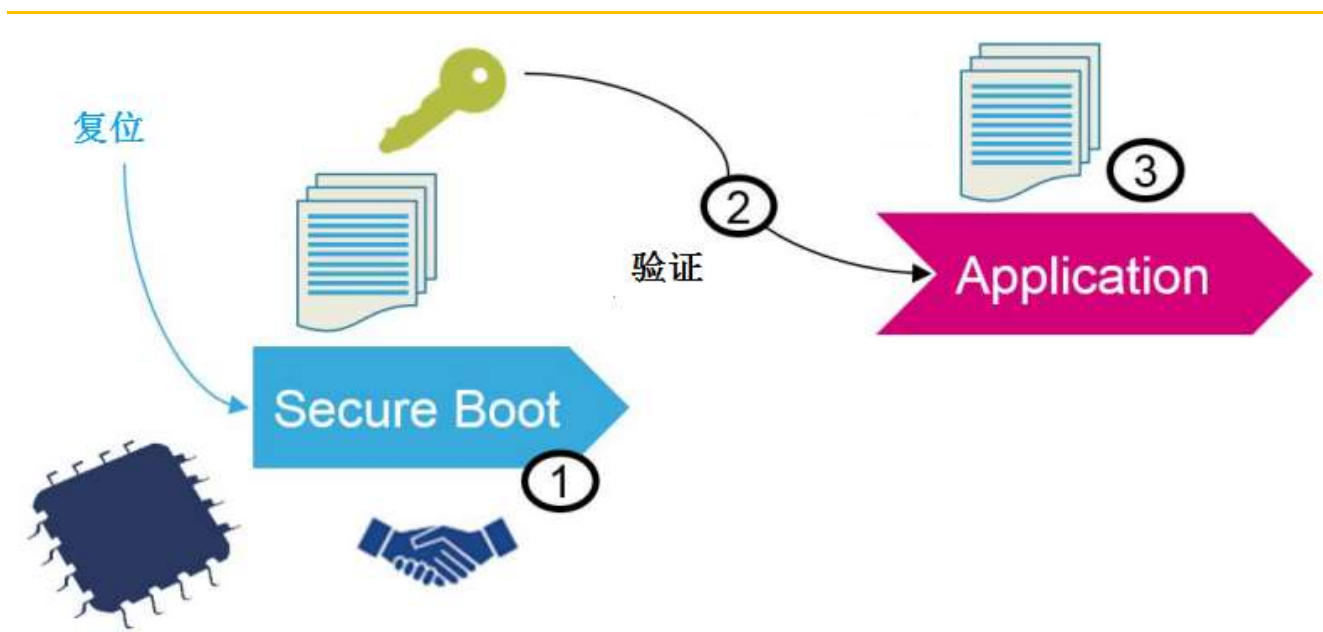
Part Number ▲	Software Version ▼	Marketing Status ▼	Supplier ▼	Order from ST ▼
X-CUBE-SBSFU	1.0.0	Active	ST	<a href="#">Validating</a>

