DATASHEET

为IOT设备制造商提供灵活的单芯片身份

使用Intrinsic-ID的设备指纹技术和GlobalSign的高容量证书服务，以低成本提供唯一的，基于硬件的安全身份

intrinsici - id的身份识别算法是利用现有的SRAM来创建植根于硬件的独特的、不可欺骗的设备指纹。 GlobalSign对这些指纹进行认证，并增加了PKI功能，从而创建了在IOT生态系统中可以信任的强大设备标识。

不可克隆密钥意味着不可克隆设备

物联网提供商需要解决关键的安全问题，包括身份验证，隐私和完整性。GlobalSign的云规模PKI服务可以发布和管理设备的标识和身份验证凭据，从而使制造商能够在其产品和生态系统中构建并部署强大的身份策略。

改造并增强现有设计的安全性

可以将基于软件的SRAM PUF改装到现有的微处理器中。

单芯片解决方案简化了设计并降低了成本

利用现有微处理器的安全功能，无需使用外部加密芯片-减少了零件数量并降低了成本。考虑：

- 无芯片-芯片接口总线可确保安全
- 无需驱动程序或接口库
- 没有芯片实现共享的隐私数据
- 减少零件数量

为IoT的公钥基础设施

基于PKI的设备身份凭证可实现身份验证，隐私性和数据完整性-这对于IoT部署至关重要。

物联网广泛的互操作性

由SRAM PUF生成的密钥，经GlobalSign认证并包含在X.509证书中，可为最受欢迎的IoT协议提供强大的设备身份验证，其中包括：

- HTTP
- MQTT
- WebSocket
- XMPP
- CoAP
- TCP
- UDP
- SSL / TLS / DTLS

产品优势

凭借强大的设备标识，智能设备制造商可以消除过度生产和伪造，并实现增值服务，例如选择性功能控制，预测性维护和智能分析。

GlobalSign和Intrinsic-ID的联合解决方案是一种经济有效的选择。经过验证的设备标识是基于硬件的且可以适应任何现有制造流程。

- 解决方案是对现有芯片进行改造；无需额外的硬件
- 不可克隆的临时密码密钥可防止欺骗性设备甚至最先进的侵入性硬件攻击
- 基于PKI的证书支持大多数流行的IoT协议的设备身份验证
- 具有ECC算法和简化证书请求格式的受约束设备的轻量级密码支持功能
- 高容量注册服务，每秒可发布数千个设备ID
- 供应流程是自动化的，可以构建到现有的生产流程中

为IOT设备制造商提供灵活的单芯片身份

DATASHEET

简化的设备标识

Intrinsic-ID和GlobalSign提供了一种灵活且可扩展的设备标识解决方案，该解决方案易于集成并适应现有环境，支持大量需求且不需要现场支持。

■ 自动配置和注册

将身份供应集成到现有的制造工作流中，以最大限度地提高吞吐量并简化物流。自动化IoT云平台注册任务，包括：

- 设备注册
- 角色和权限策略分配
- 与旧库存系统集成

■ 强大，安全的身份和密码解决方案

SRAM的初始状态提供了确定性信号分量，该信号分量可用于导出唯一的设备标识密钥对（Quiddikey）和非确定性噪声分量，这些噪声分量可作为为随机数发生器（iRNG）注入种子的良好熵源

从基于SRAM的PUF生成的独特指纹可以在各种工作条件（例如温度，电压和湿度等）下可靠地重建。

■ 基于云端的优势

借助GlobalSign的PKI经验和基础架构，基于云的配置可提供更高的安全性，保证的正常运行时间以及增强控制和审核功能。消除对现场设备的需求，可以提高扩展性并削减维护成本。

