Bring Your Own Key for Microsoft Azure Key Vault

nShield® HSM Integration Guide

2026-01-28

Member of
Microsoft Intelligent Security Association

Microsoft Security

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configurations . . . 1
    1.2. Supported nShield hardware and software versions . . . 1
    1.3. Supported nShield functionality . . . 2
    1.4. Requirements . . . 2
2. Integration overview . . . 5
3. Prepare the online (internet-connected) computer . . . 6
    3.1. Upgrade PowerShell . . . 6
    3.2. Install the Azure PowerShell module . . . 7
    3.3. Install the Azure CLI . . . 7
    3.4. Sign into Azure with Az PowerShell . . . 8
4. Prepare the off-line computer . . . 10
    4.1. Install the Security World software . . . 10
    4.2. Install the Entrust nShield HSM . . . 10
    4.3. Create a security world . . . 11
    4.4. Install the Cloud Integration Option Pack (CIOP) . . . 12
5. Create the Key Exchange Key in Azure . . . 14
    5.1. Update key vault SKU to premium tier . . . 14
    5.2. Create the Key Exchange Key (KEK) . . . 15
    5.3. Download the KEK to the online computer . . . 16
6. Generate, wrap, and export your own key . . . 18
7. Upload the wrapped key to Azure . . . 20
8. Appendix . . . 22
9. Glossary . . . 23
10. Additional resources and related products . . . 24
    10.1. nShield HSMs . . . 24
    10.2. nShield as a Service . . . 24
    10.3. Entrust products . . . 24
    10.4. nShield product documentation . . . 24

Chapter 1. Introduction

This integration covers the creation and transfer of a cryptographic key for use with Azure Bring Your Own Key (BYOK) for Key Vault.

This cryptographic key is known as a tenant key if used with the Azure Rights Management Service (Azure RMS) and Azure Information Protection. The key is created within the protection of the nShield Hardware Security Module (HSM) on the customer's premises. It is then securely transferred to Microsoft Azure.

The benefits of using an nShield HSM include:

- Secure storage of the private key.
- FIPS 140 validated hardware.

1.1. Product configurations

Entrust has successfully tested the use of an nShield HSM to generate and transfer a key into a Microsoft Azure Key Vault in the following configurations:

Internet-connected computer:

Product	Version
Base OS	Windows 11

Offline computer:

Product	Version
Base OS	Windows Server 2025

If migrating from a tenant key managed by Microsoft to BYOK and you are using Microsoft Office 2010, you will need to contact Microsoft Support before proceeding with BYOK. This is because Microsoft Office 2010 with Azure RMS requires some additional configuration steps prior to migration to BYOK.

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

HSM	Security World	Firmware	Cloud Integration Option Pack (CIOP)
Edge	13.6.12 (LTS 4)	12.72.2 (FIPS 140-2 certified)	2.3.0
Edge	12.80.4	12.50.8	
Edge	12.80.4	12.72.0	
Edge	12.80.4	12.60.6	
Edge	12.71.0	12.50.8	
Edge	12.71.0	12.60.6	

1.3. Supported nShield functionality

Feature	Support
Key Generation	Yes
Key Management	Yes
Key Import	Yes
Key Recovery	Yes
1-of-N Operator Card Set	Yes
K-of-N Operator Card Set	Yes
Softcards	Yes
Module-only Key	Yes
FIPS 140 Level 3 Support	Yes
Load Sharing	Yes
Fail Over	Yes

1.4. Requirements

- Access to the Entrust TrustedCare Portal. This portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.
- A premium Azure resource group. This level is required to use HSM-backed keys with

Azure Key Vault. See Azure Key Vault pricing.

- An Entrust nShield HSM to protect your keys.
- A dedicated offline computer to host the security world, for example a personal computer (PC). This computer will not be connected to a network via IP cable or Wi-Fi. It will be completely isolated.
- An online (internet-connected) computer or virtual machine to manage the Azure account.
- Portable media like a USB thumb drive.

Familiarize yourself with:

- nShield Product Documentation.
- CIOP v2.3.0 Install and User Guide. There you will find information on the key types available.
- Managing the root key for your Azure Rights Management service.

For creation of the Security World:

- Determine who within the organization will act as custodians of the ACS cards and their attendance at the key generation ceremony.
- Obtain enough blank smartcards to create the Administrator Card Set (ACS). Six cards are delivered with the nShield HSM.
- Define the Security World parameters as part of the preparation stage of the BYOK installation. For details of the security implications of the choices, see Security World infrastructure.

Setting	Description
FIPS 140 Level	Sets the operational compliance level of the HSM.
ACS quorum size (K-of-N)	Specifies the number of cards in the ACS (N) and the number of cards required to instantiate the Security World (the quorum or K). Choose a value of K and N to provide a degree of resiliency in the unlikely event of card failure, or lost card.
Cipher suite	Sets the symmetric algorithm to be used for the Security World module key. The choices are AES or AES (SP800-131A compliant).

