Entrust and Red Hat deliver security and trust in the cloud

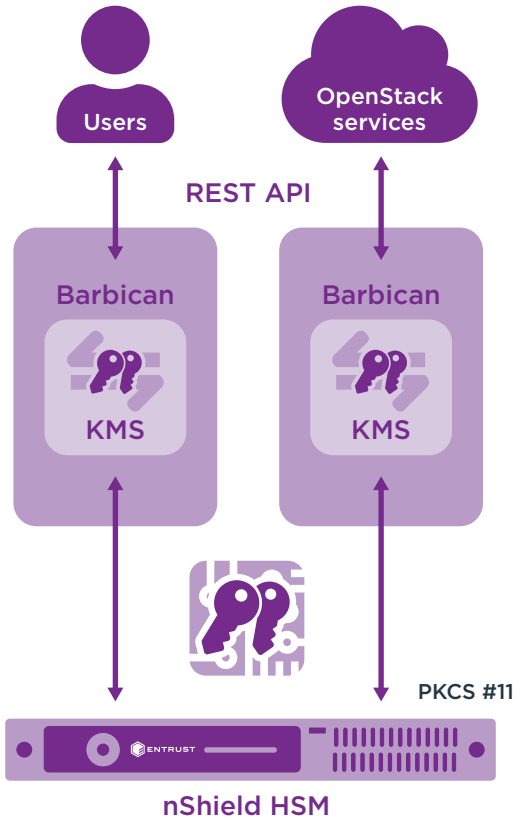
Red Hat OpenStack Barbican secures your secrets and keys in the cloud with Entrust nShield® HSMs

HIGHLIGHTS

- Offer consistent secure storage, provisioning, and management of secrets and keys used by OpenStack cloud applications
- Enable fine-grained and uniform control and scalability
- Ensure sensitive materials are never visible to applications
- Segment cryptographic components by OpenStack projects
- Deliver FIPS 140-2 and Common Criteria EAL 4+ HSM root of trust

The problem: securing secrets and keys used by OpenStack applications in the cloud

Applications using cryptography to control access and to protect the confidentiality and integrity of the data they process need secure storage, provisioning, and management of secrets and keys. Without a common key management system (KMS), individual applications rely on custom built key stores in various locations, with no demarcation between storage and execution space. Making the system only as strong as the weakest KMS implementation, this weakens the overall security of the applications.



Entrust nShield Connect hardware security module (HSM) protects the storage, transport, and secure keys used by the Red Hat Barbican OpenStack common KMS. nShield HSMs can be deployed on-premises or as a service.

LEARN MORE AT ENTRUST.COM/HSM

Entrust and Red Hat deliver security and trust in the cloud

The challenge: maintaining secrets and keys in a centralized and secured cloud environment

OpenStack cloud services provide convenience, quick deployment, and scalability. However, lack of separation between storage and application space create scenarios where cryptographic material used by applications can be scattered in software, creating a high risk of compromise. Ensuring that these materials are stored and managed centrally, securely, and in a uniform manner is essential for the robustness and trustworthiness of service.

The solution: Barbican OpenStack service for managing secrets and keys in the cloud

Since the release of Red Hat OpenStack Platform 15, Red Hat ships Barbican, OpenStack's common KMS. Barbican is a REST API service designed to address the cryptographic material management needs of users and OpenStack services. Barbican facilitates secure storage, provisioning, and management of secrets and keys used by applications, including key generation, lifecycle management, and revocation. As a component of OpenStack, Barbican supports symmetric and asymmetric key types. Barbican's availability allows encrypted volume support (via Cinder), signed image verification support in Glance, and the use of logical, secure compartments in which to store tenant secrets and keys for individual applications.

Red Hat OpenStack Platform integrates with the Entrust nShield Connect HSMs to provide enhanced security and compliance, as well as a certified source of entropy for generating keys. nShield HSMs protects the master key used to secure the storage, transport, and service keys managed by Barbican, providing a robust FIPS 140-2 Level 3 and Common Criteria EAL 4+ root of trust for OpenStack. As a robust certification management system, Barbican integrated with nShield Connect HSMs, provides a foundation for large public key infrastructure (PKI) deployments, and offers the scalability and reliability needed for such environments. Coupled with the most widely deployed HSMs, the combined solution provides the powerful security needed for growing cloud deployments.

Why use Entrust nShield HSMs and Barbican in Red Hat OpenStack platform?

Cryptographic keys handled outside the secure boundary of a certified nShield HSM are significantly more vulnerable to attack, which can lead to the compromise of critical data. nShield HSMs provides a proven and auditable means to secure valuable key materials, and to perform cryptographic processes. Entrust nShield HSM integration with Barbican delivers comprehensive logical and physical protection of the master key protecting critical operational keys.

Entrust and Red Hat deliver security and trust in the cloud

The combination delivers an auditable method for managing secrets and keys used by OpenStack end points and for enforcing security policies. By providing a mechanism to enforce security policies and a secure tamper resistant environment to safeguard master keys, end users can trust the security of OpenStack services.

Entrust nShield Connect HSMs enable users and OpenStack services to:

- Secure master keys within a carefully designed cryptographic boundary that uses robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee key is always accessible when needed by the Barbican OpenStack service
- Segregate application and key management functions

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 is the world's leading provider of open source solutions for the enterprise. In addition to Red Hat OpenStack, solutions include Red Hat Enterprise Linux, Red Hat Certificate System, and Red Hat OpenShift platforms, among a broad range of management and services. Entrust nShield HSMs are certified with Red Hat Certificate System, and the Red Hat OpenStack and OpenShift platforms.

www.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/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com