Microsoft
Azure Key Vault

Integration Guide

Utimaco HSM

utimaco®

Imprint

Copyright 2020	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 Aachen
	Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
	EMEA +49 800-627-3081
	APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	06/10/2025
Status	PUBLISHED
Document No.	IG-2025-0006

Table of Contents

1 Introduction

Thank you for purchasing our CryptoServer security system. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or comments.

1.1 About this Guide

This guide describes how to bring your own key into the Azure Key Vault BYOK with the Utimaco Hardware Security Module (HSM).

1.1.1 Target Audience for this Guide

This guide is intended for Azure administrators and HSM administrators.

1.1.2 Document Conventions

We use the following document conventions:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Document conventions

We use special icons to highlight the most important notes and information.

Here, you find important safety information that should be followed.

Here, you find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

Certifications

Chapters with certification-specific content are marked accordingly at the beginning of the chapter, e.g. FIPS 140-3.

1.1.3 Abbreviations

We use the following abbreviations in this guide:

Abbreviation	*Meaning*
HSM	Hardware Security Module
BYOK	Bring Your Own Key
PKCS#11	Public-Key Cryptography Standard #11
CAT	Crypto Administration Tool
P11CAT	PKCS#11 Crypto Administration Tool
CLI	Command line interface
KEK	Key Exchange Key
MBK	Master Backup Key

2 Overview

2.1 Azure Key Vault

Azure Key Vault is a cloud service for securely storing and accessing "secrets". A secret is any information that you want to carefully control access to. Such examples can be API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed HSM pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. Managed HSM pools only support HSM-backed keys which need an HSM. See also Azure Key Vault REST API overview for complete details.

2.2 Utimaco CryptoServer HSM

CryptoServer is a hardware security module developed by Utimaco IS GmbH. CryptoServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3 Prerequisites and Requirements

Ensure the system environment you will be using meets the following hardware and software requirements.

This guide assumes that you already have a working Azure subscription and users created on the portal to be able to configure the Azure Key Vault.

3.1 Software Requirements

Software	*Software Requirements*
Operating system	Windows, Linux
BYOK tool	byoktool developed by Utimaco
Java	Version 8, Update 271 or higher
P11tool2	PKCS 11 command line tool
Microsoft Azure CLI	Version 2.14.1

List of Software Requirements

3.2 Hardware Requirements

Hardware	*Hardware Requirements*
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.30.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.30.0 or higher

List of Hardware Requirements

4 Implementing BYOK

Please,

make

sure

that

you

change

the

labels

in

brackets

to

what

suits

your

use

case

the

best.

Example:

Change

<

resource_group>

to

AzureKeyVaultGroup

4.1 Prerequisites

4.1.1 Azure CLI

The version of the Azure CLI used in this guide is 2.15.0. For more information regarding the most recent release, please see the Azure CLI Release Notes from Microsoft.

4.1.2 Azure Key Vault Premium

An active Azure subscription with a Preimum tier key vault to be able to create HSMprotected keys.

4.1.3 Utimaco byoktool

To simplify the key export and import process of tenant keys, Utimaco has created an HSM Bring Your Own Key tool. Please reach out to Utimaco so this tool can be provided to you. The byoktool supports all key types (PKCS#11, CNG, JCE, CXI). The storage of keys is still restricted to the internal storage on the Utimaco CryptoServer HSM. The BYOK tool does not support key creation, only migration. That is why it is important that the settings of the keys' attributes, that you would like to migrate, are set to extractable.

For more information regarding the commands and command parameters please check the Microsoft Azure CLI documentation.

4.2 Administered HSM

An HSM should be administered prior to the steps described in this guide. For more information about how to do so, please check the documentation on the corresponding Product CD.

4.3 Generating Key Exchange Key (KEK)

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

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

4.3.1 Generating Azure Key Vault

1. Open the command line interpreter and login with the following command:

   ›_ Console

   ```
   > az login
   ```

2. To create the Azure Key Vault, you will need to create a resource group. Please use the following command to create your own resource group.

   ›_ Console

   ```
   > az group create --location "<location>" --name "<resource_group>"
   ```

3. Create an Azure Key Vault with premium SKU.

   ›_ Console

   ```
   > az keyvault create --location "<location>" --name "<keyvault>"
      --resource-group "<resource_group>" --sku premium
   ```

For more information regarding the commands and command parameters, please check the Microsoft Azure CLI documentation.

4.3.2 Creating a KEK

1. Create a KEK with the key operations set to import. The KEK can be an RSA key of different sizes such as: 2048-bit, 3072-bit or 4096-bit. It is advisable to create a key with the length suitable for your use case.

   ›_ Console

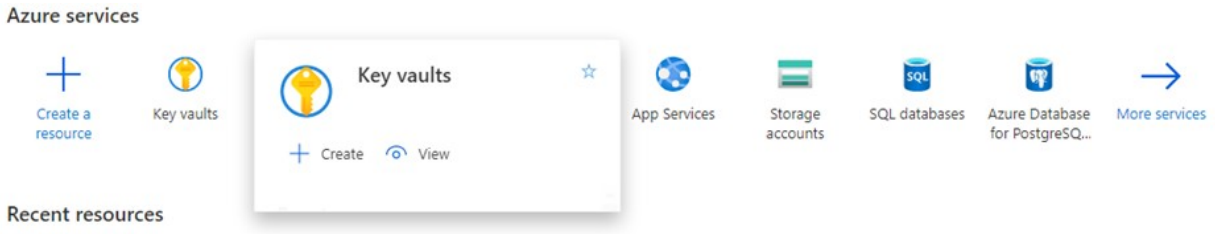
   ```
   > az keyvault key create --name "<keyvault_key>" --vault-name "<keyvault>"
    --kty RSA-HSM

    --size 2048 --ops import
   ```

After the successfully executed command, please make sure to note down the key identifier ("kid") in the command printout as it will be used for generating your tenant key.

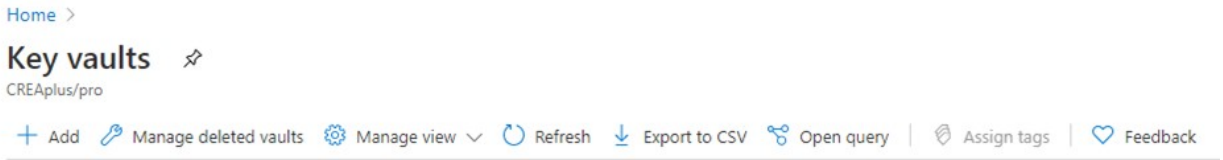
4.3.3 Generating Azure Key Vault with Azure Porta

It is also possible to create an Azure Key vault in the Azure Web Portal. To do so, follow the next steps.

