YubiHSM 2: Back Up and Restore

Yubico

Jul 22, 2022

CONTENTS

CHAPTER

ONE

INTRODUCTION

The YubiHSM 2 supports encrypted export and import of objects using a symmetric AES-CCM based scheme. You can perform these operations using:

- YubiHSM Shell for backing up and restoring
- YubiHSM Setup for backing up alone (not restoring)
- YubiHSM Key Storage Provider for backing up and restoring certificate as well as private key.

CHAPTER

TWO

BACK UP AND RESTORE USING YUBIHSM SHELL

2.1 Back Up

Make sure you have a Wrap Key with the following capabilities set:

- `export-wrapped`
- `import-wrapped`
- applicable Delegated Capabilities

```
$ yubihsm-shell -a get-pseudo-random --count=32 --out=wrap.key
...
yubihsm-shell -a put-wrap-key -c export-wrapped,import-wrapped --delegated=sign-pkcs,
↪decrypt-pkcs,exportable-under-wrap --in=wrap.key
...
Stored Wrap key 0xd581
```

Any Object in the same Domain and with the Capability `exportable-under-wrap` and Capabilities matching the Wrap Key's Delegated Capabilities can be exported, provided that this Wrap Key is present:

```
$ yubihsm-shell -a generate-asymmetric-key -A rsa2048 -c exportable-under-wrap,sign-pkcs,
↪decrypt-pkcs
...
Generated Asymmetric key 0x6e77
yubihsm-shell -a get-wrapped --wrap-id=0xd581 --object-id=0x6e77 -t asymmetric-key --
↪out=key_6e77.yhw
...
```

You now have an encrypted backup of the Asymmetric Key `0x6e77` in the file `key_6e77.yhw`.

Important: The file `wrap.key` here contains the Wrap Key loaded into your YubiHSM in clear text. It should therefore be considered sensitive.

2.2 Restore

This assumes a fresh device where you want to restore the previously backed up key `0x6e77`

```
$ yubihsm-shell -a put-wrap-key -A aes256-ccm-wrap -c export-wrapped,import-wrapped --
↪delegated=sign-pkcs,decrypt-pkcs,exportable-under-wrap --in=wrap.key -i 0xd581
...
Stored Wrap key 0xd581
yubihsm-shell -a put-wrapped --wrap-id=0xd581 --in=key_6e77.yhw
...
Object imported as 0x6e77 of type asymmetric-key
```

CHAPTER

THREE

BACK UP USING YUBIHSM SETUP

The YubiHSM 2 Setup Tool can be used to back up all exportable objects simultaneously:

```
$ yubihsm-setup dump
Enter the wrapping key ID to use for exporting objects: 0xd581
...
Successfully exported object Asymmetric with ID 0x6e77 to ./0x6e77.yhw
All done
```

CHAPTER

FOUR

BACK UP AND RESTORE USING YUBIHSM KSP

YubiHSM Key Storage Provider (KSP) enables backing up and restoring the keys managed using this tool.

Note: Microsoft Active Directory Certificate Services (ADCS) does not set the `NCRYPT_ALLOW_EXPORT_FLAG` when generating a key, either through the setup UI or the `Install-ADCSCertificationAuthority` PowerShell module.

When creating an ADCS root CA key using the YubiHSM 2, we add the `exportable-under-wrap` Capability by default. Back up and restore functionality is therefore available using the following manual processes.

1. *Identify Your Private Key Container Name*
2. *Back Up the Target Certificate*
3. *Back Up the Target Private Key*
4. *Restore the Target Private Key*
5. *Restore the Target Certificate*.

4.1 Identify Your Private Key Container Name

Step 1
To view the currently installed certificates in the Local Machine "My" store, open an elevated command prompt/shell by using the certutil command `PS1> certutil -store My`

Step 2
Find the target certificate in the list and then find its `Key Container` property. The Provider property should be the same as `YubiHSM Key Storage Provider`.

Step 3
To identify the certificate, record the `Cert Hash` property.

4.2 Back Up the Target Certificate

Using any available means (`certmgr.msc`, PowerShell, `certutil`), export the target certificate, but without the private key in DER format.

Note: The YubiHSM does not provide a mechanism for returning the raw private key to Windows, so generating a PKCS#12 container is not currently possible.

For example, to export the certificate in .crt format to a file named <Cert Hash>.crt, use the command `PS1> certutil -split -store My <Cert Hash>`.

4.3 Back Up the Target Private Key

Export the target private key with the `label` property equal to the `Key Container` property. To do this,

1. Use an Authentication Key with the `export-wrapped` capability set.
2. Use the instructions for exporting a private key under wrap via `yubihsm-shell` (see *Back Up*).

4.4 Restore the Target Private Key

Import the target private key file to your backup YubiHSM. To do this,

1. Use an Authentication Key with the `import-wrapped` capability set.
2. Use the instructions for importing a private key under wrap via `yubihsm-shell` (see *Restore*).

The imported key object should have the same `Label` property as the original object.

4.5 Restore the Target Certificate

Before the certificate is imported to the local machine, it does not have an associated private key.

Step 1
Move the target certificate file generated as per *Back Up* to the target machine by importing the certificate to the LocalMachine "My" store. Use your preferred method.

Step 2
Re-associate the certificate to the private key by using the `-repairstore` functionality of `certutil`.

Step 3
Verify that the target private key is visible via the YubiHSM KSP: list all private keys (and their corresponding container names - which are equal to the `Label` property in the YubiHSM visible to the current Authentication Key) by using

```
PS1> certutil -key -csp "YubiHSM Key Storage Provider"
```

Step 4
Open an elevated prompt and execute the command:

```
PS1> certutil -repairstore MY <Cert Hash>
```

Step 5
To verify that the certificate has been associated with the YubiHSM Key Storage Provider and has the correct `Key Container` property value, repeat the steps under *Identify Your Private Key Container Name*.

CHAPTER

FIVE

COPYRIGHT

Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Contact Information

Yubico Inc.
530 Lytton Street
Suite 301
Palo Alto, CA 94301
USA

Click the links to:

- Submit a support request
- Send a Contact Me request
- See additional contact options for getting touch with us

Document Updated

2022-07-22 00:50:54 UTC