



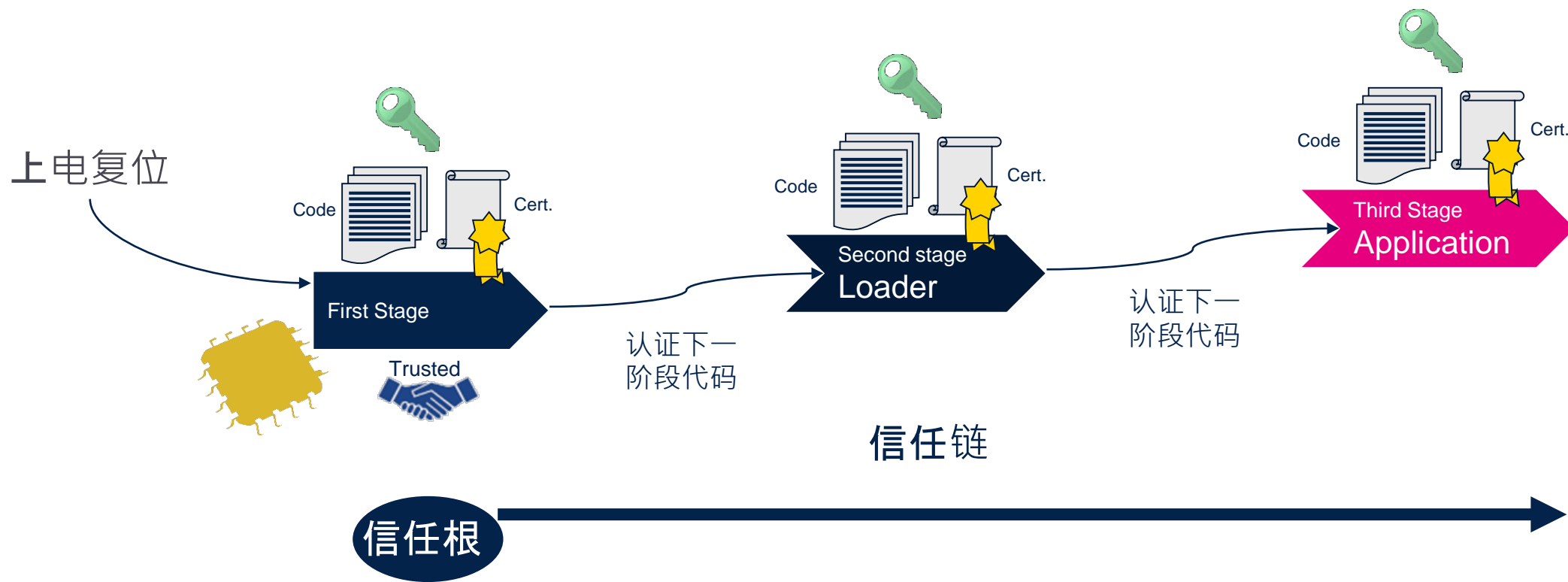
life.augmented

STM32 生态系统 第十八期

信息安全 . Information Security

9. SBSFU原理介绍

2020.03



- 信任根/Root of Trust

- 唯一启动入口
- 启动代码不能被bypass
- 启动代码不能被修改

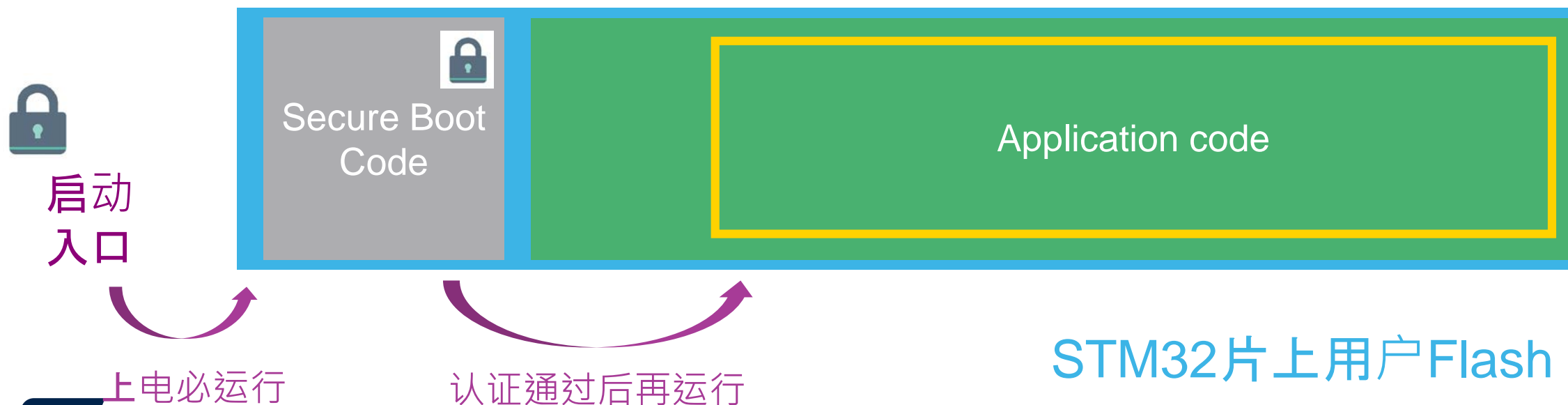
- 安全启动代码

- 检查和设置当前安全环境
- 认证下一阶段要运行的代码
- 认证通过才跳转执行

安全启动，作为信任根

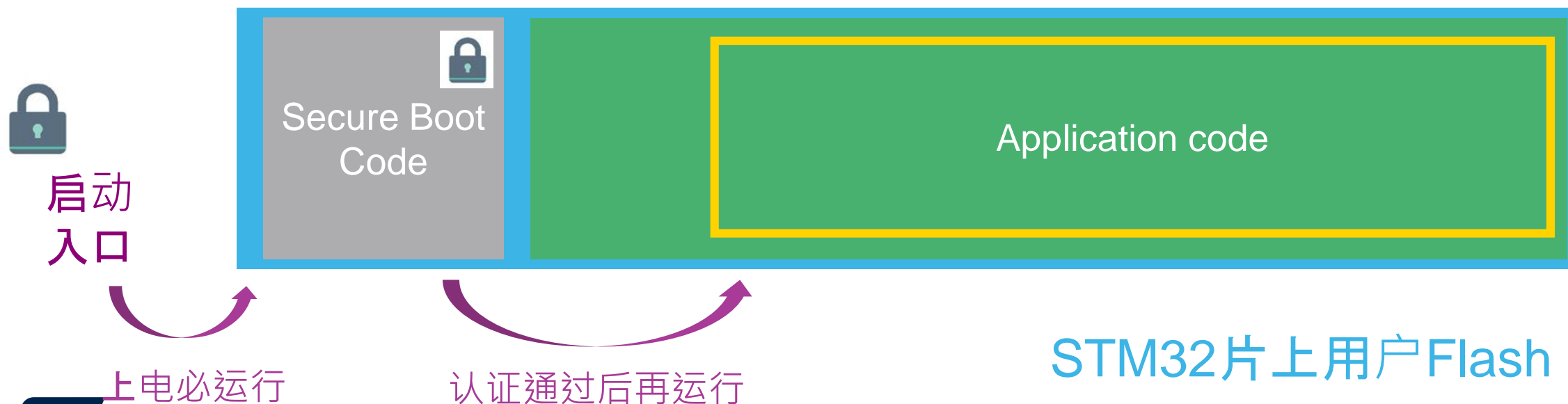
- 安全启动，和用户应用一样，都是一段代码，放在片上的用户闪存中
- 复位后运行的代码只能是这段“安全启动”
- 这段“安全启动”代码，由用户开发，设备出厂后不能再修改

} 信任根



安全启动，如何认证下一阶段代码

- “安全启动”代码，检查应用代码的签名，核实(广义的) “message integrity”