批准通过后，你会收到一份邮件，邮件里会包含下载连接。

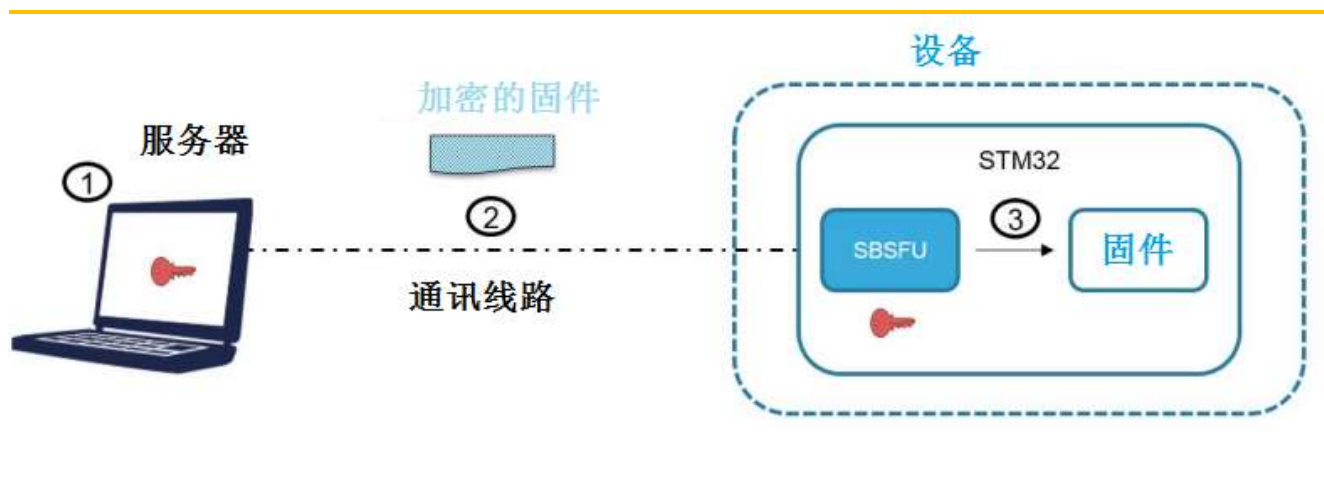
Part Number ▲	Software Version ▼	Marketing Status ▼	Supplier ▼	Order from ST ▼
X-CUBE-SBSFU	1.0.0	Active	ST	<a href="#">Download</a>

### SBSFU 简介

STM32 安全启动（secure boot，简称 SB）功能检查并使能 STM32 安全功能。在执行应用程序前，“安全启动”检查应用程序的完整性以及合法性。若应用程序被非法修改，或者应用程序不具有有效的签名，则应用程序将不会被执行。“安全启动”这段代码的执行，则利用 STM32 的安全 IP，被设计成不可被跳过。



STM32 安全固件更新（secured firmware update，简称 SFU）则接收经过加密的固件，对它进行解密，在烧写升级的固件前验证它的完整性以及合法性。不完整或者非法来源的固件将不会用来升级。



### SBSFU 安全技术概述

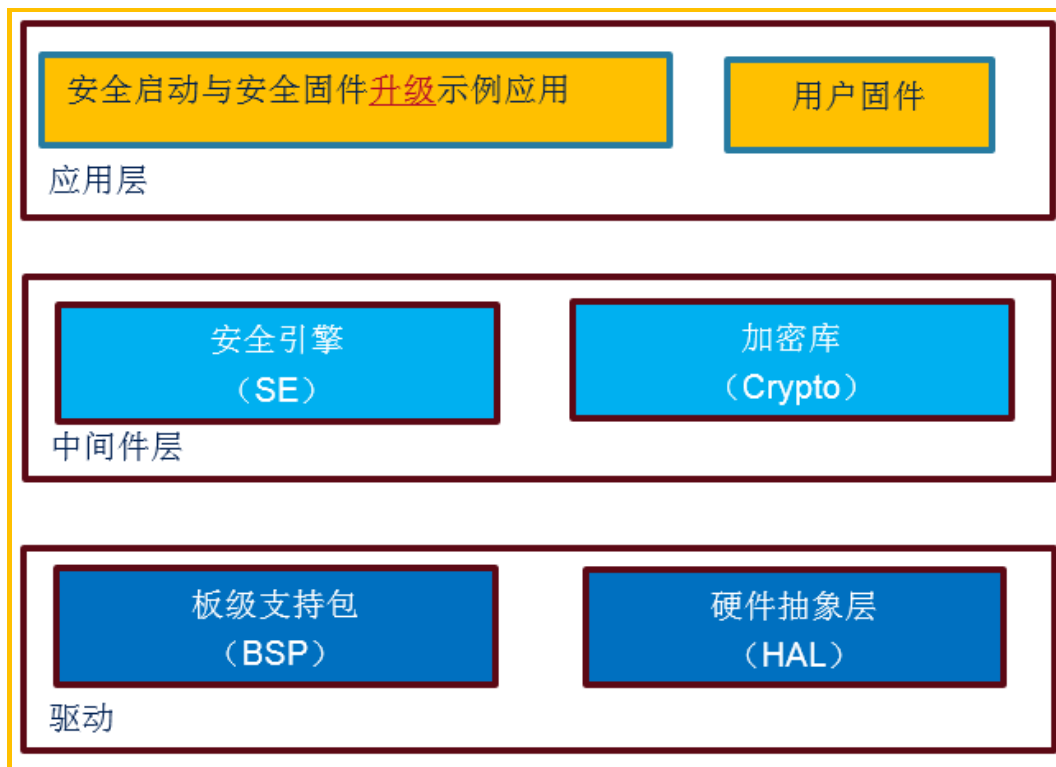
现实世界中 MCU 产品并非部署在安全的环境里，总是会面临各种各样的威胁和攻击。SBSFU 使用各类 STM32 IP 来构建安全防线，包括：

