



life.augmented

STM32 生态系统 第二十二期

信息安全 . Information Security

13. 安全固件烧录/SFI

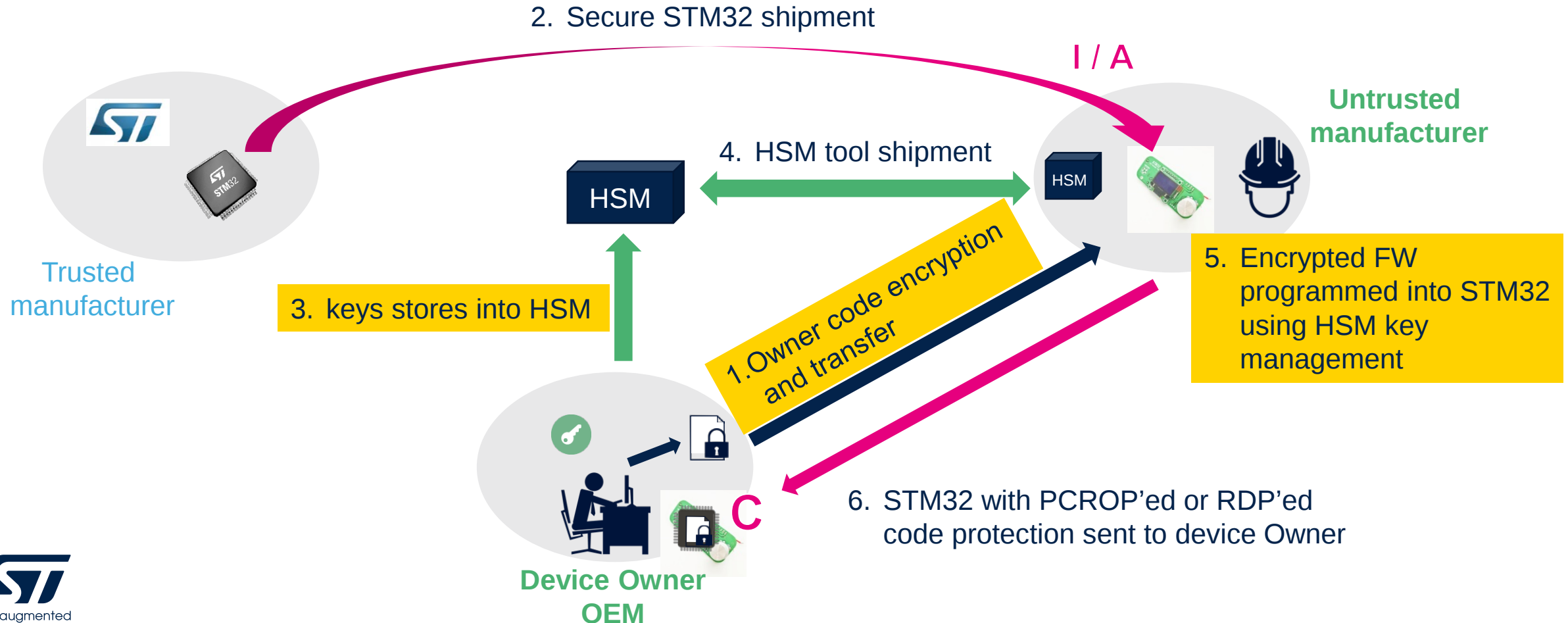
2020.03

Secure firmware install

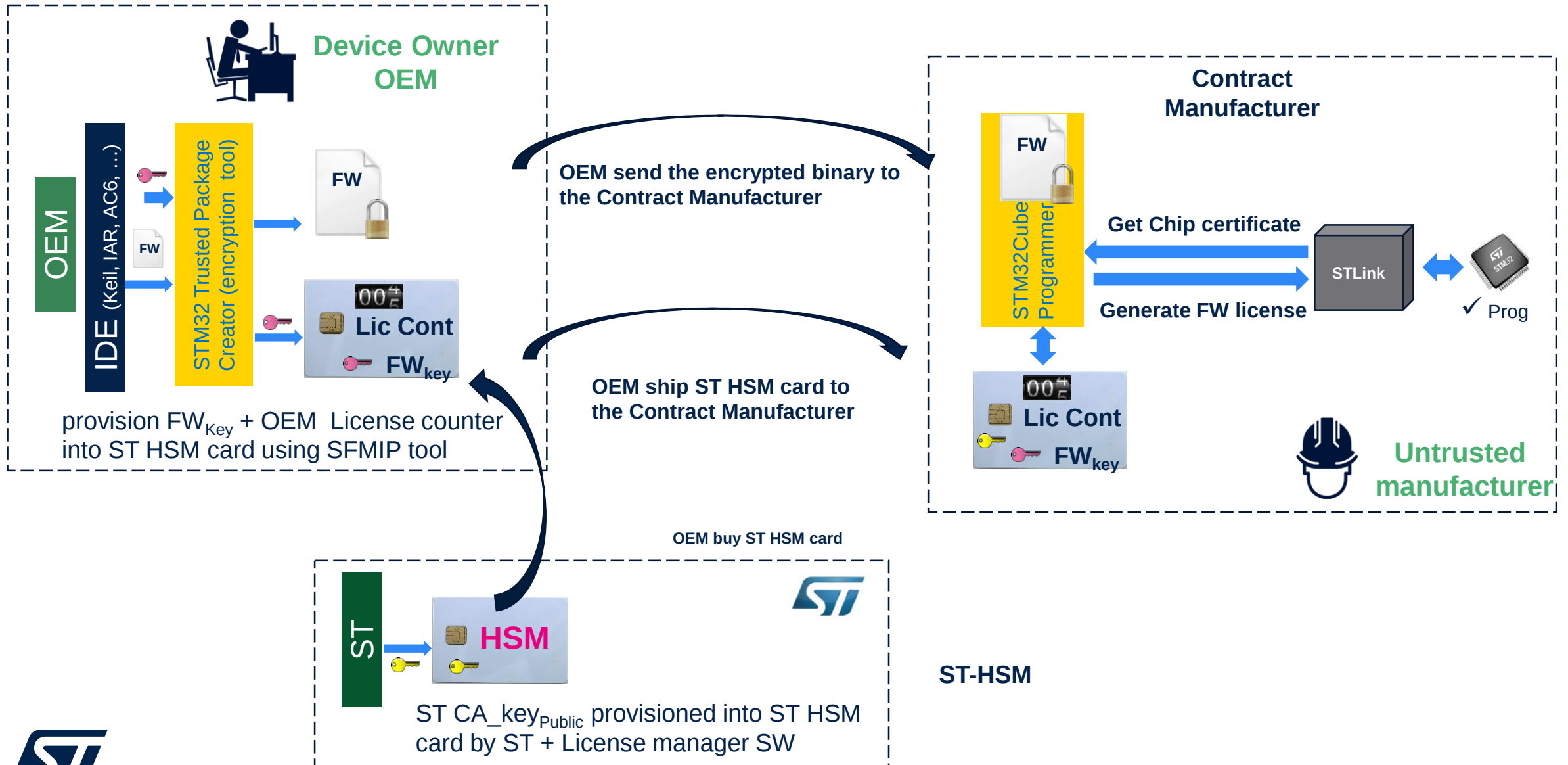
- SFI可以解决什么问题？
 - 如何确保OEM研发的固件，在第三方(不可靠)产线上不会泄露
 - 如何控制OEM研发的固件，被烧录的次数
- SFI给出的答案：
 - 使用签名过的证书对目标芯片进行验证 → 确实是STM32
 - 烧录器外部总线上传输的是固件密文 → 保证OEM固件的保密性
 - 使用License文件 → 控制烧录的次数

