nCIPHER

BYOK & HYOK

José María Pérez Romero
Sales Engineer Southern Europe

What is ‘Bring Your Own Key’?

- A solution for controlling & protecting data in the cloud using a cryptographic key securely generated on your premises in a nCipher Hardware Security Module (HSM)
- Cryptographic protection is applied to the key before it is transferred to the cloud service provider
- The cloud service provider cannot ‘recover’ the key, modify permissions on the key or view the key in plaintext
- The key remains under your control and protected by nCipher HSMs
- The security of the key can be attested to at all points in the generation, transfer and storage process using provided utilities

Overview of the BYOK key generation and transfer process

- Setup local Security World using the supplied nShield Edge HSM
- Generate a cryptographic key within the local Security World
- Use the BYOK toolset to modify the protections assigned to the key such that it can be securely transferred to the Cloud
- Transfer the key to the Cloud Provider
- Provide attestation that the transfer has been successful, that the key is protected within the Cloud Provider Security World on verifiable nCipher HSMs and cannot be extracted or used by the Cloud Provider
- Test that the key can be used with the required application(s)

Our customer testimonial

- Despite not having external requirements or compliance reasons, we want to follow the best practices in key custody
- We have to be prepared for any problem (including hacking) with our Cloud Providers.
- If we do not want our customers' data exposed, then using BYOK is a must

1. Download the Azure Key Vault BYOK toolset

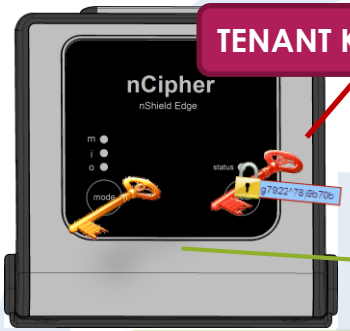
ONLINE COMPUTER

OFFLINE COMPUTER

2. Generating SecWorld + Tenant Key

new-world

generatekey



TENANT KEY

MODULE KEY

- AES 256
- Generated with HSM RNG
- Stored into NVRAM
- Backed up onto ACS

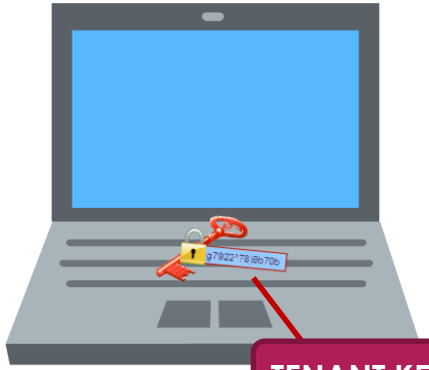
BACKUP!
We can recover and re-upload the Tenant Key with:
SecWorld files + Key file + ACS

Administrator Card Set

***K-of-N* Policy:**
N = total number of cards
K = cards required to Admin

Any combination of K cards recreates Module Key

3. Editing Tenant Key ACL



TENANT KEY

OFFLINE COMPUTER

Editing Tenant Key's ACL

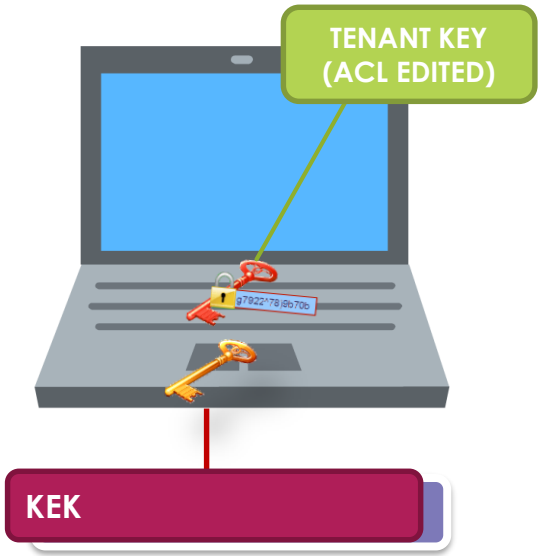
Non-exportable

....

The much reduced permissions restrict what Microsoft can do with the customer tenant key. For example, Microsoft cannot export the key in plain text, modify key protections/permissions…

TENANT KEY (ACL EDITED)

4. Encrypt with Microsoft KEK



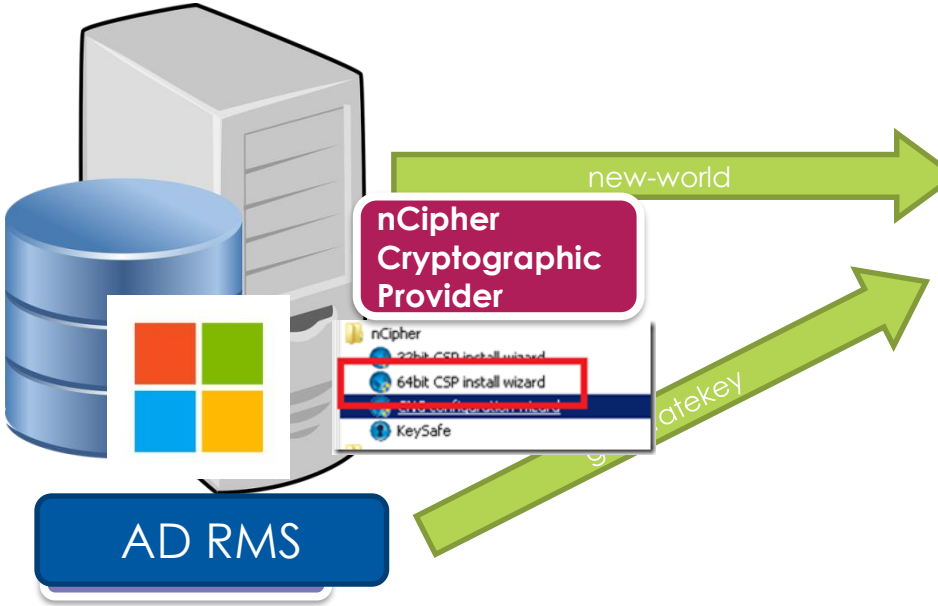
5. Upload the key to the Microsoft Key Vault