- 使用加解密工具来保证系统的**完整性**，**合法性**以及**保密性**。SBSFU 使用了对称密钥 **AES-GCM** 算法工具来进行固件的解密以及验证。解密算法可由软件实现，也可由 STM32 内建的加解密硬件 IP 引擎实现。
- 使用 STM32 内建安全功能诸如内存保护技术来阻止外部通过 JTAG 或者内部恶意代码的攻击。SBSFU 使用了以下 STM32 安全功能来确保安全启动和安全固件更新的目标。



### SBSFU 的架构

SBSFU 整体架构如下。应用层分为两大部分，一部分是安全启动，检查固件的合法性，进行固件下载和烧写；一部分是用户固件，功能则由用户定制。



安全启动中的**安全引擎 (SE) 中间件**，提供了一个受保护的环境，来保护所有的关键数据和操作——包括进行加解密操作时时访问密钥等。受保护的代码和数据都是通过唯一的调用门进行访问，不可能在调用门之外来执行受保护代码或者访问关键数据。

### SBSFU 编译

需要按顺序对下列工程进行编译, 因为他们之间存在依赖关系。

#### 1. SE\_KeyLib

编译成功后的输出是一个库, SE\_Key\_CM4\_IAR.a。这个库提供获取密钥的功能。这个密钥是由 SBSFU 用来解密和验证后续应用程序合法性的。密钥在这里不是以”数据“的形式出现, 而是以”一段可执行代码“的形式存储, 被 STM32 安全机制 (PCROP) 保护。

X-CUBE-SBSFU 固件包里提供了一个专门的工具 KeysInject, 来进行密钥到代码的转换, 位于 STM32CubeExpansion\_SBSFU\_V1.0.0\Middlewares\ST\STM32\_Secure\_Engine\Utilities\KeysInject\Binary\KeysInject.exe。在 windows 的命令行窗口输入以下命令: 其中两个参数是用户指定的密钥字符串 (在这里使用相同的密钥)。

```
KeysInject.exe OEM_KEY_COMPANY1 OEM_KEY_COMPANY1
```

生成的 key\_table.txt 的内容应被复制到 SE\_Key.c 的数组 SE\_ReadKeyCode[44] 中。并且该字符串由用户制作一个对应的二进制文件 OEM\_KEY\_COMPANY1\_key.bin，后面再生成加密的用户固件时需要。

## 2. SE\_CoreBin

安全引擎的核心二进制文件。它作为安全引擎中间件，提供唯一的调用门（Calling gate，参见 STM32L4 参考手册中的“防火墙（Firewall）”一章）给 SBSFU 示例应用来调用加解密函数。

SE\_KeyLib 的输出 SE\_Key\_CM4\_IAR.a，会被该工程使用。

## 3. SB\_SFU

安全启动与安全固件更新示例应用。它使用之前生成的 SE\_CoreBin。在启动时，（安全启动程序“SB”）验证用户固件的签名或者认证码（MAC）来决定是否跳到用户程序执行。（安全固件更新“SFU”）如果在启动时检测到有新的固件更新，则下载加密固件，验证，以及解密安装。

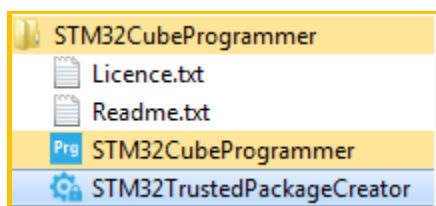
## 4. UserAppExample

用户程序。编译输出是一个可执行程序。它也可以用来进行新版本固件（用户程序）下载，但是，它不会进行验证与安装。验证与安装时通过重启后的安全启动程序（SecureBoot）完成的。

