Hold Your Own Key for high assurance key management

Microsoft

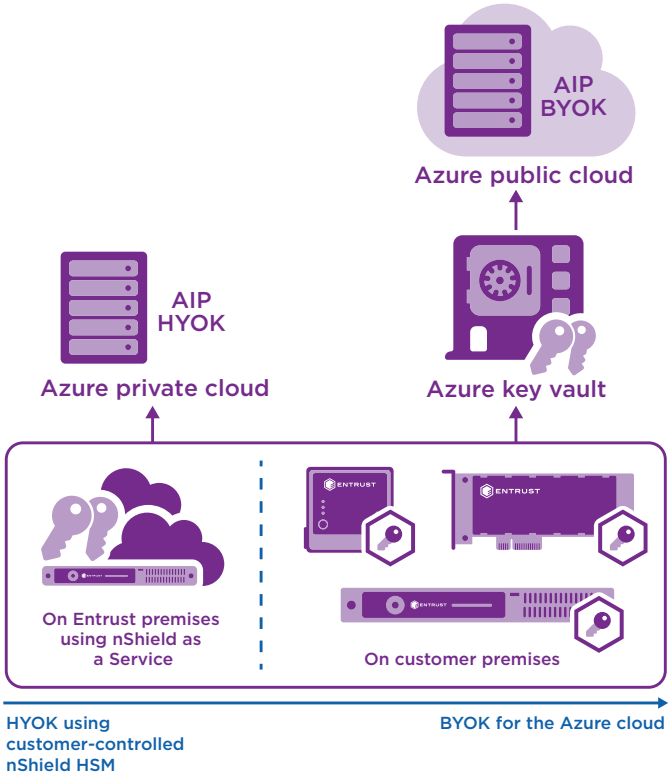
Microsoft and Entrust deliver persistent information protection and key management option that puts you in control in the cloud

HIGHLIGHTS

- Apply access and usage controls on the data you exchange
- Hold and protect your keys with HSMs you control
- Deliver FIPS 140-2 certified lifecycle key management
- Ensure keys are never visible to Microsoft

Microsoft Azure Information Protection (AIP) protects the data exchanged within your collaborative work environment by embedding enforceable security policies on the data assets, no matter the data type. As a cloud service, you can run AIP on-demand without IT infrastructure, and ensure that your information is protected across organizational boundaries.

AIP employs cryptography to deliver controlled access and persistent protection to your data. The security of AIP depends on the level of protection given to the critical cryptographic keys. The exposure of the cryptographic keys compromises your sensitive data.



Whether using AIP on-premises, in a hybrid configuration, or completely in the cloud, Entrust nShield® HSMs deliver indispensable control over your critical keys.

LEARN MORE AT ENTRUST.COM/HSM

Hold Your Own Key for high assurance key management

The challenge: highly sensitive data requires the cryptographic key to remain on-premises

While most content can be served by securely stored keys in Azure, some sensitive content can never be shared or transmitted outside your own security perimeter. The security for this sensitive content needs to be on-premises only, with very limited access and sharing.

To manage your most sensitive data within your own security perimeter, AIP offers the option of Hold Your Own Key (HYOK) that is enabled by an on-premises component, with key management provided through an Entrust hardware security module (HSM), which can be located on the customer premises or in the as a Service environment.

Entrust nShield® HSMs create a locked cage protecting your critical keys and enhancing the security of your sensitive data.

The solution: HYOK deployments with enhanced key control from Entrust

Entrust nShield HSMs create tight controls around the management and use of the cryptographic keys used in AIP deployments.

Entrust nShield HSMs provide you a hardware solution to protect your critical keys. nShield HSMs safeguards and manages the keys completely independent from the software environment, enabling you to hold and have complete control of your key.

Your key will be generated and managed inside the security boundary of your own nShield HSM, giving you the ability to protect your most sensitive data.

Why use Entrust HSMs with AIP and HYOK

Entrust HSMs give you the flexibility to use AIP on your terms to match your data security needs - whether on-premises, in the cloud, or in a hybrid configuration. nShield HSMs:

- Secure the key within a FIPS 140-2 certified cryptographic boundary
- Employ robust access control mechanisms with enforced separation of duties, so the key is only used for its authorized purpose
- Ensure key availability using key management, storage, and redundancy features

If you plan to use Azure Key Vault to store your keys and use them with AIP, Entrust can also help you enhance the security of your keys. You can generate your keys using the nShield HSMs that you control, and securely transfer them to Azure Key Vault. The Bring Your Own Key (BYOK) capability puts you in control over your keys and the security of your data in the cloud.

Hold Your Own Key for high assurance key management

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
- Are certified to FIPS 140-2 Level and Common Criteria certification

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

- For high-volume key generation and management (or as part of a hybrid deployment), nShield Solo HSM embedded PCIe cards and nShield Connect HSM network-attached appliances provide high-performance hardware security
- nShield Connect HSMs can be deployed on customer premises or in the nShield as a Service environment
- For low-volume on-premises key generation as part of the BYOK capability, nShield Edge HSM provides convenient USB-attached hardware security

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 create and share content and build collaborative processes. Systems based on Microsoft solutions maximize productivity. To protect data, Microsoft AIP uses cryptography to establish trustworthy business environments that:

- Manage identities across organizations
- Distribute certificates for authentication
- Control user access rights to data resources
- Provide total information protection

www.microsoft.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