THALES

Microsoft Azure Key Vault BYOK: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-013885-002
Revision	D
Release Date	5 September 2023

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

The integration of Microsoft Azure Key Vault with Thales Luna Hardware Security Modules (HSMs) in a Bring Your Own Key (BYOK) approach presents a powerful combination of cloud-based key management and hardware-level security. Azure Key Vault serves as a centralized platform for securely generating, storing, and managing cryptographic keys, while Thales Luna HSMs offer an extra layer of protection by housing these keys in a dedicated and tamper-resistant hardware environment. This integration ensures enhanced security, regulatory compliance, and granular control over key lifecycle, empowering organizations to safeguard sensitive data with stringent access controls, separation of duties, and robust key isolation. The synergy of Azure Key Vault and Thales Luna HSMs is particularly beneficial for hybrid cloud scenarios, providing a streamlined approach to key management while minimizing risks associated with insider threats and unauthorized access.

Supported HSM Devices

This integration supports:

- Thales Luna Network HSM 7 with firmware version 7.3 and above.
- Thales Luna PCIe HSM 7 with firmware version 7.3 and above.
- Thales Luna U700 USB HSM with partition in KE mode.
- Luna Cloud HSM with Key Export.

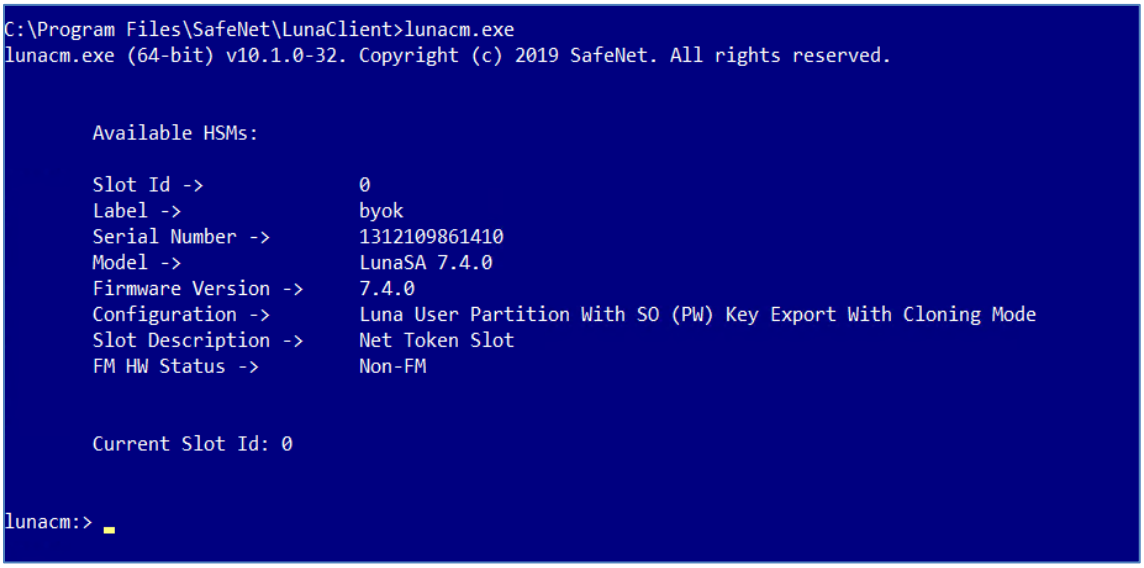
Configuring Luna HSM

To configure Luna HSM:

1. Ensure that the HSM is set up, initialized, provisioned and ready for deployment.
2. Create a partition, establish a Network Trust Link (NTL) between the HSM and client, and enable the client to access the partition.
3. Initialize the partition and Crypto Officer Role.