## 固件加密与包装

要创建加密的固件，需要使用 **STM32 Trusted Package Creator tool**。该软件，需先从

<http://www.st.com/en/development-tools/stm32cubeprog.html> 下载 **en.stm32cubeprog.zip**，安装时勾选 **STM32 Trusted Package Creator tool** 即可。



打开 **STM32 Trusted Package Creator tool**，选择“SFU”标签项，随后做如下设置

- 固件路径：

这是之前编译的用户程序输出，即之前需要编译的四个文件中的“4. UserAppExample”

例如：STM32CubeExpansion\_SBSFU\_V1.0.0/Projects/STM32L476RG-

Nucleo/Applications/UserAppExample/EWARM/UserAppExample\_A/Exe/UserAppExample\_A.bin

- 密钥文件路径：

这是之前通过 KeysInject 工具产生的密钥二进制文件。SBSFU 软件包里已经提供了一个。

例如：STM32CubeExpansion\_SBSFU\_V1.0.0/Projects/STM32L476RG-

Nucleo/Applications/UserAppExample/Binary/OEM\_KEY\_COMPANY1\_key.bin

- 96-bits Nonce 随机数文件路径：

用户可根据需要进行定制，软件包里已经提供了一个。

例如：STM32CubeExpansion\_SBSFU\_V1.0.0/Projects/STM32L476RG-Nucleo/Applications/UserAppExample/Binary/nonce.bin

