# Laboratory_15: Mounting a Certificate Authority and perform a secure automated certificate management.

## Installation

- Install step
    - sudo apt-get update && sudo apt-get install -y --no-install-recommends curl vim gpg ca-certificates
    - sudo curl -fsSL https://packages.smallstep.com/keys/apt/repo-signing-key.gpg -o /etc/apt/trusted.gpg.d/smallstep.asc && \ echo 'deb [signed-by=/etc/apt/trusted.gpg.d/smallstep.asc] https://packages.smallstep.com/stable/debian debs main' \ | sudo tee /etc/apt/sources.list.d/smallstep.list deb [signed-by=/etc/apt/trusted.gpg.d/smallstep.asc] https://packages.smallstep.com/stable/debian debs main
    - sudo apt-get update && sudo apt-get -y install step-cli
- sudo apt-get update && sudo apt-get install -y tshark

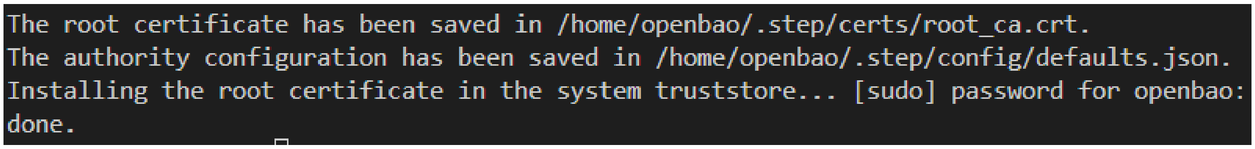
## CA deployment

- Deployment:

```
docker run -it -v step:/home/step \
  -p 9000:9000 \
  -e "DOCKER_STEPCA_INIT_NAME=Smallstep" \
  -e "DOCKER_STEPCA_INIT_DNS_NAMES=localhost,$(hostname -f)" \
  -e "DOCKER_STEPCA_INIT_REMOTE_MANAGEMENT=true" \
  smallstep/step-ca
```

- Collect:
    - CA administrative username
    - CA administrative password
- Check CA status:
    - curl https://localhost:9000/health
        - Output: {"status":"ok"}

- Obtain password:
    - CA_FINGERPRINT=$(docker run -v step:/home/step smallstep/step-ca step certificate fingerprint certs/root_ca.crt)
    - step ca bootstrap --ca-url https://localhost:9000 --fingerprint $CA_FINGERPRINT –install
    - Login:



```
The root certificate has been saved in /home/openbao/.step/certs/root_ca.crt.
The authority configuration has been saved in /home/openbao/.step/config/defaults.json.
Installing the root certificate in the system truststore... [sudo] password for openbao:
done.
```

## Get a certificate

1. Once you have a certificate authority up and running, the step ca certificate command is a one-step option for generating a private key and obtaining a signed certificate:

   step ca certificate svc.example.com svc.crt svc.key

2. You can check your work using step certificate inspect:

   step certificate inspect svc.crt --short

## Sign a certificate signing request (CSR)

3. Generating a private key and a certificate request (CSR) file

   step certificate create --csr foo.example.com foo.csr foo.key

4. Asking the CA to sign the CSR and return a certificate

   step ca sign foo.csr foo.crt

5. sudo tshark -i any -f "tcp port 9000" -w step_ca_traffic.pcap

## Issue a certificate using a Single-use CA Token (CSR)

6. CA generates a token for the client who has the JWK's encrypted private key password:

```
TOKEN=$(step ca token localhost)
echo $TOKEN | step crypto jwt inspect --insecure
```

7. Generate the CSR:

```
step certificate create --csr localhost localhost.csr localhost.key
```

8. Get the CSR signed, using the token:

```
step ca sign --token $TOKEN localhost.csr localhost.crt
```

## Renew a certificate

9. Certificate renewal is easy, and is authenticated using the existing private key:

```
step ca renew foo.crt foo.key
```

## Revoke a certificate

10. Revoke the svc.crt certificate we created earlier:

```
step ca revoke --cert svc.crt --key svc.key
```

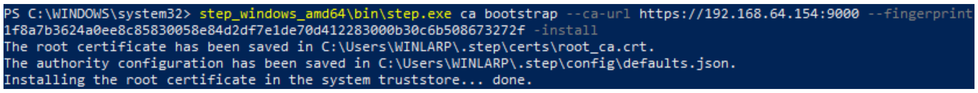
## Validate Certificate

11. Install step client in windows:

- curl.exe -LO https://dl.smallstep.com/cli/docs-cli-install/latest/step_windows_amd64.zip
- Expand-Archive -LiteralPath .\step_windows_amd64.zip -DestinationPath .

- step_windows_amd64\bin\step.exe version

12. Apply on Windows:
    a. step_windows_amd64\bin\step.exe ca bootstrap --ca-url https://192.168.64.154:9000 --fingerprint 1f8a7b3624a0ee8c85830058e84d2df7e1de70d412283000b30c6b508673272f –install



```
PS C:\WINDOWS\system32> step_windows_amd64\bin\step.exe ca bootstrap --ca-url https://192.168.64.154:9000 --fingerprint
1f8a7b3624a0ee8c85830058e84d2df7e1de70d412283000b30c6b508673272f -install
The root certificate has been saved in C:\Users\WINLARP\.step\certs\root_ca.crt.
The authority configuration has been saved in C:\Users\WINLARP\.step\config\defaults.json.
Installing the root certificate in the system truststore... done.
```