4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
```



5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

> **NOTE:** For a detailed description of the steps involved in Luna HSM configuration, refer to Thales Luna HSM Documentation.

Using Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the Luna HSM in FIPS mode, you have to make the following change in configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

> **NOTE:** For Universal Client 10.x onwards, above setting is not required. This setting is applicable for Luna Client 7.x only.

Configuring Luna Cloud HSM Service

To configure Luna Cloud HSM:

1. Transfer the downloaded .zip file to your Client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.

3. Extract or untar the appropriate client package for your operating system. Do not extract to a new subdirectory; place the files in the client install directory.

   `[Windows]`

   `cvclient-min.zip`

4. Run the `setenv` script to create a new configuration file containing information required by the Luna Cloud HSM service.

   `[Windows]`

   Right-click `setenv.cmd` and select `Run as Administrator.`

   > **Note:** To add the Luna Cloud HSM configuration to an already installed UC client, Open a command prompt as Administrator and use the **-addcloudhsm** option when running the **setenv** script.

5. Run the **LunaCM** utility and verify the Cloud HSM service is listed.

   > **NOTE:** For a detailed description of the steps involved in Luna Cloud HSM configuration, refer to Luna Cloud HSM documentation.

Prerequisites

Ensure that the following prerequisites are in place before initiating the Azure BYOK use case.

Setting Required Partition Policies

An HSM partition must have the following policies set before it is used for generating the BYOK Tenant Key.

- Private Key Cloning must be **OFF** to wrap the Tenant key.

  `0: Allow private key cloning : 0`

- Private Key Wrapping must be **ON** to wrap the Tenant key.

  `1: Allow private key wrapping : 1`

- Secret Key Wrapping must be **ON** to wrap the AES key generated by BYOK utility.

  `5: Allow secret key wrapping : 1`

- CBC-PAD (un)wrap must be **ON** to allow padding for any key wrap/unwrap.

  `34: Allow CBC-PAD (un)wrap keys of any size : 1`

- Optionally, keep the multipurpose key policy **ON** if you require multipurpose keys. If the policy is in **OFF** state, you can generate the key with a single purpose (Encrypt/Decrypt or Sign/Verify or Derive), but cannot club these attributes on a single key.

  `10: Allow multipurpose keys : 1`

All listed policies must be set as described above to successfully generate and wrap the Tenant Key using BYOK utility.

Downloading HSM BYOK Tool

To simplify the key export and import process of tenant keys, Thales has created an `hsmbyok` utility. The utility is available to download from the Thales Customer Support portal.

> **NOTE:** KB Article for Luna 7 HSM BYOK utility is KB0021016.
> DOW ID for Luna 7 HSM BYOK utility is DOW0004730.

Installing Microsoft Azure CLI

Installing Microsoft Azure CLI is a prerequisite for executing the commands outlined in this guide. These commands should be executed within the environment where both the Microsoft Azure CLI and Luna HSM client are installed. You can download the Microsoft Azure CLI from the following link: https://docs.microsoft.com/cli/azure/install-azure-cli

> **NOTE:** Azure CLI version 2.0.82 or newer is required for Azure Key Vault BYOK operations.

Obtaining Azure Key Vault Premium Subscription

To support HSM-protected keys, you are required to obtain Azure Key Vault Premium P2 subscription that includes HSM support for Azure Key Vault.

Supported Key Types

This integration is certified with Luna HSM on following type of keys:

Key Name	Key Type	Key Size/Curve	Origin of the Key	Description
Key Exchange Key (KEK)	RSA-HSM	2,048-bit 3,072-bit 4,096-bit	Azure Key Vault (Managed HSM)	An HSM-backed RSA key pair generated in Managed HSM
Target Key (Tenant Key)	RSA-HSM	2,048-bit 3,072-bit 4,096-bit	Luna HSM	The key to be transferred to the Managed HSM
	EC-HSM	P-256 P-384 P-521	Luna HSM	The key to be transferred to the Managed HSM

Generate and Transfer your tenant key from Luna HSM to the Key Vault Managed HSM

Here are the key stages to generate and transfer your tenant key from Luna HSM to Azure Key Vault Managed HSM:

> Generating Key Exchange Key (KEK)

> Downloading KEK Public Key

> Generating and Preparing your Tenant Key

> Transferring Tenant Key to Azure Key Vault

Generating Key Exchange Key (KEK)

The Key Exchange Key (KEK) is an RSA key that is generated within the Key Vault HSM. To ensure a secure and accurate KEK generation process, it is essential to adhere to the following steps:

> The KEK should be an RSA-HSM key, with options for 2048-bit, 3072-bit, and 4096-bit encryption.

> The KEK must be generated within the same Managed HSM in the Key Vault where you plan to import the tenant key.

> The generated KEK must have its key operation set to “import”.

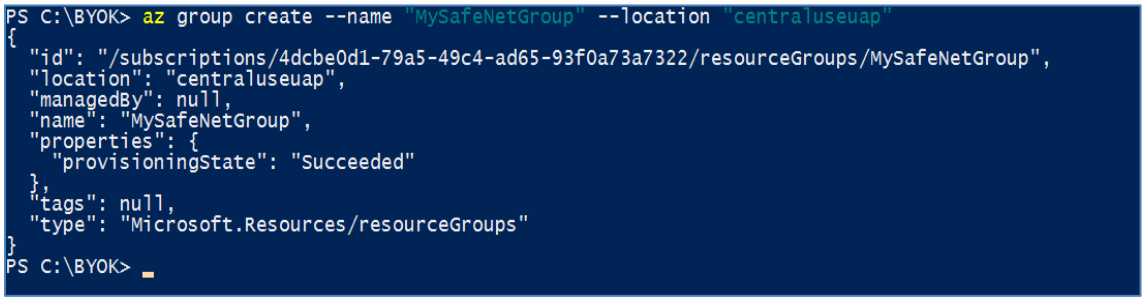
To generate a KEK:

1. Open PowerShell on your workstation where both Luna Client and Azure CLI are installed and operational. Log in to the Azure portal using the subscription that grants access to Azure Key Vault. When promoted, provide your Azure credentials.

   ```
   PS C:\BYOK> az login
   ```

2. Use the `az group create` command to create a resource group that is required for the Azure Key Vault setup. For example:

```
PS C:\BYOK> az group create --name "<resource_group>" --location
"centraluseuap"
```



NOTE: Replace "<resource_group>" with the actual name of your resource group. Check the Microsoft Docs for supported locations where the Key Vault Managed HSM is available:

https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/?products=key-vault&regions=all

3. Use the `az keyvault create` command to build a key vault with a premium SKU. For example:

```
PS C:\BYOK> az keyvault create --location centraluseuap --name <key_vault> --
resource-group <resource_group> --sku premium
```

NOTE: Replace <key_vault> and <resource_group> with your specific resource group and key vault name.

4. Use the `az keyvault key create` command to create KEK with key operations set to `import`. Here, replace `KEK2048-BYOK` with the name you want for your KEK within the Azure HSM Key Vault:

```
PS C:\BYOK> az keyvault key create --name KEK2048-BYOK --vault-name <key_vault>
--kty RSA-HSM --size 2048 --ops import
```

Please remember to replace `<key_vault>` with the name of your selected Azure HSM Key Vault name. Once you've successfully generated the KEK, be sure to take note of its unique key identifier for use in the following steps. It'll look something like this:

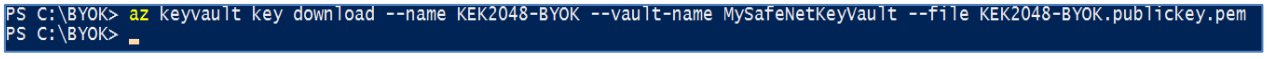
`https://mysafenetkeyvault.vault.azure.net/keys/KEK2048-BYOK/cdf405fb31414d4fb3b003d9dd5c4284`

> **NOTE:** Keep in mind that your KEK could be an RSA key of size 2048-bit, 3072-bit, or 4096-bit, depending on your requirements.

Downloading KEK Public Key

To encrypt your tenant key, you'll need the Public Key of the KEK. Use the `az keyvault key download` command to download the KEK public key in PEM format. Ensure that `KEK2048-BYOK.publickey.pem` matches your KEK Public Key's name in PEM format.

