



Microsoft Azure Key Vault BYOK

INTEGRATION GUIDE

THALES LUNA HSM

Document Information

Document Part Number	007-013885-002
Release Date	3 June 2020

Revision History

Revision	Date	Reason
A	19 February 2020	New
B	3 June 2020	Update

Trademarks, Copyrights, and Third-Party Software

Copyright © 2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

CONTENTS

Supported HSM Devices.....	4
Configuring Luna HSM.....	4
Using Luna HSM in FIPS Mode.....	5
Prerequisites	5
Setting Required Partition Policies	5
Downloading HSM BYOK Tool	5
Installing Microsoft Azure CLI.....	6
Obtaining Azure Key Vault Premium Subscription	6
Generating Key Exchange Key (KEK)	6
Downloading KEK Public Key	8
Generating and Preparing your Tenant Key	8
Transferring Tenant Key to Azure Key Vault	11
Contacting Customer Support	13
Customer Support Portal.....	13
Telephone Support.....	13
Email Support.....	13

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.

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
```

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v10.1.0-32. Copyright (c) 2019 SafeNet. All rights reserved.

Available HSMs:

Slot Id ->          0
Label ->           byok
Serial Number ->   1312109861410
Model ->           LunaSA 7.4.0
Firmware Version -> 7.4.0
Configuration ->   Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status ->    Non-FM

Current Slot Id: 0

lunacm:> █
```

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, above setting is not required. This setting is applicable for Luna Client 7.x only.

Prerequisites

Ensure that you fulfill the following prerequisites.

Setting Required Partition Policies

A partition must have the following policies settings for the partition that 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/uwrap.
34: Allow CBC-PAD (un)wrap keys of any size : 1
- > Optionally, keep the multipurpose key policy **OFF** if you don't want to generate multipurpose keys. In the **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

Install the Microsoft Azure CLI on your system to run commands mentioned in this guide. You can run the commands in this instruction wherever you have installed the Microsoft Azure CLI and Luna HSM client. The link to download Microsoft Azure CLI is: <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

Obtaining Azure Key Vault Premium Subscription

To support HSM-protected keys, you are required to obtain Azure Key Vault Premium Service subscription along with existing Azure Cloud subscription.

Generating Key Exchange Key (KEK)

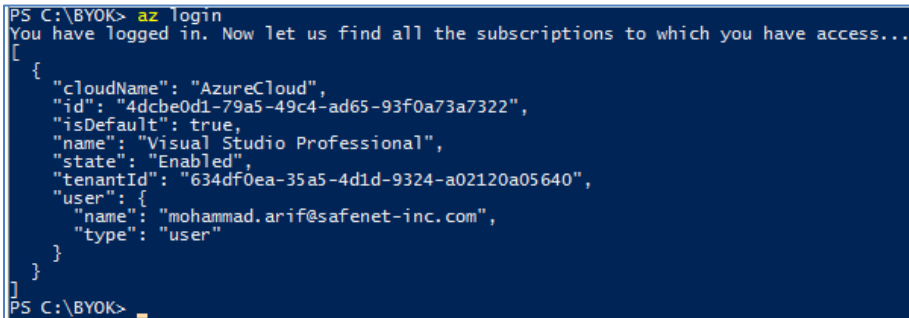
The KEK (Key Exchange Key) is an RSA key generated in Key Vault HSM. KEK must be:

- > An RSA-HSM key (2048-bit or 3072-bit or 4096-bit)
- > Generated in the same key vault where you intend to import the tenant key
- > Created with allowed key operations set to import

To Generate Key Exchange Key (KEK):

1. Open the PowerShell and Log on to the azure portal that has the required subscription for using Azure Key Vault and provide your azure credentials.