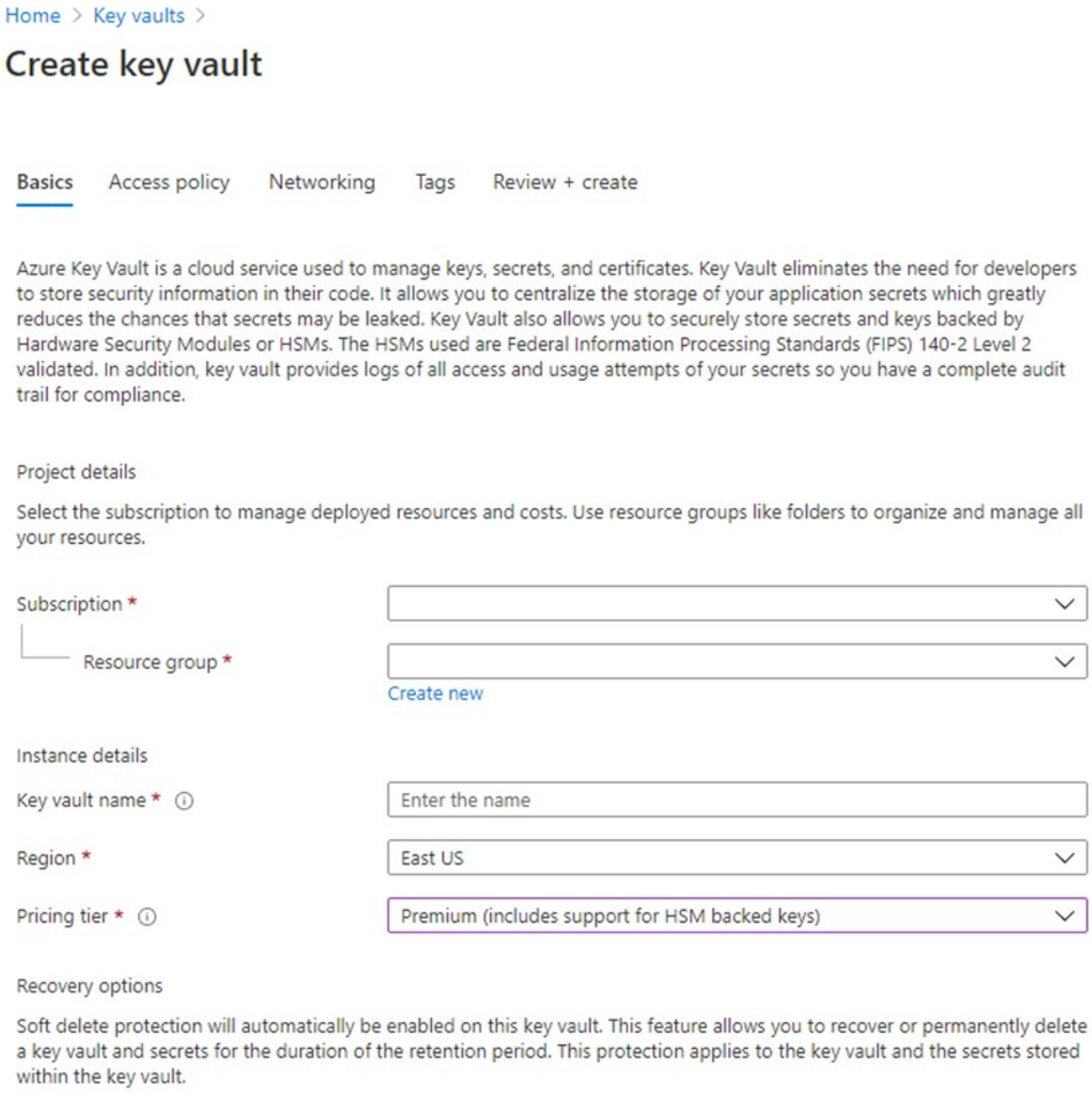
1. Navigate to http://portal.azure.com and login to your Azure Account.
2. Locate the Key vaults Azure service, click on it to get redirected to your Key vaults.

