THALES

www.thales-esecurity.com

MICROSOFT AZURE KEY VAULT AND THALES NSHIELD PUT YOU IN CONTROL OF YOUR SENSITIVE DATA AND KEYS IN THE CLOUD

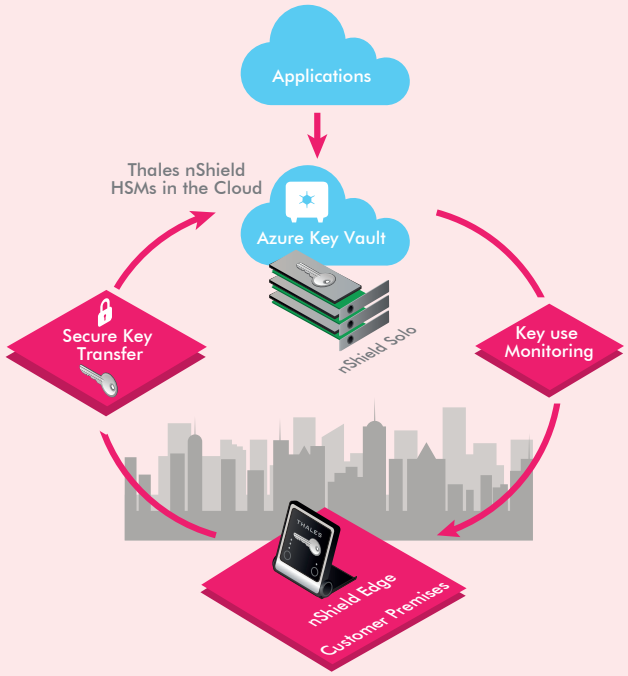
Solution Benefits

- Safeguard keys in a FIPS 140-2 certified environment to help meet compliance requirements
- 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
- Deploy and scale quickly, and enable pay-as-you-go service

Microsoft

Thales e-Security

Microsoft and Thales Deliver Enhanced Security and Trust in the Cloud with Unique Bring Your Own Key Solution



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

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.

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.

MICROSOFT AND THALES DELIVER ENHANCED SECURITY AND TRUST IN THE CLOUD WITH UNIQUE BRING YOUR OWN KEY SOLUTION

The Solution: Microsoft Azure Key Vault with enhanced key controls enabled by Thales nShield

Microsoft Azure Key Vault provides you with the ability to create your own secure container in the cloud. Using Thales nShield hardware security modules (HSMs) to safeguard and manage your sensitive data and keys, Microsoft Azure Key Vault enables you to maintain control. Thales 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 Thales 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 a Thales "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 Thales HSMs with Microsoft Azure Key Vault

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

Thales

Thales 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. Thales 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

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

- For high-volume on-premises key generation and management (or as part of a hybrid deployment), the nShield Solo embedded PCIe card and nShield Connect network-attached appliance provide high performance hardware-based security
- For low-volume on-premises key generation as part of the BYOK capability, nShield Edge provides convenient USB-attached hardware-based security

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

For more detailed technical specifications, please visit **www.thales-esecurity.com/byok** or **https://azure.microsoft.com/services/key-vault**

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com