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



```
PS C:\BYOK> az login
You have logged in. Now let us find all the subscriptions to which you have access...
[
  {
    "cloudName": "AzureCloud",
    "id": "4dcbe0d1-79a5-49c4-ad65-93f0a73a7322",
    "isDefault": true,
    "name": "Visual Studio Professional",
    "state": "Enabled",
    "tenantId": "634df0ea-35a5-4d1d-9324-a02120a05640",
    "user": {
      "name": "mohammad.arif@safenet-inc.com",
      "type": "user"
    }
  }
]
PS C:\BYOK> _
```

2. Use the **az group create** command to create a resource group that is required to create the Azure Key Vault.

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

```
PS C:\BYOK> az group create --name "MySafeNetGroup" --location "centraluseup"
{
  "id": "/subscriptions/4dcbe0d1-79a5-49c4-ad65-93f0a73a7322/resourceGroups/MySafeNetGroup",
  "location": "centraluseup",
  "managedBy": null,
  "name": "MySafeNetGroup",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
PS C:\BYOK>
```

NOTE: Replace the <resource_group> with actual name of your resource group. Currently only Central US EUAP and East US EUAP are supported for generating the KEK.

3. Use the **az keyvault create** command to create a key vault with premium SKU.

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

```
PS C:\BYOK> az keyvault create --location centraluseup --name MySafeNetKeyVault --resource-group MySafeNetGroup --sku premium
{
  "id": "/subscriptions/4dcbe0d1-79a5-49c4-ad65-93f0a73a7322/resourceGroups/MySafeNetGroup/providers/Microsoft.KeyVault/vaults/MySafeNetKeyVault",
  "location": "centraluseup",
  "name": "MySafeNetKeyVault",
  "properties": {
    "accessPolicies": [
      {
        "applicationId": null,
        "objectId": "e5b474f3-ce31-4dcb-91ef-4c54d7c1e0eb",
        "permissions": {
          "certificates": [
            "get",
            "list",
            "delete",
            "create",
            "import",
            "update",
            "managecontacts",
            "getissuers",
            "listissuers",
            "setissuers",
            "deleteissuers",
            "manageissuers",
            "recover"
          ],
          "keys": [
            "get",
            "create",
            "delete",
            "list",
            "update",
            "import",
            "backup",
            "restore",
            "recover"
          ],
          "secrets": [
            "get",
            "list",
            "delete",
            "backup",
            "restore",
            "recover"
          ],
          "storage": [
            "get",
            "list",
            "delete",
            "set",
            "update",
            "regeneratekey",
            "setsas",
            "listsas",
            "getsas",
            "deletesas"
          ]
        }
      }
    ],
    "tenantId": "634df0ea-35a5-4d1d-9324-a02120a05640"
  },
  "createMode": null,
  "enablePurgeProtection": null,
  "enableSoftDelete": null,
  "enabledForDeployment": false,
  "enabledForDiskEncryption": null,
  "enabledForTemplateDeployment": null,
  "networkAcls": null,
  "provisioningState": "Succeeded",
  "sku": {
    "name": "premium"
  },
  "tenantId": "634df0ea-35a5-4d1d-9324-a02120a05640",
  "vaultUri": "https://mysafenetkeyvault.vault.azure.net/"
},
  "resourceGroup": "MySafeNetGroup",
  "tags": {},
  "type": "Microsoft.KeyVault/vaults"
}
PS C:\BYOK>
```