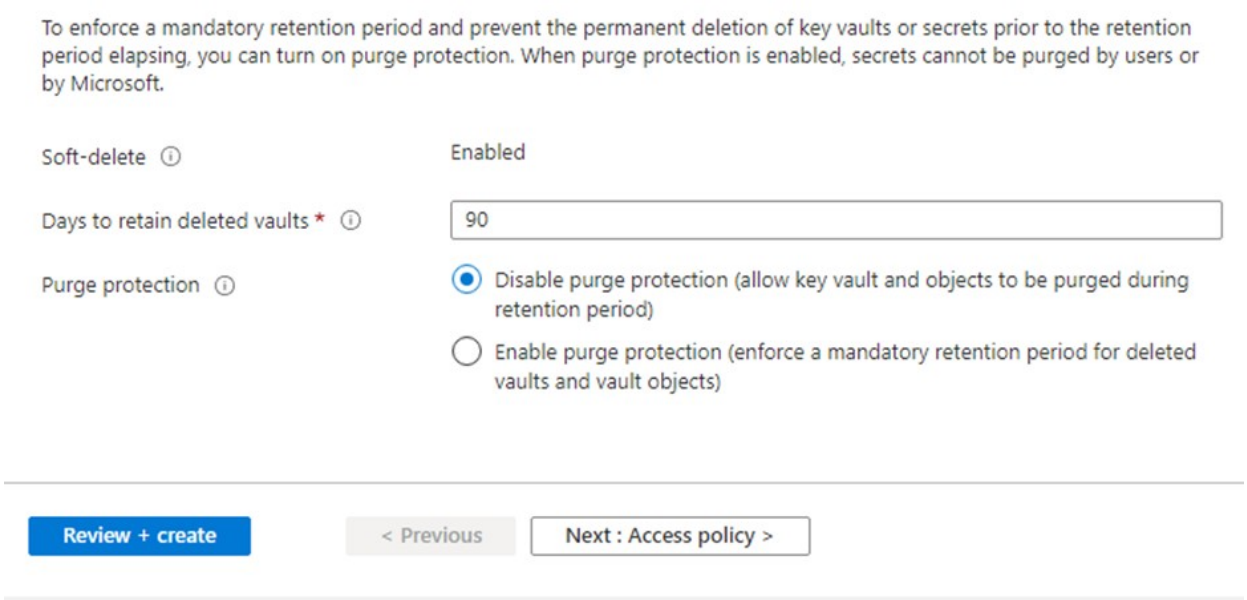


3. Click on **+ Add** to start the process of adding a Key vault.

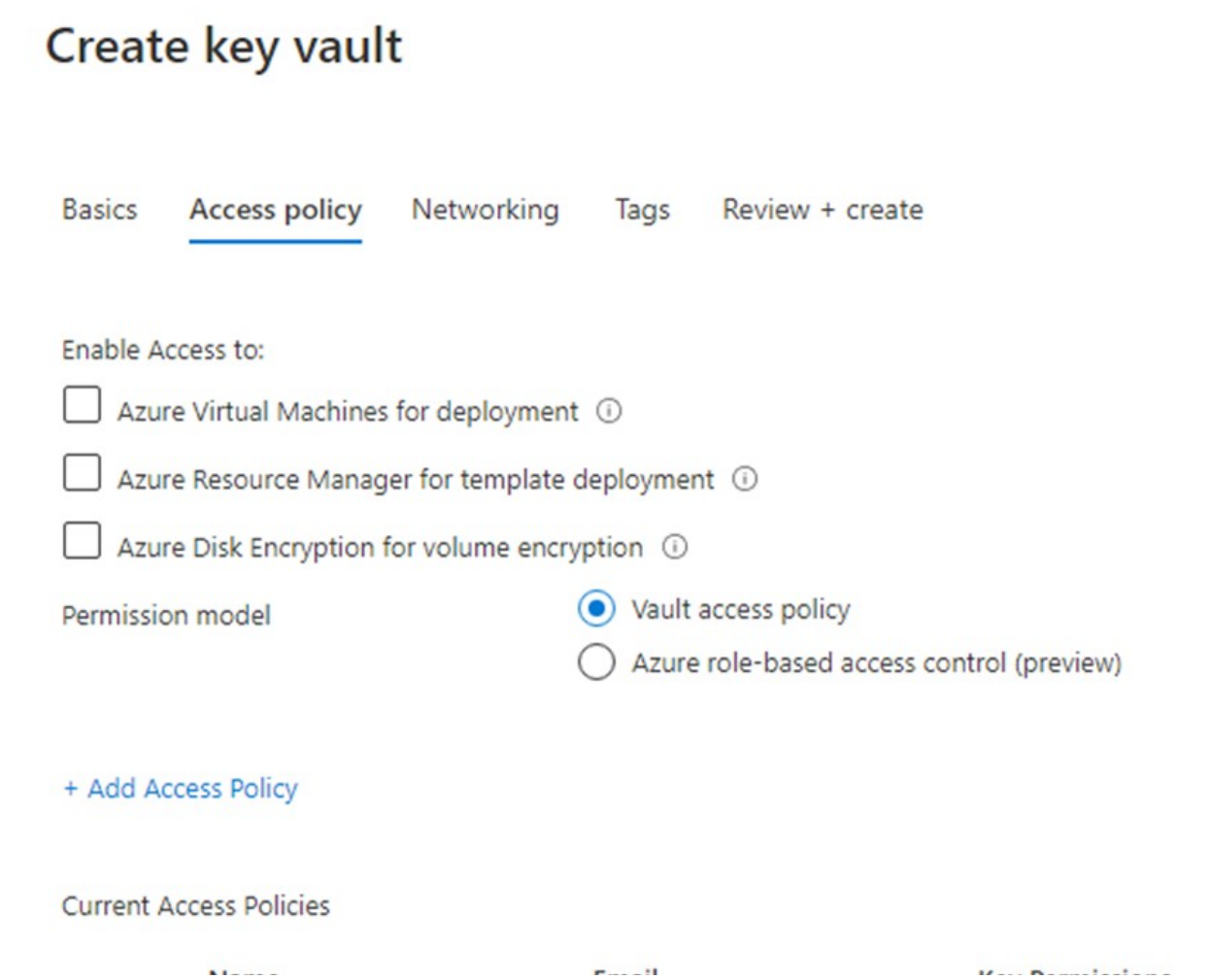


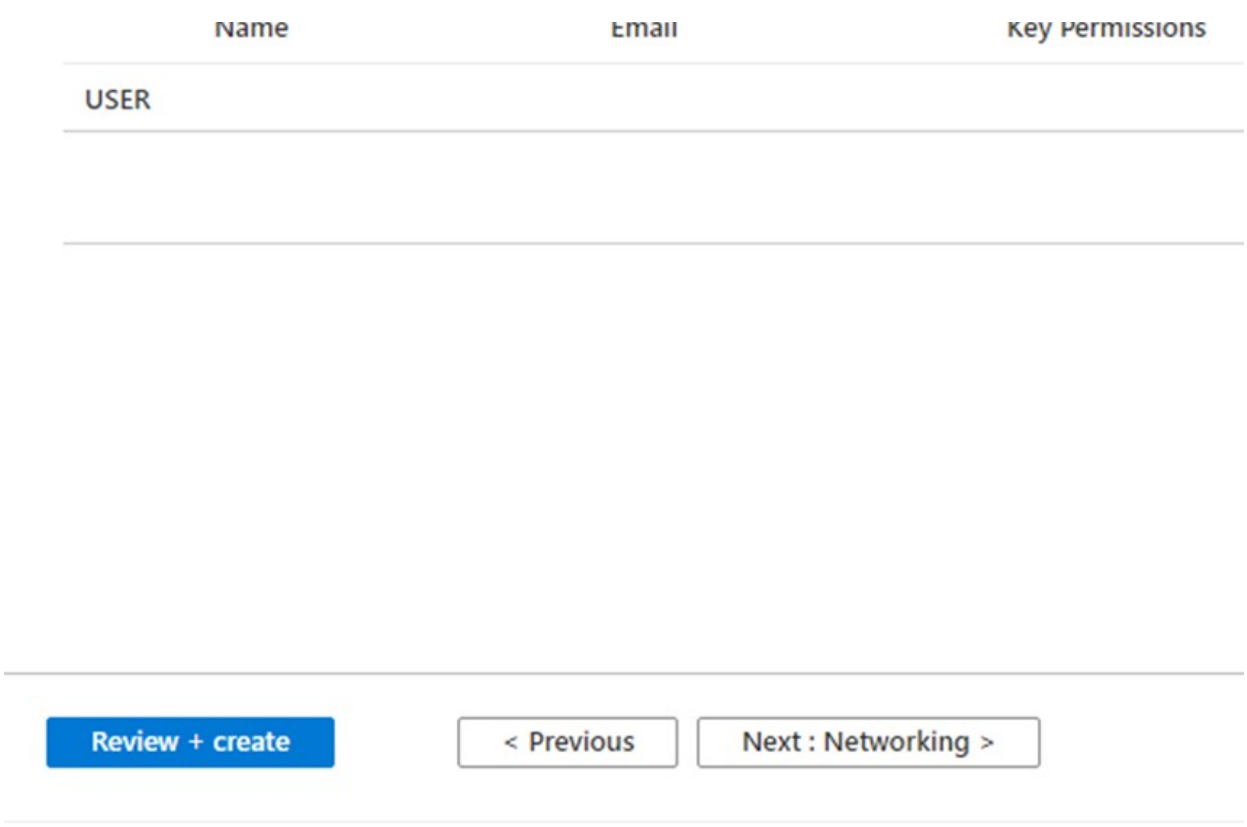
4. Select your subscription and the resource group. Enter the name of the Key vault you will be using, as well as the Region. Make sure to select the Premium pricing tier to include support for the HSM backed keys. Set the Recovery Options according to your company policies.



