如何使用STSAFE-A防止对象遭受克隆和伪造

目录

4 伪造：一种切实存在的威胁
5 提供身份验证解决方案STSAFE-A
6 身份验证过程工作原理
7 使用STSAFE-A确保安全加密稳健性
8 结论

伪造：
一种切实存在的威胁

多年来，企业一直饱受伪造行为的困扰。伪造行为通常与奢侈品有关，但其影响范围也扩展到了耗材、配件和外设等电子器件。

所有对象都面临伪造风险...

墨盒、电池、医疗耗材和电子器件配件在我们日常生活中无处不在。虽然这些物品看似基本且需要定期更换，但它们是许多企业业务模式的关键组成部分，对其解决方案的质量至关重要。

4640亿美元

2019年国际贸易中假冒产品的交易额[1]

...产生严重后果

如果在器件或解决方案中使用耗材的复制品或克隆品，则会产生各种不利后果。可能会在收入损失、安全性和品牌形象方面产生显著影响。

是否有解决方案？

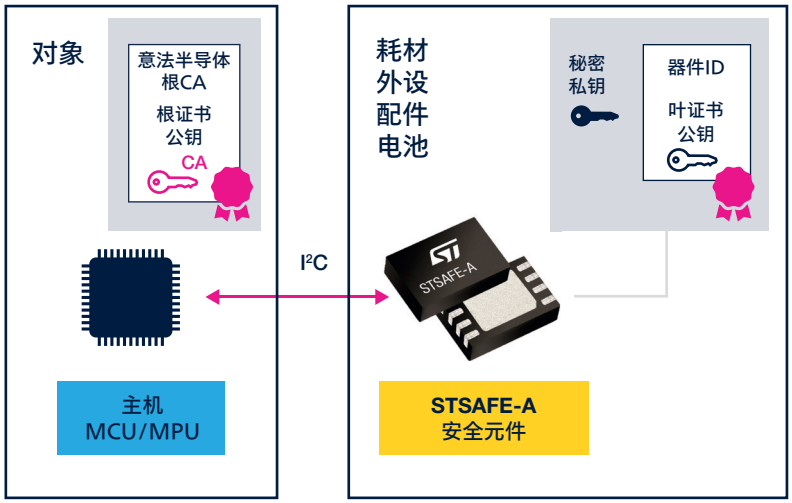
如果器件制造商能够在其产品中内置可靠的身份验证解决方案，从而快速准确地辨别对象真伪，那会怎样？

来源1：https://www.oecd-ilibrary.org/sites/74c81154-en/index.html?itemId=/content/publication/74c81154-en

提供身份验证解决方案
STSAFE-A

关于STSAFE-A

STSAFE-A是一种能够对对象进行严格身份验证的解决方案。STSAFE-A基于经过独立第三方认证的安全元件，具有定制的命令集，可执行器件身份验证并监控器件使用。



用于产品身份验证的优化片上系统(SoC)

STSAFE预先加载了机密信息和X.509证书，可执行严格的对象身份验证。其中还包含一个基本应用编程接口，可实现用于身份验证的安全协议。

对象本地主机MCU/MPU的配套芯片

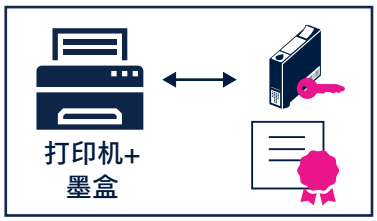
STSAFE-A通过一个简单的I²C接口连接到本地主机。

在意法半导体安全生产基地进行个性化处理

在意法半导体安全生产基地，可以使用客户特定的对象机密信息对STSAFE-A进行个性化处理。

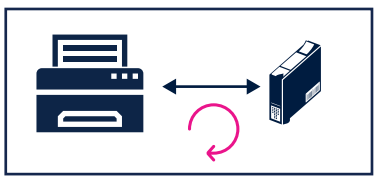
产品功能

为了确保最终产品的真实性，STSAFE-A提供三个主要功能：



验证对象真伪

STSAFE-A拥有基于非对称ECDSA协议和X509证书的身份验证协议。其中内置包含器件唯一标识的器件叶证书。意法半导体还充当证书颁发机构(CA)，并提供根证书来证明STSAFE-A叶证书的真实性。具体来说，以打印机及其墨盒为例，打印机将能够验证墨盒的真伪。



