



## 基于PKI的物联网

### 物联网安全始于PKI

为什么我们要把事情联系起来...好处很简单...更好的控制，效率和优化。当所有的东西都连接在一起，相互交流，共同工作时，我们可以随时随地访问和控制这些东西，收集、共享和分析数据，以便更好地管理我们的家庭、我们的健康、我们的汽车、我们工作的环境和我们行业的运营。所有这些都导致了更高性能的系统，成本节省，效率和新的收入来源。

#### 物联网安全挑战

随着我们继续将越来越多的事物连接到互联网上，安全性变得越来越具有挑战性，风险也就越大。GlobalSign的物联网战略主要集中于高价值生态系统，例如工业物联网，在此工业中，企业依赖于“始终在线”连接的网络物理系统，安全基础设施以及数据安全性和隐私性。单个安全事件可能会对公司及其客户产生重大影响。物联网安全面临的挑战是，标准和框架目前还处于开发的早期阶段，而且还不清楚从何入手。公钥基础设施（PKI）是一种基于标准并已在当今设备中得到验证的安全技术。PKI多年来一直通过提供信任和高度保证来保护与网络连接设备的安全，使其能够管理物联网的数字证书和身份。

#### PKI入门

身份和信任是物联网安全不可或缺的组成部分通过为每个“事物”提供一个独特的身份，PKI应该成为任何物联网安全策略的基础。凭借独特而强大的设备标识，当设备联机时，可以进行身份验证，确保其他设备、服务和用户之间的安全通信，并证明其完整性。由于PKI是一项成熟的技术，因此可以立即在您的物联网生态系统中实施，并且在将它们引入时可以轻松地与物联网安全解决方案的其他组件集成。

### 为什么选择 PKI?

- 基于PKI的身份支持大多数流行的物联网协议的隐私，数据完整性和设备身份的验证
- 具有ECC算法和简化的证书请求格式的受限设备的轻量级密码支持功能
- 大容量注册服务，每秒可发布数千个设备id
- 全球超过2500万张证书依赖GlobalSign根提供的公共信任
- 可以构建到现有生产流程中的自动供应流程

## 安全设备身份

在实施物联网解决方案或制造连接设备时，应从一开始就内置身份和安全性。PKI支持的强设备标识可以实现物联网安全的基本原理：身份验证、加密和完整性。

### ■ 身份认证

当设备连接到网络时，它必须在其他设备、服务和用户之间进行身份验证并建立信任。一旦建立信任关系，设备，用户和服务就可以安全地交流和处理信息

### ■ 加密

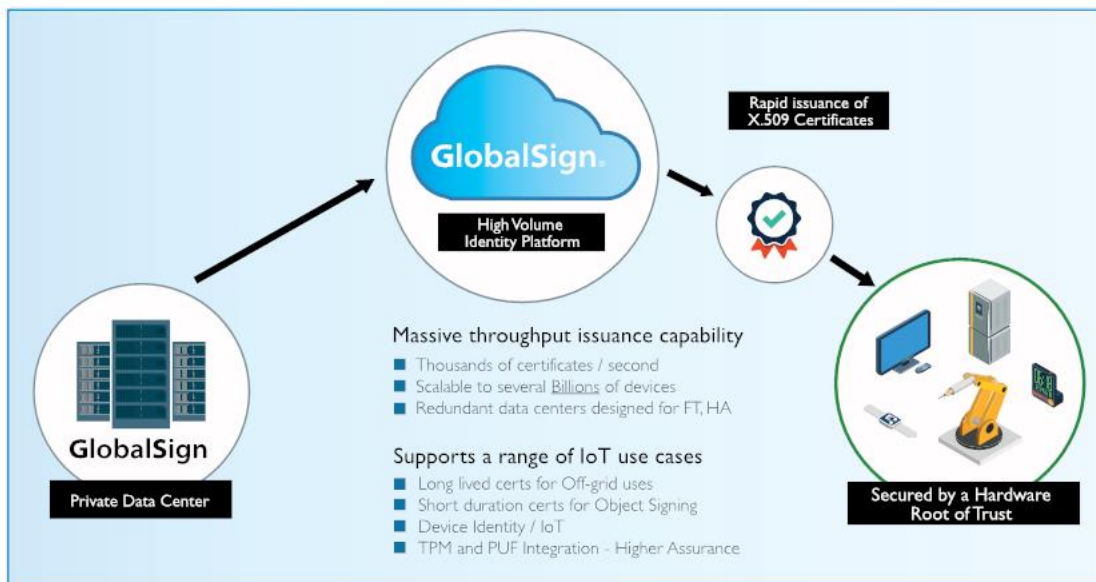
随着更多事物的连接，将生成，收集和共享更多数据。这些数据可能包括必须保持私密性和安全性的个人，敏感和财务信息-通常是在符合法规的情况下。与设备标识绑定的强大加密机制可以确保数据加密和通信安全，从而使正在传输的数据保持安全和私密

### ■ 诚信

设备的完整性始于证明它说的是什么。通过独特的强大设备标识，PKI可以确保设备，软件和固件是合法的

## 为什么要建立身份呢？

- **获得竞争优势**  
在您的物联网设备和服务中建立身份，以利用安全功能作为竞争优势
- **提供卓越用户体验**  
简化安全性和身份识别，为您的客户和用户积极的用户体验
- **品牌声誉和诚信**  
确保产品和软件代码是合法的。不要让假冒产品和恶意软件影响您的品牌
- **保证隐私和安全**  
确保敏感数据保持私密性，并且不会因恶意攻击而损害客户和用户的安全



### 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: +86 021-60952260  
www.globalsign.cn