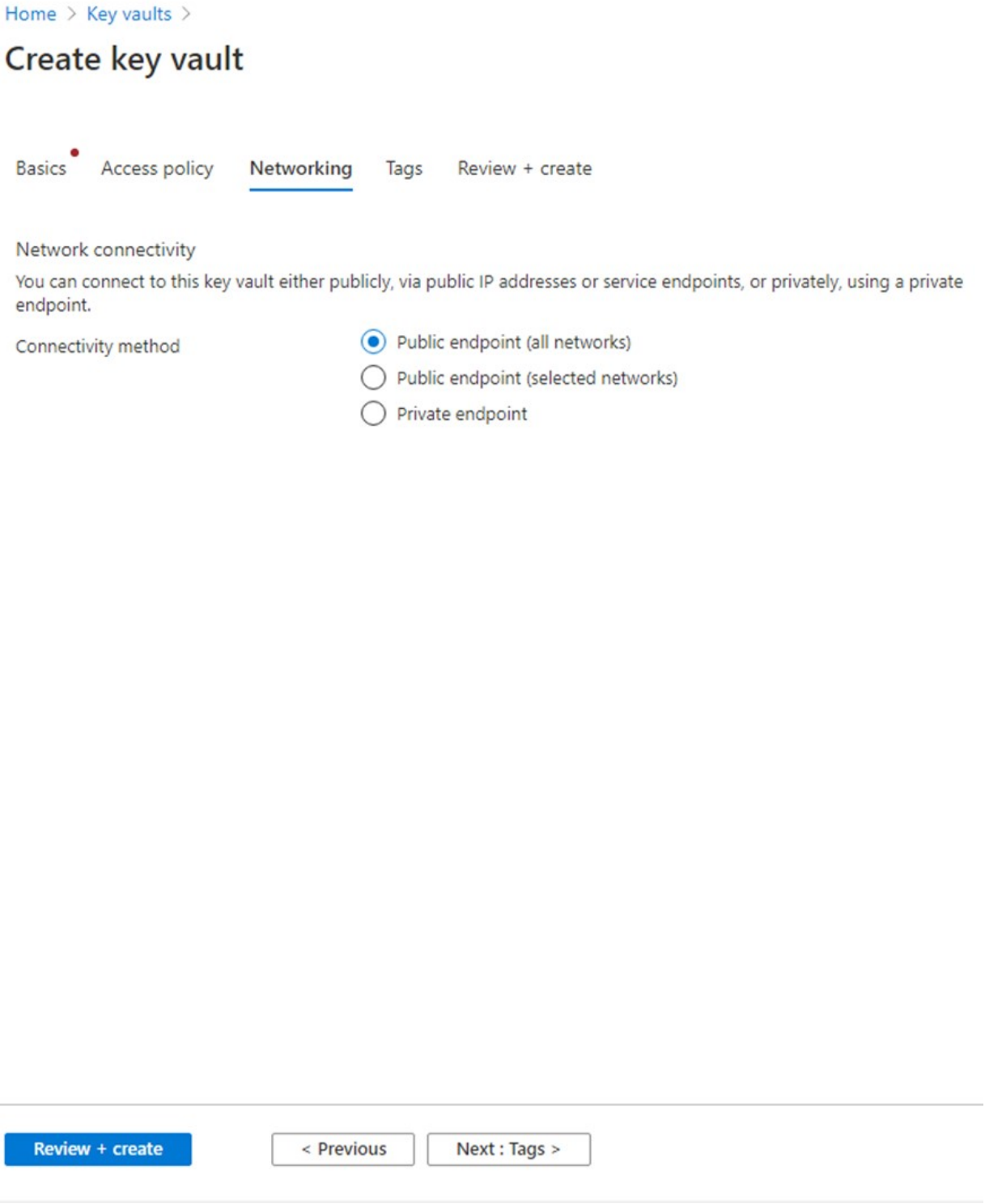


5. Enable access to your selected users and administer the policy, which is the most suitable for your company.

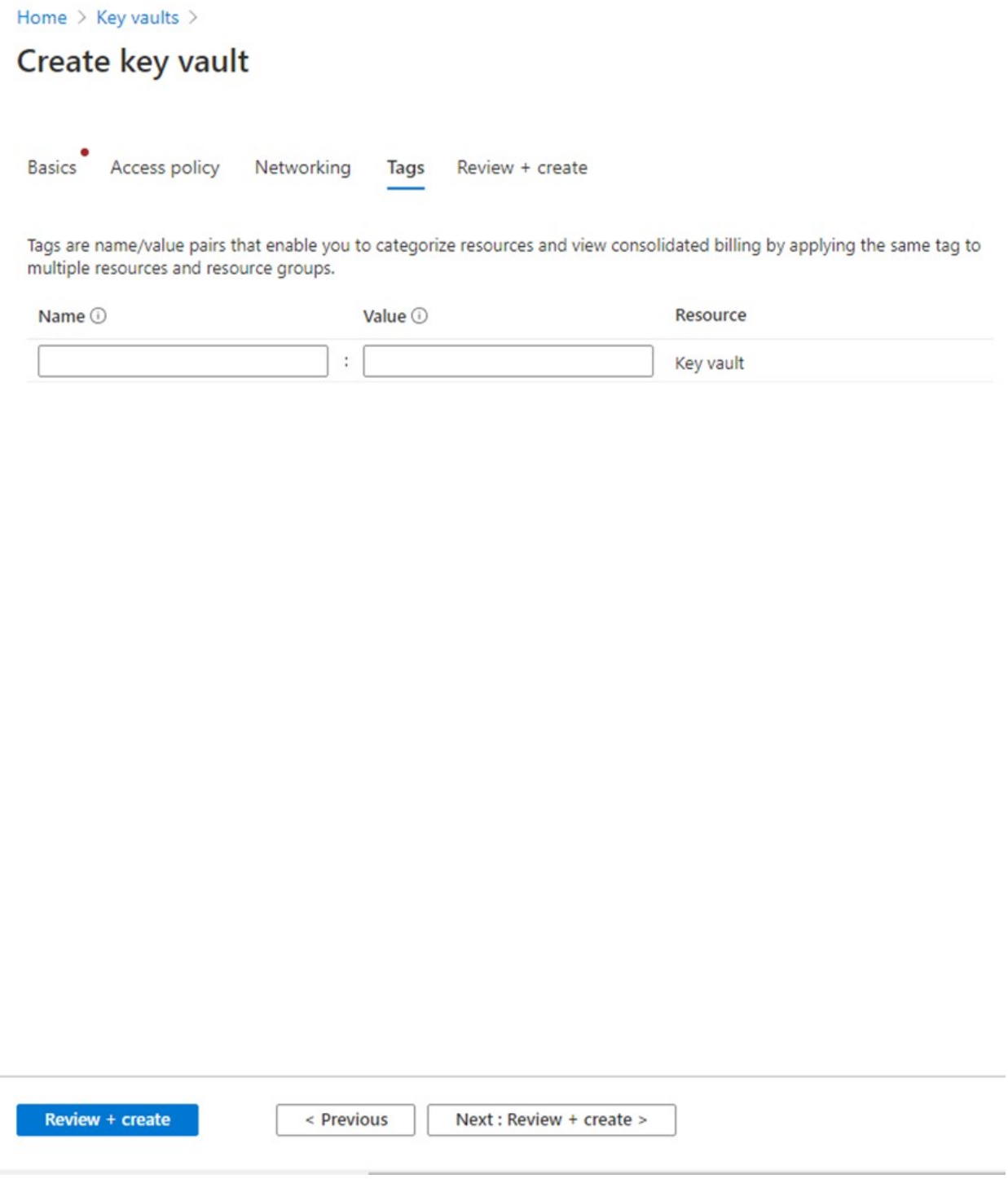




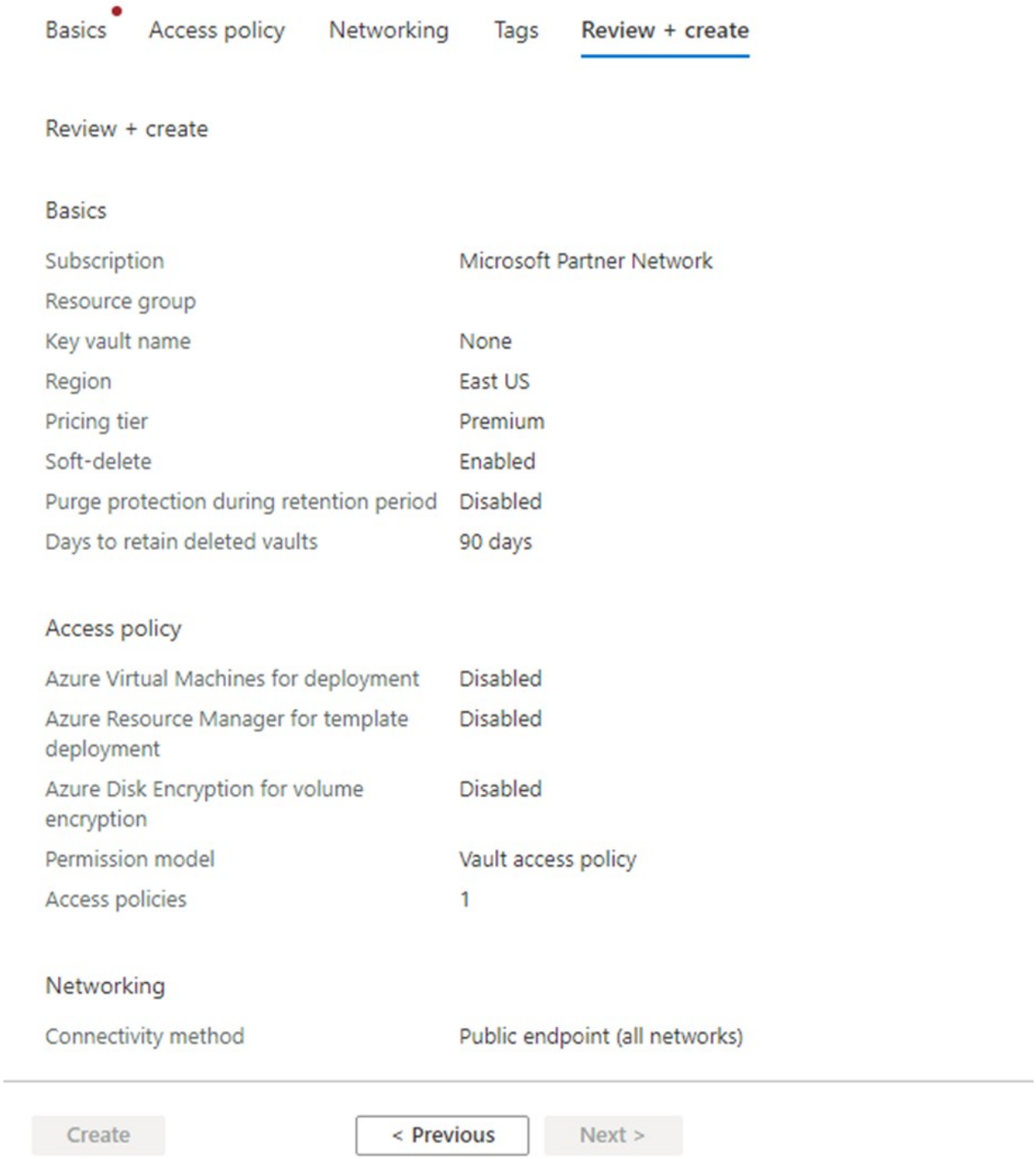
6. Select your connectivity method.



