DATASHEET

IoT 设备证书 & 证书清单

将证书存储在安全、集中的存储库中定制配置文件和模板以满足身份验证要求保护设备和供应链免受新出现的威胁

设备证书是物联网公钥基础设施（PKI）的关键组件。它可以保护身份并启用身份验证。PKI是IoT安全的事实认证机制。GlobalSign的IoT标识平台支持X.509，SSL/TLS/最终实体证书和802.1AR证书（IDevID和LDevID）。

创建强大而独特的设备标识

设备证书有许多名称：安全证书、数字证书、PKI证书或设备身份证书。它是一个由证书颁发机构（CA）发布的电子编码文件，将数学上相关的密钥对绑定到设备，创建一个强大且唯一的设备标识，并提供必要的凭据来保护它。设备身份证书是终端真实性的证明

在IoT中，设备标识通常用于物联网设备、终端或网关，但可以是用户、服务、客户端、应用程序或整个生态系统。在代码签名的情况下，它验证软件更新的作者和发行者是它所指的人，并且是可靠和安全的。在PKI中使用时，它可以确保身份验证、加密和数据完整性，并在整个生命周期中对其进行保护。

将证书存储在安全、集中的存储库中

证书存储是管理成百上千的证书。GlobalSign的IoT标识平台专为IoT设计，IoT边缘注册，我们的注册服务可以满足寻求集成PKI的组织的需求由CA证书支持的注册。我们IoT解决方案的一个关键特征是证书清单：一个存储在其中的与已颁发证书的数据库一致的、可检索的证书信息的中心位置。

可以查询具有安全证书存储的证书库存，以查找内部ID号、颁发CA的证书、证书状态（已颁发、已吊销、未知）或其他重要证书详细信息。它消除了在多个位置手动存储，以便于管理。

自定义证书配置文件和模板以满足苛刻的IoT身份验证要求

默认X.509证书配置文件不适合所有IoT用例。 IoT设备及其连接的环境是独特的，需要个性化的证书配置，以与其保护的设备和环境保持一致。X.509 v3证书允许私有扩展定义，如授权密钥标识符、证书策略、策略约束、密钥使用、扩展密钥使用等，用于将其他属性与端点标识相关联。

优势

IoT 设备证书

- X.509 SSL/TLS/终端实体证书
  - 客户端证书
  - 代码签名证书
- 802.1AR 证书
  - IDevID (初始证书)
  - LDevID (操作证书)
- 基于PKI的IoT标识平台和设备标识证书可确保IoT设备的身份验证、加密和数据完整性，并在其整个生命周期中对其进行保护
- 证书清单功能简化、保护和集中证书存储
- 可定制的证书配置文件和模板可满足IoT生态系统的独特要求
- DevID证书体系结构保护IoT设备、生态系统和供应链免受新出现的威胁

IoT 数字证书适用于谁?

- IoT设备制造商在其连接产品中包括具有证书认证身份（IDevID）的组件
- 关键基础设施运营商希望减少本地设备注册、注册和管理的高昂运营费用和责任
- 半导体制造商生产身份嵌入式微控制器或可信平台模块（TPM），为下游供应链安全创造竞争优势
- IoT开发商希望通过部署从生产中保护设备身份

根据RFC 5280，补充其规范使公司能够“……通过额外的授权、保证或操作要求来满足专业应用领域或环境的要求”。

证书模板是GlobalSign CA用于接受证书签名请求（CSR）的基于规则的格式或参数集。还可以自定义这些证书，以便在提供证书时定义证书详细信息，因此所有客户证书都是一致的和可重复的，从而确保证书和数据完整性以及安全的身份验证。

我们的IoT边缘注册包括一个专用的证书模板引擎来实现这一点。它创建了模板证书数据的逻辑映射，并且能够在根据注册策略进行身份验证的同时，从外部源动态生成自定义证书字段。它通过利用IoT边缘注册固有的可扩展插件体系结构来实现这一点，因此客户可以获得安全的资源调配一致性。

保护设备和供应链免受新出现的威胁

证书保护技术不断发展。虽然许多实例仍然使用X.509 PKI架构模型，但正在出现更高级的模型，旨在保护身份免受供应链和量子计算威胁。

IEEE 802.1AR安全设备标识标准基于X.509证书，是本地和城域网中安全设备标识的广泛接受的国际标准。它引入了安全设备标识符（DevID）的概念，旨在用作可互操作的安全设备身份验证凭据。GlobalSign支持此标准。

在此模型中，每个IoT设备都会收到一份出生证明，在部署时，该出生证明可以交换或用于验证操作证书。出生证书或初始设备标识（IDevID）通常寿命较长，最好由安全硬件（如可信平台模块（TPM））进行保护。它代表了设备的核心标识。它通过供应链（如仓库存储）或在从制造商到买方的运输过程中保护设备身份。本地设备标识（LDevID）是一个本地重要的访问级别证书，持续时间较短，并提供对部署环境的访问。它类似于驾照。

该模型对于密码灵活性，或对量子计算的进步带来的密码算法和密钥威胁的响应能力特别有用。使用IDevID到LDevID体系结构的组织可以通过自动响应在设备生命周期内改变算法、信任链和安全假设来适应威胁。随着威胁的出现，DevID体系结构还可以管理证书轮换或重新注册访问凭据以做到进一步的保护。

这种方法为应对不可预见的威胁提供了稳健、灵活和深思熟虑的对策。

Tel: +86 021-609522601

www.globalsign.cn