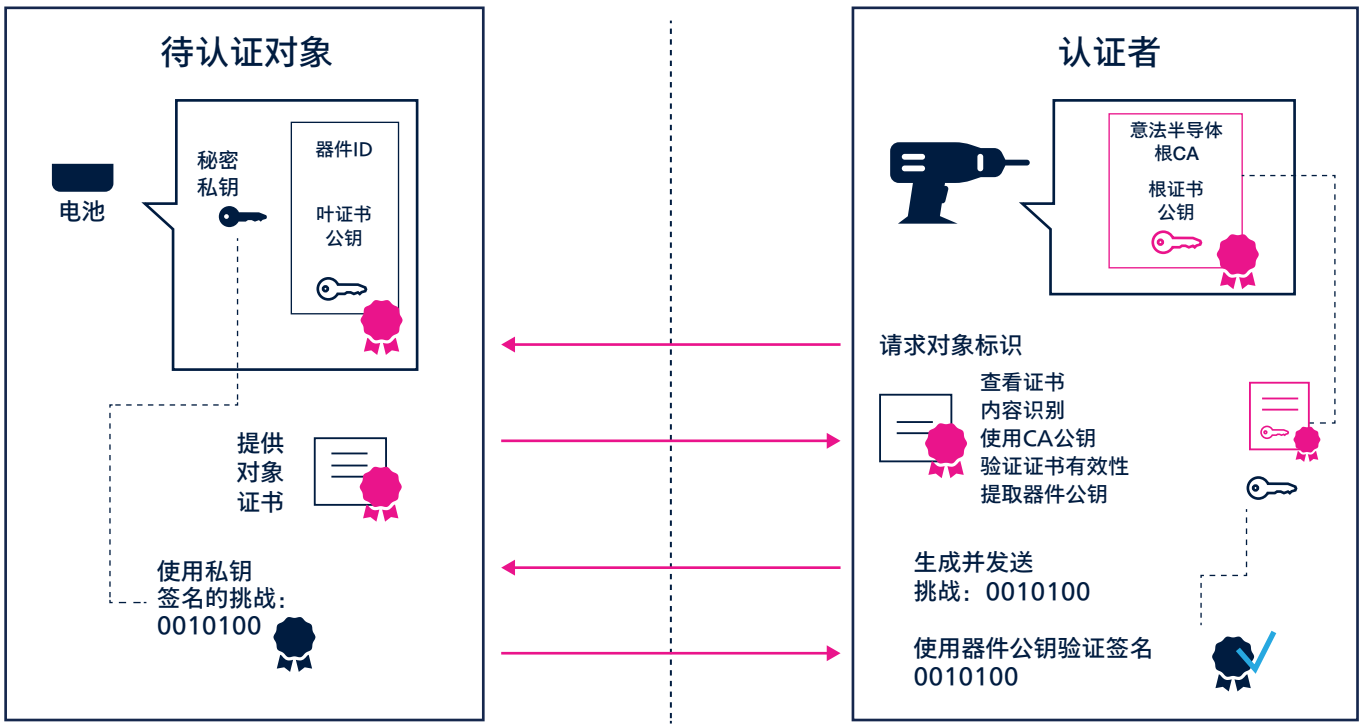
跟踪使用次数

STSAFE-A具有安全计数器，支持跟踪器件的使用次数。例如，打印机可以跟踪墨盒的使用次数。

安全存储数据

此外，STSAFE-A内置非易失性存储器，用于存储器件信息和机密信息。此存储器可以分区，并且能够设置访问条件以确保数据的安全存储。

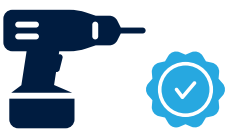
身份验证过程工作原理



STSAFE-A是一种安全元件，用于嵌入到需要身份验证的对象（在本用例中为电池）中。该安全元件内含电池证书，其中包含一个公钥和一个秘密私钥。相反，电钻充当验证器，其中包含证书颁发机构(CA)及其公钥。

