GlobalSign
GMO INTERNET GROUP

INTRINSIC ID

DATENBLATT

Flexible Einchip-Identitäten für Hersteller von Iot Geräten

Einmalige und sichere Identitäten, verankert in der Hardware. Dank Intrinsic-IDs Fingerprint-Technologie und GlobalSigns Zertifikatsdienst für große Mengen

Der Identitäts-Algorithmus für Intrinsic-IDs macht sich bestehende SRAM zu Nutze, um einmalige, fälschungssichere Fingerprints in der Hardware eines Geräts zu verankern. GlobalSign zertifiziert die Fingerprints und fügt PKI-Fähigkeiten hinzu. Dadurch entstehen starke Identitäten, denen im IoT-System vertraut wird.

- **Wenn Schlüssel fälschungssicher sind, sind auch die Geräte sicher**
  IoT-Anbieter müssen kritische Sicherheitsaspekte wie Authentifizierung, Datenschutz und -intergrität lösen. GlobalSigns Cloud-basierte PKI Dienste können Identifizierung und Authentifizierungsdetails für Geräte ausstellen und verwalten. Hersteller können so starke Identitäten in Ihre Produkte und Systeme integrieren.
- **Sicherheit nachträglich hinzufügen und verbessern**
  Ein Software-basierter SRAM PUF kann nachträglich in Ihre bestehenden Microprozessoren eingefügt werden.
- **Ein-Chip Loesung vereinfacht Design und senkt Kosten**
  Nutzen Sie bestehende Sicherheitsfeatures Ihrer bestehenden Mikroprozessoren. Sie sparen sich einen externen kryptografischen Chip - weniger Teile und niedrigere Kosten für Sie. Bedenken Sie:
  - Chip-Chip Interface Bus muss nicht gesichert werden
  - Keine Driver oder Interface Libraries notwendig
  - Keine Chip-Chip geteilten Geheimnisse
  - Weniger Teile
- **PKI für IoT**
  PKI-basierte Geräteidentitäten ermöglichen Authentifizierung, Datenschutz und -integrität - alle wichtig für IoT Entwicklungen.
- **Breite IoT-Kompatibilität**
  Von SRAM PUF-abgeleitete Schlüssel, die in zertifizierten X.509 Zertifikaten von GlobalSign eingeschlossen sind, bieten starke Geräte-Authentifizierung für die beliebtesten IoT Protokolle:
  - HTTP
  - MQTT
  - WebSocket
  - XMPP
  - CoAP
  - TCP
  - UDP
  - SSL / TLS / DTLS

VORTEILE

Hersteller können mit starken Identitäten für Geräte Produktfälschungen und Überschussproduktion verhindern und wertbringende Extras wie wahlweise Produkteigenschaften, vorhersehbare Wartung und smarte Analysen hinzufügen.

Die gemeinsame Lösung von GlobalSign und Intrinsic-ID ist eine kostengünstige Option um einmalige, zertifizierte Identitäten für Geräte in bestehende Produktionsabläufe einzubauen:

- Lösung kann nachträglich auf bestehende Chips geladen werden; keine zusätzliche Hardware nötig
- Fälschungssichere, kurzlebige kryptografische Schlüssel schützen gegen bösartige Geräte und die fortgeschrittensten invasiven Hardware-Angriffe
- PKI-basierte Logindetails für Geräte-Authentifizierung für die beliebtesten IoT-Protokolle
- Einfache kryptografische Unterstützung für eingeschränkte Geräte mit ECC Algorithmus und angepassten Formaten der Zertifikatsantragsstellung
- Ausstellung in großen Mengen: Tausende von Geräte-IDs pro Sekunde ausstellen
- Automatisierte Bereitstellung kann in bestehende Produktionsabläufe integriert werden

Flexible Einchip-Identitäten für Hersteller von Iot Geräten

DATENBLATT

Anpassungsfähige Geräteidentitäten

Intrinsic-ID und GlobalSign bieten eine Lösung für flexible und skalierbare Geräteidentitäten. Sie können einfach in bestehende Umgebungen integriert werden, sind für große Mengen möglich und benötigen keinen Support vor Ort.

Automatisierte Bereitstellung & Ausstellung

Integrieren Sie Identitäten in bestehende Produktionsabläufe, um Durchsatz zu erhöhen und Logistik zu vereinfachen. Aufgaben der IoT Cloud Plattform können automatisiert werden, wie z.B.:

- Geräteregistrierung
- Rollen- und Genehmigungszuteilung
- Integration mit bestehenden Inventursystemen

Robuste, sichere Identitäts- & Kryptografie-Lösung

Zuerst wird ein gesteuertes Signal abgegeben, mit dem ein einmaliges Schlüsselpaar abgeleitet werden kann (Quiddikey) und ein nicht-gesteuerter Rauschanteil, der eine gute Entropie-Quelle für einen zufälligen Nummergenerator (iRNG) ist.

Der einmalige Fingerprint kann vom SRAM-basierten PUF stammen und ist auch in Betrieb (Temperaturschwankungen, Stromspannung und Luftfeuchtigkeit) verlässlich.