- 固件版本：

我们设置成 1.0。

以下是加密的用户应用程序对应的两部分（文件头和文件体）对应的路径。

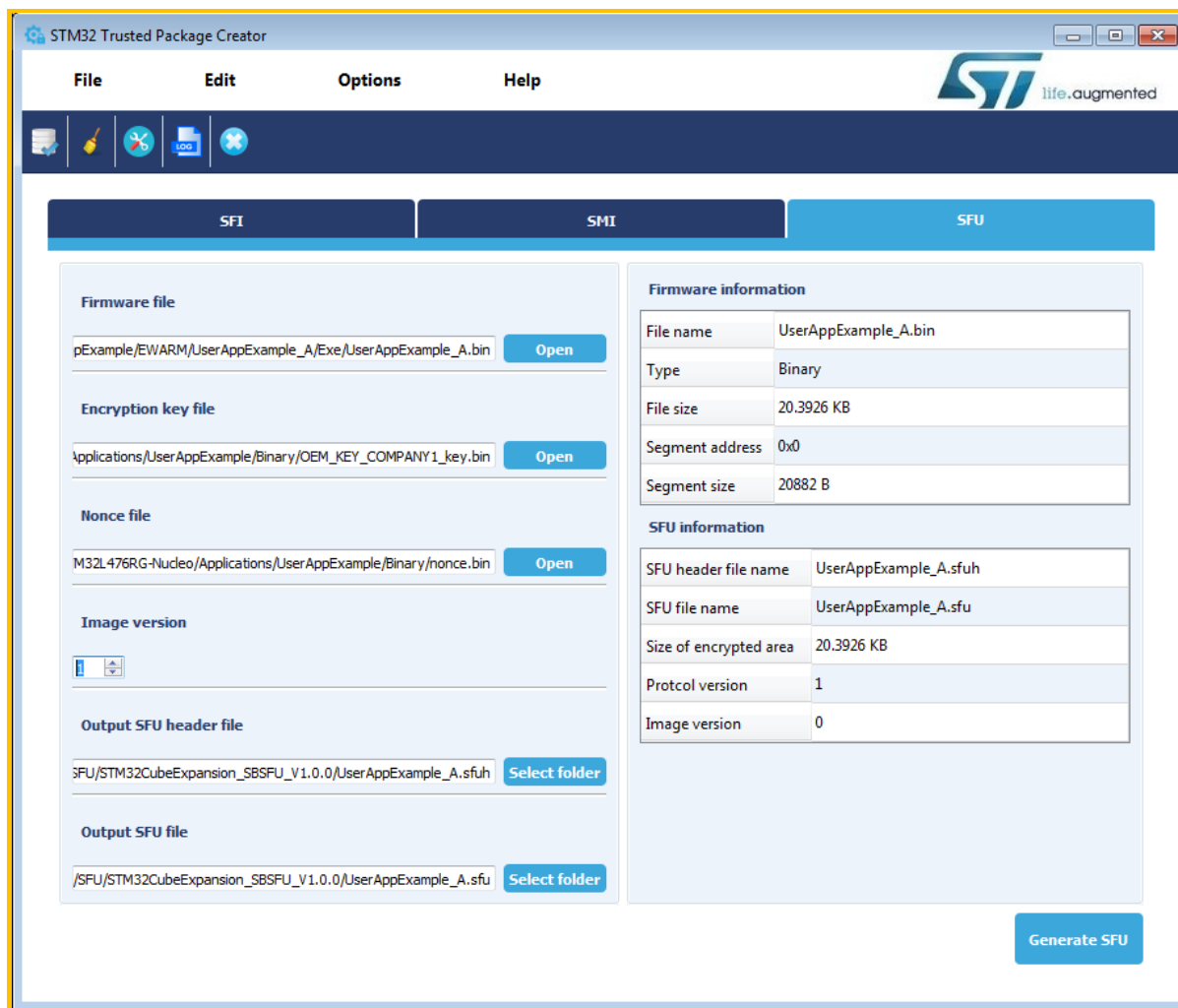
- SFU 头的输出路径：

可任意设置，这里设置为工作目录 STM32CubeExpansion\_SBSFU\_V1.0.0。

- SFU 文件的输出路径：

可任意设置，这里设置为工作目录 STM32CubeExpansion\_SBSFU\_V1.0.0。

然后点击生成按钮，就可以生成相应的安全固件的头信息以及数据文件。



Firmware information	
File name	UserAppExample_A.bin
Type	Binary
File size	20.3926 KB
Segment address	0x0
Segment size	20882 B

SFU information	
SFU header file name	UserAppExample_A.sfuh
SFU file name	UserAppExample_A.sfu
Size of encrypted area	20.3926 KB
Protocol version	1
Image version	0

Generate SFU

## 下载用户固件

首先是下载 SBSFU。SBSFU 是直接编译后的结果。注意，不要选择调试，因为安全启动内部配置成不可调试。然后根据提示信息，对板子电源进行下拔插。我们使用的串口工具是 TeraTerm。如何配置 Teraterm，请参考其他 STM32 文档。

Applying RDP-1 Level. You might need to unplug/plug the USB cable!....

重新连接串口中断，比如 TeraTerm，你就可以看到安全启动与安全固件更新示例正在运行。我们还没有把用户应用编译下载下去，所以这里发现不了有效的固件。

```
[SB00T] System Security Check successfully passed. Starting...
[SPWIMG] Slot #0 @: 8091800 / Slot #1 @: 8012000 / Swap @: 808d800

=====
(C) COPYRIGHT 2017 STMicroelectronics
=====
Secure Boot and Secure Firmware Update
=====

[SB00T] SECURE ENGINE INITIALIZATION SUCCESSFUL
[SB00T] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Hardware reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was: No error. Success.
[SB00T] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
No download requested
[SB00T] STATE: CHECK USER FW STATUS
No valid FW found in the active slot nor new encrypted FW found in the UserApp download area
Hold User Button during at least 500 msec to force FW update .....
█
```

接下来就是下载用户的安全固件。在进行这一步之前，先要确保已经如前所述，使用 **STM32 Trusted Package Creator tool** 工具生成了用户安全固件。然后，再重启开发板，按住蓝色用户按钮。然后在串口就可以看到如下输出：