7. If needed add tags to categorize resources and view consolidated billing.

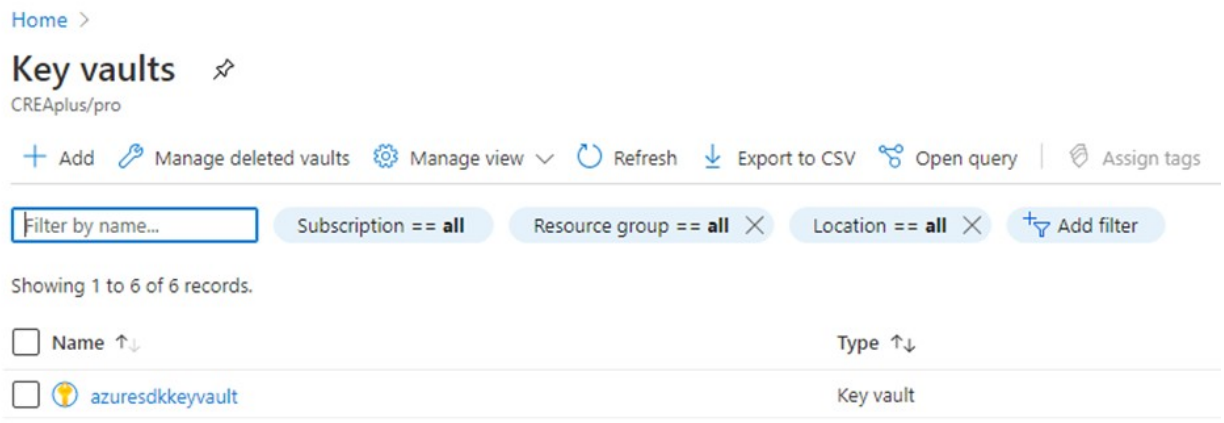


8. Review and creation of the Key vault. After the reviewing click on Create to finish the creation of the Key vault.

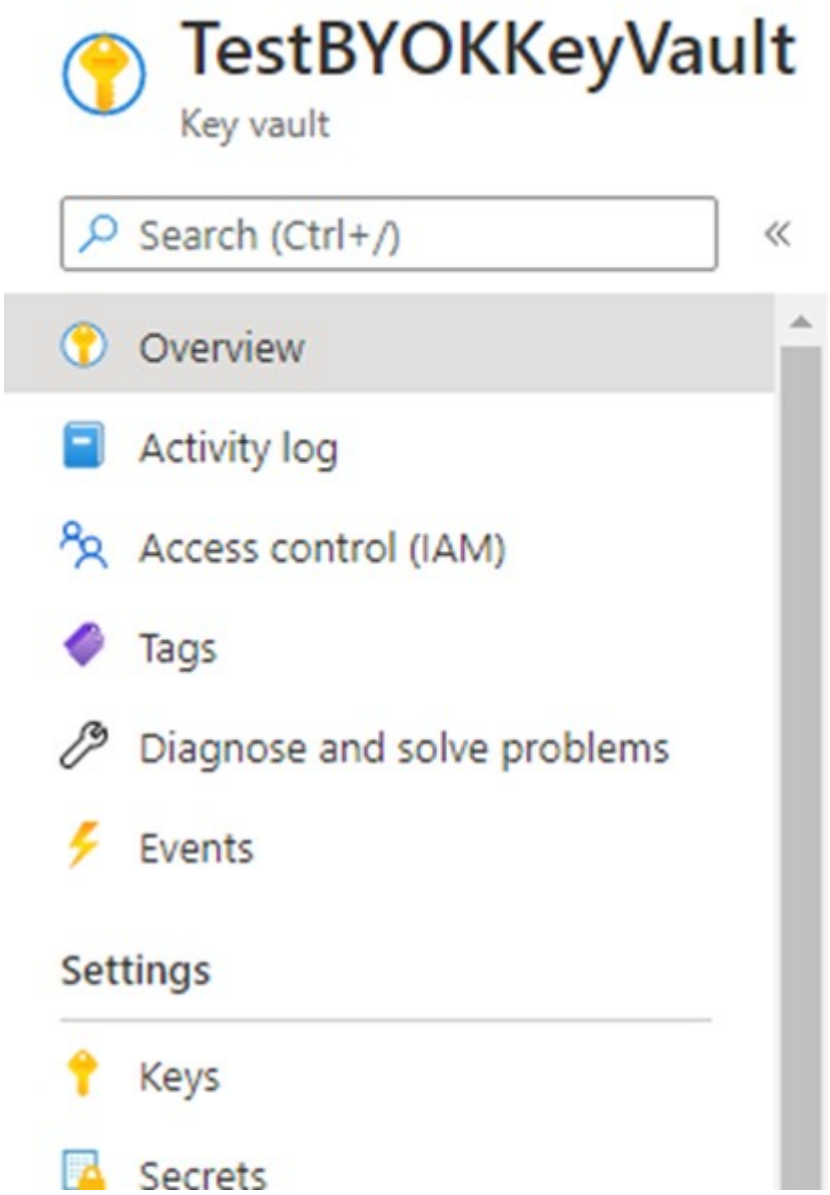


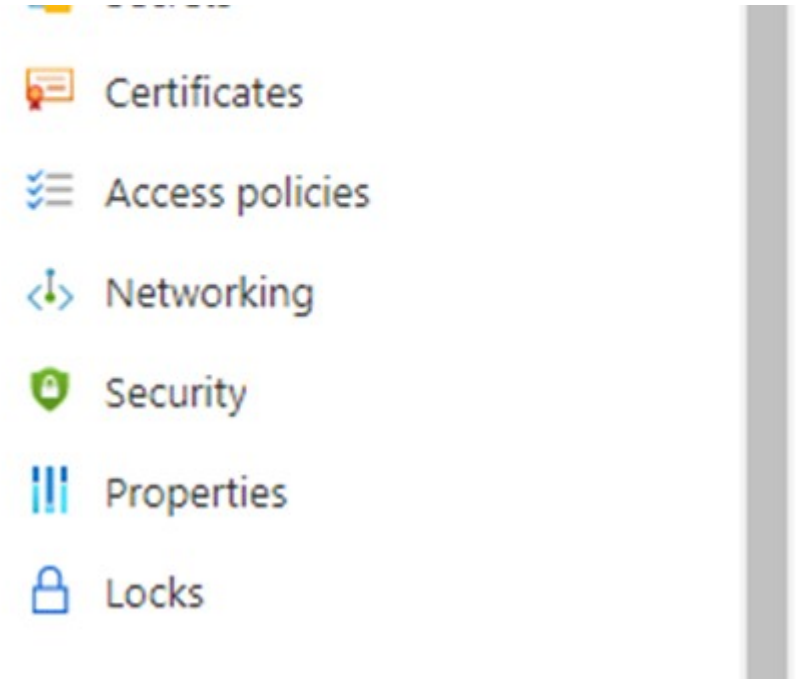
4.3.4 Creating KEK with Azure Portal

To create a key within your recently created Key vault, click on the name of your Azure Key vault and follow the next steps.

