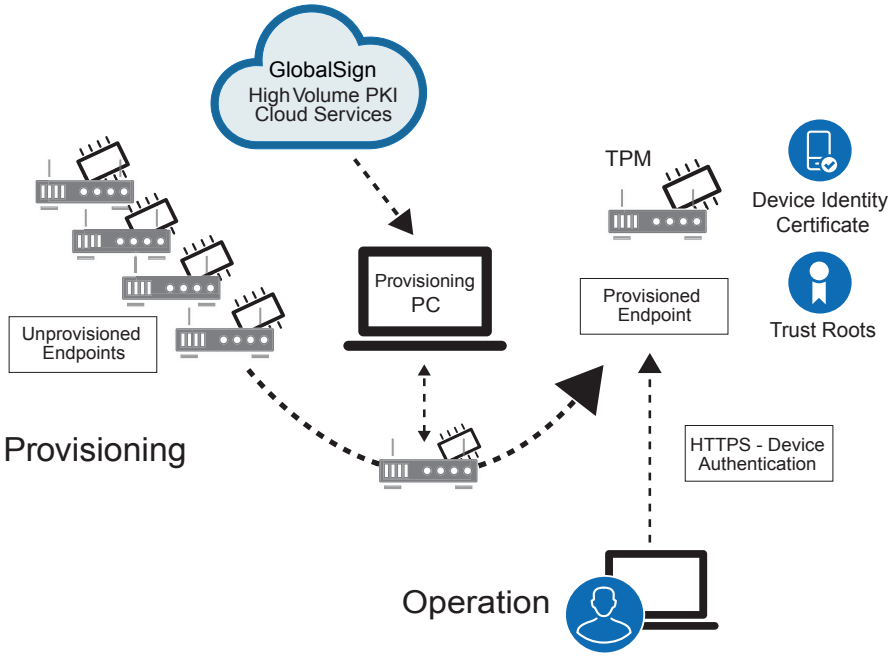
DATASHEET

Strong Device Identity at IoT Scale

Securely authenticating to and controlling hardware using GlobalSign's cloud-based High Volume Certificate Services and Infineon's OPTIGA™ TPM

IoT providers need to address critical security concerns including authentication, privacy and integrity. Mitigating risks in securing trust credentials, as well as building proven solutions at IoT scale, are addressed in the Strong Device Identity proof of concept (POC), which combines GlobalSign's high scale cloud-based PKI service and Infineon's OPTIGA™ TPM.

The GlobalSign and Infineon POC shows how the provisioning and operation of IoT endpoints can leverage PKI and secure hardware in a scalable method. Combining both these technologies illustrates how to mitigate against risks like key compromise and identity spoofing, while also being able to extend trust and deployment models at massive scale. In the POC, we introduce a provisioning PC, which automates the steps for certificate enrollment through to GlobalSign's high-scale cloud-based PKI service.



WHAT DOES THE POC SHOW?

AUTOMATED DEVICE PROVISIONING

- Analogous to units coming through a manufacturing line or being enrolled in an environment
- Secure identity generation
- Illustration of support for massive identity velocity

OPERATION WITH CRYPTOGRAPHIC DEVICE IDENTITY

- Strong authentication
- Encrypted communications

Feature Overview & Alternative Approach

Feature / Component	Used in Demo	Alternative Implementation Approaches
Interface to Device	SSH / IP	RPC / Serial-RS-232-TTL
Enrollment Volume and Sequence	Single in serial fashion for single device	Certificate issuing services in parallel to hundreds or thousands of devices
Secure Crypto Processor	Infineon OPTIGA™ TPM	OPTIGA™ Trust P OPTIGA™ Trust E OPTIGA™ Trust
Device Environment	Linux	Windows / RTOS / Embedded / Any Platform
Provisioning Process	Run on a Provisioning PC	Run on device directly Run in cloud services
Demonstrated Security Use Case	Device Identity & Authentication	Device Integrity / Attestation Secure Boot Code Signing & Secure Updates Feature Control / Brand Protection / Anti-Piracy
Operation Architecture	Device acting as server	Device acting as client or server Gateway / Multi-tier Device-to-Device
PKI Features	Private Hierarchy RSA 2048 Medium Duration Certificate No CRL or OCSP services	Public Hierarchy ECC Short Duration or Long Duration certificates CRL or OCSP services

What Technologies Meet Security and Scale of the IoT?

PKI (Public Key Infrastructure)

- Proven technology ready for devices and machines
- Provides essential information security capabilities
- Brand interoperability
- Provided by GlobalSign's High Volume Certificate Services

Secure Crypto Processors

- Secure the keys and cryptographic operations with hardware
- Provided by Infineon's OPTIGA TPM

Better Together

- Mitigate against risks like key compromise and identity spoofing
- Extend trust and deployment models at massive scale

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