Setting	Description
Delegation	Sets the required quorum of cards from the ACS for various operation such as setting the real time clock (RTC) and allowing read/write access to NVRAM. The default is to use the same quorum (K) value as that needed to instantiate the Security World.
Key recovery	Determines whether application keys can be recovered if the Softcard protecting the application key is lost. This is on by default.
Passphrase recovery	Determines whether passphrases in use with Softcards can be replaced without knowing the original passphrase. This is off by default.

Chapter 2. Integration overview

1. Create a Key Exchange Key (KEK) in Azure and download it to the online computer.
2. Transfer the KEK using media, for example a USB thumb drive, to the offline computer.
3. Wrap your on-premise HSM protected key with the KEK.
4. Transfer the wrapped key using media to the online computer.
5. Upload the wrapped key to Azure.

Chapter 3. Prepare the online (internet-connected) computer

All procedures in this section should be completed on the online (internet-connected) computer.

3.1. Upgrade PowerShell

1. Open a PowerShell console with administrator privileges.
2. Check the version of PowerShell. Version 7 or higher is recommended. If so, go to the next section. Otherwise, continue to the next step.

```
> $PSVersionTable.PSVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      22000  3260
```

3. Search for the latest version of PowerShell

```
> winget search --id Microsoft.PowerShell
The `msstore` source requires that you view the following agreements before using.
Terms of Transaction: https://aka.ms/microsoft-store-terms-of-transaction
The source requires the current machine's 2-letter geographic region to be sent to the backend service to
function properly (ex. "US").

Do you agree to all the source agreements terms?
[Y] Yes  [N] No: Y
Name               Id                           Version Source
-----------------------------------------------------------------
PowerShell         Microsoft.PowerShell         7.5.4.0 winget
PowerShell Preview Microsoft.PowerShell.Preview 7.6.0.5 winget
```

4. Upgrade the PowerShell version.

```
> winget install --id Microsoft.PowerShell --source winget
Found PowerShell [Microsoft.PowerShell] Version 7.5.4.0
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://github.com/PowerShell/PowerShell/releases/download/v7.5.4/PowerShell-7.5.4-win-x64.msi
                                                                  107 MB /  107 MB
Successfully verified installer hash
Starting package install...
Successfully installed
```

5. The default execution policy only allows digitally signed scripts to protect you against hacks from downloaded scripts. All Microsoft scripts are digitally signed. However, your own local scripts may not be digitally signed. These would not be allowed to run

under the default execution policy. The following command changes the execution policy to allow your own unsigned scripts to run. When prompted, enter **A** for yes to all.

```
> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy
might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
```

6. Verify the execution policy change made above.

```
> Get-ExecutionPolicy
RemoteSigned
```

3.2. Install the Azure PowerShell module

1. Open a PowerShell console with administrator privileges.
2. Enter the following command. The command prompt will return when the installation has completed.

```
> Install-Module -Name Az -Repository PSGallery -Force
```

3. The Az module needs to be imported before it can be used. The command prompt will return when the module has completed loading.

```
> Import-Module Az
WARNING: The names of some imported commands from the module 'Az.Cdn.private' include unapproved verbs that
might make
them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again
with the
Verbose parameter. For a list of approved verbs, type Get-Verb.
...
```

4. Verify the Az module is properly loaded and ready for use.

```
> Get-Module -Name Az*

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     5.3.1      Az.Accounts                         {Add-AzEnvironment, Clear-AzConfig, Clear-
AzContext, Clear...
```

3.3. Install the Azure CLI

1. Open a PowerShell console with administrator privileges.
2. Enter the following command.

```
> winget install --exact --id Microsoft.AzureCLI
Found Microsoft Azure CLI [Microsoft.AzureCLI] Version 2.80.0
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://azcliprod.blob.core.windows.net/msi/azure-cli-2.80.0-x64.msi
                                                                  65.6 MB / 65.6 MB
Successfully verified installer hash
Starting package install...
Successfully installed
Notes: Winget installs the 64-bit CLI on 64-bit OS by default now. If you have used the 32-bit CLI before,
please follow this guide to migrate to 64-bit version: https://learn.microsoft.com/cli/azure/install-azure-
cli-windows#migrate-to-64-bit-azure-cli
```

3. Close the PowerShell console.
4. Open a new PowerShell console with administrator privileges and test the installation by running the following command.

```
> az

Welcome to Azure CLI!
---------------------
Use `az -h` to see available commands or go to https://aka.ms/cli.
...
```

3.4. Sign into Azure with Az PowerShell

1. Open a PowerShell console with administrator privileges.
2. Sign into Azure. If multiple subscriptions are listed, enter the one to be used for BYOK.

```
> az login --tenant <tenant-id>
```