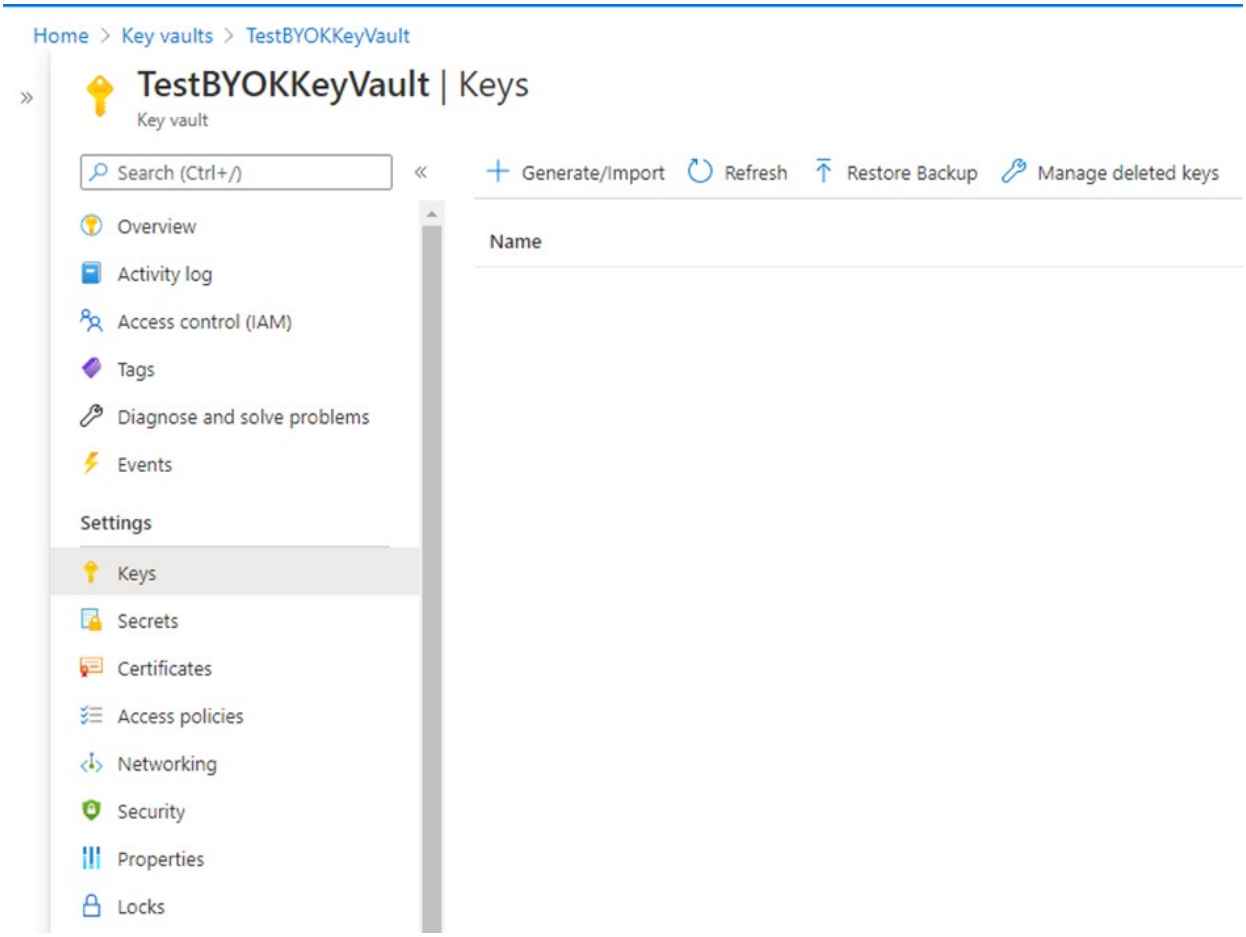


1. Under the Settings menu select the Keys.

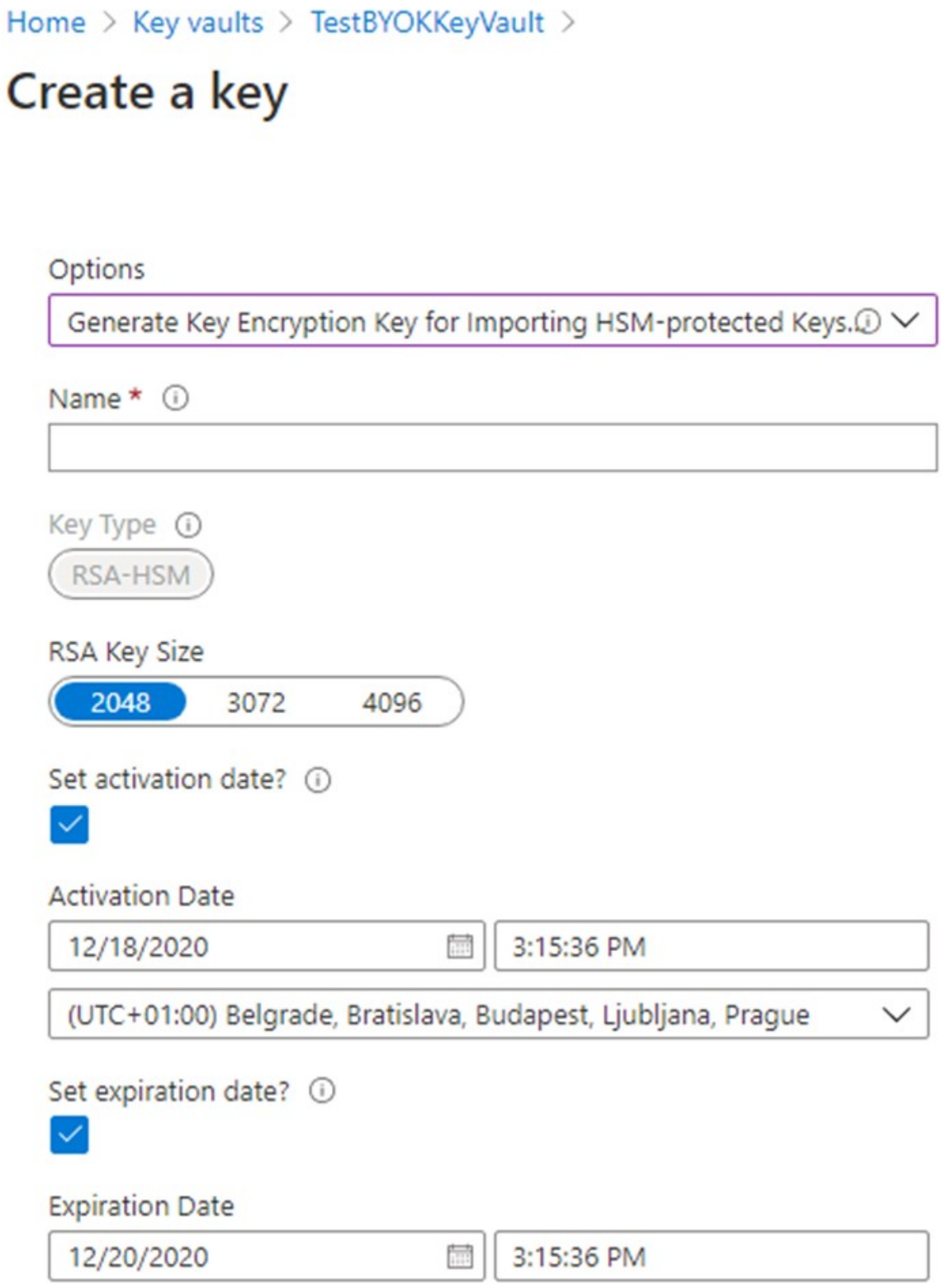




2. Click on Generate/Import.



3. In the Options drop-down menu select **Generate Key Encryption Key for importing HSM-protected Keys**, add a name to the key and select the **RSA key size**. If needed, set the activation and expiration date for the key.



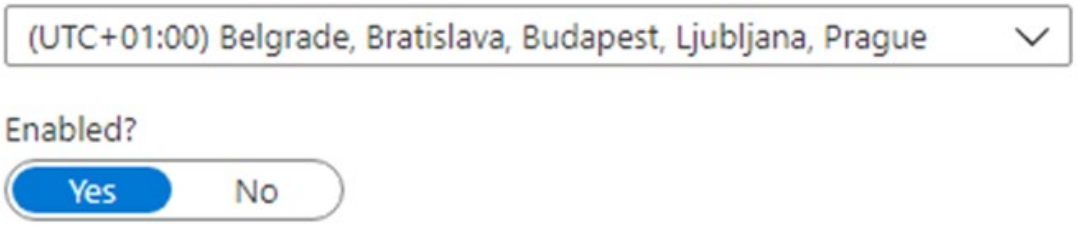
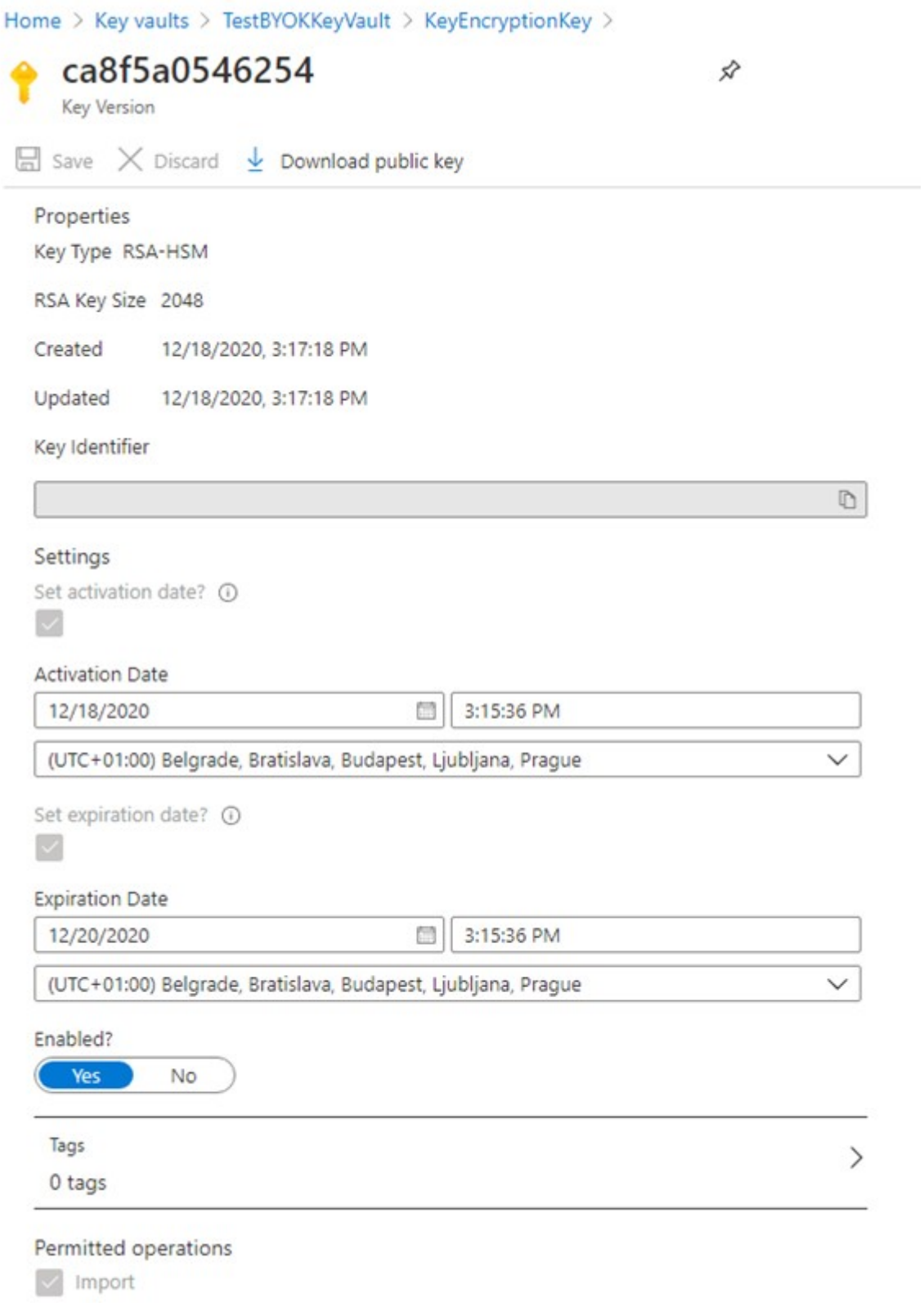


Figure 11 : Example of Create a Key page

4. The key that was just created has an identifier which will be needed in the next steps. To find this Key Identifier, click on the newly created key in your Key Vault to display its properties. The Key Identifier will be needed in the steps Generating and preparing your tenant key.


Home > Key vaults > TestBYOKKeyVault > KeyEncryptionKey >
ca8f5a0546254
Key Version
Save
Discard
Download public key
Properties
Key Type RSA-HSM
RSA Key Size 2048
Created 12/18/2020, 3:17:18 PM
Updated 12/18/2020, 3:17:18 PM
Key Identifier
Settings
Set activation date?
Activation Date
12/18/2020
3:15:36 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Set expiration date?
Expiration Date
12/20/2020
3:15:36 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Enabled?
Yes
No
Tags
0 tags
Permitted operations
Import

4.4 Downloading KEK Public Key

You will need to download the Public Key of the Key Exchange Key, generated on the Azure HSM Key Vault. The Public Key of the KEK will be used to encrypt your tenant key.

Please, execute the following command to download the KEK public key in the `*.pem` format.