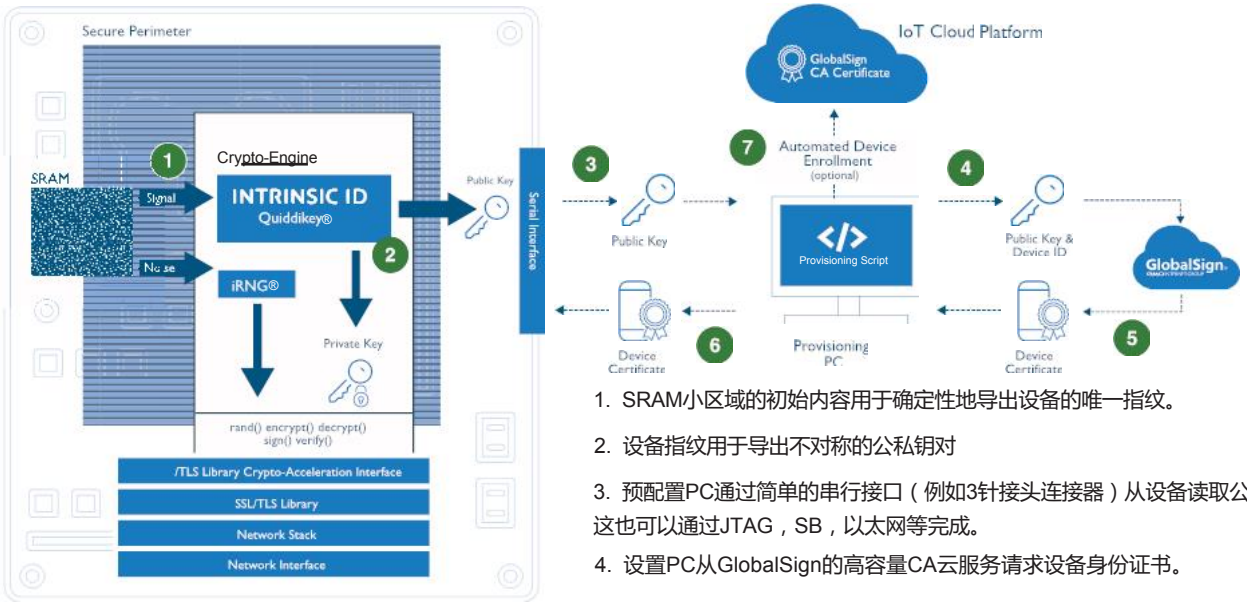
■ 规模和定制

GlobalSign的基于云的高容量证书发行服务是专门为满足最高产量需求而设计的。该服务非常灵活，可以支持各种PKI信任模型，加密算法，并使用较轻量级的证书注册，所有这些都可以满足受约束的IoT设备的需求。

可以提供内置到固件加载，功能测试或自定义编程操作中，并且可以支持各种编程接口，例如：

- UART / USART / RS-232
- USB / SPI / I2C
- Network / Ethernet / WiFi

工作原理-设备身份配置



1. SRAM小区域的初始内容用于确定性地导出设备的唯一指纹。
2. 设备指纹用于导出不对称的公私钥对
3. 预配置PC通过简单的串行接口（例如3针接头连接器）从设备读取公钥。这也可以通过JTAG，SB，以太网等完成。
4. 设置PC从GlobalSign的高容量CA云服务请求设备身份证书。
5. GlobalSign的高容量CA云服务向配置PC颁发设备身份证书。
6. 预配置PC将设备证书发送到设备以存储在非易失性存储器中。 设备身份配置现已完成。现在可以将设备身份证书用于SSL / TLS上下文中的身份验证。
7. （可选）可以将PC配置为云平台上的自动注册设备。

关于GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，致力于帮助全球的企业，大型企业，云服务提供商和物联网创新者保护在线通信，管理数百万个经过验证的数字身份，并自动进行身份验证和加密。 其高规格的公钥基础设施（ PKI ）和身份解决方案支持包括万物互联网IoE ）在内的数十亿服务，设备，人员和事物。

Tel: +86 02609522601
www.globalsign.cn

GlobalSign
GMO INTERNET GROUP