PrimeKey®

Using DPoD to secure EJBCA PKI signature keys in AWS

This blog post outlines the procedure to use the DPoD HSM on Demand service for CA signing keys on EJBCA in AWS.

Overview

The process comprises the following operations

- Create a DPoD HSM on Demand Service
    - Create and download a DPoD Service Client package
- Create an EJBCA Cloud instance in AWS
- Configure the EJBCA instance to use the HSM on Demand Service
    - Copy the DPoD Service Client package to the AWS instance
    - Initialize the DPoD HSM on Demand Service
- Use the DPoD HSM on Demand from EJBCA
    - Create a Crypto Token in EJBCA
    - Create a CA in EJBCA

Pre-requisites

A DPoD account that can be used to create a new HSM on Demand Service.

An AWS account that can be used to create an EJBCA instance in AWS (30 day trial available)

Create a DPoD HSM on Demand Service

The following provides a brief walk-through of setting up and connecting to a DPoD HSM on Demand Service.

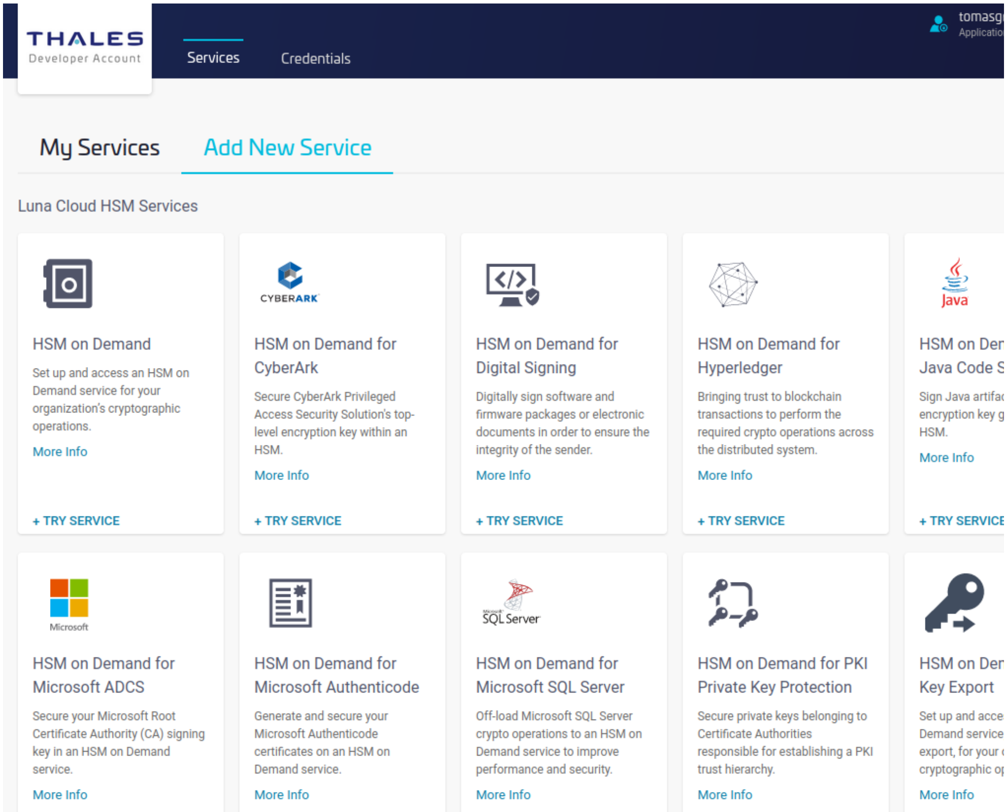
Create Service and Download Client

Log into your DPoD account and select the Services tab.

Create the Service and Download Client

Once logged into the DPoD portal, the Accounts main page is displayed. To create the service and download the client, do the following:

1. To add a service, click **Services** on the top menu and then click **Add New Service**.
2. To create a new service for **HSM on Demand**, click **Try Service** to start the wizard.



Luna Cloud HSM Services

HSM on Demand

Set up and access an HSM on Demand service for your organization's cryptographic operations.

More Info

+ TRY SERVICE

HSM on Demand for CyberArk

Secure CyberArk Privileged Access Security Solution's top-level encryption key within an HSM.

More Info

+ TRY SERVICE

HSM on Demand for Digital Signing

Digitally sign software and firmware packages or electronic documents in order to ensure the integrity of the sender.

More Info

+ TRY SERVICE

HSM on Demand for Hyperledger

Bringing trust to blockchain transactions to perform the required crypto operations across the distributed system.

More Info

+ TRY SERVICE

HSM on Der
Java Code S

Sign Java artifac
encryption key g
HSM.