消息认证/message authentication

Hash函数

- SHA-2

结合对称加解密技术

结合非对称加解密技术

消息认证

- HMAC, AES-GCM
- 使用RSA/ECC签名

狭义
完整性

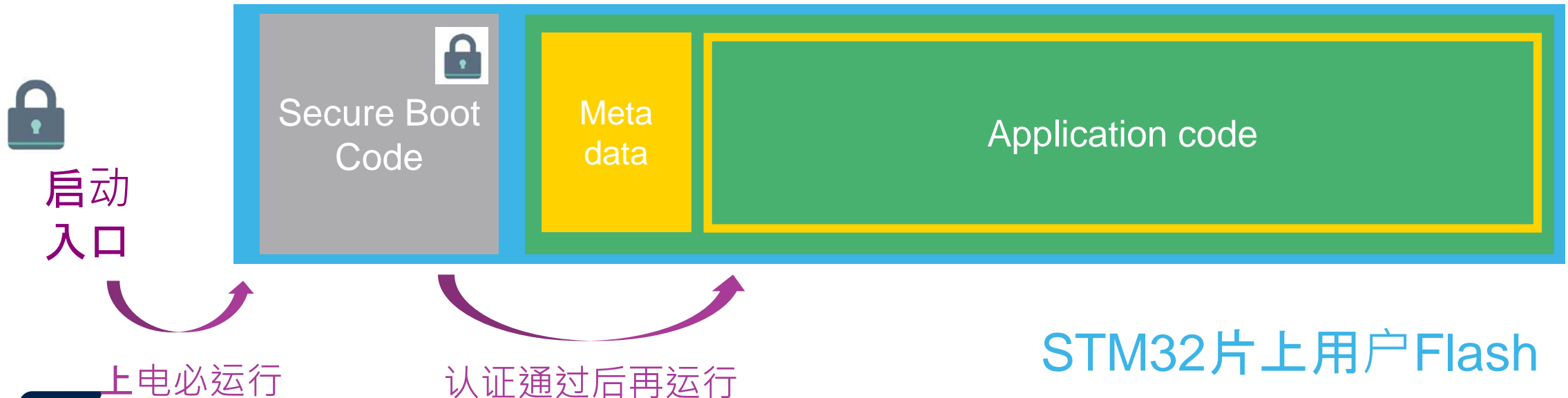
消息没有改变

消息确实是期望
的发送方发过来的

