Entrust Delivers Self-Managed PKI Solutions for Enterprise Security

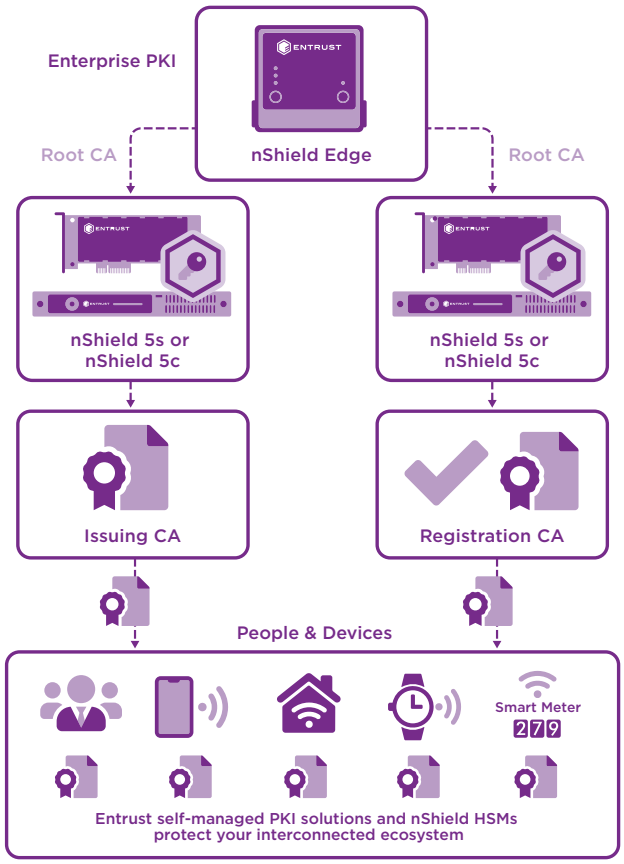
Deploy and maintain secured identity management solutions with Entrust services and hardware security modules

HIGHLIGHTS

- Protect identities of both individuals and devices
- Develop effective processes and procedures for PKI management
- Assess the health of existing PKI deployments
- Migrate PKIs to meet expanding security demands
- Facilitate security auditing and compliance

The problem: Growing adoption of interconnected technologies is stretching the capabilities of existing public key infrastructures (PKIs) and driving the need for new, scalable solutions.

The growing use of cryptographic-enabled applications and the impact of the Internet of Things (IoT) is creating unprecedented new demands on PKIs. Expanding credentialing requirements and the need to manage how devices and sensors securely connect to close network ecosystems is driving enterprises to reassess the health of their existing PKIs. Paired with changing security standards, enterprises are rethinking their PKI implementation strategies and, in some cases, redesigning and migrating to more robust, future-ready PKI deployments.



Learn more at entrust.com/HSM

Self-Managed PKI Solutions to Address Enterprise-Specific Security Needs

The challenge: Maintaining a strong root of trust across the enterprise PKI that fulfills the operational demands of more security-sensitive applications

With more security-sensitive applications using PKIs, the security of underpinning private keys is essential. According to the 2024 Ponemon Institute© State of Zero Trust & Encryption Study, the top three applications using digital certificates include TLS/SSL for public-facing websites, mobile device authentication, and private cloud-based applications. Digital certificates enable identification of applications and devices, in addition to authentication within trusted ecosystems. This requires the protection and management of increasing numbers of private keys in an automated and trusted manner.

The solution: Entrust self-managed PKI offerings combine expert consultancy services with the right security hardware to assist customers from requirements definition through deployment and training

Enterprise PKI requirements are typically unique depending on their business, their clients, and the applications they support. Entrust's self-managed PKI offerings combine technical expertise in the design and implementation of organizational PKIs, along with the necessary security hardware to establish a robust root of trust.

Services include:

- Initial requirements assessment with processes and procedures development
- Design and implementation of the PKI infrastructure
- Consultancy support for high-availability, redundant environments, or laboratory settings to help customers build their own PKI skills

For customers deploying PKIs for the first time, Entrust provides comprehensive documentation, deployment services, and supporting security hardware. For customers with existing and growing PKI deployments, services include health checks, migration support – such as SHA migration service – and the required security hardware.

Entrust nShield® hardware security modules (HSMs) increase the assurance level of PKI deployments. Designed to protect and manage underpinning private keys in a certified, isolated environment, Entrust nShield HSMs support PKIs from from leading providers like Microsoft, Red Hat, Entrust, and Insta, using standard cryptographic application programming interfaces (CAPIs).

nSield 5c network attached HSM

Learn more at entrust.com/HSM

Self-Managed PKI Solutions to Address Enterprise-Specific Security Needs

Why use Entrust HSMs with self-managed PKIs

The deployment of more security-critical applications and connected devices is placing increased demand on PKIs, requiring them to not only protect the root certificate authority (CA) private keys of individual and device certificates issued across domains, but also their registration. Organizational PKIs not using HSMs to protect their private keys leave themselves vulnerable to disruption, with potentially severe consequences. HSMs provide a hardened environment that protects security-critical keys from theft and misuse and enables full lifecycle management with failover support. Binding certificate issuance to identity checks and approvals using an HSM has been an important lesson learned from CA security compromises. Certified to stringent security standards, including FIPS 140-3 Level 3 and Common Criteria EAL4+, Entrust nShield HSMs:

- Store root CA and enrollment keys in a secure, tamper-resistant environment
- Manage administrator access with smart-card-based policies and two-factor authentication
- Comply with regulatory requirements for the public sector, financial services, and enterprises

Identity credential management

Simplifying the management of identity credentials across the enterprise, including virtualized environments, Entrust nShield HSMs help organizations meet audit and compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Payment Services Directive (PSD2). nShield HSMs are available in the following models to meet specific customer needs:

- nShield Edge HSM: A portable USB-attached HSM for offline root CAs and developer applications
- nShield 5s/nShield Solo XC: An embedded PCI Express high-performance HSM for servers
- nShield 5c/nShield Connect XC: A network-attached high-performance HSM for data centers

Learn More

To learn more about Entrust nShield HSMs, visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data, visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact