nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

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

- 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

Hold your own key for high assurance key management

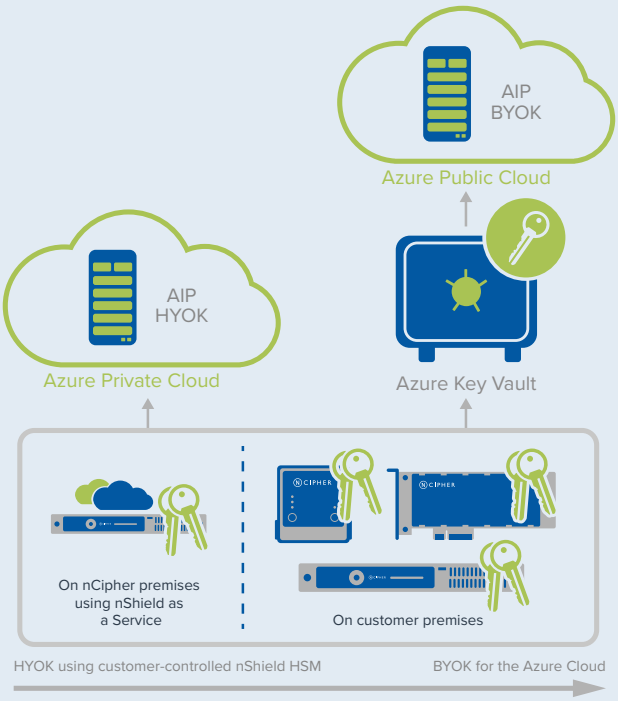
Microsoft Azure Information Protection (AIP) protects the data exchanged within your collaborative work environment by embedding enforceable security policies on the data assets, no matter the data type. As a cloud service, you can run AIP on-demand without IT infrastructure, and ensure that your information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

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 nCipher hardware security module (HSM), which can be located on the customer premises or in the nShield as a Service environment.



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

Hold your own key for high assurance key management

nCipher 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 NCIPHER

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

nCipher nShield HSMs provide you a hardware solution to protect your critical keys. nShield 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 NCIPHER HSMs WITH AIP AND HYOK

nCipher 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, nCipher 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.

NCIPHER 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

NCIPHER 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 embedded PCIe cards and nShield Connect 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 provides convenient USB-attached hardware security

NCIPHER, AN ENTRUST DATACARD COMPANY

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies—cloud, IoT, blockchain, digital payments—and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control—today, tomorrow, at all times.

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

For more information visit
www.ncipher.com or www.microsoft.com

Search: nCipherSecurity

nCipher AN ENTRUST DATACARD COMPANY