# 如何使用STSAFE-A基于联网对象提供安全服务

# 目录

# 联网器件市场概述

安全摄像头、水泵、心率监测器...
这些对象有一个共同点，那就是如今它们都已实现了联网。无论我们身处何方，是在家里、城里还是工业基础设施当中，身边都会环绕着形形色色的联网器件。推动这波“联网浪潮”的因素有很多，其中之一就是器件销售方式的改变。


## 从传统的业务模式...

在先前的销售模式下，企业通常会在商店中出售器件。尽管这种销售模式存在一些优势，但缺点同样不容忽视。其中最大的一个缺点就是销售一台器件只能产生一次性收入，而且企业很难从客户口中得到有关使用体验的反馈。

## ...转向基于服务的销售方法

有鉴于此，企业纷纷对原有的业务模式进行了扩展——开始销售额外的周期性服务。该销售方法不仅能够增加企业的经常性收入和提升客户粘性，而且有助于企业获得客户的直接反馈。

## 新兴技术的蓬勃发展推动了这一过程

多项新兴技术的出现推动了这一业务模式的演变过程，其中包括带有传感器和执行器的联网对象、云端数据处理和人工智能 (AI) 等等。

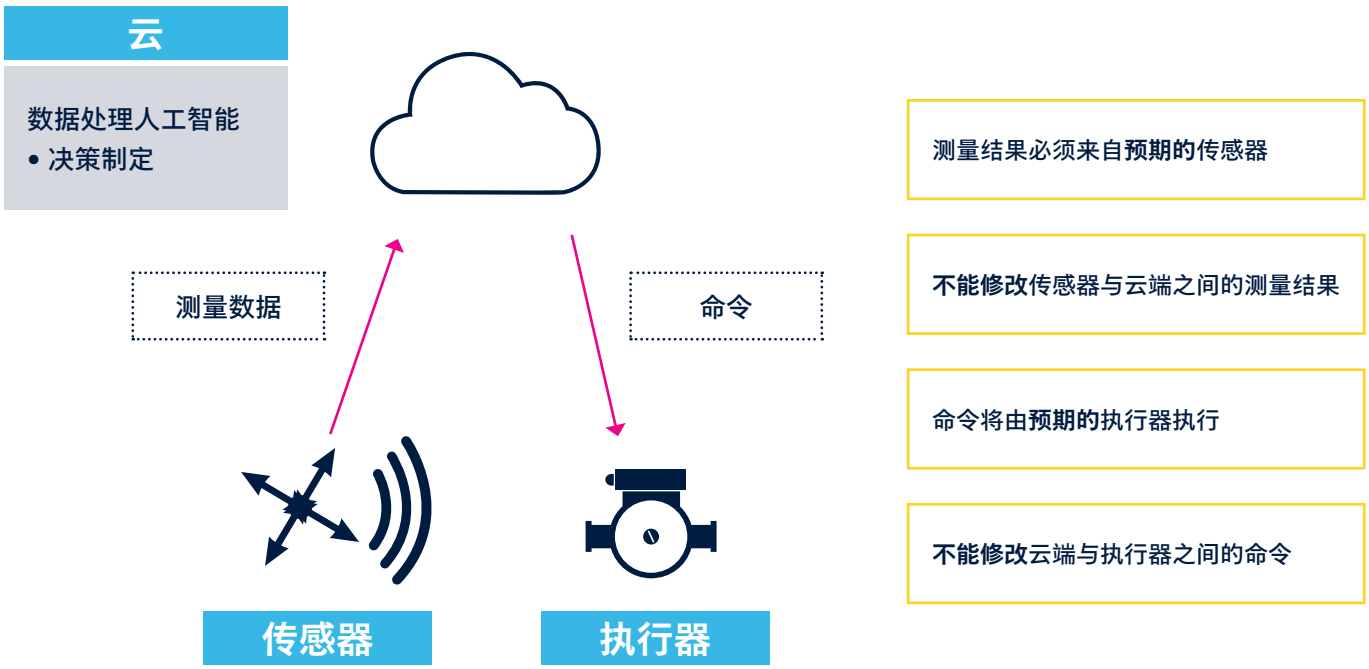