SFI 过程中的用户体验

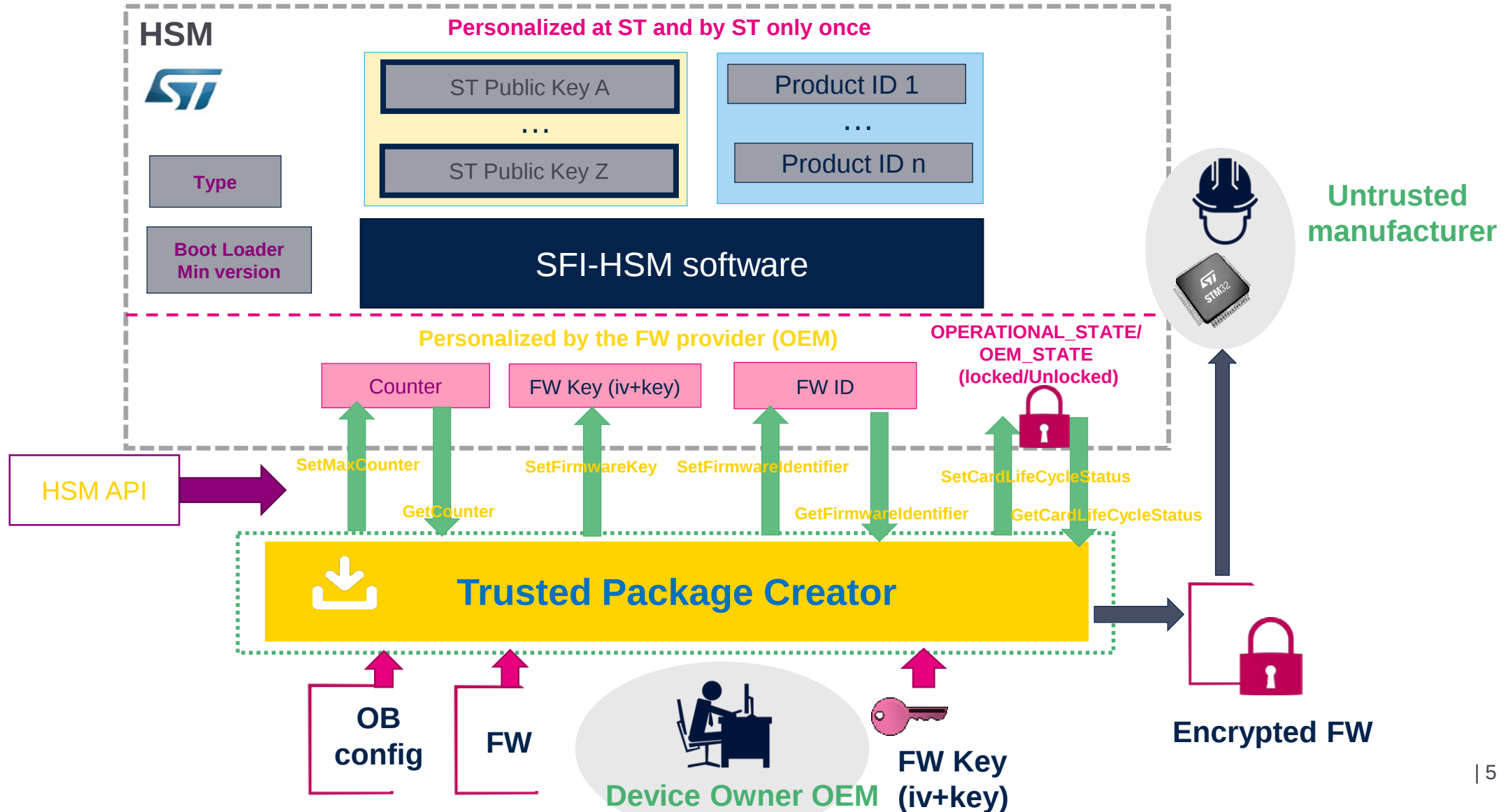
- ➡ Hardware/Silicon flow
- ➡ Encryption keys flow
- ➡ Software flow



SFI 过程中的技术实现



SFI 过程 . OEM方的技术实现



SFI 过程 . 产线方的技术实现

HSM

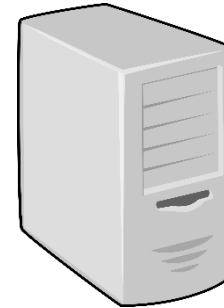
1. Check certificate using **ST Public Key**
2. Check chip **Product** type and version
3. Generate license using certified **Chip Public Key**
4. **Count** number of chip license requests



OEM-CM

Production line

This Chip **Certificate**



SFI Image
Encrypted **FW** +
Config



life.augmented

- 实现原理
 - STM32芯片里预置身份信息（公私钥对、ST证书）、安全服务代码
 - 固件加密工具软件、固件安全烧录工具软件
 - 可控制烧录次数和生成licenee文件的HSM
- 目前已经支持SFI服务的STM32系列
 - L462CE、H753、H7B3、L5全系列
 - 其他型号，可根据客户要求定制
- 相关资料
 - AN4992, SFI服务概览
 - UM2238, STM32 trusted package creator工具软件介绍
 - AN5054, 使用STM32Cubeprogrammer做安全烧录

Type	Part numbers	Order code
Microcontrollers	STM32H753xl	All order codes supported (refer to datasheet ordering information section)
	STM32H7B3xl	
	STM32L462CE	STM32L462CEU6F ⁽¹⁾
	STM32L5xxxx	Entire STM32L5 Series, referred hereafter as STM32L5



谢 谢

© STMicroelectronics - All rights reserved.

The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.

