GlobalSign
GMO INTERNET GROUP

INTRINSIC ID

DATASHEET

Flexible One-Chip Identities for IoT Device Manufacturers

Provision unique, hardware-rooted secure identities at low cost using Intrinsic-ID's device fingerprinting technology and GlobalSign's High Volume Certificate Services

Intrinsic-ID's identity algorithms leverage existing SRAM to create unique, unspoofable device fingerprints rooted in hardware. GlobalSign certifies these fingerprints and adds PKI capabilities, creating strong device identities that can be trusted in IoT ecosystems.

- **Uncloneable Keys Mean Uncloneable Devices**
  IoT providers need to address critical security concerns including authentication, privacy and integrity. GlobalSign's cloud scale PKI service can issue and manage identification and authentication credentials for devices enabling manufacturers to build and deploy a robust and strong identity strategy into their products and ecosystems.

- **Retrofit and Enhance the Security of Existing Designs**
  A software-based SRAM PUF can be retrofitted into your existing microprocessor.

- **Single Chip Solution Simplifies Design & Lowers Costs**
  Leveraging the security features of your existing microprocessor eliminates the need for an external cryptographic chip - reducing parts count and lowering costs. Consider:
  - No chip-chip interface bus to secure
  - No drivers or interface libraries needed
  - No chip-chip shared secrets
  - Reduced parts count

- **PKI for IoT**
  PKI-based device identity credentials enable authentication, privacy, and data integrity - all critical for IoT deployments.

- **Broad IoT Interoperability**
  SRAM PUF-derived keys, certified and included in X.509 certificates issued by GlobalSign, provide strong device authentication for the most popular IoT protocols, including:
  - HTTP
  - MQTT
  - WebSocket
  - XMPP
  - CoAP
  - TCP
  - UDP
  - SSL / TLS / DTLS

BENEFITS

With strong device identity, smart device manufacturers can eliminate overproduction and counterfeiting, and enable value-adds, such as selective feature control, predictive maintenance, and smart analytics.

This GlobalSign and Intrinsic-ID joint solution is a cost-effective option for provisioning unique, certified device identities rooted in hardware that can be adapted to any existing manufacturing workflow.

- Solution can be retrofitted to existing chips; no additional hardware needed
- Uncloneable, ephemeral cryptographic keys protect against spoofed devices and even the most advanced invasive hardware attacks
- PKI-based credentials support device authentication for most popular IoT protocols
- Lightweight cryptographic support capabilities for constrained devices with ECC algorithms and streamlined certificate request formats
- High volume enrollment service capable of issuing thousands of device IDs per second
- Provisioning process is automated and can be built into existing manufacturing flows

Flexible One-Chip Identities for IoT Device Manufacturers

DATASHEET

Streamlined Device Identity

Intrinsic-ID and GlobalSign provide a flexible and scalable device identity solution that is easy to integrate and adapt to existing environments, supports high volume needs, and doesn't require on-site support.

Automated Provisioning & Enrollment

Integrate identity provisioning into existing manufacturing workflows to maximize throughput and simplify logistics. Automate IoT cloud platform enrollment tasks, including:

- Device registration
- Role and permission policy assignment
- Integration with legacy inventory systems

Robust, Secure Identity & Cryptography Solution

The initial state of SRAM provides A deterministic signal component which can be used to derive a unique device identity key pair (Quiddikey) and a non-deterministic noise component which can serve as a good source of entropy for seeding a random number generator (iRNG).

The unique fingerprint derived from a SRAM-based PUF is reliably reconstructed over a wide range of operating conditions, such as temperature, voltage, and humidity.

Cloud-based Advantage

Cloud-based provisioning, leveraging GlobalSign's PKI experience and infrastructure, offers increased security, guaranteed uptime, and enhanced control and auditing capabilities. Removing the need for on-site appliances makes increases scalability and cuts maintenance costs.