More Info

+ TRY SERVICE

HSM on Demand for Microsoft ADCS

Secure your Microsoft Root Certificate Authority (CA) signing key in an HSM on Demand service.

More Info

HSM on Demand for Microsoft Authenticode

Generate and secure your Microsoft Authenticode certificates on an HSM on Demand service.

More Info

HSM on Demand for Microsoft SQL Server

Off-load Microsoft SQL Server crypto operations to an HSM on Demand service to improve performance and security.

More Info

HSM on Demand for PKI Private Key Protection

Secure private keys belonging to Certificate Authorities responsible for establishing a PKI trust hierarchy.

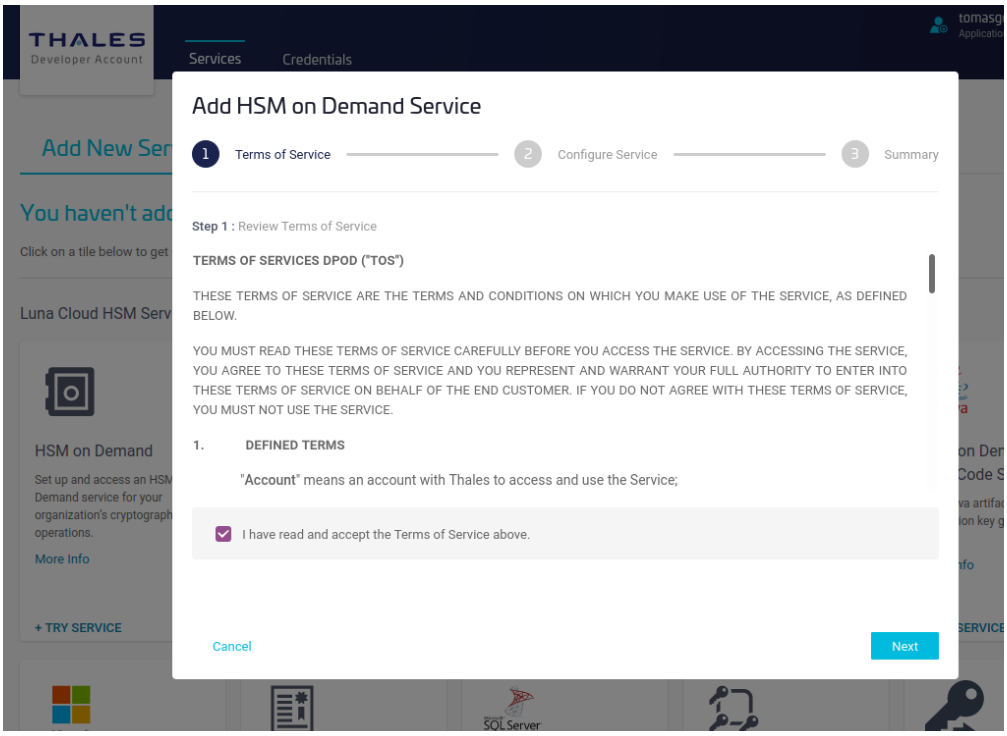
More Info

HSM on Der
Key Export

Set up and acce
Demand service
export, for your
cryptographic op

More Info

3. Review the terms of the service and click **Next**.



Add HSM on Demand Service

1 Terms of Service — 2 Configure Service — 3 Summary

Step 1 : Review Terms of Service

TERMS OF SERVICES DPOD ("TOS")

THESE TERMS OF SERVICE ARE THE TERMS AND CONDITIONS ON WHICH YOU MAKE USE OF THE SERVICE, AS DEFINED BELOW.

YOU MUST READ THESE TERMS OF SERVICE CAREFULLY BEFORE YOU ACCESS THE SERVICE. BY ACCESSING THE SERVICE, YOU AGREE TO THESE TERMS OF SERVICE AND YOU REPRESENT AND WARRANT YOUR FULL AUTHORITY TO ENTER INTO THESE TERMS OF SERVICE ON BEHALF OF THE END CUSTOMER. IF YOU DO NOT AGREE WITH THESE TERMS OF SERVICE, YOU MUST NOT USE THE SERVICE.