电钻是如何对其电池进行身份验证的？

1. 该过程始于电钻向电池请求对象标识。
2. 电池向电钻提供其证书
3. 然后，电钻使用其CA公钥 验证证书的有效性
4. 证明有效后，电钻从电池证书中提取公钥
5. 电钻生成一个挑战并将其发送到电池
6. 该使用秘密私钥 签名的挑战被发送回电钻
7. 最后，电钻使用之前从电池证书中提取的公钥 对该挑战的签名进行验证



身份验证完成
正品电池

使用STSAFE-A确保安全加密稳健性

先进的认证安全性，可保护机密信息

STSAFE-A基于前沿的安全加密技术，类似于银行卡和数字身份证所使用的技术。STSAFE-A是一种安全元件，其中包含复杂的反制措施，可有效抵御物理和逻辑攻击。

安全加密反制措施	防止遭受远程攻击	防止芯片遭受攻击	经公认的外部权威机构认证

意法半导体安全元件及其开发环境和生产过程均由外部独立实验室和认证机构定期进行审核和认证。

这些独立组织负责确认意法半导体的解决方案是否符合严格的安全标准。例如，STSAFE-A110已通过通用标准(CC) EAL5+ AVA_VAN5认证。

意法半导体可确保配置安全

在意法半导体安全生产基地，可以使用器件机密信息和证书对STSAFE-A进行个性化处理。此项服务的最小订单量(MOQ)为5 Ku。

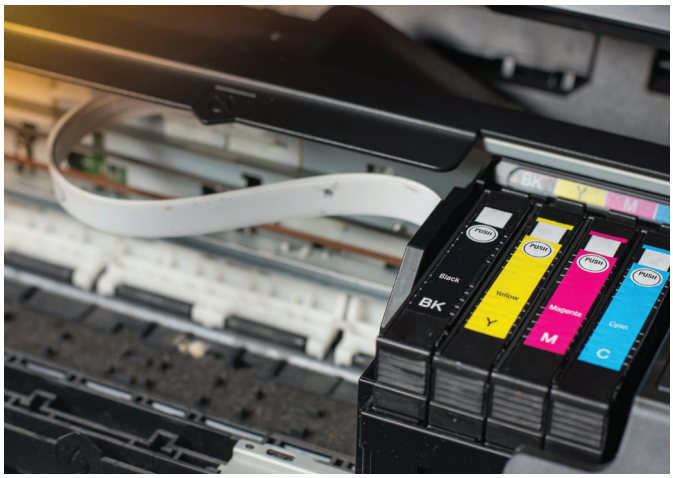
给器件和耗材制造商带来的优势

- 无需处理敏感数据或机密信息
- 无需对客户生产线进行专项投资
- 无需对安全技能进行专项投资
- 无需在线加载数据
- 无生产停滞的风险
- 客户可以选择外部合作伙伴或EMS，无需担心安全问题

结论

STSAFE-A是一种片上系统(SoC)解决方案，利用先进的硬件安全加密技术提供适用于各种对象的简单可靠身份验证解决方案。

为了简化对象生产过程并确保其安全，在意法半导体安全生产基地，可以使用客户特定的信息对STSAFE-A进行个性化处理。最后，STSAFE-A拥有全面的硬件和软件生态系统，便于不具备特定安全知识的器件制造商能够轻松进行集成。



想要实现更高目标?

了解关于我们产品的更多信息

联系您当地的意法半导体销售办事处或查找经销商

意法半导体致力于创造以人为本的技术解决方案

有关意法半导体产品和解决方案的更多信息，请访问www.st.com

订购代码：**BR2403STSAFEA**