# nShield Bring Your Own Key enables cloud customers to gain greater control over data security

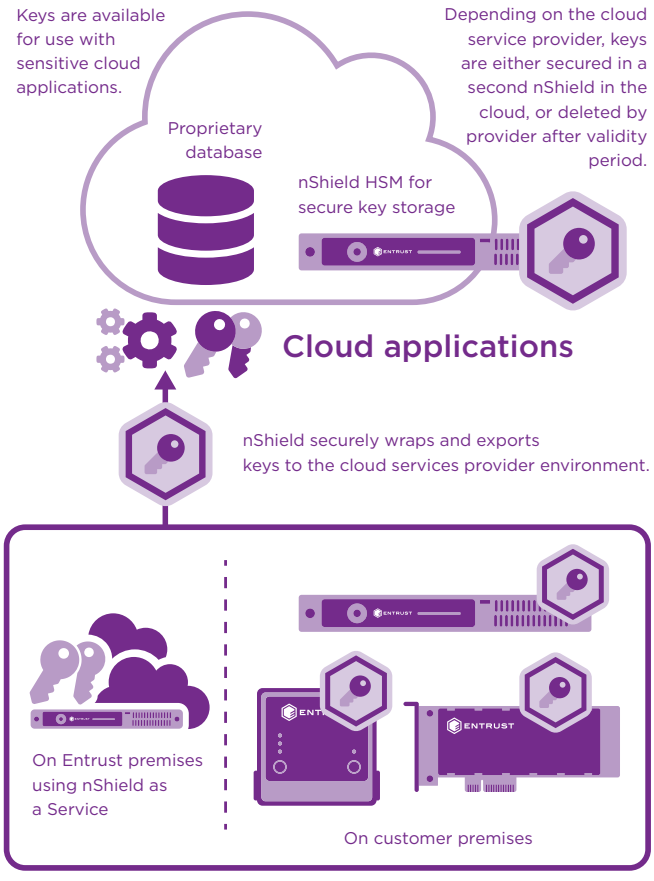
## Cloud convenience meets security

### HIGHLIGHTS

- Safer key management practices that strengthen the security of your sensitive data in the cloud
- Stronger key generation using the Entrust nShield® high-entropy random number generator, which is protected by FIPS-certified hardware
- Greater control over keys—use your own nShield hardware security modules (HSMs) in your own environment to create and securely export your keys to the cloud
- More consistent key management operations, whether your keys are used in the cloud or on premises

With nShield HSMs you can bring your own keys (BYOK) to your cloud applications, whether you're using Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure.

nShield high-assurance HSMs enable you to continue to benefit from the flexibility and economy of cloud services, while strengthening the security of your key management practices and gaining greater control over your keys.




Entrust's unique Security World architecture provides secure long term storage and disaster recovery protection of master keys.

**LEARN MORE AT ENTRUST.COM/HSM**

# Enabling cloud customers gain greater control over data security

## What nShield BYOK does

With nShield BYOK, you can use your nShield HSMs to generate, store, and manage the keys you count on to secure your sensitive cloud-hosted applications, databases, and bulk storage. nShield BYOK delivers these capabilities:

- Rely on hardware root of trust. Your nShield HSMs are highly reliable, FIPS 140-2 Level 3 certified, tamper-resistant devices. These HSMs serve as the root of trust of your cloud services, enabling you to safely generate and secure your encryption and signing keys.
- Use nShield to manage your keys. When sensitive data resides in your cloud-hosted applications, you can rely on your nShield HSMs to generate and wrap your keys, and securely deliver them to your cloud applications.
- Control the availability of your keys. Because you exclusively control your nShield HSMs, whether on your own premises or in the nShield as a Service environment, you decide when keys are generated and exported. By controlling the master copy, you also control when and whether further exports to your cloud provider occur.
- Choose your cloud provider. With nShield BYOK, you decide which cloud provider to use for each key. This gives you the flexibility to choose the right cloud from your on-premises or as a service nShield environments for your different applications, while benefiting from nShield high-assurance key generation and protection.

## Getting started with nShield BYOK

To start using nShield BYOK for AWS, GCP or Azure, you will need an nShield HSM. You can choose from the following solutions:

- nShield Connect, a network-attached appliance.
- nShield Solo, a server-embedded PCIe card.
- nShield Edge, a USB-connected device for low volume applications.
- nShield as a Service, using subscription-based nShield Connect HSMs

For the highest assurance use Entrust BYOK with Microsoft Azure. See: docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-Entrust If you require assistance with the deployment the following optional package is available for purchase:

**Bring Your Own Key,**
**Azure Professional Services**
This package includes an nShield Edge, integration delivered by the Entrust Professional Services team, and one year of maintenance.

You can also purchase nShield Connect, Solo, or Edge HSMs and professional services separately.

To use nShield BYOK with AWS, GCP or Microsoft Azure using the Microsoft open standards method, you will need the following Entrust package:

**Cloud Integration Option Pack**
This option pack contains all you need to use your on-premises nShield HSMs to generate wrap, securely transport and lease your keys to AWS or GCP or Microsoft Azure using Azure BYOK.

You can integrate nShield BYOK with AWS GCP or Azure yourself, or you can use Entrust Professional Services to help you get connected seamlessly and efficiently.

# Enabling cloud customers gain greater control over data security

## How nShield BYOK works

Entrust provides the mechanisms that let you use your nShield HSMs to generate keys, secure long-term storage, and export your keys into the cloud. Once your keys are exported into the cloud from your on-premises or as a service nShield, you'll manage keys according to one of the following approaches:

**If you are using Microsoft Azure...**
For the highest assurance using Microsoft Azure choose Entrust BYOK. This controls the conditions that must be met to allow a key to be uploaded to Azure and tightly restricts what MSFT can do with it once it is there.

You will securely transfer your keys to the nShield HSM running within the Azure infrastructure, so you get HSM security at both ends.

**If you are using AWS or GCP...**
You will lease your keys to AWS or GCP for temporary use in the cloud. After a pre-determined time period, your keys in the cloud will be destroyed. If needed, you can again lease the keys stored in your HSM.

Whichever public cloud service you choose, generating your own key and controlling its export helps you to establish strong safeguards around sensitive data and applications in the cloud.

## 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.

## 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**