Fortanix®

Integration Guide

USING DATA SECURITY MANAGER WITH HYPERLEDGER FABRIC

VERSION 1.0

Fortanix Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | United States of America | +1 (650) 943-2484 |

info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This document describes how to integrate **Fortanix Data Security Manager (DSM)** with **Hyperledger Fabric**. Hyperledger Fabric allows for using HSM to store private keys used for various Fabric operations. It also allows users to configure BCCSP (Blockchain Cryptographic Service Provider) with HSM using the PKCS#11 Standard API. This document describes configuring the PKCS#11 client provided by Fortanix with Hyperledger Fabric.

2.0 PREREQUISITES

- Set up Go using the official document from https://go.dev/dl/.
- Setup Docker using the official documentation https://docs.docker.com/engine/install/ubuntu.
- Ensure the system has installed the following packages: GIT, OpenSSL, GNU Compiler Collection (GCC), and Make.
- The Fortanix DSM integration with Hyperledger Fabric is tested for the following configurations:
    - Fabric-CA 1.5.5
    - Fortanix PKCS#11 client 4.8.2070
    - Docker version 20.10.17, build 100c701
    - Go 1.18.3
    - Host OS Ubuntu 20.04.4 LTS (Focal Fossa)
    - Container OS Ubuntu 20.04 LTS

3.0 REFERENCES FOR SETUP

- Refer to https://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html for setting up the Hyperledger Fabric network and other elements.
- For Fortanix DSM PKCS # 11 Library, go to https://support.fortanix.com/hc/en-us/articles/360016160451-Clients-PKCS-11-Library.
- This document covers the integration of Fortanix DSM with Hyperledger Fabric and provides a minimal example of the Hyperledger Fabric setup. Please refer to the official docs for production setup.

4.0 SET UP FORTANIX PKCS#11 CLIENT

1. Get the PKCS#11 **DEB package** from the following link (tested with Fortanix DSM version 4.8.2070)
   https://support.fortanix.com/hc/en-us/sections/4408769080724-PKCS-11
2. Use the following command to install the client on the host system.

```
sudo dpkg -i <pkg.deb>
```

3. The DEB installer copies the Fortanix DSM PKCS#11 shared object file (also called a library or module) to the location `/opt/fortanix/pkcs11/fortanix_pkcs11.so`.
4. The shared object file is mounted to the docker container as explained in the *section* "*Configure and Start the Hyperledger Fabric CA Server*".

5.0 BUILD HYPERLEDGER FABRIC CA WITH PKCS#11 ENABLED

1. Get the source code for Fabric CA at https://github.com/hyperledger/fabric-ca.
2. The default Dockerfile of Hyperledger Fabric CA uses Alpine Linux as the base image and for compiling the Fabric CA. The Fortanix DSM PKCS#11 client does not currently support Alpine Linux. Changing the OS to Ubuntu enables you to use the client.

NOTE: To change the OS to Ubuntu, edit the Dockerfile at the location `images/fabric-ca/Dockerfile`.

```
ARG GO_VER
ARG ALPINE_VER

FROM golang:1.18.5-bullseye as builder
ARG GO_LDFLAGS
ARG GO_TAGS

RUN apt update && apt install -y build-essential musl git;
```

```
ADD . /build/fabric-ca
WORKDIR /build/fabric-ca
RUN go install -tags "${GO_TAGS}" -ldflags "${GO_LDFLAGS}" \
github.com/hyperledger/fabric-ca/cmd/fabric-ca-server \
&& go install -tags "${GO_TAGS}" -ldflags "${GO_LDFLAGS}" \
github.com/hyperledger/fabric-ca/cmd/fabric-ca-client

FROM ubuntu:20.04
RUN apt update && apt install -y build-essential musl ca-certificates;
ENV FABRIC_CA_HOME /etc/hyperledger/fabric-ca-server
COPY --from=builder /go/bin /usr/local/bin
EXPOSE 7054
CMD fabric-ca-server start -b admin:adminpw
```

3. Build the container image.

```
GO_TAGS=pkcs11 make docker
```

4. The following images will be created.

```
REPOSITORY              TAG           IMAGE_UD      CREATED       SIZE
hyperledger/fabric-ca   1.5.5         b52c013d8c00  6 days ago    434MB
hyperledger/fabric-ca   amd64-1.5.5   b52c013d8c00  6 days ago    434MB
hyperledger/fabric-ca   latest        6b52c013d8c00 6 days ago    434MB
```

6.0 SET UP FORTANIX DSM – CREATE ACCOUNT, GROUP, AND APP

This section explains how to create an app and copy its API key to mount the PKCS#11 shared object file to the docker container as described in the *section "Configure and Start the Hyperledger Fabric CA Server*".