```
PS C:\BYOK> az keyvault key download --name KEK2048-BYOK --vault-name
MySafeNetKeyVault --file KEK2048-BYOK.publickey.pem
```



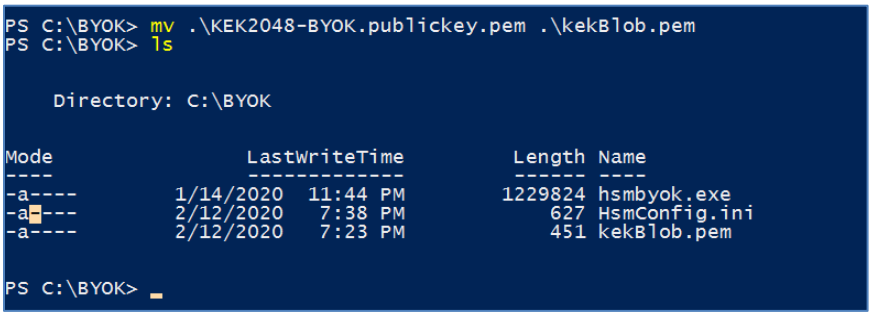
Generating and Preparing your Tenant Key

To create and ready your tenant key, follow these streamlined steps:

1. Extract the BYOK tool you downloaded from the Thales Support Portal into a designated directory. Inside the tool, you'll find a utility named **hsmbyok**. This utility has a dual purpose: generating a tenant key and creating a Key Transfer Package (a BYOK file). The BYOK tool leverages the key identifier obtained in a previous step and the PEM file that you downloaded in another step to generate an encrypted tenant key in the BYOK format.
2. Transfer the PEM file that you downloaded in a previous step into the same directory where you extracted the BYOK tool.
3. Rename the downloaded PEM file to the name required by BYOK tool using the following command:

   ```
   PS C:\BYOK> mv .\KEK2048-BYOK.publickey.pem .\kekBlob.pem
   ```

   Ensure that both the BYOK utility and `kekBlob.pem` file coexist in the same directory for seamless operations.



4. Create an **HsmConfig.ini** in the same directory as the BYOK utility and PEM file. Its contents should be structured like the following example:

```
[ byok ]
  ; cryptoki library
  libraryName = "C:\Program Files\SafeNet\LunaClient\cryptoki.dll"

  ; label of partition
  tokenLabel = "byok"

  ; available ciphers for wrapping
  wrappingCiphers = CKG_MGF1_SHA1, CKM_AES_KWP

  ; label of key to find/generate
  targetKeyName = "my-target-key-rsa2048"
```

```
  ; details of key to generate
  targetKeySpec = CKK_RSA, 2048, none
  targetKeyFlags = CKF_ENCRYPT, CKF_DECRYPT, CKF_SIGN, CKF_VERIFY,
CKF_DERIVE, CKF_TOKEN, CKF_MODIFIABLE,
CKF_EXTRACTABLE,CKF_CREATE_IF_NOT_FOUND


  ; Azure kid
  kid = "https://mysafenetkeyvault.vault.azure.net/keys/KEK2048-
BYOK/cdf405fb31414d4fb3b003d9dd5c4284"
  ; Azure schema
  SchemaVersion = "1.0.0.0"
```

Remember the following details as you set up your `HsmConfig.ini`:

- `tokenLabel` represents your HSM partition label.
- `targetKeyName` is the name of the key to be generated if it doesn't already exist.
- `kid` refers to the key identifier generated in a previous step.
- For `targetKeySpec`, specify supported keys in the following manner:

  `CKK_RSA, 2048, none` (for RSA Keys)

  `CKK_EC, 384, "P-384"` (for EC Keys)

```
Supported EC curveName / curveAliasName:


    "X9_62_prime256v1"  "P-256"
    "secp384r1"         "P-384"
    "secp521r1"         "P-521"
```

NOTE: In case policy 10 is off, the target key will be a single-purpose key and you need to use only one of the following attributes for `targetKeyFlags`, in addition to `CKF_TOKEN`, `CKF_MODIFIABLE`, `CKF_EXTRACTABLE`, and `CKF_CREATE_IF_NOT_FOUND`:

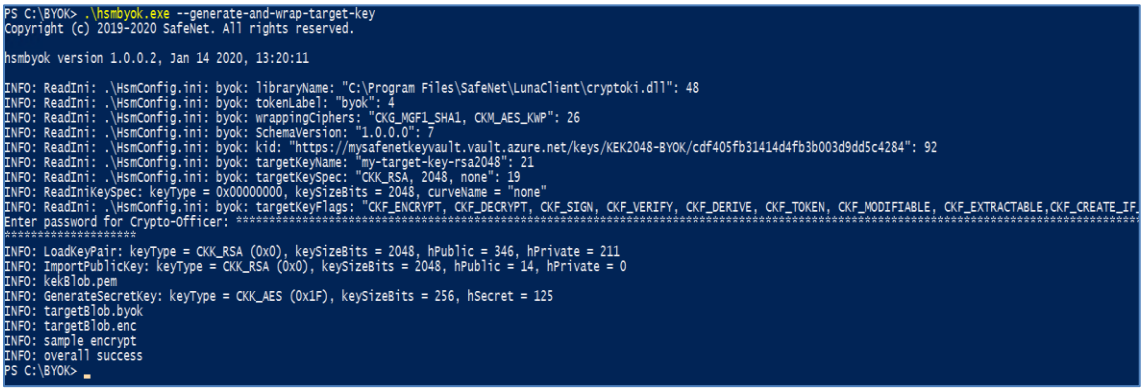
`CKF_ENCRYPT, CKF_DECRYPT`

`CKF_SIGN, CKF_VERIFY`

`CKF_DERIVE`

5. Run the `hsmbyok` utility to create the Key Transfer Package (a byok file).