# 联网器件原理简介

## 这种基于服务的业务模式的条件

如需实现此种业务模式，我们需要满足以下三个条件：

- 服务必须可用
- 服务必须可靠
- 服务必须保证客户信息的隐私性

请注意，在此种业务模式下，客户需要为相关服务支付费用。因此，他们对服务品质的预期也会更高。



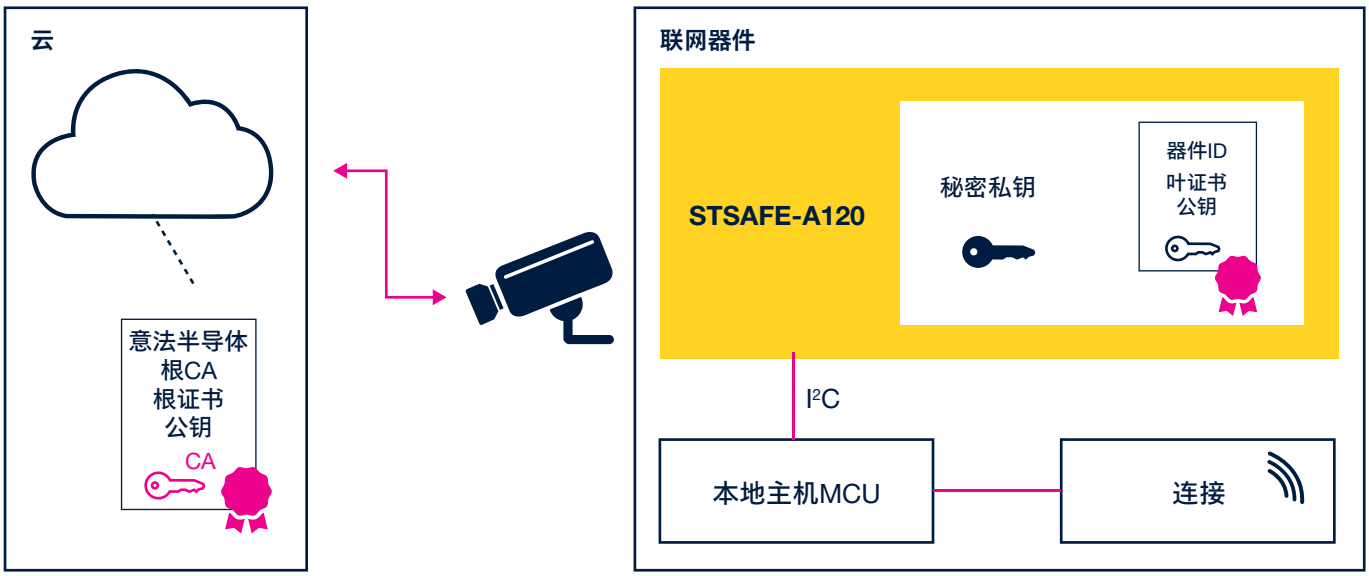

为确保满足上述四项要求，我们可以实施以下两项措施：

- **传感器和执行器身份验证：**为了确保由一侧的预期传感器提供测量结果，并由另一侧的预期执行器执行命令，我们需要对这两个器件分别进行身份验证。
- **数据和命令签名与加密：**为了确保一侧的传感器和云端之间不会修改测量结果，且另一侧的云端和执行器之间不会修改命令，我们需要对数据和命令进行签名和加密。

# 提供身份验证解决方案
# STSAFE-A

## STSAFE-A简介

STSAFE-A是一种能够对对象进行安全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X509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