6.1 CREATE AN ACCOUNT IN FORTANIX DSM

1. Sign up for an account at https://sdkms.fortanix.com or https://amer.smartkey.io/#/.

Refer to the Fortanix DSM Getting Started guide for more details.

6.2 CREATE A FORTANIX DSM GROUP

1. Create a Fortanix DSM group.

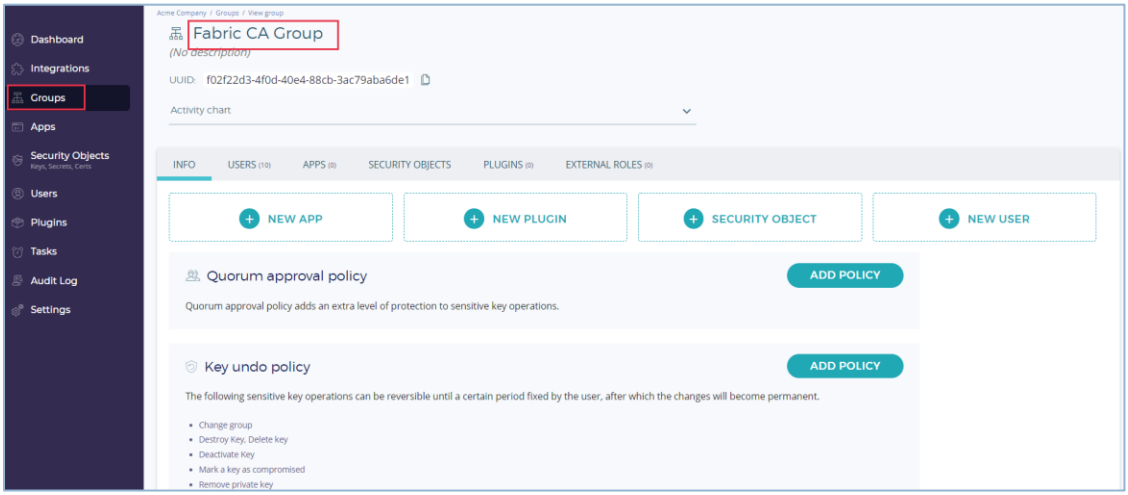

FIGURE 1: CREATE GROUP

6.3 CREATE AN APP IN FORTANIX DSM

Create an app in Fortanix DSM of type **REST API** and copy the app's **API Key**. The API key is used to mount the PKCS#11 shared object file to the docker container as described in the *section* "*Configure and Start the Hyperledger Fabric CA Server*".