```
PS C:\BYOK> .\hsmbyok.exe --generate-and-wrap-target-key
```



This action will generate the "targetBlob.byok" file in JSON format, which contains the following information:

```
{
  "schema_version": "1.0.0",
  "header":
  {
    "kid": "<key identifier of the KEK>",
    "alg": "dir",
    "enc": "CKM_RSA_AES_KEY_WRAP"
  },
  "ciphertext":"BASE64URL(<ciphertext contents>)"
  "generator": "byok tool name and version; source HSM name and firmware version"
}
```

Transferring Tenant Key to Azure Key Vault

For the final steps of transferring your tenant key to Azure Key Vault, proceed as follows:

1. Utilize the `az keyvault key import` command to upload the byok file created in a previous step.

   For RSA Keys:

   ```
   PS C:\BYOK> az keyvault key import --vault-name MySafeNetKeyVault --name SafeNetRSA2048HSMkey --byok-file .\targetBlob.byok --protection hsm
   ```

   Here, `SafeNetRSA2048HSMkey` is name of your RSA tenant key imported into the Azure HSM Key Vault.

   For EC Keys:

   ```
   PS C:\BYOK> az keyvault key import --vault-name MySafeNetKeyVault --name SafeNetEC256HSMkey --byok-file .\targetBlob.byok --kty EC --curve "P-256" --protection hsm
   ```

Note: When importing an EC key, it's essential to utilize the --kty EC --curve command along with the appropriate value. However, for RSA keys, this specification isn't necessary as it's the default key type.

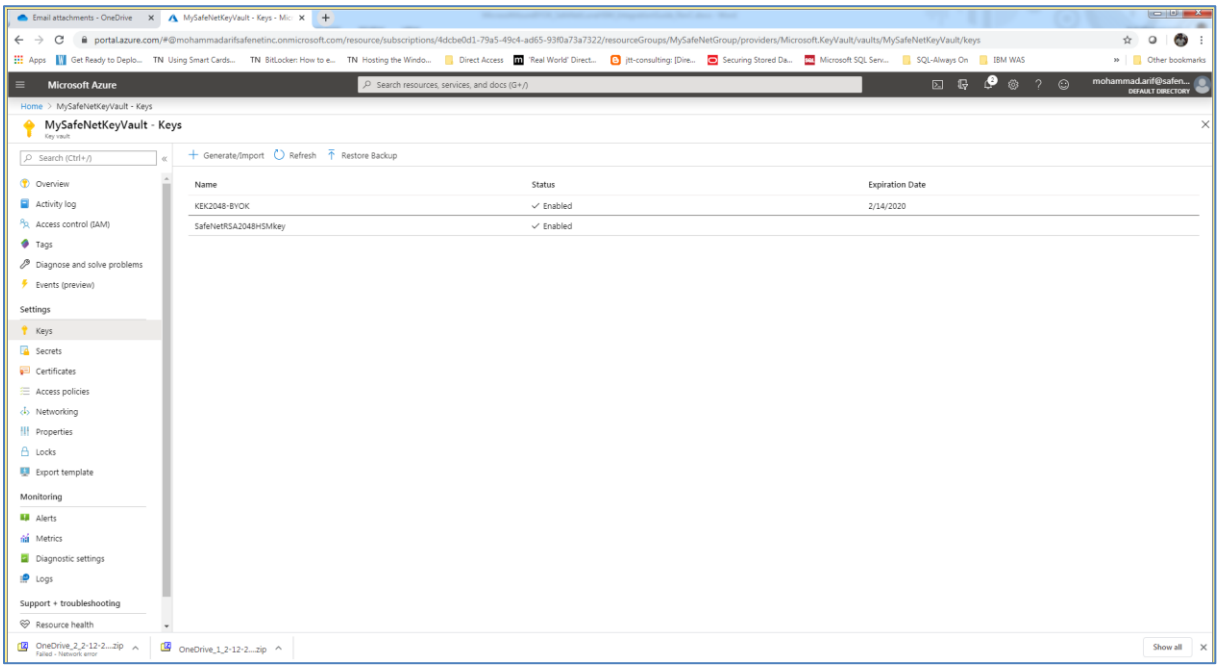
```
PS C:\BYOK> az keyvault key import --vault-name MySafeNetKeyVault --name SafeNetRSA2048HSMkey --byok-file .\targetBlob.byok --protection hsm
{
  "attributes": {
    "created": "2020-02-12T16:49:24+00:00",
    "enabled": true,
    "expires": null,
    "notBefore": null,
    "recoverableDays": 0,
    "recoveryLevel": "Purgeable",
    "updated": "2020-02-12T16:49:24+00:00"
  },
  "key": {
    "crv": null,
    "d": null,
    "dp": null,
    "dq": null,
    "e": "AAEAAQ==",
    "k": null,
    "keyOps": [
      "encrypt",
      "decrypt",
      "sign",
      "verify",
      "wrapKey",
      "unwrapKey"
    ],
    "kid": "https://mysafenetkeyvault.vault.azure.net/keys/SafeNetRSA2048HSMkey/1da3d9493b5d490581d5aa911530c890",
    "kty": "RSA-HSM",
    "n": "3eAZjbBfQZu/YlHZ1yXFd7pSajYeNgOPi5Zuxsxxq1bwl4vPOwmkFgfUZ2SAYUTqrmb5x29HaOmMrtys1gz2hOPc3mczfYklzIKM/TkPS6KsK7geWze9HfDd7240/iiVD1al3L5uKfOSHUxEUv6K8govcQ4KLeiBQh1E16Ds32XnY/DO9rTex+kDmSs46OVdz+dBWxWPotMKx8m8zhdX9JlpSCPFCigzSsTNjsFLAfeI6Or1bQ==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
    "x": null,
    "y": null
  },
  "managed": null,
  "tags": null
}
PS C:\BYOK>
```

2. Use the `az keyvault key show` command to display the imported tenant key.

   `PS C:\BYOK> az keyvault key show --vault-name MySafeNetKeyVault --name SafeNetRSA2048HSMKey`