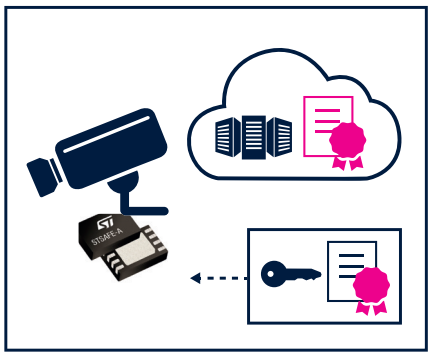
STSAFE-A通过一个简单的I²C接口连接到本地主机。

## 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。

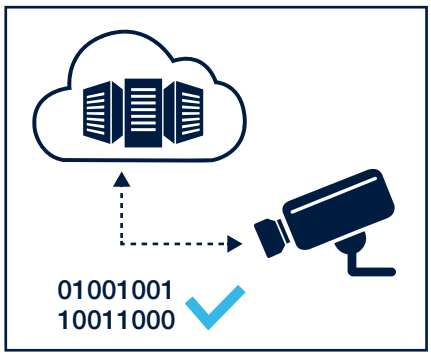
## 关键产品功能

为确保实现与云端的安全连接，STSAFE-A将负责执行以下四项主任务：



### 执行器件身份验证

STSAFE-A预装有X509证书以及用于执行器件身份验证的安全协议。

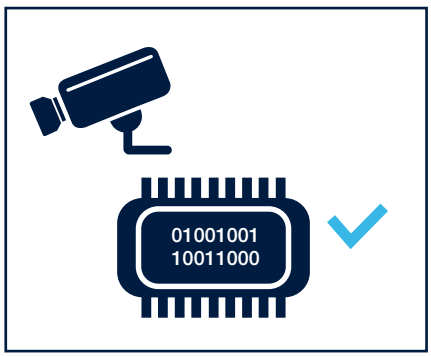



### 创建与云端的安全连接

STSAFE-A将通过数据签名和/或加密来确保已交换数据的完整性和保密性例如，系统将对安全摄像头和基于云的服务器之间交换的数据进行签名和/或加密处理。

### 安全存储连接凭据和敏感数据

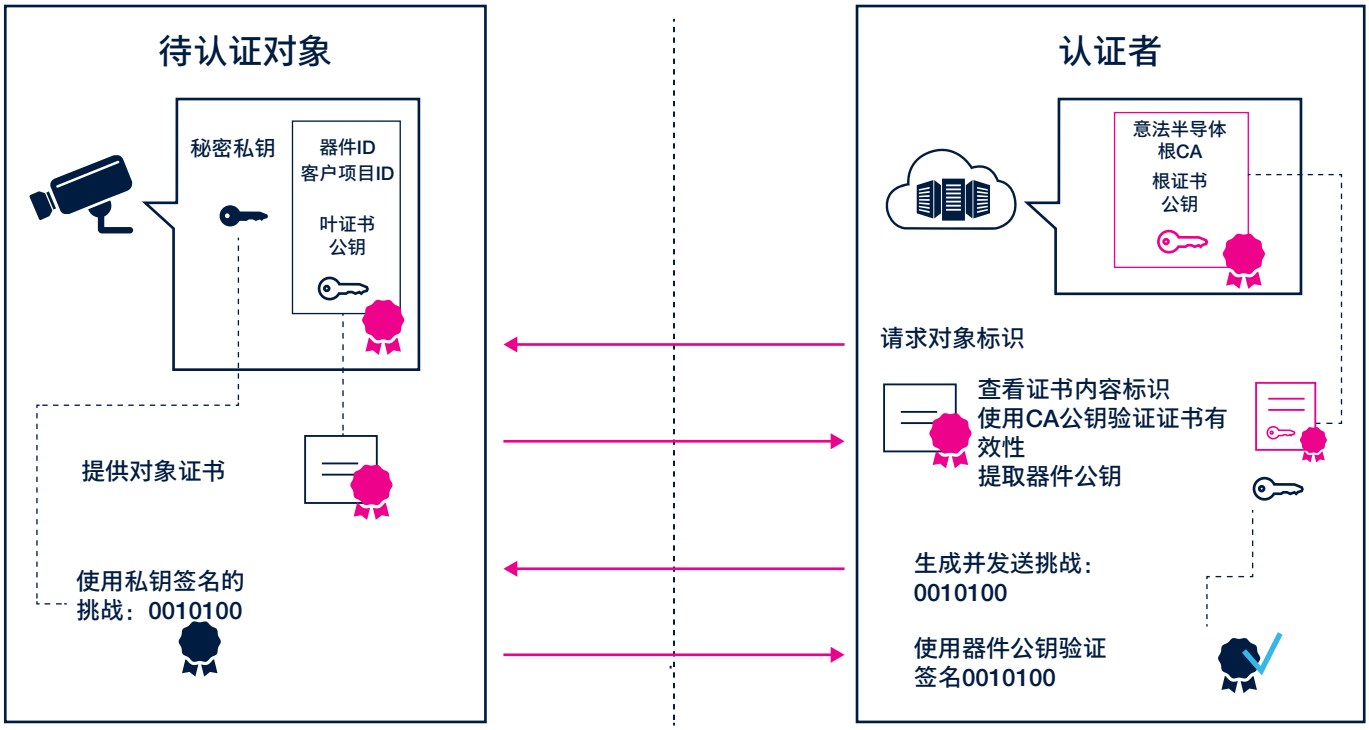
STSAFE-A可确保将凭据和敏感数据安全地存储到安全元件 (SE) 存储和器件的非易失性存储器 (NVM) 中。