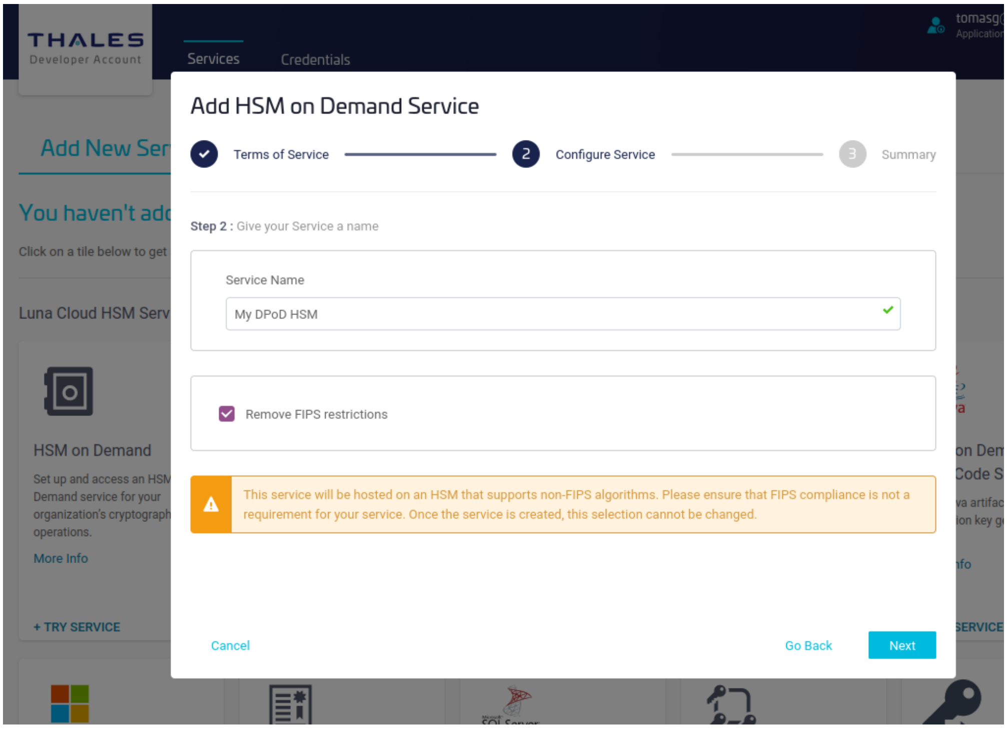
1. DEFINED TERMS

"**Account**" means an account with Thales to access and use the Service;

☑ I have read and accept the Terms of Service above.

Cancel Next

4. Specify a name for the service and select **Remove FIPS restrictions** to allow the use of non-FIPS algorithms such as other than NIST EC curves, or Ed25519. Click **Next**.



Add HSM on Demand Service

✓ Terms of Service — 2 Configure Service — 3 Summary

Step 2 : Give your Service a name

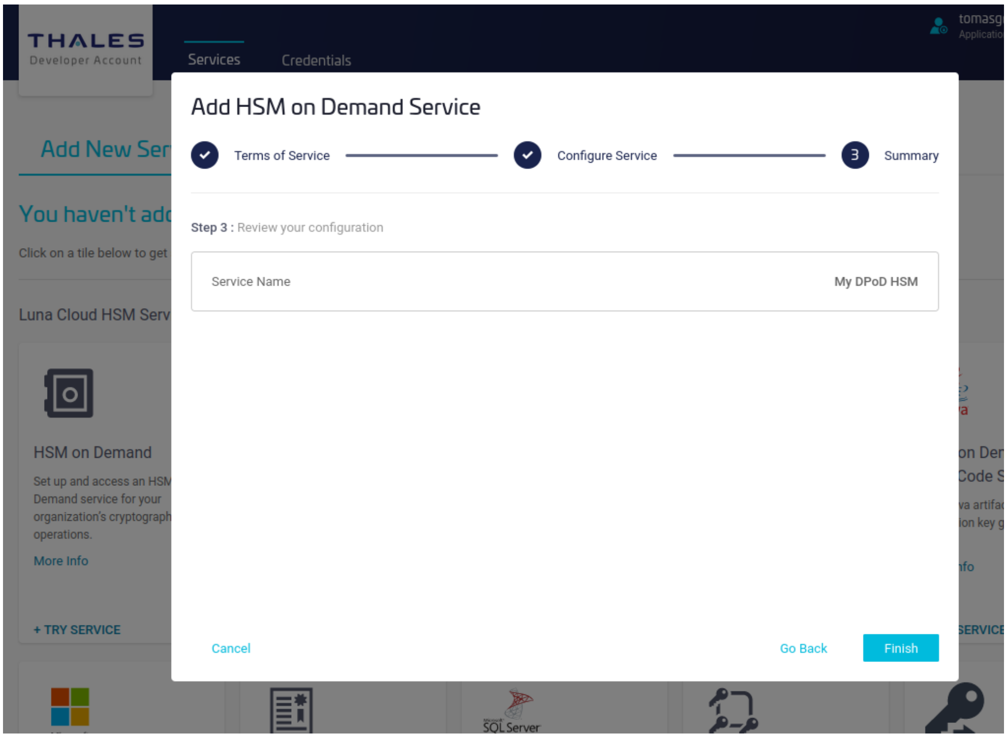
Service Name: My DPoD HSM ✓

☑ Remove FIPS restrictions

This service will be hosted on an HSM that supports non-FIPS algorithms. Please ensure that FIPS compliance is not a requirement for your service. Once the service is created, this selection cannot be changed.