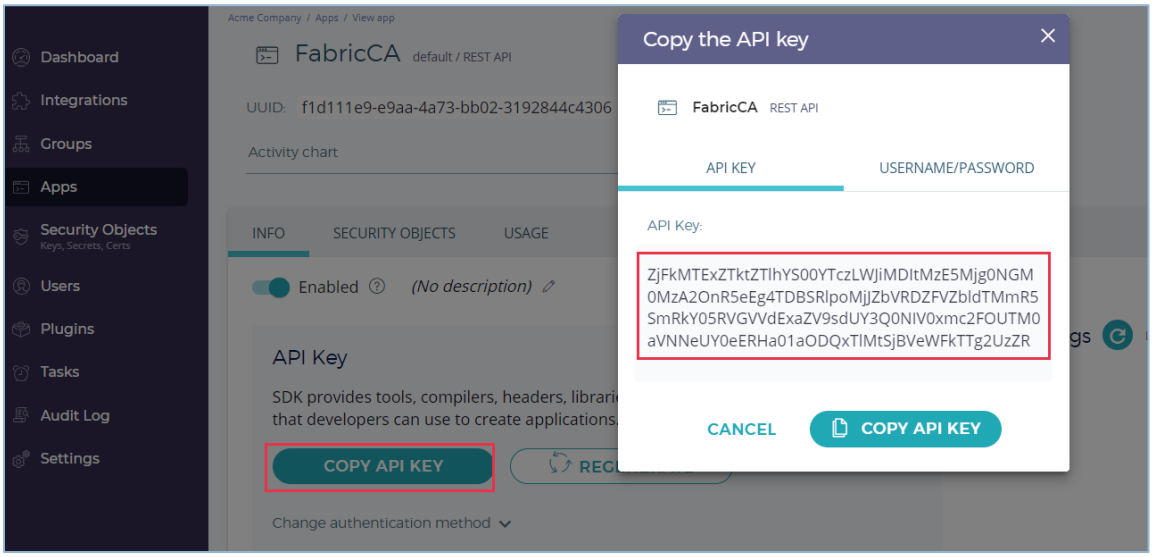

FIGURE 2: CREATE AN APP AND COPY THE API KEY

7.0 CONFIGURE AND START THE HYPERLEDGER FABRIC CA SERVER

1. Mount the volume for the PKCS#11 shared object.

```
-v /opt/fortanix/pkcs11:/etc/hyperledger/fabric
```

2. Run the following command to create a folder called `server_config` from the current working directory.

```
docker run -it -v ${PWD}/server_config:/etc/hyperledger/fabric-ca-
server -v /opt/fortanix/pkcs11:/etc/hyperledger/fabric
hyperledger/fabric-ca bash
```

This will persist the `/etc/hyperledger/fabric-ca-server` on the host system.

3. Run `fabric-ca-server` to generate the config file from inside the container using the following command:

```
fabric-ca-server start -b admin:adminpw
```

Press **CTRL + X** or **CRTL+C** to exit the program.

4. Edit the `fabric-ca-server-config.yaml` file in `/etc/hyperledger/fabric-ca-server/` using the following command.

```
vi fabric-ca-server-config.yaml
```

5. Add the following to the `bccsp` section of the above file.

```
bccsp:
  default: PKCS11
  pkcs11:
    Library: "/etc/hyperledger/fabric/fortanix_pkcs11.so"
    hash: SHA2
    security: 256
```

```
    Label: "Fortanix Token"
      Pin: file://etc/hyperledger/fabric/fortanix_pkcs11.conf
```

6. Edit the `fortanix_pkcs11.conf` file as pointed by the `Pin` field in the `fabric-ca-server-config.yaml` file. This can be put in the same path as `/opt/fortanix/pkcs11`, so mounting `-v /opt/fortanix/pkcs11 :/etc/hyperledger/fabric` will also mount the `fortanix_pkcs11.conf` file.

```
api_endpoint = "https://sdkms.fortanix.com"
api_key="<API_KEY>"
app_id="<APP_UUID>"

[log]
system = false # Unix only, logs to syslog
file = "/var/log/p11.log"
```

7. The `api_endpoint` refers to the instance of Fortanix DSM you set up your account on, `api_key` is the API key of the Fortanix DSM app created in *section "Create an App in Fortanix DSM"*, `app_id` is the UUID of the same app. Logging can be set using this config file, the paths are in context of the container.
8. Delete any keystores in `/etc/hyperledger/fabric-ca-server` such as the `MSP` directory and the old `.pem` file so that new keystores are generated with the HSM when the server is started.
9. Start the CA server using the following command:

```
fabric-ca-server start -b admin:adminpw
```

8.0 ENROLLING AND REGISTERING A FABRIC CA CLIENT

1. Start the CA server if it is not currently running. This is needed for the Enroll operation.
2. Enroll the client using the credentials used in *Step 9* of the previous *section "Configure and Start the Hyperledger Fabric CA Server"*.

```
fabric-ca-client enroll -u http://admin:adminpw@localhost:7054
```

3. This will create a client config YAML file in the location `/etc/hyperledger/fabric-ca-server`.
4. Edit the `bccsp` section and copy the server BCCSP configuration for the client.
5. Run the `enroll` command to enroll the client.

```
fabric-ca-client enroll -u http://admin:adminpw@localhost:7054
```

6. Register the client using the following syntax:

```
fabric-ca-client register --id.name ica.example --id.type client --
                                id.secret root --csr.names
C=es,ST=madrid,L=Madrid,O=example.com --csr.cn ica.example -m ica.example
                                --id.attrs '"hf.IntermediateCA=true"' -u
http://localhost:7054 --loglevel debug
```

9.0 PEERS AND ORDERING NODES

1. To set up peers and ordering nodes with Fortanix DSM, edit the corresponding YAML file for each node. Use the same PKCS#11 bccsp settings to edit either the `core.yaml` or `orderer.yaml` files.
2. Run the same `enroll` commands from respective orderer or peer nodes to enroll it with the Fabric CA server that is using Fortanix DSM.

Refer to the official Hyperledger Fabric Documentation for folder structure and the network setup.

10.0 DOCUMENT INFORMATION

10.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/8723554765332-Using-Fortanix-Data-Security-Manager-with-Hyperledger-Fabric

10.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com