



## PKI-basierte Identitäten auf IoT-Geräten bereitstellen und verwalten

Als Teil der IoT Identity Plattform von GlobalSign ist IoT Edge Enroll ein vollwertiger Registrierungsclient, der zur Bereitstellung und Verwaltung von PKI-basierten Identitäten für IoT-Geräte aller Art verwendet wird. Die Bereitstellung dieser eindeutigen Identitäten für Geräte bietet Vertrauen im Ökosystem. Sie ermöglicht die gegenseitige Authentifizierung zwischen Geräten und Systemen, verhindert Spoofing- oder Betrüger-Geräte und schützt die Kommunikation vor Überwachung oder Manipulation.

IoT Edge Enroll bietet eine flexible und skalierbare Möglichkeit, diese Identitäten über den gesamten Gerätelebenszyklus hinweg bereitzustellen und zu verwalten. Dazu gehören zusätzliche Funktionen wie Geräte-RA, Verwaltung des Zertifikatslebenszyklus und erweiterte Protokollunterstützung.

### GlobalSign IoT Identity Plattform

Vollständige Verwaltung des Lebenszyklus von Geräteidentitäten in einem Cloud-basierten Dienst



GlobalSign CA mit dedizierten Widerrufsdiensten



Moderne, sichere RESTful API



Bis zu 3.000 Zertifikate pro Sekunde ausstellbar

### GlobalSign IoT Edge Enroll

#### Geräteregistrierung

- Whitelisting
- Challenge-Response
- Richtlinienbasiert (Zeit, Ort)
- Eingebetteter Vertrauensanker

#### Geräte-Support

- Registrierungsprotokolle - CMC, EST, SCEP
- Kommunikationsprotokolle - HTTP, CoAP, MQTT
- Unterstützung für Secure Elements - SRAM PUF, TPM (1.2 & 2.0), secure MCU

#### Weitere Merkmale

- Generierung privater Schlüssel
- Unterstützung für PKCS #7, #12, #10
- Stapelverarbeitung von Zertifikaten und Zertifikatanforderungen
- Schlüsselhinterlegung
- HSM Integration

#### Sicherheitsmerkmale

- TLS-Kommunikation
- Secure Element Integration
- RSA und ECC Support

#### Servicemodelle

- Öffentliche/private Cloud
- Vor Ort
- GlobalSign Managed Services

#### Flexibilität der CA

- Wählen Sie zwischen GlobalSigns öffentlicher CA, dedizierter privater CA, GlobalSign IoT CA

### IoT Endpunkte



## Hauptmerkmale

### Geräte-Registrierungsstelle (RA)

- Steuern Sie über eine vom Benutzer hochgeladene Geräte-Whitelist, welche IoT-Geräte Zertifikate erhalten dürfen.
- Vollständige Kontrolle über eine separate REST-API-Schnittstelle, wie Hinzufügen, Pflegen und Löschen eines Teils oder einer ganzen Whitelist.
- In einem Multi-Gateway-Szenario verhindert das Whitelisting außerdem, dass fälschlicherweise und/oder wiederholt Identitäten an nicht autorisierte Geräte ausgestellt werden.
- Diese Funktion kann bei Bedarf ein- und ausgeschaltet werden.

### Sicherheitsmerkmale

- TLS-Kommunikation (optional) zwischen IoT Edge Enroll und den IoT-Geräten, die Zertifikate anfordern.
- Die Kommunikation zwischen IoT Edge Enroll und anderen Komponenten der IoT Identity Plattform von GlobalSign ist immer durch gegenseitiges TLS geschützt (Deaktivierung nicht möglich).

### Geräte-Support

- Support für verschiedene Gerätereistungsprotokolle: CMC, EST, SCEP
- Support für verschiedene Kommunikationsprotokolle: HTTP, Secure CoAP, MQTT
- Support für Sicherheitselemente: SRAM PUF, TPM (1.2 & 2.0), secure MCU (e.g., STMicro STSAFE, Renesas RX)

### Über GlobalSign

GlobalSign ist der führende Anbieter von vertrauenswürdigen Identitäts- und Sicherheitslösungen, die es Unternehmen, Großunternehmen, Cloud-Service-Anbietern und IoT-Innovatoren auf der ganzen Welt ermöglichen, Online-Kommunikation zu sichern, Millionen von verifizierten digitalen Identitäten zu verwalten und Authentifizierung und Verschlüsselung zu automatisieren. Mit Lösungen für hochskalierte Public Key Infrastructure (PKI) und Identitäten unterstützt das Unternehmen Milliarden von Geräten, Personen und Dingen innerhalb des Internet of Things (IoT).

### Weitere Merkmale

- IoT Edge Enroll kann öffentlich-private Schlüsselpaare mit dem Standard-PKCS#12-Format im Namen von IoT-Geräten generieren. Dies ist besonders nützlich für Geräte mit eingeschränkten Ressourcen, die dies nicht selbst tun können. Private Schlüssel werden anschließend vom Server gelöscht.
- Bei größeren Geräten unterstützt IoT Edge Enroll das Standard-PKCS #7-Format, das einen öffentlichen Schlüssel akzeptiert und ein X.509-Zertifikat zurückgibt. Dadurch wird sichergestellt, dass keine privaten Schlüssel auf IoT Edge Enroll oder an einem anderen Ort als dem Gerät gespeichert werden.
- Die Erneuerung von Geräte-Identitäten wird über einen dedizierten Neu-Registrierungsendpunkt unterstützt, der eine bereits bereitgestellte Identität validiert und sie mit einem neuen gültigen Zertifikat neu ausstellt.

### Flexible Einsatzmodelle

- IoT Edge Enroll kann auf einer Linux-Standardinstanz bereitgestellt werden und wird dann mit den spezifischen Kundenkontodaten konfiguriert.
- Die Bereitstellung kann auf einem eigenständigen physikalischen Server, einer Linux Virtual Machine oder in einer öffentlichen oder privaten Cloud-Plattform wie Amazon Web Services, Microsoft Azure usw. erfolgen.

### Flexibilität der Zertifizierungsstelle (CA)

- Gerätezertifikate können von GlobalSigns öffentlicher CA, privaten dedizierten oder Anbieter-CAs oder GlobalSigns IoT-CA ausgestellt werden.

DE: +49 800 723 7980  
EU: +32 16 89 19 00

[verkauf@globalsign.com](mailto:verkauf@globalsign.com)  
[www.globalsign.de](http://www.globalsign.de)