Cancel Go Back Next

5. Review and click **Finish**.

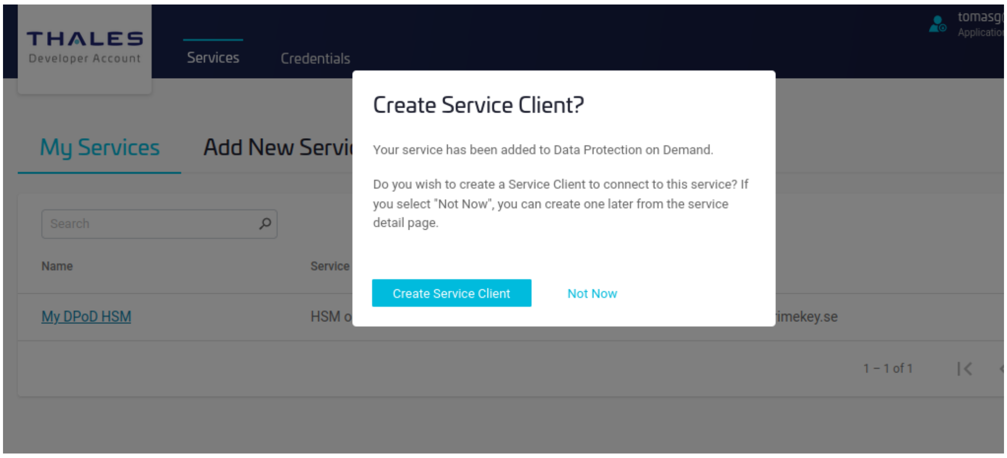


Add HSM on Demand Service

Step 3 : Review your configuration

Service Name	My DPoD HSM

6. Click C**reate Service Client** to get the client download package, which includes the certificates needed to connect to the service.

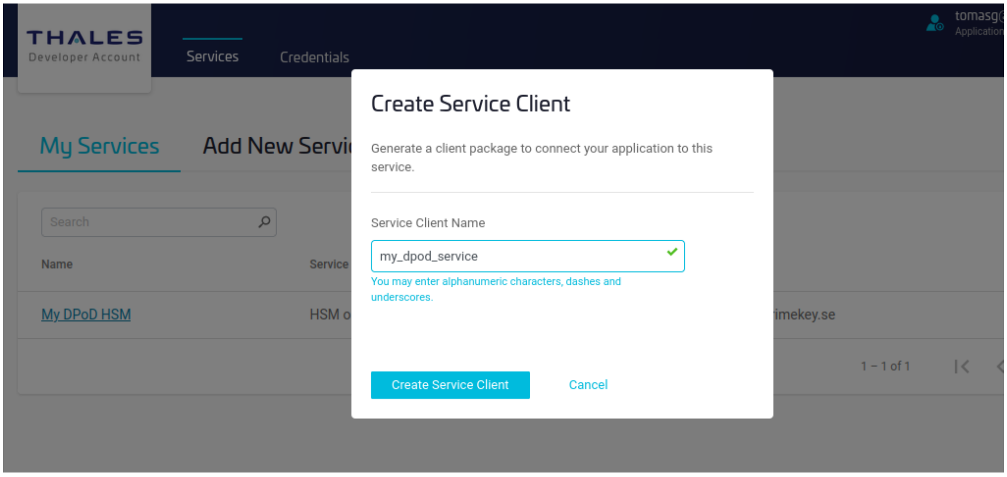


Create Service Client?

Your service has been added to Data Protection on Demand.

Do you wish to create a Service Client to connect to this service? If you select "Not Now", you can create one later from the service detail page.

7. Specify the name of the service client and click **Create Service Client.**



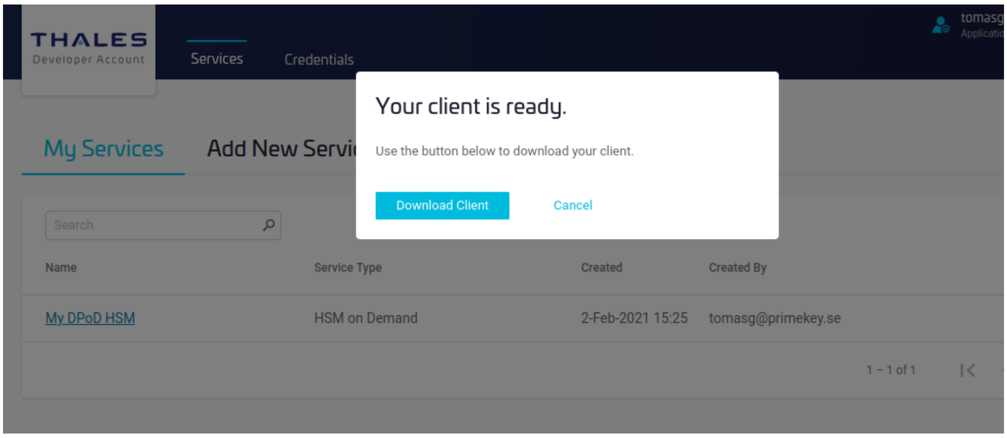
Create Service Client

Generate a client package to connect your application to this service.

