nCipher

www.ncipher.com

Cloud convenience meets security

- Safer key management practices that strengthen the security of your sensitive data in the cloud
- Stronger key generation using nShield's high-entropy random number generator, which is protected by FIPS-certified hardware
- Greater control over keys—use your own nShield 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

nShield Bring Your Own Key

Helping cloud customers gain greater control over data security

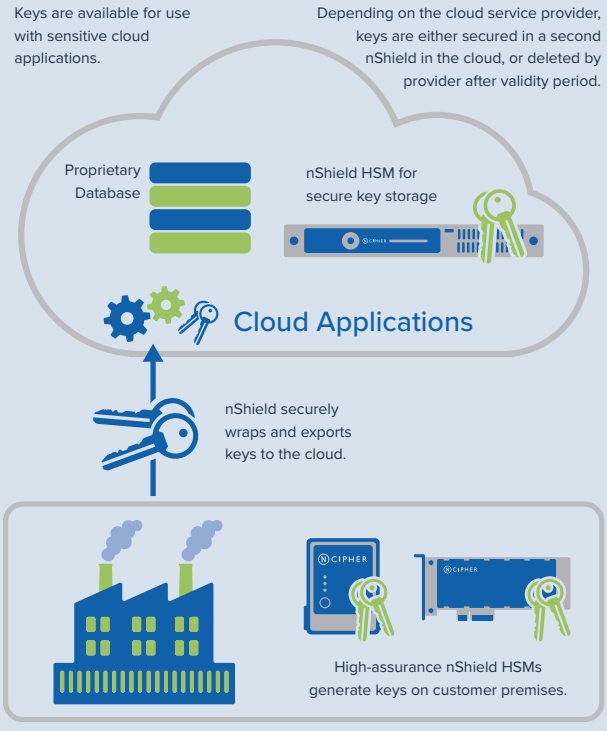
With nShield hardware security modules (HSMs) from nCipher Security, you can bring your own keys (BYOK) to your cloud applications, whether you're using Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure.

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.

Azure

aws

Google Cloud



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

nShield Bring Your Own Key

Feature Overview

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 own and exclusively control your nShield HSMs in your own environment, you decide when keys are generated and exported. Because you retain 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 environments for your different applications, while benefiting from nShield high-assurance key generation and protection

HOW NSHIELD BYOK WORKS

nCipher 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, you'll manage keys according to one of the following approaches:

If you're 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.

If you're using Microsoft Azure...

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

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.

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.

To use nShield BYOK with AWS or GCP, you will need the following nCipher package:

Cloud Integration Option Pack

This option pack contains all you need to use your on-premises nShield HSMs to generate and lease your keys to AWS or GCP.

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

To use nShield BYOK with Azure, the following package is available for purchase:

Bring Your Own Key, Azure Professional Services

This package includes an nShield Edge, integration delivered by the nCipher Professional Services team, and one year of maintenance.

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

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

Search: nCipherSecurity