For example:

```
> az login --tenant ...
Select the account you want to log in with. For more information on login with Azure CLI, see
https://go.microsoft.com/fwlink/?linkid=2271136

Retrieving subscriptions for the selection...

[Tenant and subscription selection]

 No     Subscription name     Subscription ID                       Tenant
 -----  --------------------  ------------------------------------  ------------------------------------
 [1] *  Azure subscription 1  ...                                   ...

The default is marked with an *; the default tenant is '...' and subscription is 'Azure subscription 1'
(...).

Select a subscription and tenant (Type a number or Enter for no changes):
```

```
Tenant: ...
Subscription: Azure subscription 1 (...)

[Announcements]
With the new Azure CLI login experience, you can select the subscription you want to use more easily. Learn
more about it and its configuration at https://go.microsoft.com/fwlink/?linkid=2271236

If you encounter any problem, please open an issue at https://aka.ms/azclibug

[Warning] The login output has been updated. Please be aware that it no longer displays the full list of
available subscriptions by default.
```

Chapter 4. Prepare the off-line computer

All procedures in this section should be completed on the offline computer.

4.1. Install the Security World software

1. Install the Security World software. For detailed instructions see nShield Security World Software v13.6.11 Installation Guide.
2. Add the Security World utilities path to the system path. This path is typically `C:\Program Files\nCipher\nfast\bin` or `%NFAST_HOME%\bin`
3. Open a command window and run the following utility to confirm the Security World installation. Notice the Server is **operational**.

   For example:

```
>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        CE42-591E-1AAF
 mode                 operational
 version              13.6.12
 ...
```

4.2. Install the Entrust nShield HSM

1. Take the HSM out of its box. Check the tamper evident hologram in the lower right corner of the HSM front panel.

   If this appears damaged or missing, do not use the HSM and contact Entrust TrustedCare Portal.

2. Remove all other protective packaging from the HSM.
3. Make a note of the Paper Serial Number (PSN). It can be found on the back of the HSM beneath the pull out stand and on the side of the HSM packaging box. It usually begins with **06**.
4. Store this PSN. It will be needed to obtain support.
5. Look for the USB cable found inside the packaging for the HSM. Attach the USB Standard-B connector to the HSM
6. Attach the USB Standard-A connector to a USB 2.0 connector in the offline computer. If this is the first time the HSM has been connected, you may see USB drivers installed. Wait until the driver installation has completed.

USB 2.0 connectors are color-coded black. Blue color USB connectors are for USB 3.0, and should be avoided in the case.

7. See Using the nShield Edge for information on the controls, card slot, and LEDs of the HSM.
8. Open a command window and run the following utility to verify the HSM is **operational**.

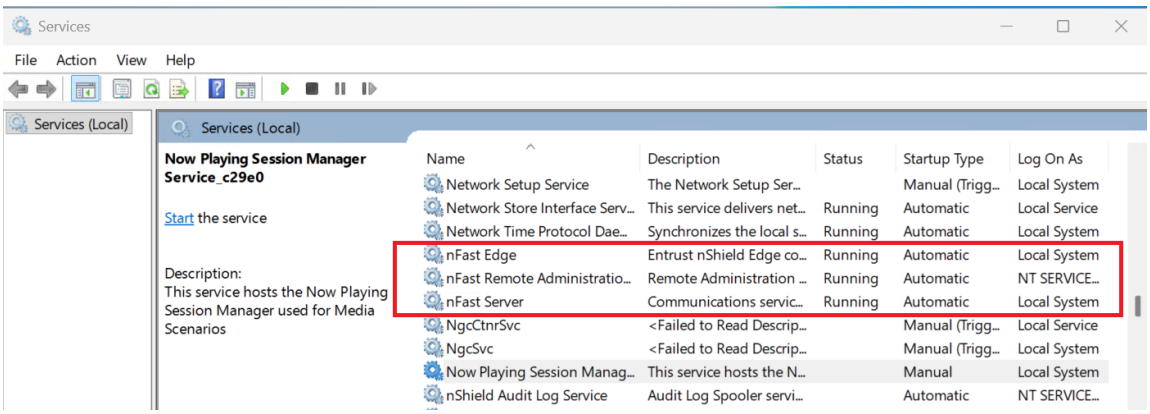
```
>enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        CE42-591E-1AAF
 mode                 operational
 version              13.6.12
 ...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        CE42-591E-1AAF
 mode                 operational
 version              12.72.2
 ...
```

9. If **Module #1** fails or there is no output, restart the hard server and try again.

   Restart using the Windows CLI:

```
>net stop "nFast Server"
>net start "nFast Server"
```

   You can also restart or with the Windows `services.msc`.



4.3. Create a security world

1. Set the HSM to initialization mode. See Using the nShield Edge for reference.

2. Create your Security World if one does not already exist or copy an existing one. Follow your organization's security policy when creating a Security World. For more information see Create a new Security World.

The administrator card set (ACS) cards cannot be duplicated after the Security World is created. You may want to create extras in case of a card failure or a lost card.