Service Client Name: my_dpod_service

You may enter alphanumeric characters, dashes and underscores.

8. Click **Download Client.**



Your client is ready.

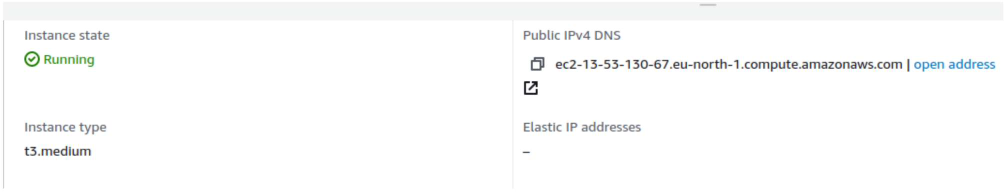
Use the button below to download your client.

Name	Service Type	Created	Created By
My DPoD HSM	HSM on Demand	2-Feb-2021 15:25	tomasg@primekey.se

Create an EJBCA Cloud instance in AWS

Follow the AWS Launch Guide from the EJBCA Documentation.

The result is a running EJBCA instance in AWS, where you can log in to the instance to the EJBCA Admin UI using a web browser, and to the terminal using SSH. After completing starting the instance you get the public DNS name of the instance from the AWS console.



Instance state
Running

Instance type
t3.medium

Public IPv4 DNS
ec2-13-53-130-67.eu-north-1.compute.amazonaws.com | open address

Elastic IP addresses
–

In this case the DNS name is *ec2-13-53-130-67.eu-north-1.compute.amazonaws.com*, which is used below in sample commands.

> ⓘ Replace the DNS name in the example CLI commands with the name of your instance.

In order to SSH into the AWS instance, you configured an SSH key during setup of the instance. In the example commands below, the SSH key name aws_ssh.pem is used.

> ⓘ Replace the name of the SSH key with the name of your key.

Configure the EJBCA instance to use the HSM on Demand Service

The steps for configuring the EJBCA instance to use the HSM on Demand service consist of installing the client package and initializing the partition on the HSM service.

Install HSM Client Package

To install the DPoD client:

1. Copy the downloaded service client zip file to the AWS instance.

```
scp -i ~/.ssh/aws_ssh.pem setup-my_dpod_service.zip ec2-
user@ec2-13-53-130-67.eu-north-1.compute.amazonaws.com:.
```

2. Log into the instance with SSH

```
ssh -i ~/.ssh/aws_ssh.pem ec2-user@ec2-13-53-130-67.eu-
north-1.compute.amazonaws.com
```

3. Unzip the downloaded client archive in `/opt/thales/dpodclient`. You can use another location but the PKCS#11 driver in this directory will be automatically detected in EJBCA version 7.5.0 and later.

```
sudo mkdir -p /opt/thales/dpodclient
sudo unzip -d /opt/thales/dpodclient setup-my_dpod_service.zip
cd /opt/thales/dpodclient
sudo tar -xvf cvclient-min.tar
```

> ⓘ You do not have to be root to run the Luna client, but installing the driver as root prevents other OS users to modify files. You however have to be able to write temporary files where you run to command `source ./setenv` below.

4. Check the connectivity with the HSM.

```
sudo su
cd /opt/thales/dpodclient
source ./setenv
./bin/64/lunacm

lunacm (64-bit) v10.2.0-111. Copyright (c) 2020 SafeNet. All rights reserved.
    Available HSMs:

    Slot Id -> 3
    Label -> tomas_ejbca_test_1
    Serial Number -> 1392941677399
    Model -> Cryptovisor7
    Firmware Version -> 7.3.0
    CV Firmware Version -> 1.4.0
    Configuration -> Luna User Partition With SO (PW) Signing With Cloning Mode
    Slot Description -> Net Token Slot
    FM HW Status -> FM Not Supported

    Current Slot Id: 3
```

Initialize Partition

Before using the HSM, you need to initialize the partition to create the access credentials that are later used to access the HSM from EJBCA.

The slot used in the example below is slot number 3, which is the number presented above when running the `lunacm` command. Use the slot number of your HSM. To use the partition, you need to create a Security Officer and a Crypto Officer. The Crypto Officer is the user in the HSM that can create objects and use them, i.e. an R/W User. Luna also defines a Crypto User which is a Read-Only User. This is typically not used from EJBCA as it does not allow to generate keys and no Crypto User is therefore created in this guide.