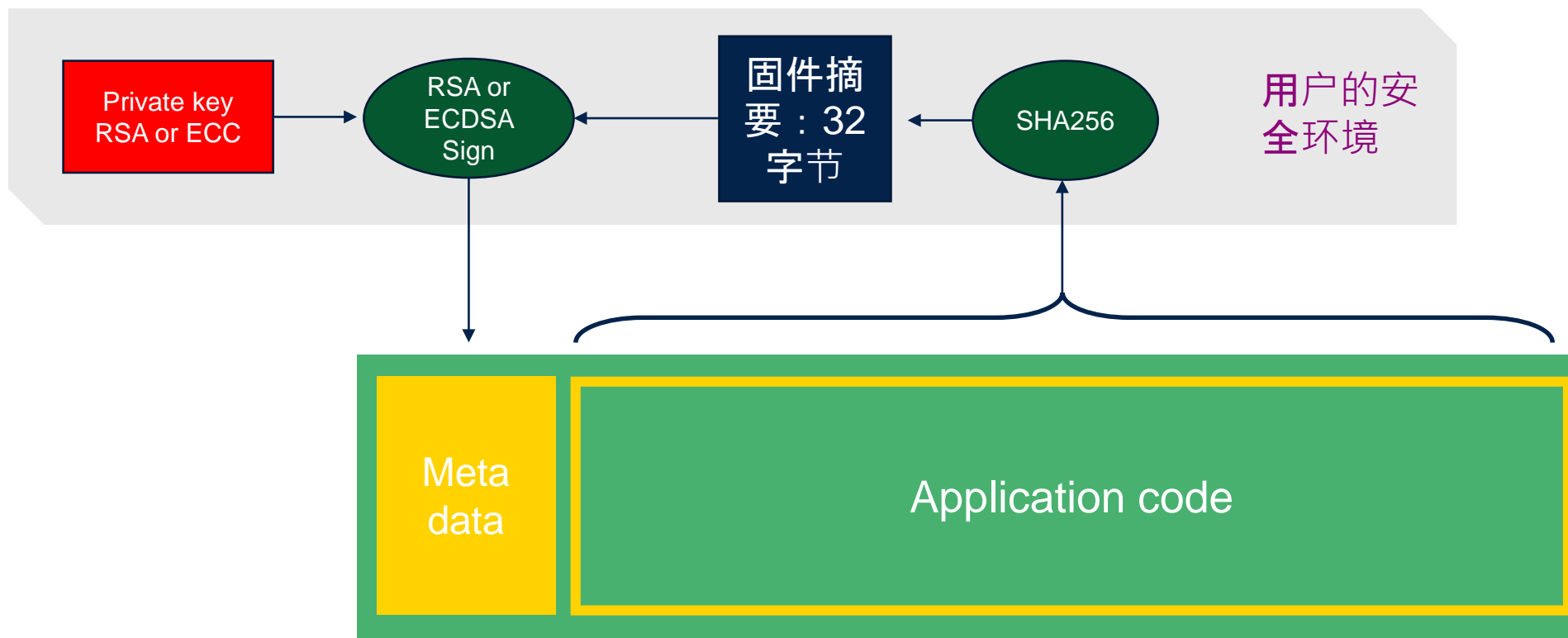
广义
完整性

安全启动，如何认证下一阶段代码

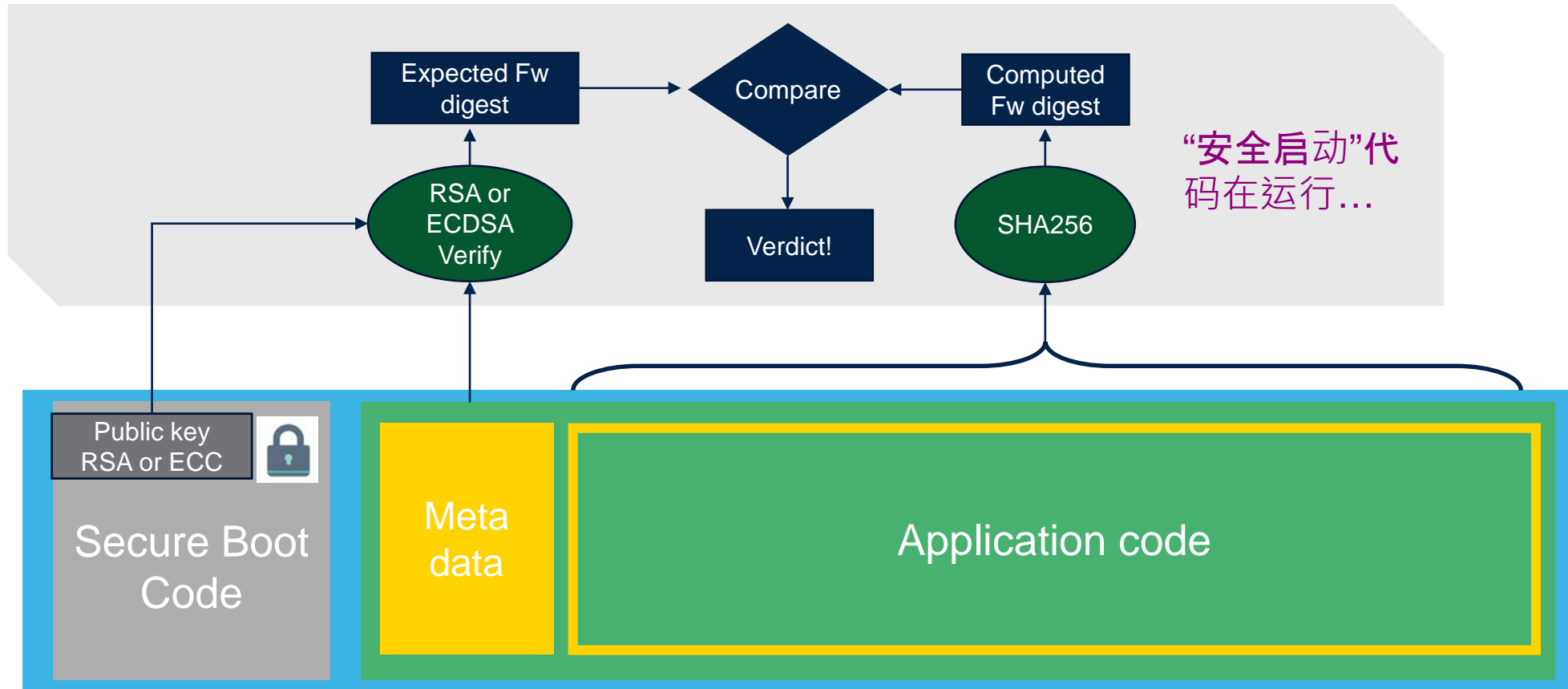
- “安全启动”代码，检查应用代码的签名，核实(广义的) “message integrity”
- 签名以应用代码元数据//Meta data的形式提供