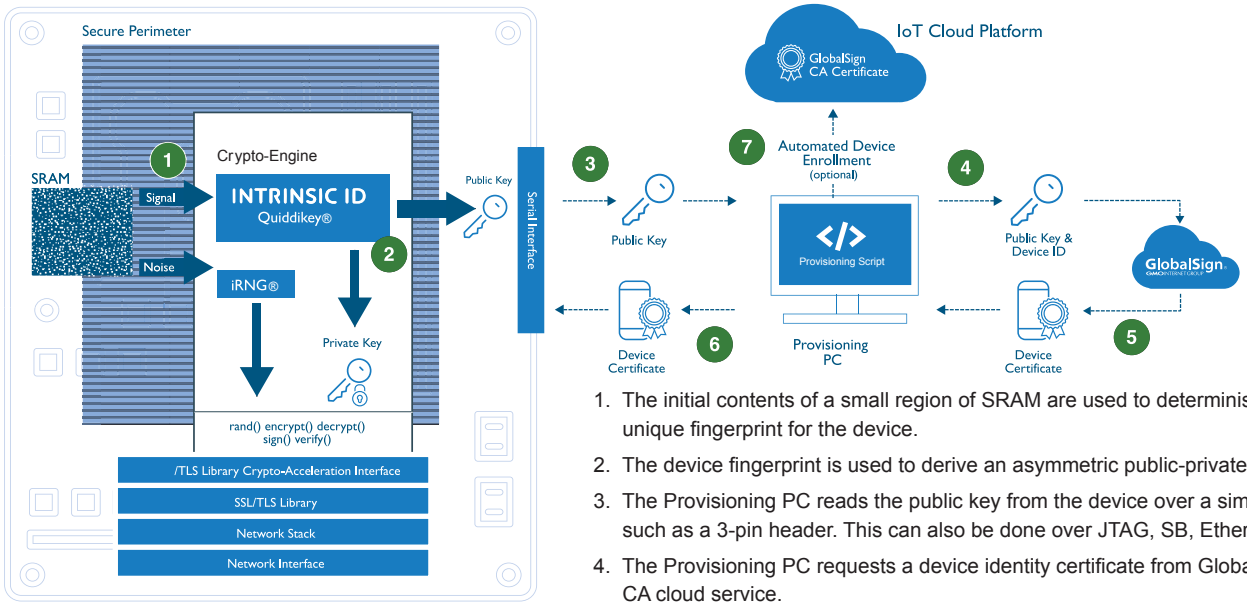
Scale & Customize

GlobalSign's cloud-based High Volume certificate issuance service is purpose-built to meet the highest production volume demands. The service is flexible to support a wide range of PKI trust models, cryptographic algorithms and uses lighter weight certificate enrollment – all to support the needs of constrained IoT devices.

Provisioning can be built into firmware loading, functional tests, or custom programming operations, and is adaptable to support a variety of programming interfaces, such as:

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

How It Works - Device Identity Provisioning



1. The initial contents of a small region of SRAM are used to deterministically derive a unique fingerprint for the device.
2. The device fingerprint is used to derive an asymmetric public-private key pair.
3. The Provisioning PC reads the public key from the device over a simple serial interface, such as a 3-pin header. This can also be done over JTAG, SB, Ethernet, etc.
4. The Provisioning PC requests a device identity certificate from GlobalSign's High Volume CA cloud service.
5. GlobalSign's High Volume CA cloud service issues the device identity certificate to the Provisioning PC.
6. The Provisioning PC sends the device certificate to the device for storage in non-volatile memory. Device identity provisioning is now complete. The device identity certificate can now be used for authentication in an SSL/TLS context.
7. Optionally, the Provisioning PC can be configured to automatically enroll a device in a cloud platform.

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).

USA: +1 603 750 7060 or +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00
sales@globalsign.com
www.globalsign.com

GlobalSign® GMO INTERNET GROUP