### 验证器件固件与更新的完整性

STSAFE-A将在初始启动时和固件更新时对器件应用固件的签名进行验证。

# 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（在本用例中为摄像头）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，云端充当验证器，其中包含证书颁发机构 (CA) 及其公钥。

## 云端如何对摄像头进行身份验证？

1. 该过程始于云端向摄像头请求对象标识。
2. 摄像头向云端提供其证书。
3. 然后，云端使用其CA公钥 验证证书的有效性。
4. 证明有效后，云端会从摄像头证书中提取公钥 。
5. 云端生成一个挑战并将其发送到摄像头。
6. 该挑战会使用秘密私钥 进行签名，然后发送回云端。
7. 最后，云端使用之前从摄像头证书中提取的公钥 对该挑战的签名进行验证。

认证完成
预期摄像头

# 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。

| 安全性反制措施 | 防止遭受远程攻击 | 防止芯片遭受攻击 | 经公认的<br>外部权威机构认证 |
|---|---|---|---|

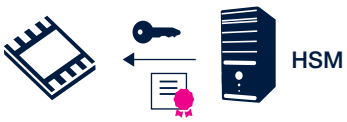
意法半导体安全元件及其开发环境和生产过程均由外部独立实验室和认证机构定期进行审核和认证。

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。

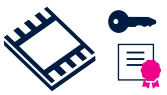

## 意法半导体可确保配置安全

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5000 pcs/单。

芯片开发和封装




使用客户信息进行
个性化处理



发货给客户

## 给器件和耗材制造商带来的优势

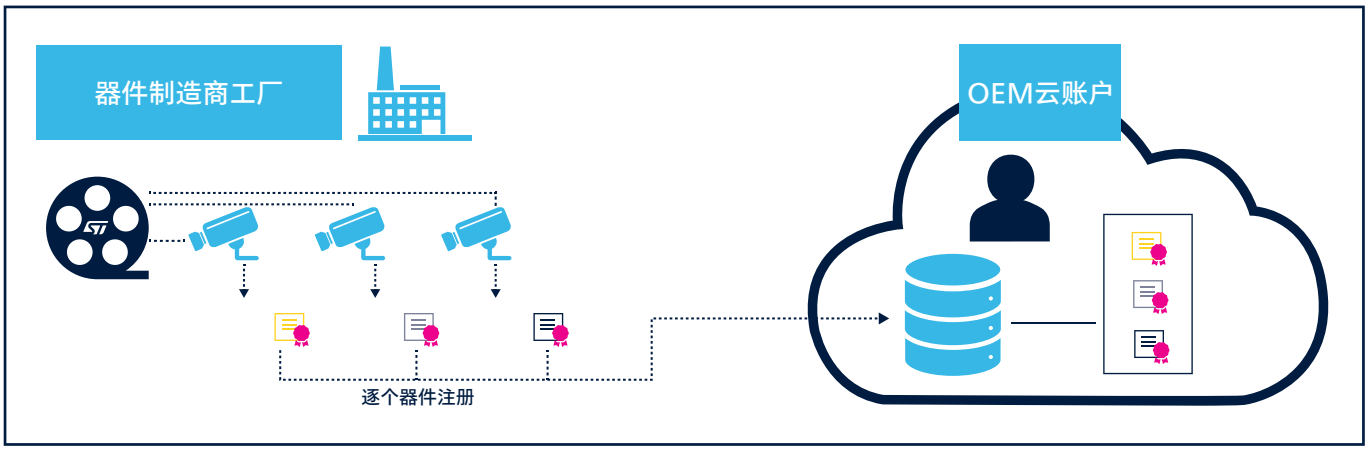
- 无需处理敏感数据或机密信息
- 无需对客户生产线进行专项投资
- 无需对安全技能进行专项投资
- 无需在线加载数据
- 无生产停滞的风险
- 客户可以选择外部合作伙伴或EMS，无需担心安全问题