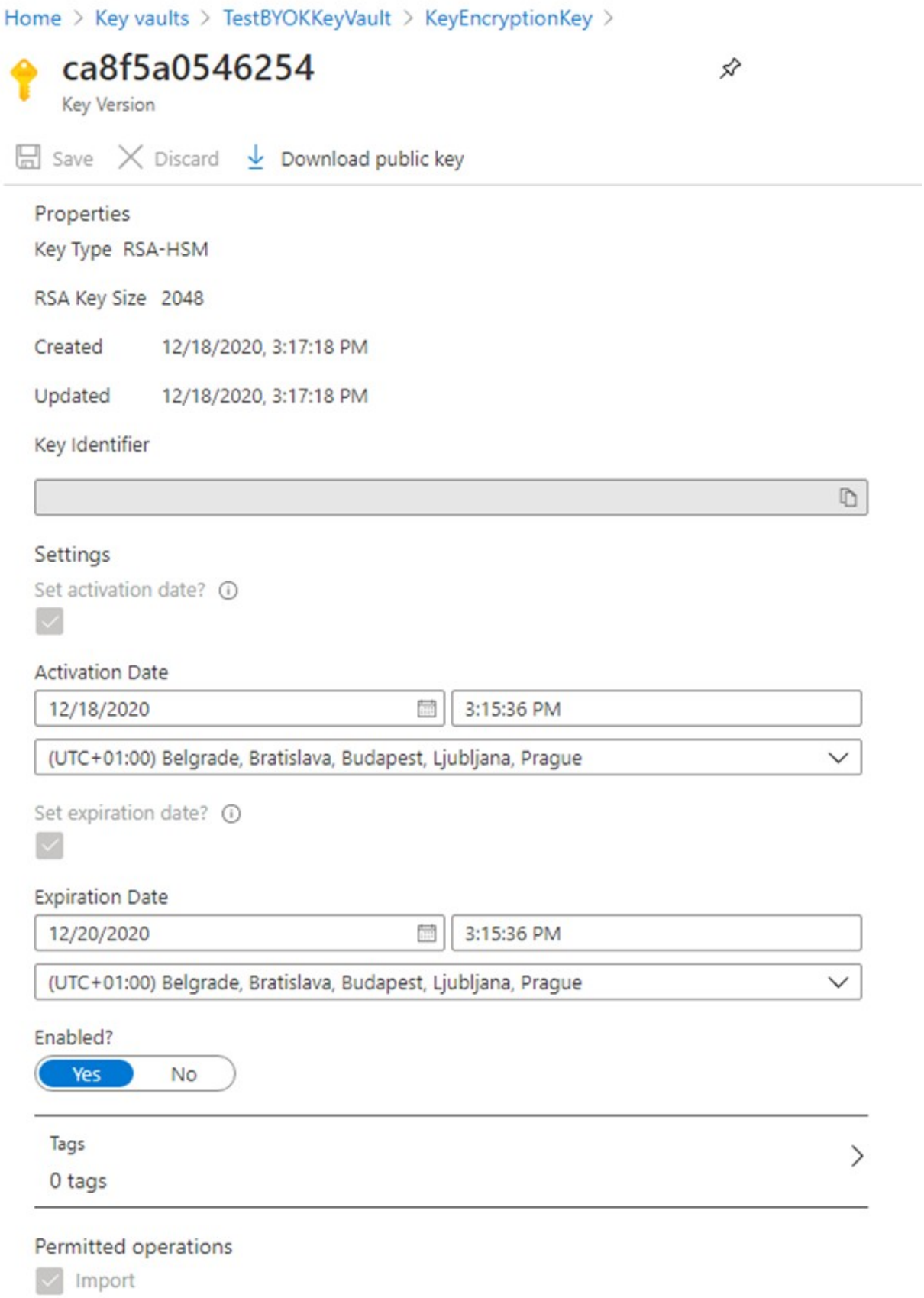
Please ensure that you have administration rights when using the command line.

›_ Console

```
> az keyvault key download --name "<keyvault_key>" --vault-name "<keyvault>" --
file <keyvault_key>.publickey.pem
```

4.4.1 Downloading KEK Public Key with Azure Portal

To download the KEK public key, navigate to your Azure Portal. Go to your Key vault and select the key you would like to download. Click on **download public key**.


Home > Key vaults > TestBYOKKeyVault > KeyEncryptionKey >
ca8f5a0546254
Key Version
Save
Discard
Download public key
Properties
Key Type RSA-HSM
RSA Key Size 2048
Created 12/18/2020, 3:17:18 PM
Updated 12/18/2020, 3:17:18 PM
Key Identifier
Settings
Set activation date?
Activation Date
12/18/2020
3:15:36 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Set expiration date?
Expiration Date
12/20/2020
3:15:36 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Enabled?
Yes
No
Tags
0 tags
Permitted operations
Import

4.5 Generating and Preparing your Tenant Key

Ensure that you have created a user that can manage crypto operations (CryptoUser). The byoktool supports all key types (PKCS#11, CNG, JCE, CXI). In this guide we will create a PKCS#11 key. For other types, please refer to the documentation provided to you on the Utimaco Product CD.

The key will be stored in the internal key storage of the HSM.

1. Use the following command to generate the tenant key:

   ›_ Console

   ```
   > p11tool2 slot=0 loginuser=<user_password> PubKeyAttr=CKA_LABEL="<tenant_public_key>",CKA_MODULUS_BITS=2048,
   PrvKeyAttr=CKA_LABEL="<tenant_private_key>",CKA_EXTRACTABLE=CK_TRUE
   GenerateKeyPair=RSA
   ```

2. Navigate to the folder where you have the byoktool saved. Execute the following command to wrap the tenant key by using the KeyVaultKey, downloaded from the Azure Key Vault:

   ›_ Console

   ```
   > byoktool.exe Dev=<IP_of_UTIMACO_HSM> LogonPass=<User>,<user_password>
   Label="<tenant_private_key>" CSP=azure PublicKey="<keyvaultkey>.publickey.pem" KID=" <kid>" WrappedKey="<WrappedKey>"
   ```

The attribute CKA_MODULUS_BITS describes the length of your key. You can change the key length to a length, that suits your use case.

The attribute CKA_EXTRACTABLE must be set to CK_TRUE!

4.6 Importing Tenant Key to Azure Key Vault

Use the Azure CLI to import the wrapped key to your Azure key vault, generated in the previous steps.

Execute the following command to import the tenant key:

›_ Console

```
> az keyvault key import --vault-name <keyvault> --name <WrappedKeyName> --byok-file " WrappedKey>"
```

Use the following command to check, if the key has been successfully imported to the Azure Key vault:

›_ Console

```
> az keyvault key show --vault-name <keyvault> --name <WrappedKeyName>
```

You can also check if the key is visible on your Azure portal.

4.7 FIPS mode

All the steps are identical to the above, when the HSM is in FIPS 140-2 approved mode. The only difference is that the backup of the entire key database is not possible. Please see refer to additional documentation on the Utimaco product CD.

5 Further Information

This document forms a part of the information and support, which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website:

http://hsm.utimaco.com

For more information regarding Azure Key Vault, please see the following links:

Key Vault BYOK documentation - How to generate & transfer HSM-protected keys – BYOK – Azure Key Vault | Microsoft Docs

Azure CLI - Install the Azure CLI | Microsoft Docs

Azure Key Vault pricing (where Premium tier is referenced) - Pricing Details - Key Vault | Microsoft Azure, this page provides side-by-side comparison of Key Vault pricing tiers and capabilities.

6 References

Reference	*Title/Company*	*Document No.*
[CSADMIN]	CryptoServer – csadm Manual/ Utimaco IS GmbH	2009-0003
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[LPKCSHD]	Learning PKCS#11 in Half a Day	2015-0008
[CSPKCSDG]	CryptoServer PKCS#11 R2 Developer Guide	2012-0007
[CSPKCSHO]	CryptoServer PKCS#11 Hands-on Guide	2015-0008

7 Contact Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Germanusstr. 4
52080 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.