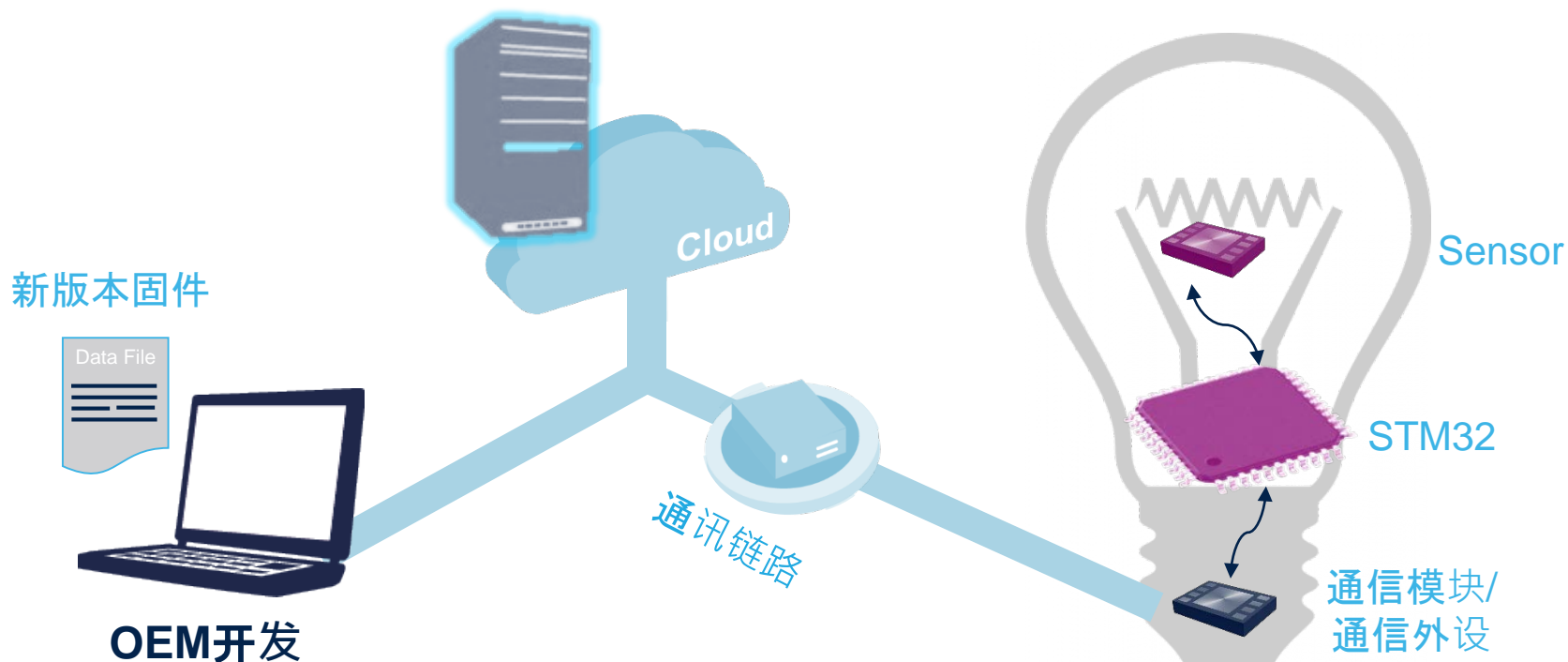
签名//元数据 是如何生成的



签名//元数据 是如何被校验的



安全固件更新

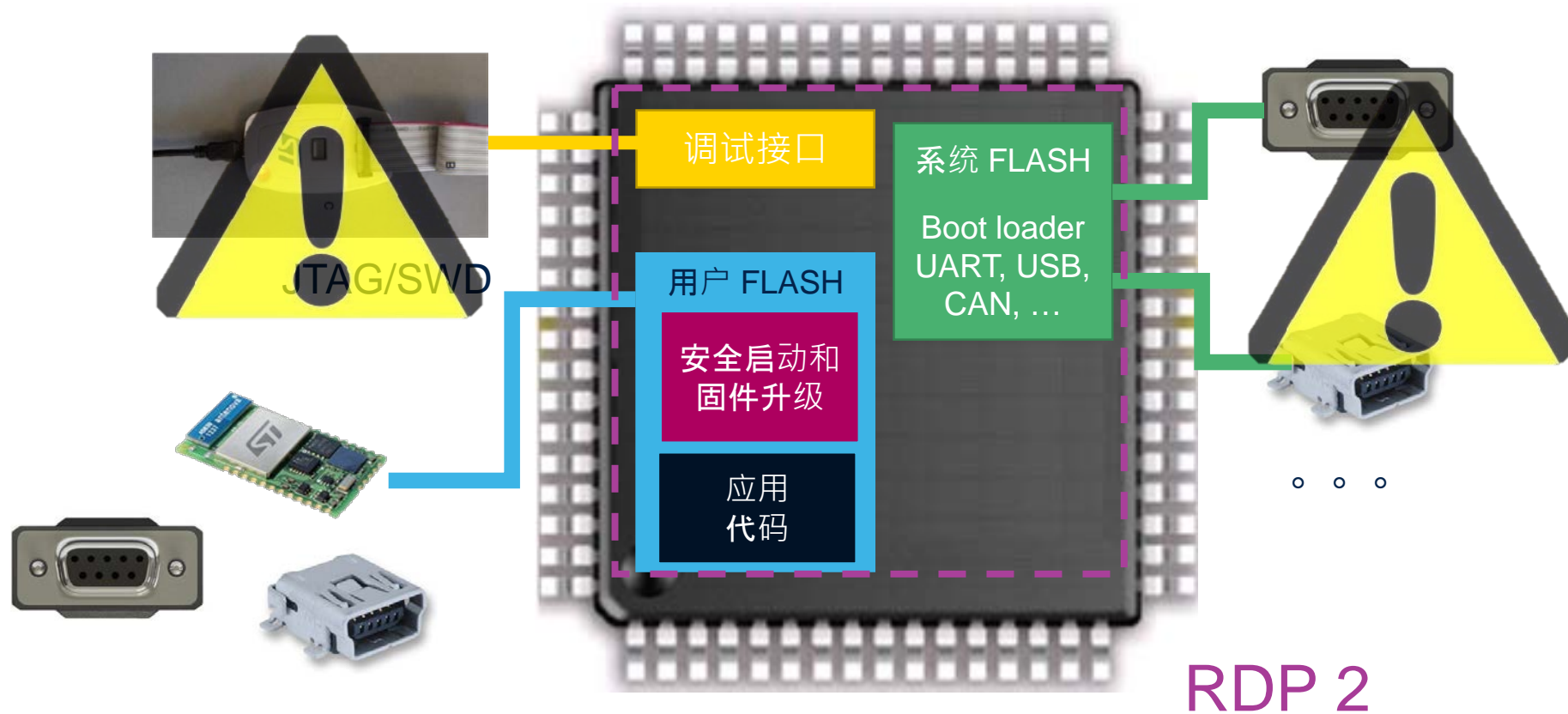