# 使用STSAFE-A将联网对象注册到云账户

对于基于联网对象的服务，其安全性取决于该服务能否针对各类对象执行严格的身份验证。该身份验证要求OEM在将对象投放市场之前，将其注册到目标服务。他们可对器件进行逐一注册，也可预先注册整个器件系列。

## 将单个器件注册到云账户

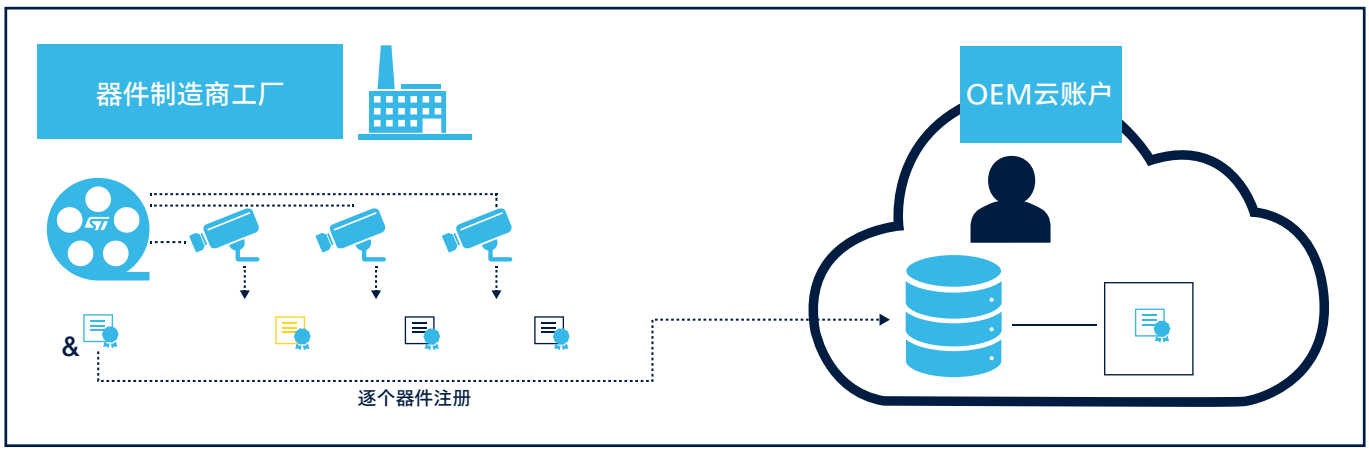
每个STSAFE-A都预装有包含唯一ID和密钥的X509证书，以便执行身份验证。拥有X509证书的云账户可使用该证书对安装有STSAFE-A的联网器件执行严格的身份验证。每个器件均可注册到云账户，方法是将其X509证书注册到云账户。



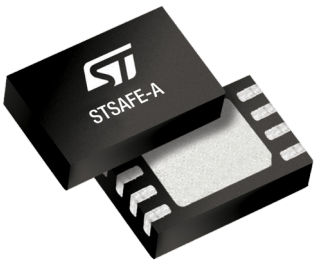

## 将单个器件注册到云账户

可通过注册单个器件系列证书，将整个器件系列注册到云账户。

器件制造商可仅需满足5K单位的最小订单量，即可向意法半导体申领此系列证书。这使得器件制造商无需逐个读取所有STSAFE-A的X509证书。



# 总结




STSAFE-A安全元件是一款基于先进硬件安全认证的优化型片上系统 (SoC)，可为器件身份验证提供简单易行的解决方案。

为保证实现较高的安全级别，我们在意法半导体安全制造工厂中对STSAFE-A的器件信息（X509证书）进行了个性化处理。

此外，STSAFE-A还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
# 科技始之于你

**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：**BR2404STSAFEACDEV**