You will now be prompted to insert N blank/new/formatted smartcards. In turn, have your ACS custodians present their allocated card, noting the serial number of the smartcard and the corresponding passphrase. Each card and passphrase should be stored in separate tamper-resistant envelopes and should be dated and signed. The cards and passphrases should not be sealed until the end of the tenant key ceremony, in case they are needed later during the ceremony.

3. Once the command exits, set the HSM to operational mode.
4. Confirm the Security World is **Usable**:

```
>nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

4.4. Install the Cloud Integration Option Pack (CIOP)

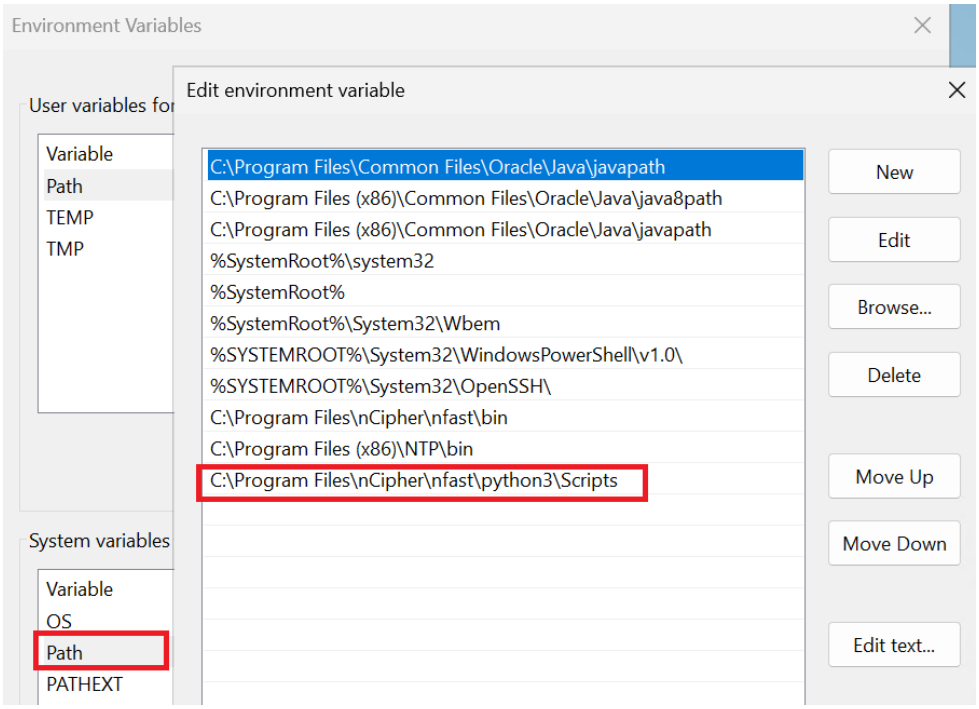
1. Install the CIOP. For detailed instructions see CIOP v2.3.0 Install and User Guide.

   For example:

```
C:\Users\Administrator\Downloads\CIOP-2.3.0\CIOP-2.3.0>"%NFAST_HOME%\python3\python.exe" -m pip install
nshield_citool-2.3.0-py3-none-any.whl
Processing c:\users\administrator\downloads\ciop-2.3.0\ciop-2.3.0\nshield_citool-2.3.0-py3-none-any.whl
Requirement already satisfied: nfpython>=1.0.1 in c:\program files\ncipher\nfast\python3\lib\site-packages
(from nshield-citool==2.3.0) (13.6.12)
Requirement already satisfied: asn1crypto>=1.4.0 in c:\program files\ncipher\nfast\python3\lib\site-
packages (from nshield-citool==2.3.0) (1.5.1)
Installing collected packages: nshield-citool
  WARNING: The script cloud_integration_tool.exe is installed in 'C:\Program
Files\nCipher\nfast\python3\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script
-location.
Successfully installed nshield-citool-2.3.0
```

```
[notice] A new release of pip is available: 24.0 -> 25.3
[notice] To update, run: C:\Program Files\nCipher\nfast\python3\python.exe -m pip install --upgrade pip

C:\Users\Administrator\Downloads\CIOP-2.3.0\CIOP-2.3.0>"C:\Program Files\nCipher\nfast\python3\python.exe"
-m pip install --upgrade pip
Requirement already satisfied: pip in c:\program files\ncipher\nfast\python3\lib\site-packages (24.0)
Collecting pip
  Downloading pip-25.3-py3-none-any.whl.metadata (4.7 kB)
Downloading pip-25.3-py3-none-any.whl (1.8 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 6.6 MB/s eta
0:00:00
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 24.0
    Uninstalling pip-24.0:
      Successfully uninstalled pip-24.0
  WARNING: The scripts pip.exe, pip3.11.exe and pip3.exe are installed in 'C:\Program
Files\nCipher\nfast\python3\Scripts' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script
-location.
Successfully installed pip-25.3
```

2. Add `C:\Program Files\nCipher\nfast\python3\Scripts` to the system path as suggested above.



Chapter 5. Create the Key Exchange Key in Azure

All procedures in this section should be completed on the online computer.

5.1. Update key vault SKU to premium tier

Skip this section if you are already on the premium tier.

1. Open a PowerShell console with administrator privileges.
2. Connect to Azure.