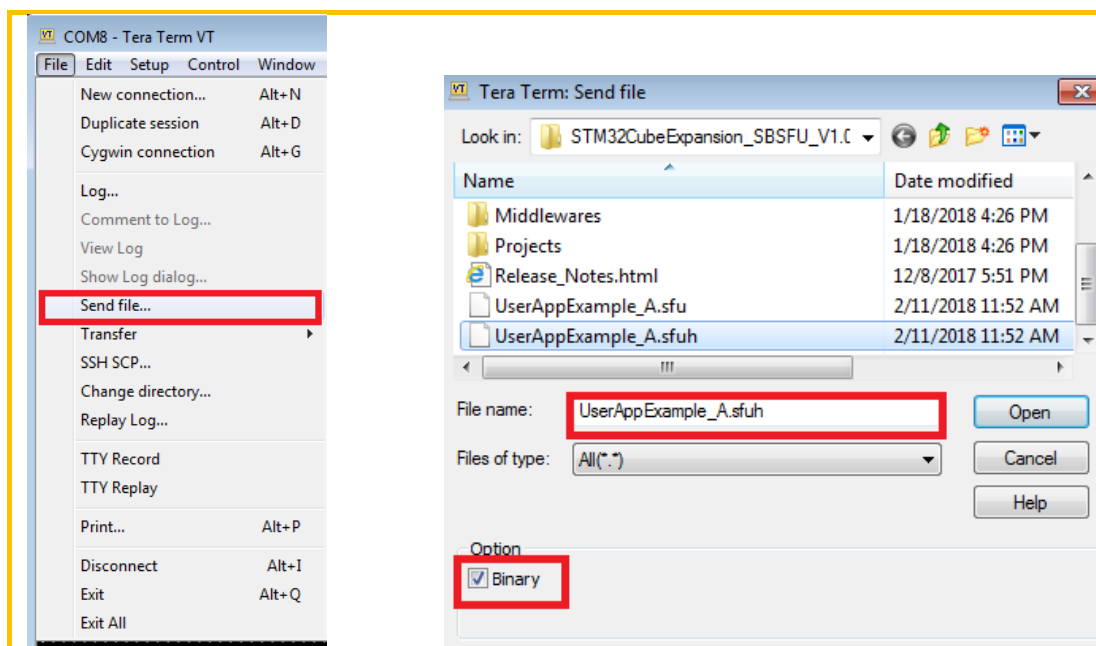


```
= [SB00T] System Security Check successfully passed. Starting...
= [SFWIMG] Slot #0 @: 8091800 / Slot #1 @: 8012000 / Swap @: 808d800

=====
= (C) COPYRIGHT 2017 STMicroelectronics
=
= Secure Boot and Secure Firmware Update
=====

= [SB00T] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SB00T] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Hardware reset!
Consecutive Boot on error counter = 0
INFO: Last execution detected error was:No error. Success.
= [SB00T] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
No download requested
= [SB00T] STATE: CHECK USER FW STATUS
No valid FW found in the active slot nor new encrypted FW found in the UserApp d
Hold User Button during at least 500 msec to force FW update ..
Forced Download
Send Header : File> Send File (check binary option!) .....
```

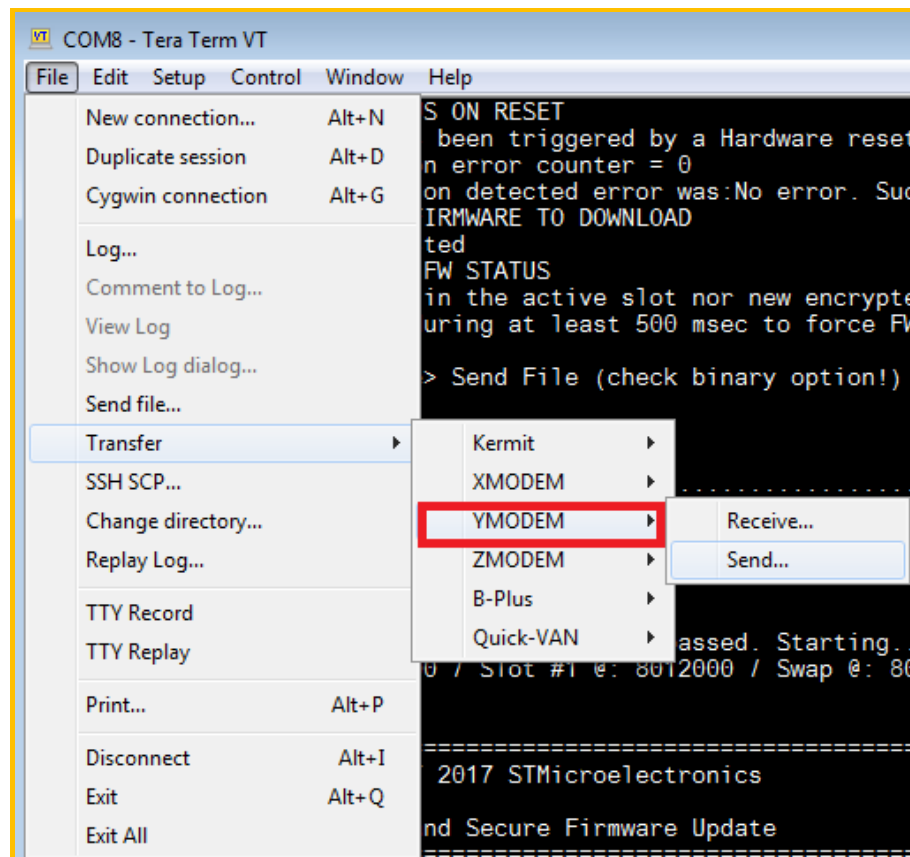
第一步是下载用户固件的头信息，即之前在 STM32 Trusted Package Creator 这个工具中生成的” UserAppExample\_A.sfuh”。选择 TeraTerm 的 File->Send。选择前面生成的固件头信息文件。注意要勾选 Binary 选项。