• 安全固件更新 /SFU

- 固件保密（可选）
- 固件完整未被篡改
- 固件来源可靠
- 传输安全
- 入口 → 安全启动

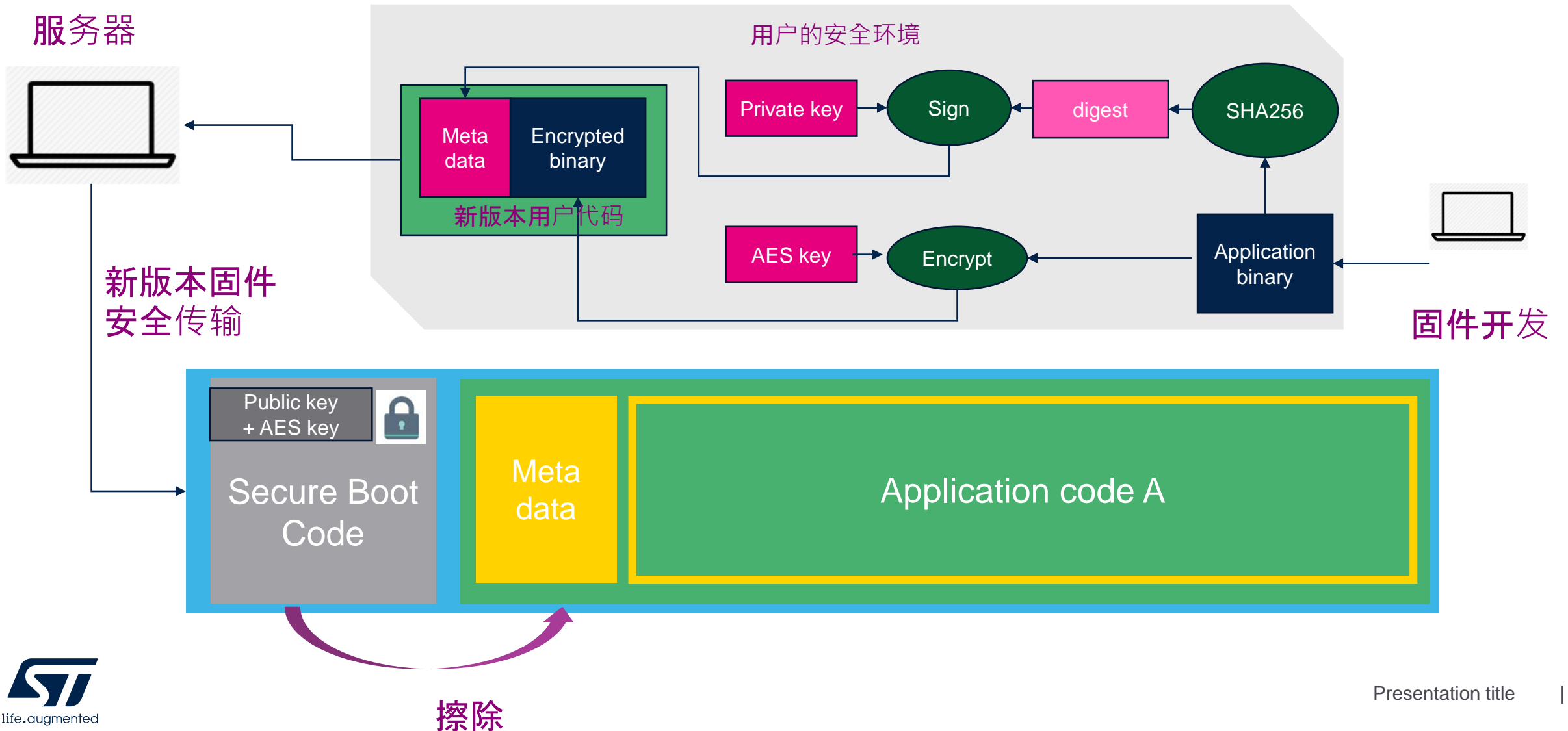