```
> Connect-AzAccount -TenantId <tenant-id> -SubscriptionId <subscription-id>
```

3. Run the following commands.

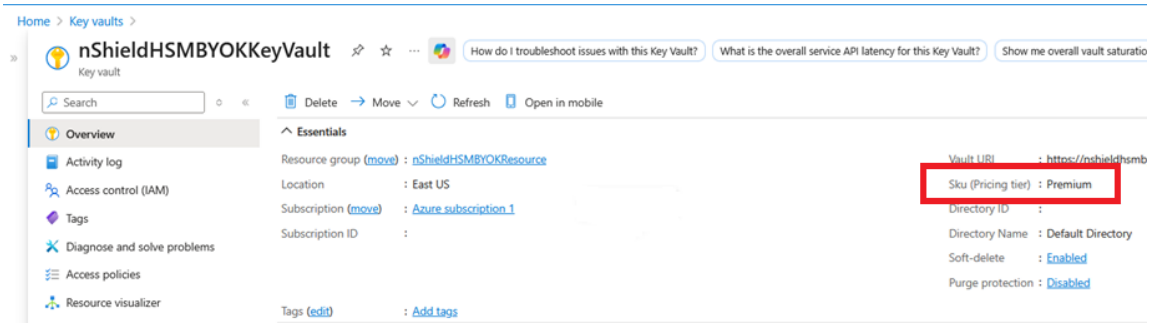
```
$vault = Get-AzResource -ResourceName <key-vault-name> -ResourceGroupName <resource-group-name>
-ResourceType Microsoft.KeyVault/vaults -ExpandProperties
```

For example:

```
$vault = Get-AzResource -ResourceName "nShieldHSMBYOKKeyVault" -ResourceGroupName "nShieldHSMBYOKResource"
-ResourceType Microsoft.KeyVault/vaults -ExpandProperties

$vault.Properties.sku.name = 'Premium'

Set-AzResource -ResourceId $vault.ResourceId -Tags $vault.Tags -Properties $vault.Properties

Confirm
Are you sure you want to update the following resource:
/subscriptions/...
vaults/nShieldHSMBYOKKeyVault
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"):

Name              : nShieldHSMBYOKKeyVault
ResourceId        : /subscriptions/.../resourceGroups/nShieldHSMBYOKResource/providers
                    /Microsoft.KeyVault/vaults/nShieldHSMBYOKKeyVault
ResourceName      : nShieldHSMBYOKKeyVault
ResourceType      : Microsoft.KeyVault/vaults
ResourceGroupName : nShieldHSMBYOKResource
Location          : eastus
SubscriptionId    : ...
Tags              : {}
Properties        : @{sku=; tenantId=...; accessPolicies=System.Object[];
                    enabledForDeployment=True; enabledForDiskEncryption=True;
enabledForTemplateDeployment=True;
                    enableSoftDelete=True; softDeleteRetentionInDays=90; enableRbacAuthorization=False;
                    vaultUri=https://nshieldhsmbyokkeyvault.vault.azure.net/; provisioningState=Succeeded}
```

4. Sign into the Azure WebGUI.

5. Verify the vault's SKU has changed to Premium as expected.



5.2. Create the Key Exchange Key (KEK)

1. Open a PowerShell console with administrator privileges.
2. Connect to Azure using the az command.

```
> az login --tenant <tenant-id>
```

3. Enter the following command to create an Azure KEK in the key vault.