Cloud-basierter Vorteil

Cloud-Bereitstellung mit GlobalSigns PKI Infrastruktur bietet mehr Sicherheit, garantierte Verfügbarkeit und verbesserte Kontroll- und Audit-Möglichkeiten. Anwendungen vor Ort werden überflüssig, Projekte können skaliert und Wartungskosten gesenkt werden.

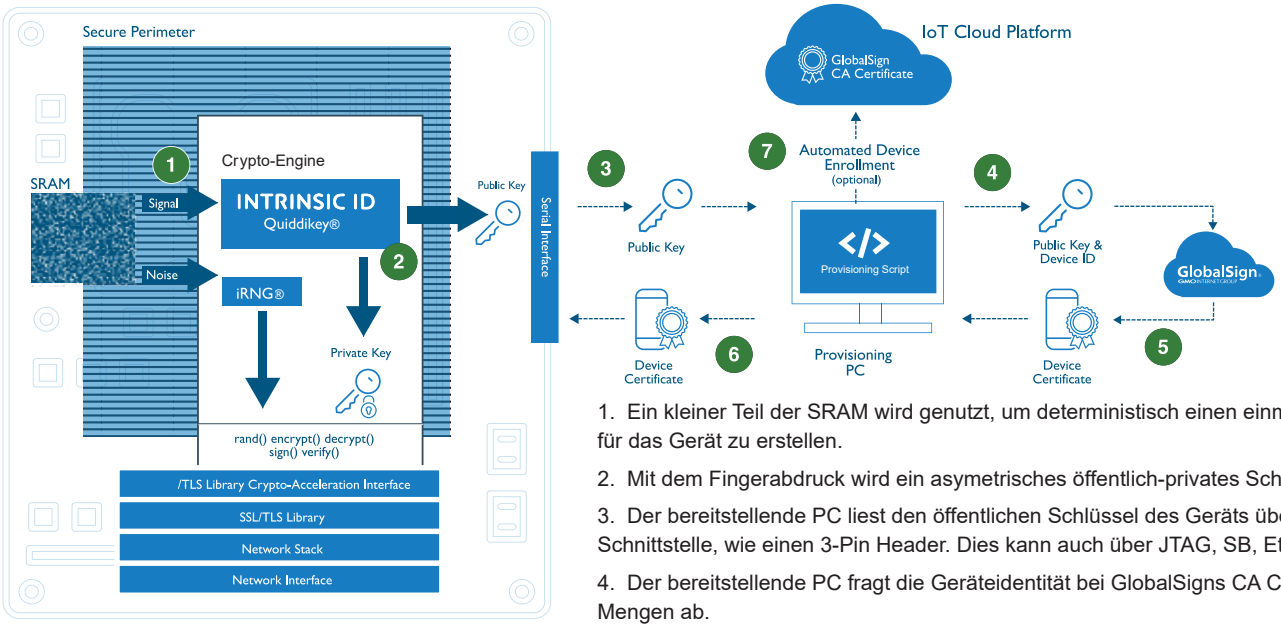
Skalieren & anpassen

GlobalSigns cloud-basierter Zertifikatsdienst hält mit den höchsten Produktionsanforderungen Schritt. Der Dienst unterstützt verschiedenste PKI-Vertrauensmodelle und kryptografische Algorithmen. Die einfache Zertifikats-bereitstellung ist perfekt für eingeschränkte IoT Geräte.

Die Bereitstellung kann Teil der Firmware-Installation, von Funktionstests oder benutzerdefinierter Programmierung werden. Es kann auf verschiedene Programm-Interfaces angepasst werden:

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

So funktioniert es - Bereitstellung von Geräteidentitaeten



1. Ein kleiner Teil der SRAM wird genutzt, um deterministisch einen einmaligen Fingerabdruck für das Gerät zu erstellen.
2. Mit dem Fingerabdruck wird ein asymetrisches öffentlich-privates Schlüsselpaar hergeleitet.
3. Der bereitstellende PC liest den öffentlichen Schlüssel des Geräts über eine einfache Schnittstelle, wie einen 3-Pin Header. Dies kann auch über JTAG, SB, Ethernet, usw. erfolgen.
4. Der bereitstellende PC fragt die Geräteidentität bei GlobalSigns CA Cloud Dienst für große Mengen ab.
5. GlobalSigns CA für große Mengen stellt die Geräteidentität an den bereitstellenden PC aus.
6. Der bereitstellende PC schickt das Gerätezertifikat an das Geräte, wo es im permanenten Speicher gesichert wird. Die Identitätsbereitstellung ist nun abgeschlossen. Die Geräteidentität kann nun zur Authentifizierung von SSL/TLS Inhalten genutzt werden.
7. Wahlweise kann der bereitstellende PC so konfiguriert werden, dass ein Gerät automatisch über eine Cloud-Plattform registriert wird.

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 Everything.

DE: +49 800 723 7980 verkauf@globalsign.com
EU: +32 16 89 19 00 www.globalsign.de

GlobalSign®
GMO INTERNET GROUP

gs-de-iid-nov-17