This is only an example…

What is ‘Hold Your Own Key’?

- A solution for controlling & protecting data on your premises is using a cryptographic key securely generated on your nShield HSM in conjunction with the Azure Information Protection Policy
- Usage rights policies and the organization's Private Key/Tenant Key are managed and kept on-premises
- The Azure Information Protection policy for labelling and classification remains managed and stored in Azure
- The key remains under your control and protected by nCipher HSMs
- It is usually combined with standard Microsoft Cloud Encryption to achieve an extra level of protection for certain documents/files.

HYOK



TENANT KEY

MODULE KEY

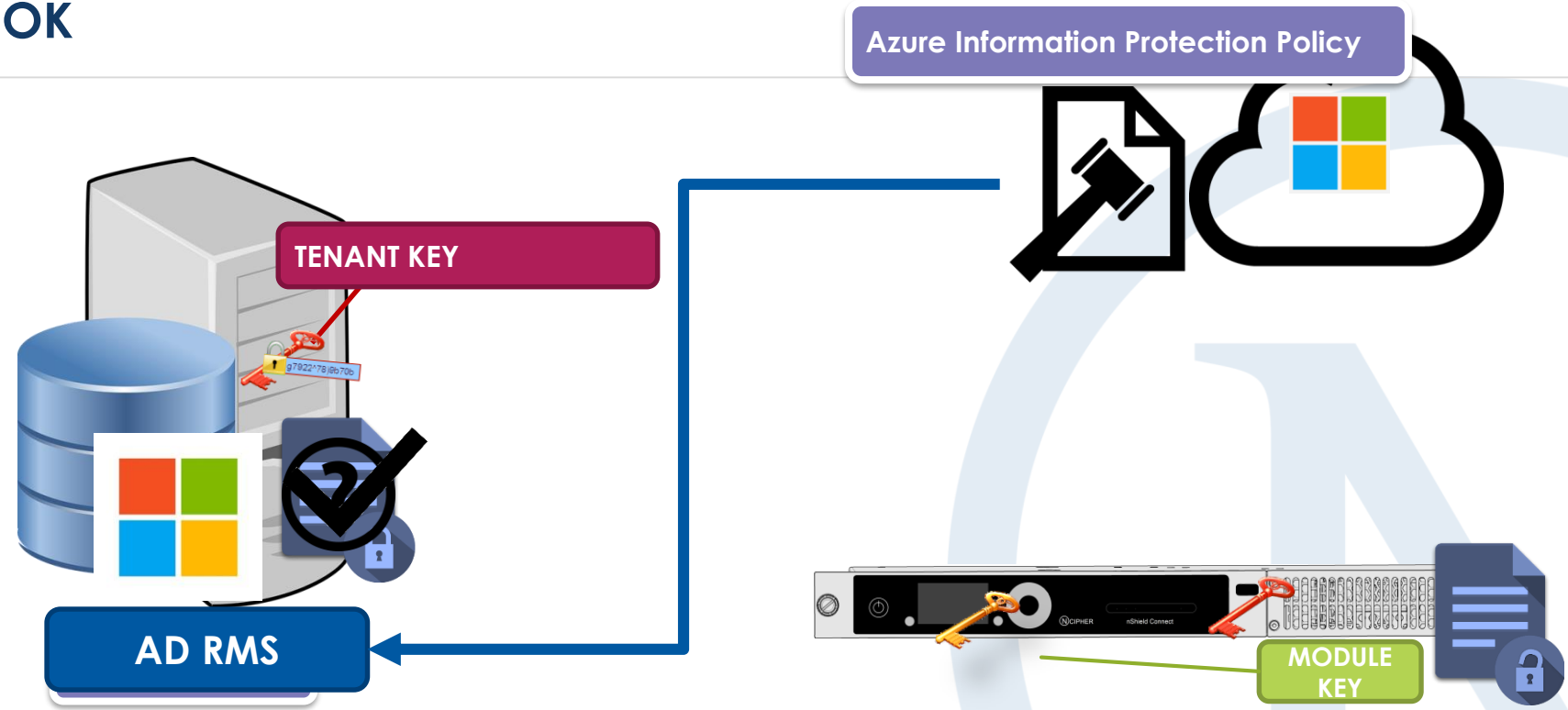
- AES 256
- Generated with HSM RNG
- Stored into NVRAM
- Backed up onto ACS

Administrator Card Set

K-of-N Policy:
N = total number of cards
K = cards required to Admin

Any combination of K cards recreates Module Key

HYOK


Azure Information Protection Policy
TENANT KEY
AD RMS
MODULE KEY

Thanks!

Questions?