```
> az keyvault key create --kty <key-type>-HSM --size <key-size> --name <kek-name> --ops import --vault-name
<key-vault-name>
```

For example:

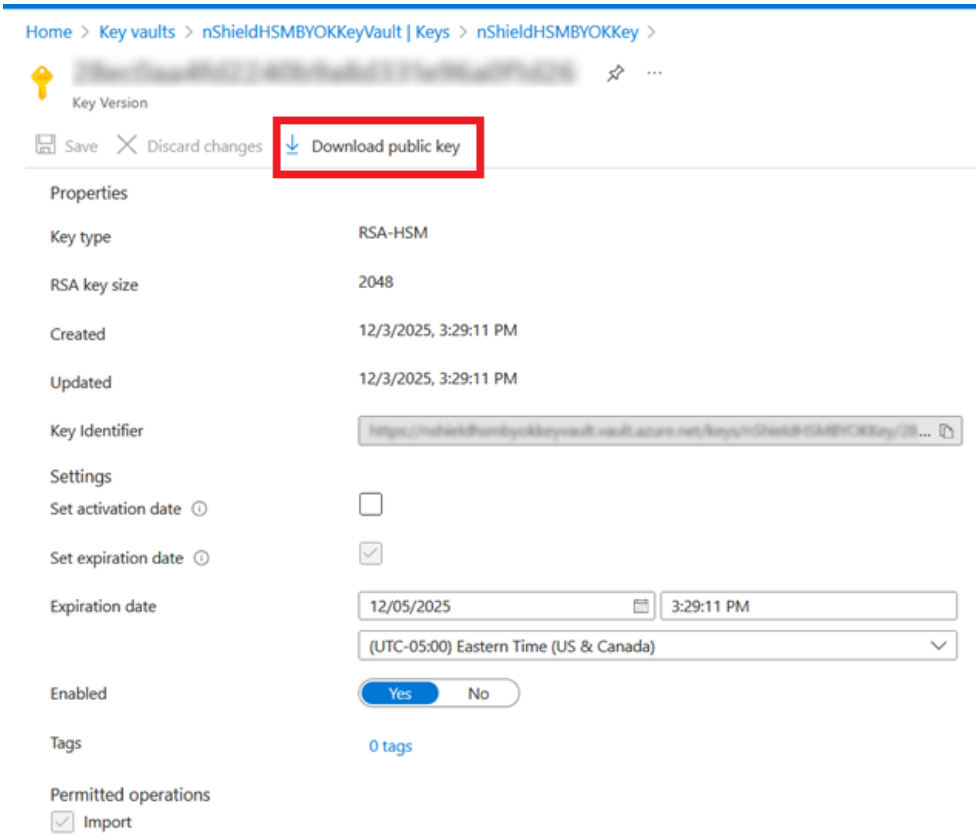
```
> az keyvault key create --kty RSA-HSM --size 2048 --name nShieldHSMBYOKKey --ops import --vault-name
nShieldHSMBYOKKeyVault
{
  "attributes": {
    "created": "2025-12-03T20:29:11+00:00",
    "enabled": true,
    "expires": "2025-12-05T20:29:11+00:00",
    "exportable": false,
    "hsmPlatform": "2",
    "notBefore": null,
    "recoverableDays": 90,
    "recoveryLevel": "Recoverable+Purgeable",
    "updated": "2025-12-03T20:29:11+00:00"
  },
  "key": {
    "crv": null,
    "d": null,
    "dp": null,
    "dq": null,
    "e": "AQAB",
    "k": null,
    "keyOps": [
      "import"
    ],
    "kid":
"https://nshieldhsmbyokkeyvault.vault.azure.net/keys/nShieldHSMBYOKKey/28ec0aa4fd2240b9a8d331e96a0f1d26",
    "kty": "RSA-HSM",
    "n":
```

```
"nzwJI3YtIMc36UrKB2lvgCn9cgvQ/GkrcWHHl24bybx0rqafff8DIIlgQ5rgvEdEkLvHwZGQQ3JyzfnQUWVoT/BtMWbeoaFPhYR1KYaThG
Uel4yFpznK2Z0s1E8UmEz2HFp0WdvPVpvcTCdQ31gLKpcluRcCVQLVeMfqDp/TSFyDvMT2xBgrbXjrLp6g7gwC2qRYL+46c60mVGr4o/RSt
SdYaXC1pMikBN6G6oL/x1scxDXMm3kAMU3fY+EysNo10Q7XRsvJE2Hn1NwtK9FBsiU4Tc/PBWc3WenJY+f1aAz4gZxVcwZ1ys4y+uD/YfV2
ef3sgHAScMeiaz1ZOe1+/Q==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
    "x": null,
    "y": null
  },
  "managed": null,
  "releasePolicy": null,
  "tags": null
}
```

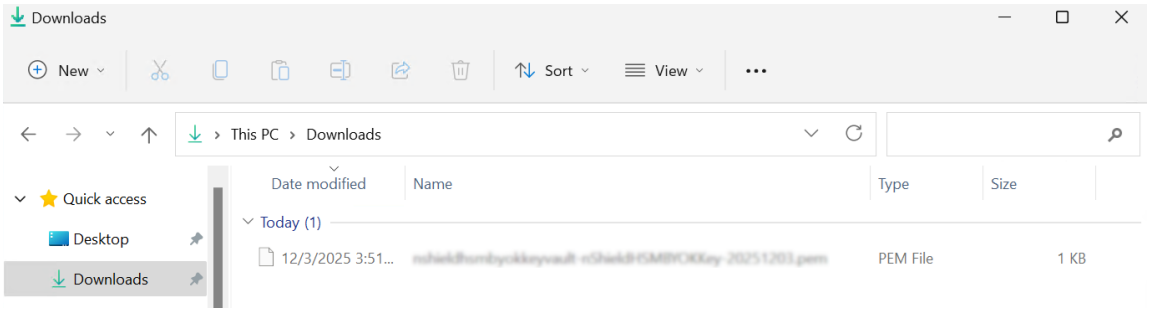

4. Notice the "kid" above. You will needed it later.

5.3. Download the KEK to the online computer

1. Sign in to the Azure WebGUI.
2. Navigate to **Key vaults > <key-vault-name> |Keys > <key-name>**. Then select the **Download public key** icon.



3. Notice the downloaded pem file.



4. Transfer the downloaded pem file using media (e.g. USB thumb drive) to the offline computer.

Chapter 6. Generate, wrap, and export your own key

All procedures in this section should be completed on the offline computer.

1. Open a Windows CLI as administrator.
2. Navigate to the folder containing the transferred pem file from the online computer.
3. Run the following command. Be ready to present the ACS/OCS to the HSM. In the following examples a new key named **mykey2azure** will be created since this key did not exist. For more info on the **cloud_integration_tool** below, see CIOP v2.3.0 Install and User Guide.