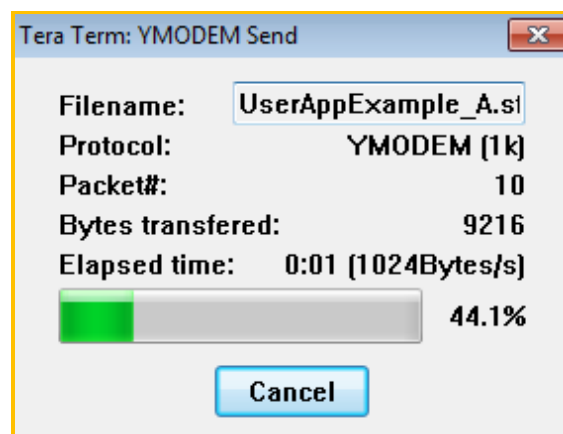
第二步才是用户

的安全固件，即之前在 STM32 Trusted Package Creator 这个工具中生成的” UserAppExample\_A.sfu”：选择 YMODEM 协议来传输文件





固件下载时，Teraterm 会弹出一个界面显示进度



下载完成后，STM32 会自动重启，进行安全启动流程，进入到用户程序。

```

= [SB00T] STATE: DOWNLOAD NEW USER FIRMWARE
    Erasing download area ...
= [SB00T] STATE: REBOOT STATE MACHINE
===== End of Execution =====

= [SB00T] System Security Check successfully passed. Starting...
= [SFWIMG] Slot #0 @: 8091800 / Slot #1 @: 8012000 / Swap @: 808d800

=====
=                                     =
=      (C) COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      Secure Boot and Secure Firmware Update      =
=====

= [SB00T] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SB00T] STATE: CHECK STATUS ON RESET
    INFO: A Reboot has been triggered by a Software reset!
    Consecutive Boot on error counter = 0
    INFO: Last execution detected error was: No error. Success.
= [SB00T] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
    No download requested
= [SB00T] STATE: CHECK USER FW STATUS
    New Fw Encrypted, to be decrypted
= [SB00T] STATE: INSTALL NEW USER FIRMWARE
= [SB00T] STATE: VERIFY USER FW SIGNATURE
= [SB00T] STATE: EXECUTE USER FIRMWARE
=====
=                                     =
=      (C) COPYRIGHT 2017 STMicroelectronics      =
=                                     =
=      User App #A                                =
=====

===== Main Menu =====

Download a new Fw Image ----- 1
Test Protections ----- 2
Test Crypto ----- 3
  
```

解密且安装

验证固件

值得一提的是，安全启动会自动设置读保护，写保护等。若想重新烧入安全启动而不是用户固件，则需要将 RDP1 改为 RDP0，同时去除写保护。

## 总结

STM32 X-CUBE-SBSFU 软件包的发布，为开发 STM32 安全程序提供了最重要的模块：安全启动与固件更新，可以让用户从高层次来使用 STM32 的各项安全功能。



## 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。