Microsoft and Entrust deliver enhanced security and trust in the cloud with unique bring your own key solution

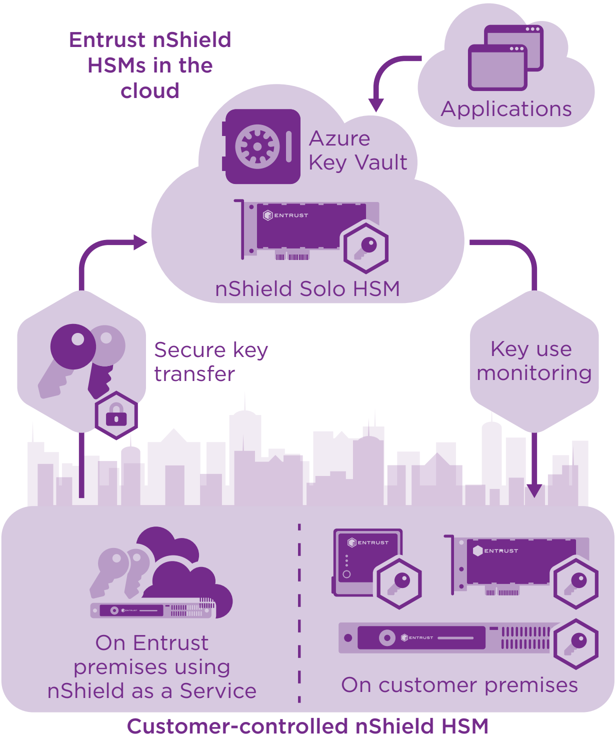
Microsoft Azure Key Vault and Entrust nshield HSMs put you in control of your sensitive data and keys in the cloud

HIGHLIGHTS

- Safeguard keys in a FIPS 140-2 certified environment
- Ensure keys are never visible to applications in the cloud
- Segregate application and key management functions
- Enable fine-grained control over encryption keys and application secrets
- Scale quickly, enabling pay-as-you-go service

The problem: public cloud services typically require you to give up control

As shared services, public cloud infrastructures do not always have a clear demarcation of tenant execution and storage space. Cloud service providers use cryptography to control access, and to protect confidentiality and integrity of sensitive data. However, the security of the services depends on the level of protection given to cryptographic keys, and exposure can compromise sensitive data.


Entrust nShield HSMs in the cloud
Applications
Azure Key Vault
nShield Solo HSM
Secure key transfer
Key use monitoring
On Entrust premises using nShield as a Service
On customer premises
Customer-controlled nShield HSM

Entrust nShield HSMs enable you to create and use your own keys to protect your data in the cloud.

LEARN MORE AT ENTRUST.COM/HSM

Enhanced security and trust in the cloud with unique bring your own key solution

The challenge: maintaining control of the cryptographic keys that secure your sensitive data

Cloud services can be quickly deployed and scaled on an as-needed basis. In order to secure your data in this environment, you need to control the encryption keys used by cloud applications. Maintaining control over encryption keys and application secrets is essential for enhanced trust and the robustness of the public cloud service.

The solution: Microsoft Azure Key Vault with enhanced key controls enabled by Entrust nShield HSMs

Microsoft Azure Key Vault provides you with the ability to create your own secure container in the cloud. Using Entrust nShield® hardware security modules (HSMs) to safeguard and manage your sensitive data and keys, Microsoft Azure Key Vault enables you to maintain control. Entrust nShield HSMs safeguard cryptographic keys independently of the software environment in the cloud. Authorized applications running in the cloud can use the keys, but cannot see them.

The bring your own key (BYOK) option allows you to use your own Entrust nShield HSM to generate and transfer keys securely to an HSM in the cloud owned by Microsoft. Microsoft gets a cache copy of your key, and appropriately authorized applications within Azure can make use of your key. The key can be replicated between HSMs for disaster recovery, but the hardware does not allow your key to be visible outside the HSMs. BYOK ensures the keys remain locked inside the certified security boundary known as an nShield "Security World." For additional security, near-real time usage logs allow you to see exactly how and when your key is used by Azure. As the key owner, you can monitor key use and revoke key access if necessary.

Why use Entrust HSMs with Microsoft Azure Key Vault?

Entrust nShield HSMs safeguard and manage the cryptographic keys that protect your sensitive data in the cloud. Entrust nShield HSMs:

- Generate and securely transfer cryptographic keys without leaving the security boundary created by Security World
- Protect the key while in Microsoft possession within a FIPS 140-2 certified cryptographic boundary
- Ensure cryptographic keys are always available and used only for authorized purposes through robust access control mechanisms and enforced separation of duties

Enhanced security and trust in the cloud with unique bring your own key solution

High assurance cloud security

Entrust nShield HSMs neutralize the perception that sensitive data maintained in the cloud is vulnerable because the cloud can only be a shared service with a shared security infrastructure. Entrust nShield HSMs:

- Protect keys in a hardened, tamper-resistant environment
- Enforce security policies, separating security functions from administrative tasks
- 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.

Microsoft

Microsoft has transformed the way businesses run their applications, create and share content, and build collaborative processes. Systems based on Microsoft Azure Key Vault make cloud services accessible and more secure. Microsoft Azure Key Vault uses cryptography to protect data, establishing trustworthy business environments that:

- Enable you to stay in control of your data and keys with an anchor to Active Directory
- Maintain cloud expectations for quick and scalable deployment and cost-effectiveness
- Support the segregation of duty between managing applications and managing 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**

Microsoft Partner
Microsoft

Gold Application Integration
Gold Datacenter

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

Contact us:
HSMinfo@entrust.com