```
>"%NFAST_HOME%\python3\python.exe" -m cloud_integration_tool microsoft-azure <your-key-name> <downloaded-pem> --azure-kek <azure-kid> --key-type <key-type>
```

Example 1: Create a module protected key named **mykey2azure**, and wrap it with the Azure KEK.

```
C:\Users\Administrator\Downloads>"%NFAST_HOME%\python3\python.exe" -m cloud_integration_tool microsoft-azure mykey2azure nshieldhsmbyokkeyvault-nShieldHSMBYOKKey-20251203.pem --azure-kek https://nshieldhsmbyokkeyvault.vault.azure.net/keys/nShieldHSMBYOKKey/28ec0aa4fd2240b9a8d331e96a0f1d26 --key-type RSA-2048
Module Protected

FIPS: insert OCS/ACS:
 Module 1: 0 cards read
 Module 1 slot 0: empty
 Module 1 slot 0: blank card
 Module 1 slot 0: empty
Card reading complete.

Provider: microsoft-azure
  Importing key 'nshieldhsmbyokkeyvault-nShieldHSMBYOKKey-20251203.pem'
Generating RSA-2048 key 'mykey2azure'
Exporting
Output json blob to KeyTransferPackage-mykey2azure.byok
Success: wrapped key exported 'KeyTransferPackage-mykey2azure.byok'
```

Example 2: Create an OCS protected key named **mykey2azure**, and wrap it with the Azure KEK. The OCS is named **testOCSpn** and has a quorum K=2.

```
C:\Users\Administrator\Downloads>"%NFAST_HOME%\python3\python.exe" -m cloud_integration_tool microsoft-azure mykey2azure nshieldhsmbyokkeyvault-nShieldHSMBYOKKey-20251203.pem --azure-kek https://nshieldhsmbyokkeyvault.vault.azure.net/keys/nShieldHSMBYOKKey/28ec0aa4fd2240b9a8d331e96a0f1d26 --key-type RSA-2048 -O testOCSpn

Loading `testOCSpn':
 Module 1: 0 cards of 2 read
 Module 1 slot 0: empty
 Module 1 slot 0: `testOCSpn' #3
 Module 1 slot 0:- passphrase supplied - reading card
 Module 1: 1 card of 2 read
```

```
 Module 1 slot 0: `testOCSpn' #3: already read
 Module 1 slot 0: empty
 Module 1 slot 0: `testOCSpn' #1
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

Provider: microsoft-azure
  Importing key 'nshieldhsmbyokkeyvault-nShieldHSMBYOKKey-20251203.pem'
Generating RSA-2048 key 'mykey2azure'
Exporting
Output json blob to KeyTransferPackage-mykey2azure.byok
Success: wrapped key exported 'KeyTransferPackage-mykey2azure.byok'
```

4. Notice the key protected by the HSM. This is the key from example 1 above.

```
>nfkminfo -k simple mykey2azure
Key AppName simple Ident mykey2azure
 BlobKA length         1092
 BlobPubKA length      484
 BlobRecoveryKA length 1480
 name                  ""
 hash                  60b7b07ac99848150073b9417ae68197b7dbada2
 recovery              Enabled
 protection            Module
 other flags           PublicKey !SEEAppKey !NVMemBlob +0x0
 gentime               2025-12-04 17:50:38
 SEE integrity key     NONE
...
No extra entries
```

5. Notice the key transfer package created.

```
C:\Users\Administrator\Downloads>dir KeyTransferPackage-mykey2azure.byok
 Volume in drive C has no label.
 Volume Serial Number is 84FA-5956

 Directory of C:\Users\Administrator\Downloads

12/04/2025  12:50 PM             2,335 KeyTransferPackage-mykey2azure.byok
               1 File(s)          2,335 bytes
               0 Dir(s)  1,915,139,063,808 bytes free
```

6. Transfer the key transfer package using media (e.g. USB thumb drive) to the online computer.

Chapter 7. Upload the wrapped key to Azure

All procedures in this section should be completed on the online computer.

1. Open a PowerShell console with administrator privileges.
2. Connect to Azure using the az command.