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

4. Use the **az keyvault key create** command to create KEK with key operations set to import.

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

```
PS C:\BYOK> az keyvault key create --name KEK2048-BYOK --vault-name MySafeNetKeyVault --key RSA-HSM --size 2048 --ops import
{
  "attributes": {
    "created": "2020-02-12T13:50:03+00:00",
    "enabled": true,
    "expires": "2020-02-14T13:50:03+00:00",
    "notBefore": null,
    "recoverableDays": 0,
    "recoveryLevel": "purgeable",
    "updated": "2020-02-12T13:50:03+00:00"
  },
  "key": {
    "crv": null,
    "d": null,
    "dp": null,
    "dq": null,
    "e": "AAEAAQ==",
    "k": null,
    "keyOps": [
      "import"
    ]
  },
  "kid": "https://mysafenetkeyvault.vault.azure.net/keys/KEK2048-BYOK/cdf405fb31414d4fb3b003d9dd5c4284",
  "kty": "RSA-HSM",
  "n": "vbVcZavtz5HLD3aog7QL2vzpSTmdIDnFtagQ8JTDKHMqG82iaFizowhvuauKvpAq2Y7AdcRHKXgt5+hnnmL9no1gA0174+RzArDviMVT/JDMiHtuGDs30I2mocCsXNdS8HSeQEVGpVakq4IEMHXzoqj9t6p938FalVL5IRw156GctFy2M6TXId5MBjGud5EgkQ4d28VNYGPxuqW4Y31VkeqCYIeqwtW==",
  "p": null,
  "q": null,
  "qi": null,
  "t": null,
  "x": null,
  "y": null
},
  "managed": null,
  "tags": null
}
PS C:\BYOK>
```

Where KEK2048-BYOK is the name of your KEK to be generated on Azure HSM key Vault. When the KEK is generated, note down the key identifier for the generated key because it will be later used in step. For example:

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

NOTE: Key Exchange Key (KEK) could be an RSA key of size 2048-bit or 3072-bit or 4096-bit.

Downloading KEK Public Key

You need to download the Public Key of the KEK generated on Azure HSM Key Vault. Public key is required to encrypt your tenant key. To Download the KEK Public Key:

5. Use the **az keyvault key download** command to download the KEK public key into a PEM format.

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

Where KEK2048-BYOK.publickey.pem is the name of your KEK Public Key in PEM format.

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

Generating and Preparing your Tenant Key

Extract the BYOK tool downloaded from Thales Support Portal in to a directory. The tool will have an hsmbyok utility that will be use to generate a tenant key and then create a Key Transfer Package (a byok file). The BYOK tool will use the key identifier from **Step 4** and PEM file you downloaded in **Step 5** to generate an encrypted tenant key in a byok file.

NOTE: Tenant key must be an RSA key of size 2048-bit or 3072-bit or 4096-bit. Importing Elliptic Curve keys is not supported at this time.

Importing RSA 4096-bit tenant key from Luna HSMs is supported for HSM firmware v7.4.0 or above.

Transfer the PEM file you downloaded in **Step 5** on your system and place the file in same location where you have extracted the BYOK tool. To Generate and Prepare Tenant Key

6. Rename the downloaded PEM file with the name required by BYOK tool using the command below.

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

Ensure that BYOK utility and `kekBlob.pem` file are present in the same directory.

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

Directory: C:\BYOK

Mode                LastWriteTime         Length Name
----                -
-a----             1/14/2020  11:44 PM     1229824 hsmbyok.exe
-a----             2/12/2020   7:38 PM         627 HsmConfig.ini
-a----             2/12/2020   7:23 PM         451 kekBlob.pem

PS C:\BYOK> _
```

7. Create INI file **HsmConfig.ini** in the same directory where byok utility and PEM file is present, with the below contents:

```
-----
[ 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"

```

Where;

tokenLabel is your HSM partition label.

targetKeyName is the name of key to be generated if don't exist.

kid is the key identifier generated in the **Step 4**.

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

