Entrust trusted identity solutions enabling digital business transformation

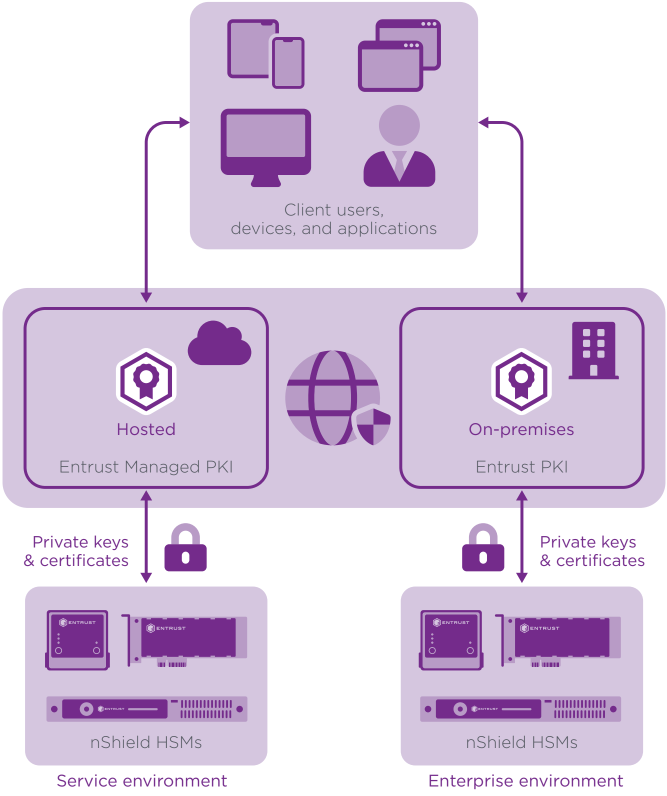
Integrated solutions enhance security of PKI deployments

HIGHLIGHTS

- Secure user identities across enterprise applications
- Control access to on-premises and hosted deployments
- Manage certificate lifecycle, including backup/recovery
- Provide root of trust to safeguard sensitive private keys
- Facilitate regulatory compliance with FIPS and Common Criteria
- Support on-premises, cloud, and hybrid deployments

The problem: increased need for trusted identity across a rapidly expanding ecosystem

The Internet of Things (IoT), mobile proliferation and the emergence of new requirements — such as supporting issuance of device certificates for Bring Your Own Device (BYOD) programs and IoT networked device enrollment — make strong identity management more important than ever. Public key infrastructure (PKI) solutions are ideally suited to establish trusted identities of users, devices, applications and services for secure access to critical enterprise systems and resources, delivering critical elements of a secure environment.



High level illustration of the components used in a typical remote administration deployment

Entrust trusted identity solutions enabling digital business transformation

The challenge: securing the management of certification authority (CA) keys

Strong protection for the private keys used by on-premises or hosted PKIs is essential to an effective security strategy. The trustworthiness of a PKI depends on the protection afforded to the private keys in the CA hierarchy and the associated verification processes. CA keys stored and managed in software can be vulnerable to advanced threats that can compromise their security. Dedicated hardware key management enhances security and reduces risk for a trusted business ecosystem.

The solution: an integrated solution with a robust root of trust

Entrust PKI solutions establish and manage certificate-based security for critical business applications. Entrust Security Manager enables customers to deploy and manage their own digital certificates. The product authenticates users, controls access and secures cryptographic applications. For customers seeking a hands-off approach, Entrust Managed PKI delivers a hosted solution.

Entrust nShield® hardware security modules (HSMs) integrate with Entrust PKI offerings to protect the confidentiality and integrity of sensitive keys. Organizations looking to extend the security of on-premises or hosted PKIs can deploy Entrust solutions with nShield HSMs, on-premises or as a service, to ensure that critical keys are never exposed to unauthorized entities. nShield HSMs securely generate, store and manage CA private keys.

Why use nShield with Entrust Security Manager and Managed PKI?

While it is possible to deploy PKIs without a hardware root of trusts, CA keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can compromise the PKIs credential issuance and certificate revocation capabilities.

The use of HSMs is widely considered best practice for PKI deployments, providing a proven and auditable way to secure valuable cryptographic material. HSMs enable organizations to:

- Secure CA keys within carefully designed cryptographic boundaries that employ robust access control mechanisms with enforced separation of duties to ensure keys are only used by authorized entities
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasing numbers of demanding applications

The Entrust Ready certification of nShield HSMs assures interoperability, ease of deployment and enhanced security.

Entrust trusted identity solutions enabling digital business transformation

Entrust nShield HSMs are high-performance cryptographic devices designed to generate, safeguard and manage sensitive key material. Certified to stringent security standards, nShield HSMs:

- Store keys in a secure, tamper-resistant environment
- Comply with regulatory requirements for public sector, financial services and enterprises
- Enforce security policies, separating security functions from administrative tasks
- Support high-performance elliptic curve cryptography (ECC)

Entrust nShield HSMs are available to match specific performance and budgetary needs:

- nShield Edge HSM: Portable USB-attached HSM for low-volume offline root CA configurations
- nShield Solo+ and Solo XC HSMs: High-performance embedded PCIe HSMs for servers and security appliances
- nShield Connect+ and Connect XC HSMs: High-performance, network-attached HSMs for high availability environments
- nShield as a Service: Subscription-based, high-performance option for greater flexibility and cost-effectiveness

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Learn more

To find out 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 keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com