Enhanced security: Entrust high assurance key protection for Red Hat Certificate System

Building trust for public key infrastructure (PKI)

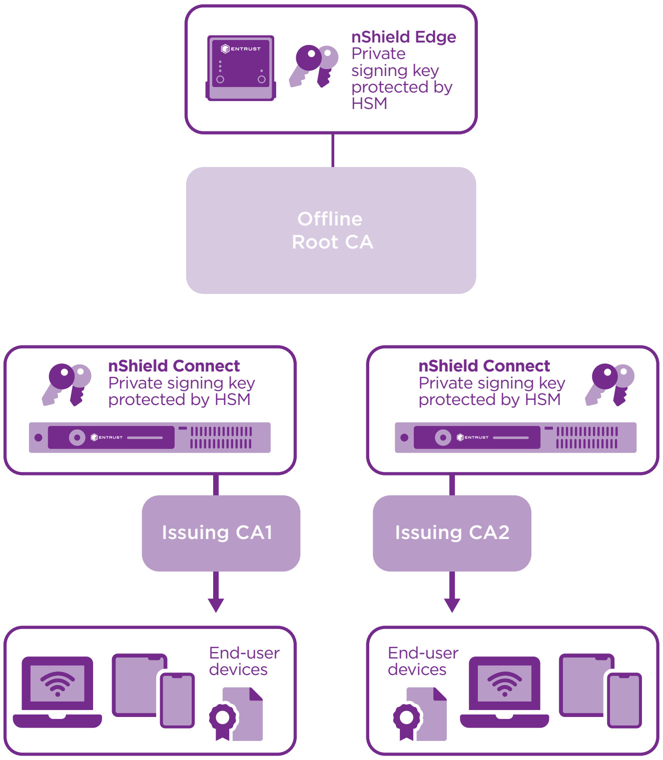
HIGHLIGHTS

- Extend security of Red Hat Certificate System for NSA Commercial Solutions for Classified (CSfC) applications
- Strengthen security framework managing user identities and keeping communications private
- Protect transactions and PKI-enabled applications
- Use NIST FIPS 140-2 certified Entrust nShield® hardware security modules (HSMs)

The Problem:

Organizational PKIs are being stretched to meet increasing number of business applications

As data breaches become more sophisticated, organizations have turned to their PKIs to protect and control access to critical applications and sensitive data. Within a PKI, the certificate authority (CA) issues electronic credentials to validate online identities and to enforce access controls. Analyzing the number of digital certificates used, the importance and value of the applications they support, and whether applications are subject to higher levels of scrutiny due to government or industry regulatory compliance, are critical factors to ensure that the PKI can meet growing demands.



nShield HSMs secure the private keys used by Red Hat Certificate System.

Learn more about our HSMs at entrust.com/HSM

High assurance key protection for Red Hat Certificate System

The Challenge:

Establishing a root of trust for identity and access controls

Protecting the integrity and security of the CA that underpins a PKI is critically important to ensure trust in business applications and on the data they protect. As PKIs increasingly support changing user access topologies including mobile and bring your own device (BYOD), organizations need to ensure that private cryptographic keys are protected and managed in a trusted manner.

The Solution:

Red Hat and Entrust together deliver robust protection of digital identities

Red Hat Certificate System issues, manages, and validates the digital identities used to bind persons, devices, or services to their corresponding private keys. The validity of each issued certificate depends upon the protection of the CA key issuing the identities. When the issuance process is executed on a server using a key stored locally in a file, that key can be vulnerable to duplication, modification, and substitution. Today, most CAs are used to issue certificates for use within an organization. Internally, certificates are typically used to perform wired and wireless authentication, secure socket layer/transport layer security (SSL/TLS) connections, and virtual private network (VPN) authentication. As expanding applications need the services of a PKI, the demands on the CAs and the need for enhanced security is paramount.

Entrust nShield HSMs increase the assurance level of the PKI by protecting the private root and signing CA keys. nShield HSMs safeguard the issuance, management, and validation processes – enabling organizations to strengthen the identity and access solution. nShield HSMs easily integrate with Red Hat Certificate System using standard cryptographic application programing interfaces (CAPI). When Entrust nShield HSMs are used, all certificate issuance and validation processing occurs within the protected confines of the HSM. Private root and signing keys are never accessible or in a readable format outside the HSM. Even during backup, archiving, and recovery processes, nShield HSMs ensure that private keys are not susceptible to manipulation and/or compromise.

High assurance key protection for Red Hat Certificate System

Why use Entrust HSMs with Red Hat Certificate System?

Breach identification, recovery, and contingency planning are important steps that can be taken to strengthen the security of a PKI. A hardened, high assurance PKI provides an environment that protects security-critical keys from theft and misuse. Binding certificate issuance to identity checks and approvals using an Entrust nShield HSM has been an important lesson learned from past CA security compromises.

Certified to stringent security standards including FIPS 140-2 Level 3 and Common Criteria EAL4+, nShield HSMs:

- Store keys for signing and issuing digital certificates in secure and tamper-resistant environment
- Manage administrator access with smart card-based policy and two-factor authentication
- Comply with regulatory requirements for public sector, financial services, and enterprises

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.

Red Hat

Red Hat provides open source solutions for the enterprise. In addition to Red Hat Certificate System, solutions include Red Hat Enterprise Linux, Red Hat OpenStack, and Red Hat OpenShift platforms, among a broad range of management and services. Entrust nShield HSMs are certified with the Red Hat Certificate System. **redhat.com**

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

Entrust, nShield, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
©2021 Entrust Corporation. All rights reserved. HS22Q2-red-hat-certificate-system-entrust-hsm-sb

ENTRUST

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