```

8. Run **hsmbyok** utility to generate and create the Key Transfer Package (a byok file).

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

```

PS C:\BYOK> .\hsmbyok.exe --generate-and-wrap-target-key
Copyright (c) 2019-2020 SafeNet. All rights reserved.

hsmbyok version 1.0.0.2, Jan 14 2020, 13:20:11

INFO: ReadIni: .\HsmConfig.ini: byok: libraryName: "C:\Program Files\SafeNet\LunaClient\cryptoki.dll": 48
INFO: ReadIni: .\HsmConfig.ini: byok: tokenLabel: "byok": 4
INFO: ReadIni: .\HsmConfig.ini: byok: wrappingCiphers: "CKG_MGF1_SHA1, CKM_AES_KWP": 26
INFO: ReadIni: .\HsmConfig.ini: byok: SchemaVersion: "1.0.0.0": 7
INFO: ReadIni: .\HsmConfig.ini: byok: kid: "https://mysafenetkeyvault.vault.azure.net/keys/KEK2048-BYOK/cdf405fb31414d4fb3b003d9dd5c4284": 92
INFO: ReadIni: .\HsmConfig.ini: byok: targetKeyName: "my-target-key-rsa2048": 21
INFO: ReadIni: .\HsmConfig.ini: byok: targetKeySpec: "CKK_RSA, 2048, none": 19
INFO: ReadIniKeySpec: keyType = 0x00000000, keySizeBits = 2048, curveName = "none"
INFO: ReadIni: .\HsmConfig.ini: byok: targetKeyFlags: "CKF_ENCRYPT, CKF_DECRYPT, CKF_SIGN, CKF_VERIFY, CKF_DERIVE, CKF_TOKEN, CKF_MODIFIABLE, CKF_EXTRACTABLE, CKF_CREATE_IF
Enter password for Crypto-Officer: *****
INFO: LoadKeyPair: keyType = CKK_RSA (0x0), keySizeBits = 2048, hPublic = 346, hPrivate = 211
INFO: ImportPublicKey: keyType = CKK_RSA (0x0), keySizeBits = 2048, hPublic = 14, hPrivate = 0
INFO: kekBlob.pem
INFO: GenerateSecretKey: keyType = CKK_AES (0x1F), keySizeBits = 256, hSecret = 125
INFO: targetBlob.byok
INFO: targetBlob.enc
INFO: sample encrypt
INFO: overall success
PS C:\BYOK>

```

It will generate the **targetBlob.byok** file in the JSON format which have the following:

```

{
  "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 this final step, use the key import command to upload the byok file that is created in the **Step 8**. If the upload is successful, you can displayed the properties of the key that you just imported in Azure HSM Key Vault. To Transfer Tenant Key in Azure Key Vault:

- Use the **az keyvault key import** command to upload the byok file containing encrypted tenant key.

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

Where `SafeNetRSA2048HSMkey` is name of your tenant key imported in to the Azure HSM Key Vault.

