DATASHEET

IoT Device Certificates & Certificate Inventory

Store certificates in a secure, centralized depository

Customize profiles & templates to tackle authentication requirements

Protect devices and supply chains from emerging threats

A device certificate is a critical component of an Internet of Things (IoT) Public Key Infrastructure (PKI). It secures identity and enables authentication. PKI is the de facto credentialing mechanism for IoT security. GlobalSign's IoT Identity Platform supports X.509 SSL/TLS/End Entity certificates and 802.1AR certificates (IDevID and LDevID).

Create Strong and Unique Device Identities

A device certificate goes by many names: security certificate, digital certificate, PKI certificate, or device identity certificate. It is an electronically encoded file, issued by a certificate authority (CA), that binds a mathematically related key pair to a device, creating a strong and unique device identity and providing the necessary credentials to secure it. Device identity certificates are proof of an endpoint's authenticity.

In IoT, the device identity is typically for an IoT device, endpoint or gateway but can be a user, service, client, application or an entire ecosystem. In the case of code signing, it authenticates that the author and distributor of software updates is who it says it is, and is reliable and secure. When used within a PKI, it secures authentication, encryption and data integrity protecting it throughout its full lifecycle.

Store Certificates in Secure, Centralized Depository

Certificate storage is a growing concern for organizations who manage hundreds or thousands of certificates. GlobalSign's IoT Identity Platform was designed specifically for the IoT, and IoT Edge Enroll – our enrollment service – addresses the needs of organizations looking for integrated PKI enrollment backed by CA certificates. One key feature of our IoT solution is a Certificate Inventory: a database of issued certificates stored in one central location for consistent, retrievable certificate information.

The Certificate Inventory, with secure certificate storage, can be queried to find internal ID numbers, certificates by the issuing CA, certificate status (issued, revoked, unknown) or other important certificate details. It eliminates manual storage in multiple locations for easier management.

Customize Certificate Profiles and Templates to Tackle Tough IoT Authentication Requirements

Default X.509 certificate profiles don't fit all IoT use cases. IoT devices and the environments they connect to are unique, requiring individualized certificate configuration to align with the devices and environments they protect. The X.509 v3 certificate permits private extension definition such as authority key identifier, certificate policies, policy constraints, key usage, extended key usage and others, for associating additional attributes with endpoint identities.

BENEFITS

IoT Device Certificates

- X.509 SSL/TLS/End Entity certificates
  - Client certificates
  - Code signing certificates
- 802.1AR certificates
  - IDevID (Birth Certificates)
  - LDevID (Operational Certificates)
- PKI-based IoT Identity Platform and device identity certificates secure authentication, encryption and data integrity of an IoT device, protecting it throughout its lifecycle
- The Certificate Inventory feature simplifies, secures, and centralizes certificate storage
- Customizable certificate profiles and templates address unique IoT ecosystem requirements
- DevID certificate architecture protects IoT devices, ecosystems, and supply chains against emerging threats

Who are IoT Digital Certificates for?

- IoT device manufacturers including components with certificate authenticated identities (IDevIDs) in their connected products
- Critical infrastructure operators looking to reduce the costly operational expense and liability of on-premise device registration, enrollment and management
- Semiconductor manufacturers producing identity-embedded microcontrollers or Trusted Platform Modules (TPMs) to create competitive advantage for downstream supply chain security
- IoT developers wanting to secure device identity from production through deployment

According to RFC 5280, supplementing their specification enables firms to "…meet the requirements of specialized application domains or environments with additional authorization, assurance, or operational requirements".

A certificate template is a rules-based format or set of parameters that the GlobalSign CA uses to accept a certificate signing request (CSR). These can also be customized to define the certificate details when provisioning certificates, so all customer certificates are consistent and repeatable, ensuring certificate and data integrity, as well as secure authentication.

Our IoT Edge Enroll includes a dedicated Certificate Templating Engine to achieve this. It creates a logical mapping of template certificate data and is capable of dynamically generating custom certificate fields from external sources while authenticating against enrollment policies. It does this by leveraging the extensible, plug-in architecture native to IoT Edge Enroll, so customers gain secure provisioning consistency.

Protect Devices and Supply Chains from Emerging Threats

Certificate protections are evolving. While many instances still employ the X.509 architectural model for PKI, more advanced models are emerging that are designed to protect identities against supply chain and quantum computing threats.

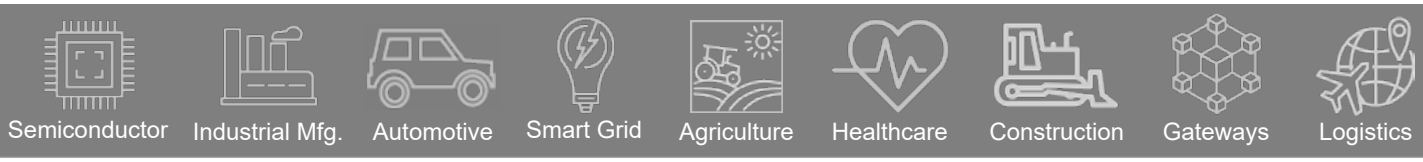
The IEEE 802.1AR Secure Device Identity standard, based on X.509 certificates, is a broadly accepted international standard for secure device identity in local and metropolitan area networks. It introduces the concept of Secure Device Identifiers (DevIDs) designed to be used as interoperable secure device authentication credentials. GlobalSign supports this standard.

In this model, each IoT device receives a birth certificate which can be exchanged for or used to validate an operational certificate when deployed. The birth certificate or initial device identity (IDevID), is typically long lived, and ideally protected by secure hardware such as a Trusted Platform Module (TPM). It is representative of the device's core identity. It protects a device identity through the supply chain such as in warehouse storage, or during shipment from manufacturer to buyer. A local device identity (LDevID), is a locally significant, access level certificate that is shorter in duration and provides access into a deployed environment. It is akin to a driver's license.

This model is especially useful for crypto-agility, or the ability to respond to cryptographic algorithm

and key threats, brought on by the advancement of quantum computing. Organizations using the IDevID to LDevID architecture can adapt to threats by changing algorithms, trust chains, and security assumptions throughout the device lifecycle, at scale via an automated response. As threats emerge, the DevID architecture can also manage certificate rotation or re-enrollment of access credentials for further protection.

This approach offers a robust, flexible, and considered response to unforeseen threats.



About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign
GMO INTERNET GROUP