Table of Contents

Introduction 1
Prerequisites 1
Configuration 1
Create keypairs 1
Modify ca.json 1
Add sshpop provisioner 2
Start the CA 2
Conclusion 3

Introduction

So you've set up a local certificate authority using the Smallstep CA software, and you're using it to issue x.509 certificates to resources on your LAN. Perhaps you followed their guide to set up a “tiny CA” using a Raspberry Pi, a YubiKey, and a hardware RNG. Now you'd like to use your certificate authority to issue SSH user and host certificates. Unfortunately, the Smallstep software doesn't make this simple, but it's still do-able. This guide will specifically address modifying the Raspberry Pi-based tiny CA to issue SSH certificates.

Prerequisites

This guide assumes your Tiny CA is up and running without problems, and running at least version 0.15.8 of the step-ca software.

Configuration

Before proceeding, you'll need to stop the CA software. Run `systemctl stop step-ca`.

Create keypairs

Next, you'll need to create the signing key pairs for host and user certificates. Run `ykman piv generate-key –algorithm ECCP256 82 ssh_host_ca_key.pem` followed by `ykman piv generate-key –algorithm ECCP256 83 ssh_user_ca_key.pem`.

You'll then need to convert the `.pem` files to SSH format. Run `ssh-keygen -i -f ssh_host_ca_key.pem -mPKCS8 > ssh_host_ca_key.pub` followed by `ssh-keygen -i -f ssh_user_ca_key.pem -mPKCS8 > ssh_user_ca_key.pub`. Move the `.pub` files to `/etc/step-ca/certs`.

Modify ca.json

You'll now need to make some edits to the Step CA config file, `/etc/step-ca/config/ca.json`.

First, tell step-ca to look for the signing keys on the YubiKey. Following the `kms` block, add the following:

```
        },
        "ssh": {
```

```
                "hostKey": "yubikey:slot-id=82",
                "userKey": "yubikey:slot-id=83"
        },
```

The first closing brace in this section is already present, but make sure to add the comma after it.

Second, edit the first provisioner in this file (the JWK one) to look like this:

```
                        {
                                "type": "JWK",
                                "name": "admin@familybrown.org",
                                "key": {
                                        "use": "sig",
                                        "kty": "EC",
                                        "kid": "foo",
                                        "crv": "P-256",
                                        "alg": "ES256",
                                        "x": "bar",
                                        "y": "baz"
                                },
                                "encryptedKey": "baz",
                                "claims": {
                                        "enableSSHCA": true
                                }
                        },
```

The part you're adding here is the `claims` section, to enable you to issue SSH certificates using this provisioner.

Add sshpop provisioner

You'll need to add another provisioner, which will be used for renewing host certificates. Run `step ca provisioner add sshpop –type sshpop –ca-config /etc/step-ca/config/ca.json`.

Start the CA

Now, start the certificate authority again. Run `systemctl start step-ca`. Confirm it's running with `systemctl status step-ca`. If not, the most likely issue is JSON formatting–make sure your edits to `ca.json` are formatted properly.

Conclusion

Your CA is now configured to issue SSH user and host certificates. You can add further provisioners as needed.