```

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",
    "ktv": "RSA-HSM",
    "n": "3eAZjbbFQzu/YlHZ1yXfD7pSajYeNg0P15Zuxsxxq1bw14vP0wmkFgFUZ2SAyUTqrmB5x29HaQmMrtys1gz2h0Pc3mczfYk1zIKM/TkP56KsK7gewze9HF0d7240/iiVd1a13L5uKf0SHUXEUv6K8g0vcQ4KLe1BQh1E16ds32Xnl/009rTex+kDmSs460vdz+dBwXwPotMkx8m8zhdX9j1pSCPFc1gzSsTNjsFLAFe160r1bq==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
    "x": null,
    "y": null
  },
  "managed": null,
  "tags": null
}
PS C:\BYOK>

```

- Use the **az keyvault key show** command to display the imported tenant key.

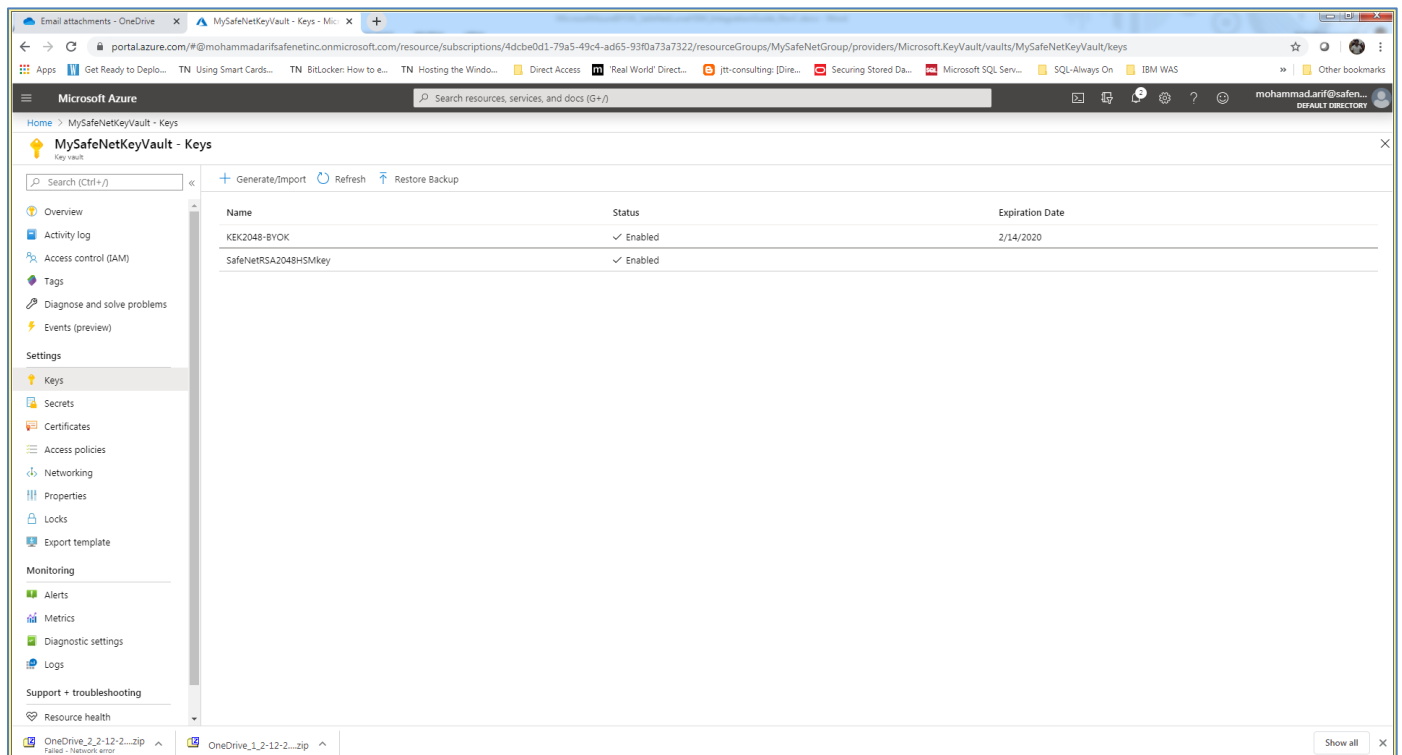
```
PS C:\BYOK> az keyvault key show --vault-name MySafeNetKeyVault --name SafeNetRSA2048HSMKey
```

```

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/Y1hZ1yXFd7pSajYeNg0Pj5ZuXsxxq1bw14vPQwmkFgFuZ2SAYUTrmb5x29HaoMmRtys1gz2h0Pc3mczfYk1zIKM/TkPS6KsK7gewze9Hfd7240/iVD1a13LSukF0SHUXEuv6K8govc4KLeibh1E16Ds32XnV/009rTex+kDmSs46oVdz+dBwXWPotMkx8m8zhdX9J1pSCPFC1gzSsTNjsFLAfEi60r1bQ==",
    "p": null,
    "q": null,
    "qi": null,
    "t": null,
    "x": null,
    "y": null
  },
  "managed": null,
  "tags": null
}

```

The RSA tenant key will also be displayed on the Azure portal under Key Vaults.



This completes the Azure Key Vault BYOK integration with Luna HSM and tenant key generated in on premise HSM is imported in to Azure Key Vault. This Tenant key is now available to use by Azure Services similar to 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.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.