安全固件更新 对入口的要求

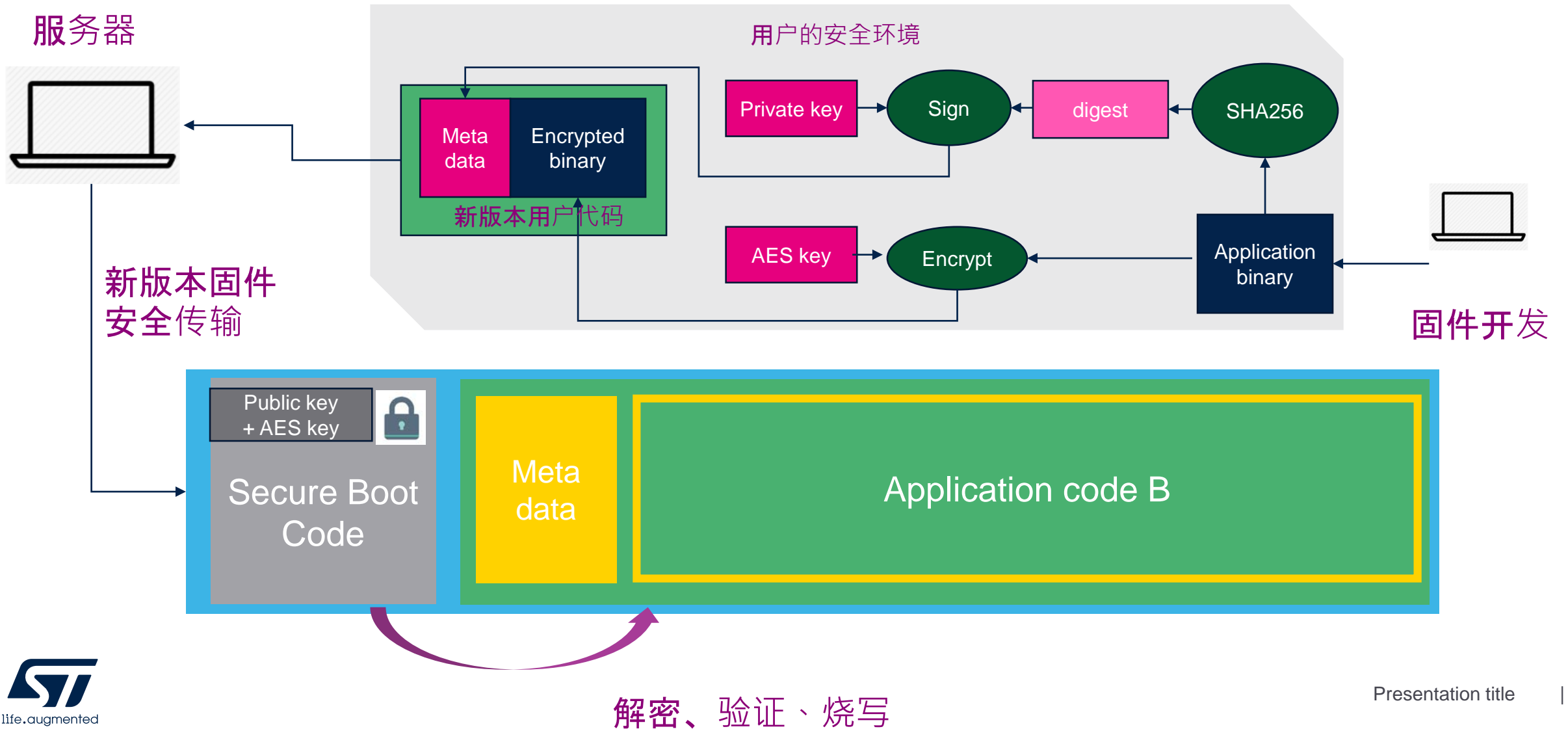


安全固件更新

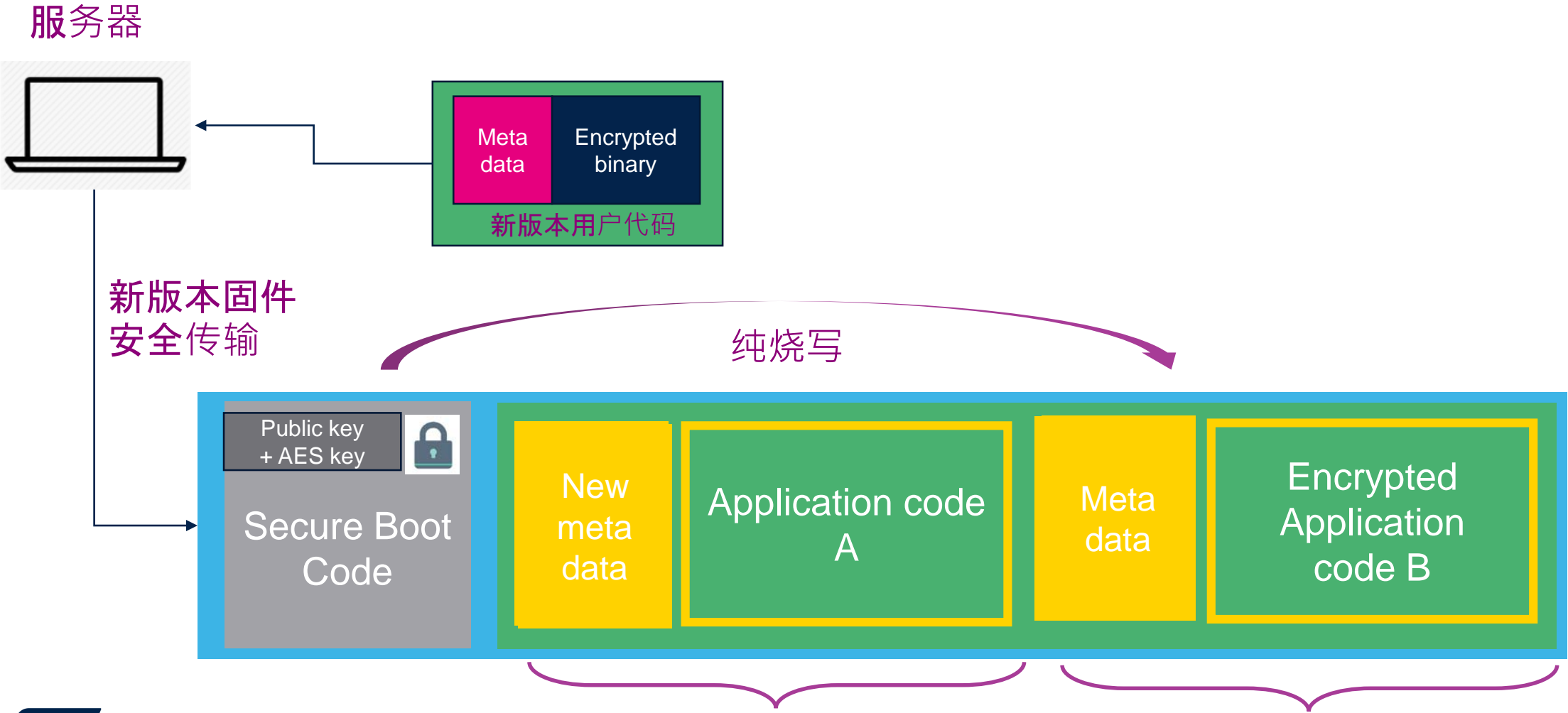
