Secure public key infrastructures with Entrust nShield HSMs

N FINITY
STRATEGIC TECHNOLOGY
PARTNER PROGRAM

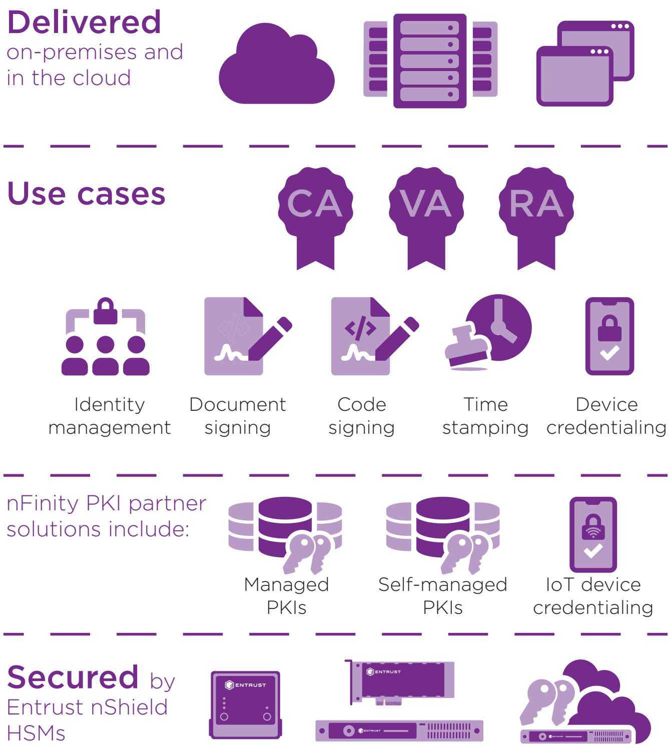
High assurance protection of the keys underpinning PKIs

HIGHLIGHTS

- Protect critical root and issuing CA keys within a tamper-resistant, FIPS 140-2 Level 3-certified HSM
- Establish strong authentication for connected devices
- Facilitate auditing and compliance with data security regulations
- Achieve enhanced levels of data security and trust
- Maintain high service levels and business agility

The challenge:

Enterprise digitalization and the burgeoning Internet of Things (IoT) bring into clear focus the need to establish trusted identities for users, devices and applications accessing systems and data. Unique and traceable identities for users and devices enable increased revenue and cost reduction through new products, services and ways to do business.



Delivered
on-premises and in the cloud

Use cases

CA VA RA

Identity management
Document signing
Code signing
Time stamping
Device credentialing

nFinity PKI partner solutions include:

Managed PKIs
Self-managed PKIs
IoT device credentialing

Secured by
Entrust nShield HSMs

CA: Certificate authority VA: Validation authority RA: Registration authority

LEARN MORE AT ENTRUST.COM/HSM

Secure public key infrastructures with nShield HSM

To capitalize on these opportunities and safeguard systems and data, it is critical to ensure that:

- The users managing the device or system are authorized to do so
- The code running on connected devices – including firmware, operating system and applications – is trusted and has not been altered
- Data in transit between devices, people, and applications is valid and protected from unauthorized changes
- Financial transactions can be secured and authenticated

A public key infrastructure (PKI) provides a mechanism by which authentic identities for users and devices – also called entities – can be established and managed. Once authenticated, these entities can access critical enterprise systems and resources, as well as complete digital signing operations. A PKI relies on digital certificates, signed by a certificate authority (CA), that bind a public key to a specific user or device. Based on this framework, the root and issuing CA private keys are attractive targets that require high assurance protection, as they represent the virtual keys to the kingdom.

The solution: PKI solutions integrated with Entrust nShield HSMs

While it is possible to deploy a PKI without a hardware root of trust, CA keys handled outside the cryptographic boundary of a certified hardware security module (HSM) can be vulnerable to attacks that compromise the PKI's credential issuance and certificate revocation capabilities.

The use of HSMs is a recognized best practice for protecting the root and issuing CA private keys that underpin PKI deployments.

Entrust nShield® HSMs are integrated with leading PKI providers to offer FIPS 140-2 Level 3 and Common Criteria EAL 4+ protection for the root and issuing CA private keys. Customers enjoy an enhanced security posture and are able to demonstrate compliance with requirements such as the Payment Card Industry Data Security Standard.

The nShield difference

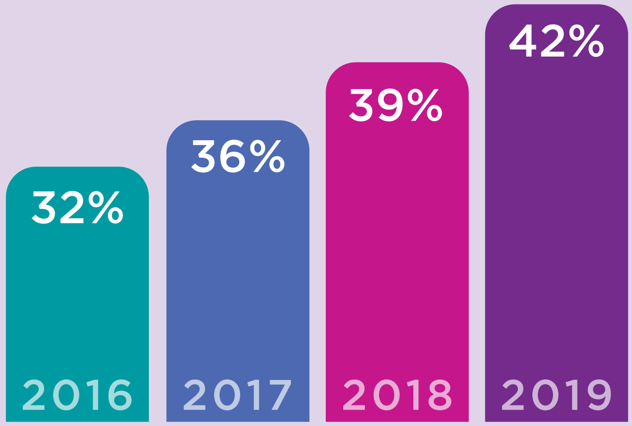
Entrust nShield HSMs provide a proven, auditable way to secure valuable cryptographic keys and material. FIPS- and Common Criteria-certified nShield HSMs:

- Secure keys within a carefully designed cryptographic boundary
- Employ robust access control mechanisms with enforced separation of duties to ensure keys are used only by authorized entities
- Ensure availability of keys by using sophisticated key management, storage and redundancy features
- Deliver high performance to support increasing numbers of demanding applications
- Scale to meet evolving demands through enhanced manageability

Entrust nShield HSMs are available in multiple form factors, while nShield as a Service provides subscription-based access to nShield Connect HSMs.

Secure public key infrastructures with nShield HSM

How do you manage the private keys for your root/policy/issuing CAs?



Hardware security modules (HSMs)

Source: 2019 Global PKI Trends Study, Ponemon Institute and Entrust

> “Organizations’ PKIs support an average of 8.5 distinct applications. This indicates that the PKI is at the core of the enterprise IT backbone.”
>
> 2019 Global PKI Trends Study, Ponemon Institute and Entrust

nFinity partners

Entrust nShield HSMs are integrated with the following PKI providers through our nFinity Technology Partner Program. Please visit our website for the latest list of partners.

axway

cybertronixx

DEVICE AUTHORITY IoT Security Simplified

digicert®

Entrust Datacard

HID HID CORPORATION

INSTA

KEYFACTOR

Microsoft

nexus

PrimeKey

Red Hat

RSA SECURITY™

SAFELAYER

TRUSTONIC

Information Security CORPORATION

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