> Ensure that you use strong passwords and have them under control so they are neither compromised, nor lost.

Initialize the partition to create the access credentials:

```
lunacm:>slot set -slot 3
    Current Slot Id: 3 (Luna User Slot 7.3.0 (PW) Signing With Cloning Mode)
Command Result : No Error

lunacm:>partition init -label my_dpod_service

    Enter password for Partition SO: W3nDwUr9TQQeZq4G
    Re-enter password for Partition SO: W3nDwUr9TQQeZq4G

    You are about to initialize the partition.
    All contents of the partition will be destroyed.
    Are you sure you wish to continue?

    Type 'proceed' to continue, or 'quit' to quit now ->proceed

    Option -domain was not specified. It is required.

    Enter the domain name: LWVjU8hqjwZBM5M4
    Re-enter the domain name: LWVjU8hqjwZBM5M4


Command Result : No Error

lunacm:>role login -name Partition SO

    enter password: W3nDwUr9TQQeZq4G

Command Result : No Error

lunacm:>role init -name Crypto Officer

    enter new password: RmKSPD7ec8uEZYB7
    re-enter new password: RmKSPD7ec8uEZYB7

Command Result : No Error

lunacm:>role logout

lunacm:>role login -name Crypto Officer

    enter password: RmKSPD7ec8uEZYB7

Command Result : No Error

lunacm:>role changepw -name Crypto Officer

    enter existing password: RmKSPD7ec8uEZYB7
    enter new password: vpvTWX2pws4LkpuF
    re-enter new password: vpvTWX2pws4LkpuF

Command Result : No Error
```

```
lunacm:>exit
```

Restart EJBCA

As you have added new PKCS#11 drivers to the AWS instance, EJBCA needs to be restarted in order to find the new driver.

```
service wildfly restart
```

⚠ There is a bug in the DPoD PKCS#11 client that causes shutdown times to be extremely long, once the DPoD client is in use. This may cause troubles using "service wildfly restart" and force you to kill wildfly processes hard. this bug is scheduled to be fixed by Thales during 2021.

Create Crypto Token in EJBCA

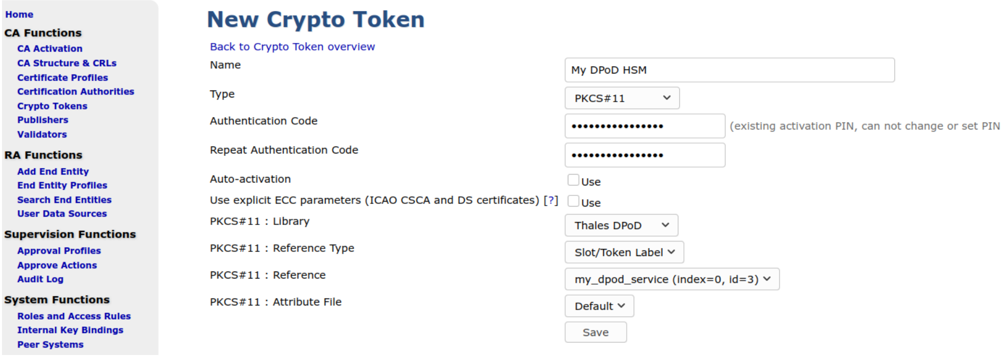
Log into the Admin UI of EJBCA at the URL (replace the DNS name with the name of your instance) https://ec2-13-53-130-67.eu-north-1.compute.amazonaws.com/ejbca/adminweb/.

You can generate a new PKCS#11 Crypto Token utilizing the Thales DPoD library (located in /opt/thales/dpodclient/libs/64/libCryptoki2.so), using the EJBCA Admin UI. It is also possible to use the command line interface, but that is not covered in this guide.

Create Crypto Token Using the EJBCA Admin UI

To create a PKCS#11 Crypto Token using the Web UI:

1. In the EJBCA Admin UI, go to **Crypto Tokens>Create new**. Select:
   a. Type: PKCS#11
   b. PKCS#11 : Library: Thales DPoD
   c. PKCS#11 : Reference Type: Slot/Token Label
   The token label should be listed (you may have to wait a few seconds to read token labels from the remote HSM).