安全固件更新 原理 – 单image



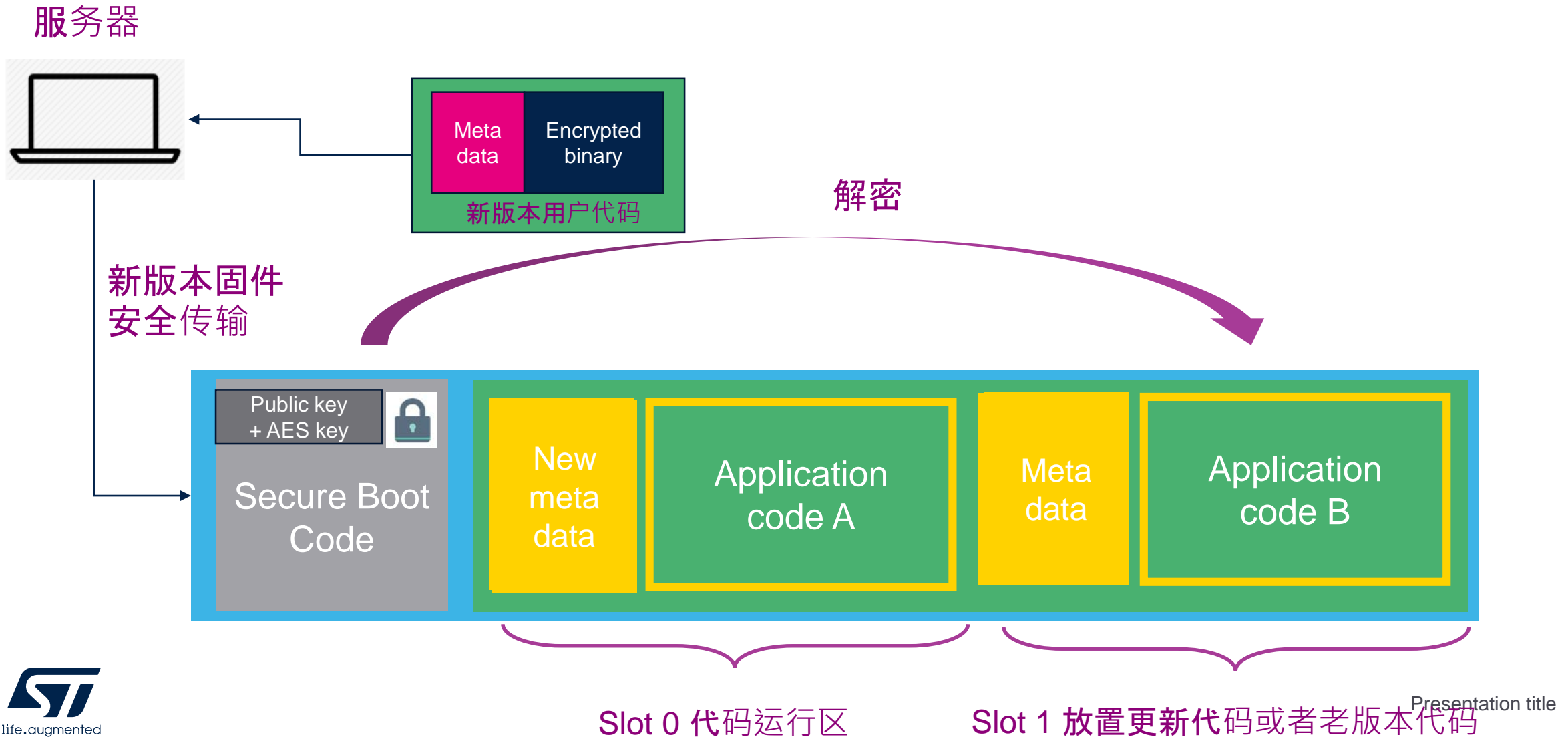
安全固件更新 原理 – 单image



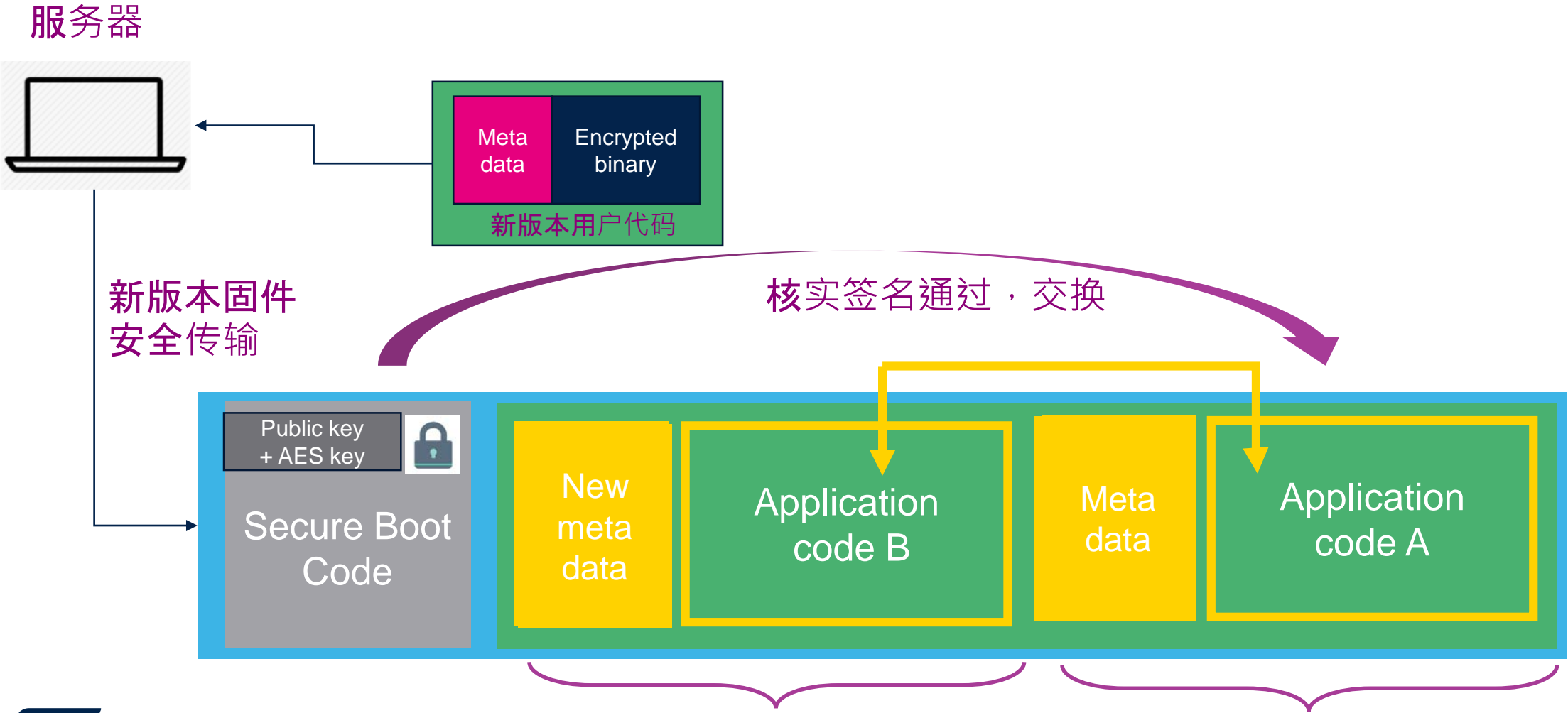
安全固件更新 原理 – 双image



安全固件更新 原理 – 双image



安全固件更新 原理 – 双image



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.

