



DATASHEET

TPM Device ID Enrollment

Utilizing PKI and TPM Hardware to Deliver Strong Device Identity

As IoT device manufacturers bring products to market, they must address critical security concerns including authentication, privacy and integrity. Public Key Infrastructure (PKI) can issue and manage identification and authentication credentials for devices using high volume certificate services from GlobalSign. Additionally, a certificate enrollment process is a critical part of IoT device security to ensure integrity and authenticity of the device and embedded code.

The certificate enrollment process binds the device certificate to the matching private key using a Certificate Authority (CA) as the root of trust – using standards, best practices, and guidance from the Trusted Computing Group (TCG). Protecting and managing the cryptographic keys is essential to providing a secure IoT ecosystem.

GlobalSign's high volume enrollment service for provisioning non-migratable (i.e., cannot be cloned or replicated) device identities to Trusted Platform Modules (TPMs) is a managed, highly scalable hosted service enabling original equipment manufacturers (OEMs) and device manufacturers to build and deploy a robust and strong identity strategy into products.

Leveraging Installed and Newly Deployed TPM Base

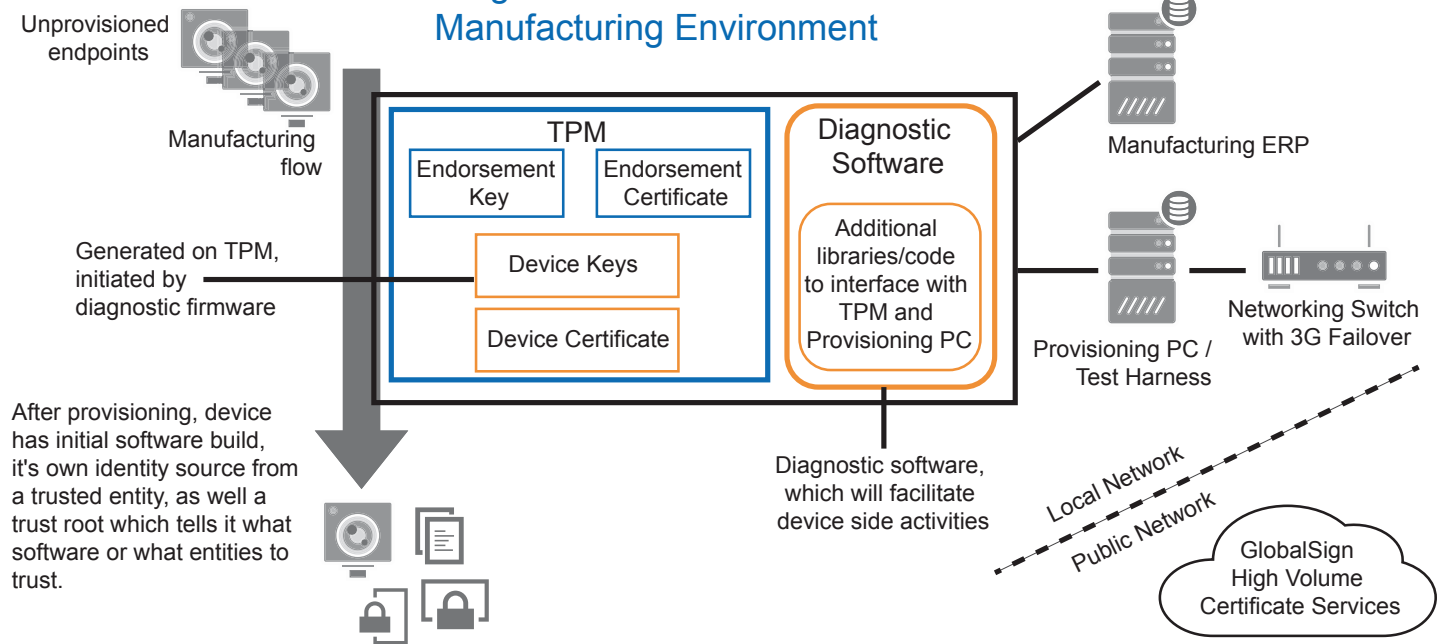
With millions of TPMs installed and deployed throughout the world, as well as numerous new IoT infrastructure products like network appliances and gateways building TPMs into their hardware security footprint, GlobalSign is able to help networking equipment vendors and gateway providers to leverage TPMs to:

- **Prevent counterfeit production in an untrusted manufacturing environment** – using a non-migratable identity, the authenticity of the device can be verified by checking the validity of the identity
- **Secure licensed feature authorization** – securely enable specific value-added feature options on specific instances of products as authorized
- **Maintain a trusted network** – authorizing network access of device can be done using a certificate that proves the identity of the device
- **Enable secure remote device management** – establish a secure communication channel with mutual authentication to perform systems management and monitoring

FEATURES

- **PKI-BASED IDENTITY**
PKI-based credentials support privacy, authentication, and data integrity
- **HARDWARE-BASED ROOT OF TRUST**
Cryptographic keys are secured and protected on TCG recommended hardware
- **SCALABLE**
High volume enrollment service capable of issuing thousands of device IDs per second
- **AUTOMATE & INTEGRATE**
Provisioning process is automated and can be built into existing manufacturing flows

Strong Device ID Enrollment in Manufacturing Environment



Feature	Benefit
Standards based - Driven from TCG best practices and standards, PKI	Interoperability, wide range of technical deployment environments and software stacks will support in operation
Custom PKI Hierarchies	Build trust models that are customized to your business environment needs
Managed Infrastructure with exportability options	No lock-in to service environment; ability to export certificate signing key material if needed
High Performance & Scalable	Can support the high volume and velocity needs of the IoT; Issue thousands of certificates per second
Cloud-based	Reduce costs for expanding to multiple manufacturing sites and ensure uptime (99.95% standard SLA)
WebTrust-audited infrastructure	Documented and audited standards for operational and physical security of PKI environment to meet compliance and risk assessment requirements
Remote issuance access control	Reduce overhead and centralize the management of remote facilities access
Ability to audit and track issuance	Know how many certificates you've issued and to which devices

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