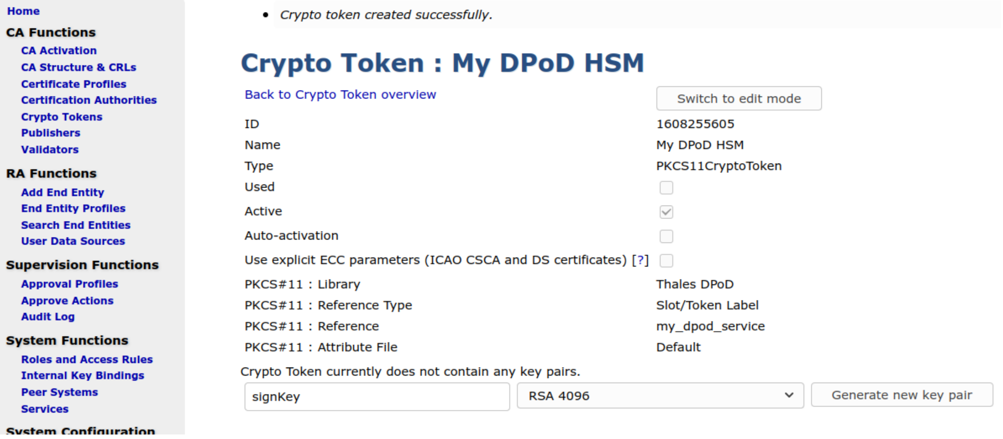
New Crypto Token

Back to Crypto Token overview

Name: My DPoD HSM
Type: PKCS#11
Authentication Code: •••••••••••••••• (existing activation PIN, can not change or set PIN
Repeat Authentication Code: ••••••••••••••••
Auto-activation: □ Use
Use explicit ECC parameters (ICAO CSCA and DS certificates) [?]: □ Use
PKCS#11 : Library: Thales DPoD
PKCS#11 : Reference Type: Slot/Token Label
PKCS#11 : Reference: my_dpod_service (index=0, id=3)
PKCS#11 : Attribute File: Default

Save

2. Enter the Crypto Officer password as **Authentication Code**, and click **Save**. Now EJBCA logs into the token, after a while you should get a list of keys, which are none on a new token.



- *Crypto token created successfully.*

Crypto Token : My DPoD HSM

Back to Crypto Token overview

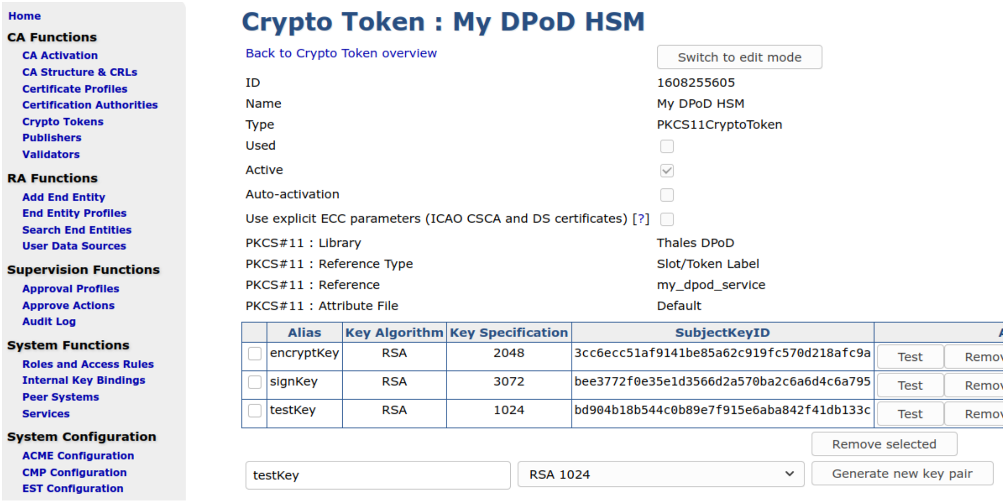
Switch to edit mode

ID	1608255605
Name	My DPoD HSM
Type	PKCS11CryptoToken
Used	□
Active	☑
Auto-activation	□
Use explicit ECC parameters (ICAO CSCA and DS certificates) [?]	□
PKCS#11 : Library	Thales DPoD
PKCS#11 : Reference Type	Slot/Token Label
PKCS#11 : Reference	my_dpod_service
PKCS#11 : Attribute File	Default

Crypto Token currently does not contain any key pairs.

signKey | RSA 4096 | Generate new key pair

3. Generate key needed for a CA



Crypto Token : My DPoD HSM

ID	1608255605
Name	My DPoD HSM
Type	PKCS11CryptoToken
Used	□
Active	☑
Auto-activation	□
Use explicit ECC parameters (ICAO CSCA and DS certificates) [?]	□
PKCS#11 : Library	Thales DPoD
PKCS#11 : Reference Type	Slot/Token Label
PKCS#11 : Reference	my_dpod_service
PKCS#11 : Attribute File	Default