```
PS C:\BYOK> az keyvault key show --vault-name MySafeNetKeyVault --name SafeNetRSA2048HSMKey
{
  "attributes": {
    "created": "2020-02-17T06:57:44+00:00",
    "enabled": true,
    "expires": null,
    "notBefore": null,
    "recoverableDays": 0,
    "recoveryLevel": "Purgeable",
    "updated": "2020-02-17T06:57:44+00:00"
  },
  "key": {
    "crv": null,
    "d": null,
    "dp": null,
    "dq": null,
    "e": "AAEAAQ==",
    "k": null,
    "keyOps": [
      "encrypt",
      "decrypt",
      "sign",
      "verify",
      "wrapKey",
      "unwrapKey"
    ],
    "kid": "https://mysafenetkeyvault.vault.azure.net/keys/SafeNetRSA2048HSMkey/08f86023365d4673b9c5539d26f4a316",
    "kty": "RSA-HSM",
    "n": "3eAZjbBfQZu/YlHZ1yXFd7pSajYeNgOPi5Zuxsxxq1bwl4vPOwmkFgfUZ2SAYUTqrmb5x29HaOmMrtys1gz2hOPc3mczfYklzIKM/TkPS6KsK7geWze9HfDd7240/iiVD1al3L5uKfOSHUxEUv6K8govcQ4KLeiBQh1E16Ds32XnY/DO9rTex+kDmSs46OVdz+dBWxWPotMKx8m8zhdX9JlpSCPFCigzSsTNjsFLAfeI6Or1bQ==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
    "x": null,
    "y": null
  },
  "managed": null,
  "tags": null
}
```

The tenant key you've imported will also appear in the Azure Key Vault under **Settings - Keys**.



This concludes the integration of Azure Key Vault BYOK with Luna HSM, allowing the import of tenant keys generated on on-premises HSMs into Azure Key Vault. These tenant keys are now accessible for utilization by Azure Services, including the creation of Azure-generated keys.

Contacting Customer Support

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.