```
> az login --tenant <tenant-id>
```

3. Enter the following command to upload the wrapped key.

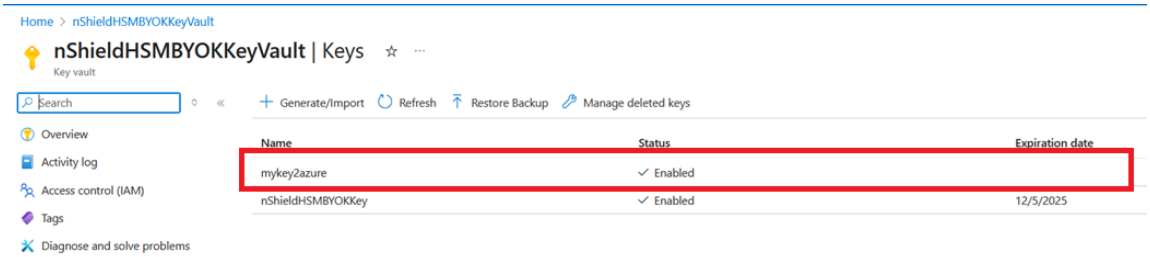
```
> az keyvault key import --vault-name <vault-name> --name <target-key-name> --byok-file <key-transfer-package>
```

For example:

```
> az keyvault key import --vault-name nShieldHSMBYOKKeyVault --name mykey2azure --byok-file KeyTransferPackage-mykey2azure.byok
{
  "attributes": {
    "created": "2025-12-04T19:41:30+00:00",
    "enabled": true,
    "expires": null,
    "exportable": false,
    "hsmPlatform": "2",
    "notBefore": null,
    "recoverableDays": 90,
    "recoveryLevel": "Recoverable+Purgeable",
    "updated": "2025-12-04T19:41:30+00:00"
  },
  "key": {
    "crv": null,
    "d": null,
    "dp": null,
    "dq": null,
    "e": "AQAB",
    "k": null,
    "keyOps": [
      "encrypt",
      "decrypt",
      "sign",
      "verify",
      "wrapKey",
      "unwrapKey"
    ],
    "kid":
"https://nshieldhsmbyokkeyvault.vault.azure.net/keys/mykey2azure/ac79c317b36546808661db25c6e20cf5",
    "kty": "RSA-HSM",
    "n":
"yfMIHuv6Mjz/+nkS5nxMxR/uFoA5MkoUc7me3awgKkLh2vvDZidsz1e6Rw0qJ31VVV/P+g6YZXSHOYrrKJHDSBb73FDqOMWzQQYTheEhSw
MLIgF9Gy2S7kQuR32jPO82f/g41ItPf9vL7KC51z3RhKPUjISpa/9O6SpIMBWEhVn6FgY8PlV9CqB0GHKGTw7X/MhRXh7Nt1BA1yOuotEzg
eNkoKetemAgnA888JbWzCCcIfUgUzB/Hixo/3aoR6HJOHPGeTBKR+AKV8mGmw4o0AQcfxOSZJVsYlnyzfPTXTw9q9q3XU0FG1lp2fLl/VmW
BGiomZr2ad/8MFgCrQsDPw==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
```

```
    "x": null,
    "y": null
  },
  "managed": null,
  "releasePolicy": null,
  "tags": null
}
```


4. Sign in to the Azure WebGUI.
5. Verify your key has been uploaded to the Azure key vault.



Chapter 8. Appendix

Operation	Description
Revoke the tenant key	This happens automatically when an organization unsubscribes from Azure RMS. This may result in loss of access to content protected via Azure RMS and the tenant key.
Refresh the tenant key	Refreshing the Azure BYOK tenant key involves updating or rotating your key that is protected by your HSM. This means repeating sections Create the Key Exchange Key in Azure, Generate, wrap, and export your own key, and Upload the wrapped key to Azure. Then the Azure services have to be updated to use the new key.
Backup and recover the tenant key	Your organization is responsible for ensuring that a copy of the tenant key is kept securely and is appropriately backup. A backup is the only way to retrieve the key. Azure RMS holds a copy of the Tokenized Key Blob that is used for recovery purposes within Azure if necessary (for example, if a node fails.) The version of the key held within Azure RMS cannot be exported.
Export the tenant key	This is not possible from Azure RMS.

Chapter 9. Glossary

Tenant key

A cryptographic key that is unique to an organization and is used as a cryptographic root of trust. The tenant key is used to secure all Rights Management cryptographic functions being undertaken by an organization within a cloud provisioned service. This helps to protect the organizations data from unauthorized third parties, including the cloud service provider.

Chapter 10. Additional resources and related products

10.1. nShield HSMs

10.2. nShield as a Service

10.3. Entrust products

10.4. nShield product documentation