	Alias	Key Algorithm	Key Specification	SubjectKeyID	A
□	encryptKey	RSA	2048	3cc6ecc51af9141be85a62c919fc570d218afc9a	Test Remov
□	signKey	RSA	3072	bee3772f0e35e1d3566d2a570ba2c6a6d4c6a795	Test Remov
□	testKey	RSA	1024	bd904b18b544c0b89e7f915e6aba842f41db133c	Test Remov

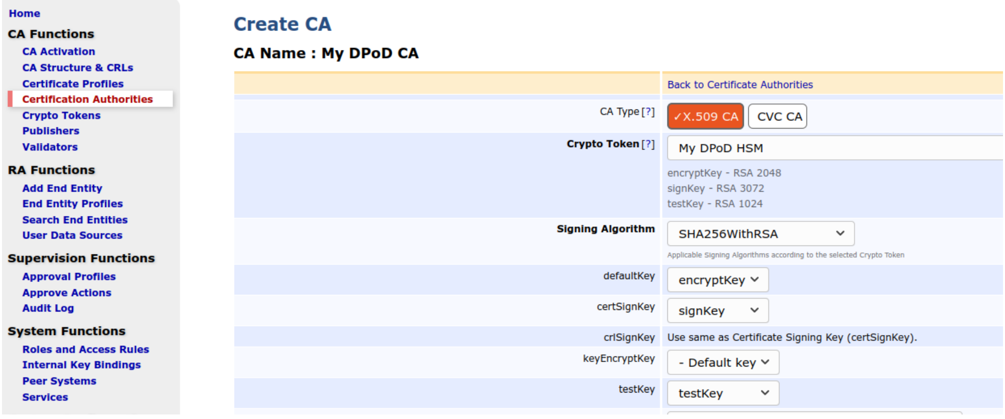
testKey | RSA 1024

With the created Crypto Token and keys, you can now go ahead and create CAs, using keys on the DPoD HSM.

Create CA Using the EJBCA Admin UI

To create a CA using the Web UI:

1. In the EJBCA Admin UI, go to **Certification Authorities**, enter a user defined CA Name in the **Add CA** input field and click **Create**.
2. In the **Crypto Token** drop-down, select the newly created Thales DPoD crypto token name.
3. In the **Signing Algorithm** drop-down select *SHA256WithRSA*. Since we chose good key names when generating keys, EJBCA will recognize them and pre-populate the key fields

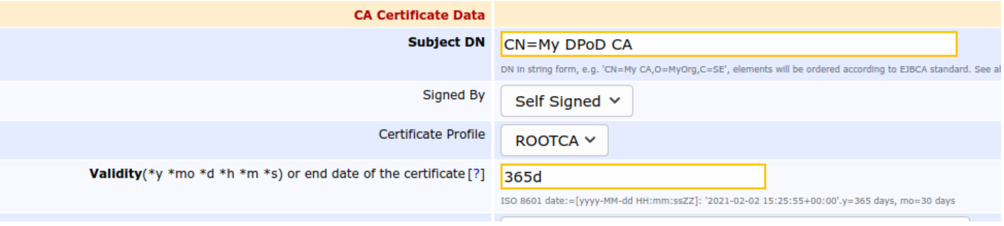


Create CA

CA Name : My DPoD CA

CA Type [?]	✓X.509 CA CVC CA
Crypto Token [?]	My DPoD HSM encryptKey - RSA 2048 signKey - RSA 3072 testKey - RSA 1024
Signing Algorithm	SHA256WithRSA Applicable Signing Algorithms according to the selected Crypto Token
defaultKey	encryptKey
certSignKey	signKey
crlSignKey	Use same as Certificate Signing Key (certSignKey).
keyEncryptKey	- Default key
testKey	testKey

4. Enter a validity in days, for example 365d for one year validity of the CA



CA Certificate Data	
Subject DN	CN=My DPoD CA DN in string form, e.g. 'CN=My CA,O=MyOrg,C=SE', elements will be ordered according to EJBCA standard. See al
Signed By	Self Signed
Certificate Profile	ROOTCA
Validity(*y *mo *d *h *m *s) or end date of the certificate [?]	365d ISO 8601 date:=[yyyy-MM-dd HH:mm:ssZZ]: '2021-02-02 15:25:55+00:00'.y=365 days, mo=30 days

5. Scroll down to the bottom and click **Create**.

And that completes the process of creating a Certification Authority using EJBCA in AWS, with keys from a DPoD Cloud HSM partition.

Published by PrimeKey Solutions AB
Solna Access, Sundbybergsvägen 1
SE-171 73 Solna, Sweden

To report errors, please send a note to .

Notice of Rights

Notice of Liability

The information in this guide is distributed on an “As Is” basis without warranty. While every precaution has been taken in the preparation of the guide, neither the authors nor PrimeKey shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in the guide or by computer software and hardware products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this guide, and PrimeKey was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this guide are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this guide.