Vault as Root CA

Here are steps you can follow to setup a vault instance as a Root CA.

> NOTE: This page assumes that you have created a single-node vault instance to serve as your Root CA.
>
> See this page for how to do that: Hashicorp Vault Setup

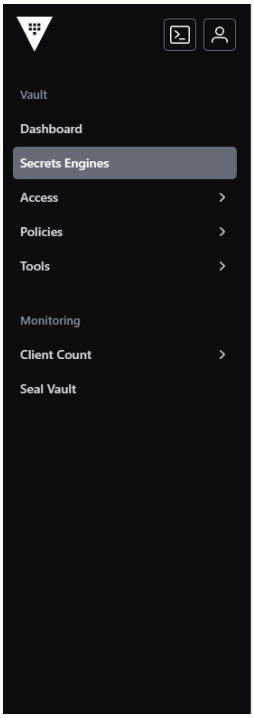
> NOTE: These steps will create a root CA with one signing key.
> You should create an intermediate CA, as well, that will perform the actual signing of certs.
> This will allow you to offline this root CA, once the intermediate CA is up.

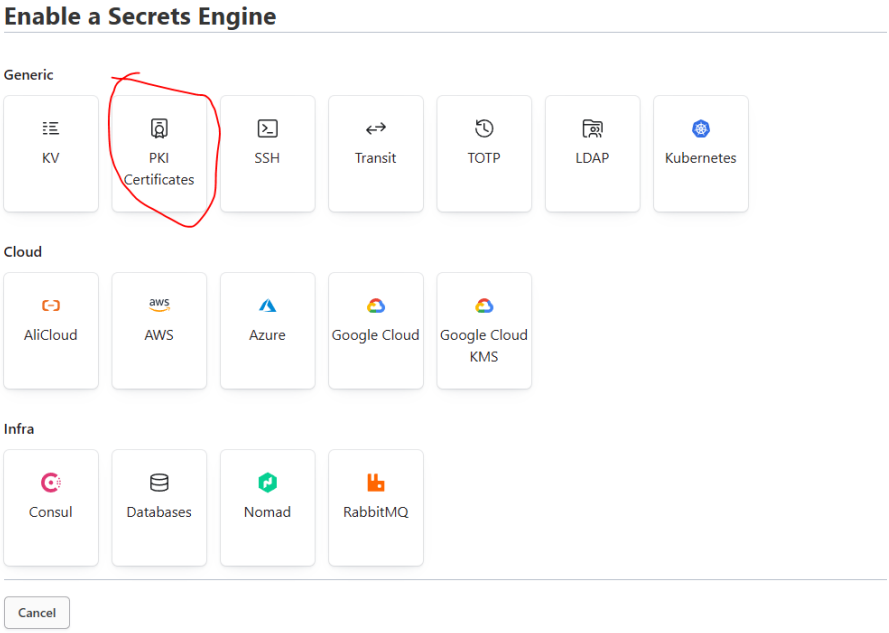
Starting the PKI Engine

> NOTE: From here down, is steps for creating a Root CA.
> If you are setting up an Intermediate CA, skip to 'Configure Intermediate CA'.

For Vault to serve as a root CA, you have to add the PKI secrets engine.

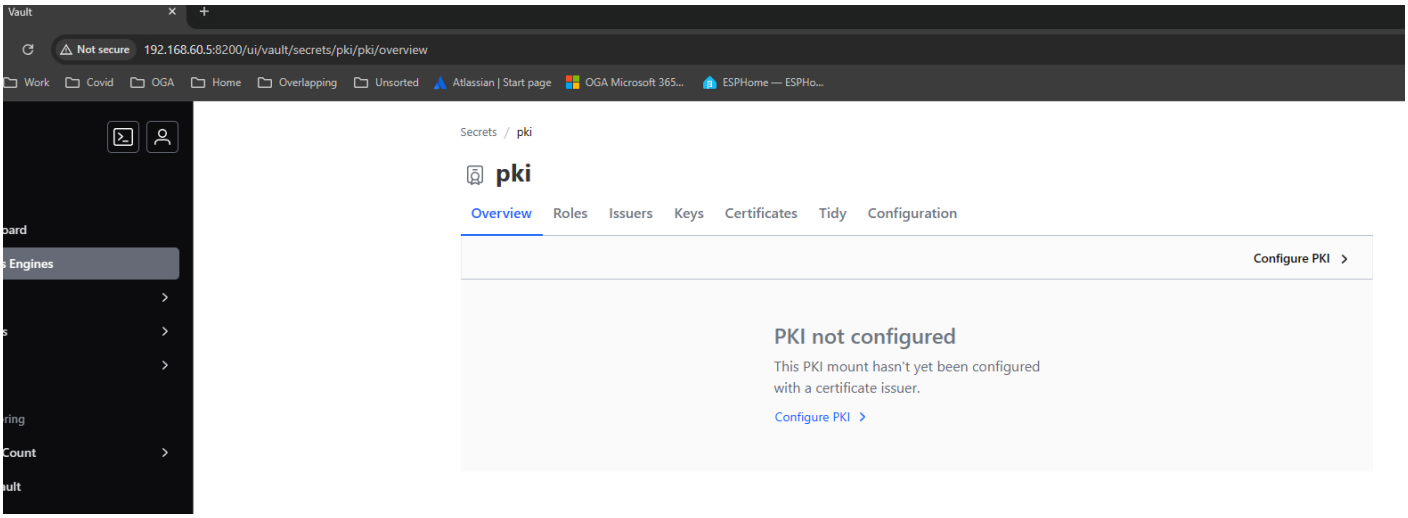
To do this, enable the pki secrets engine:



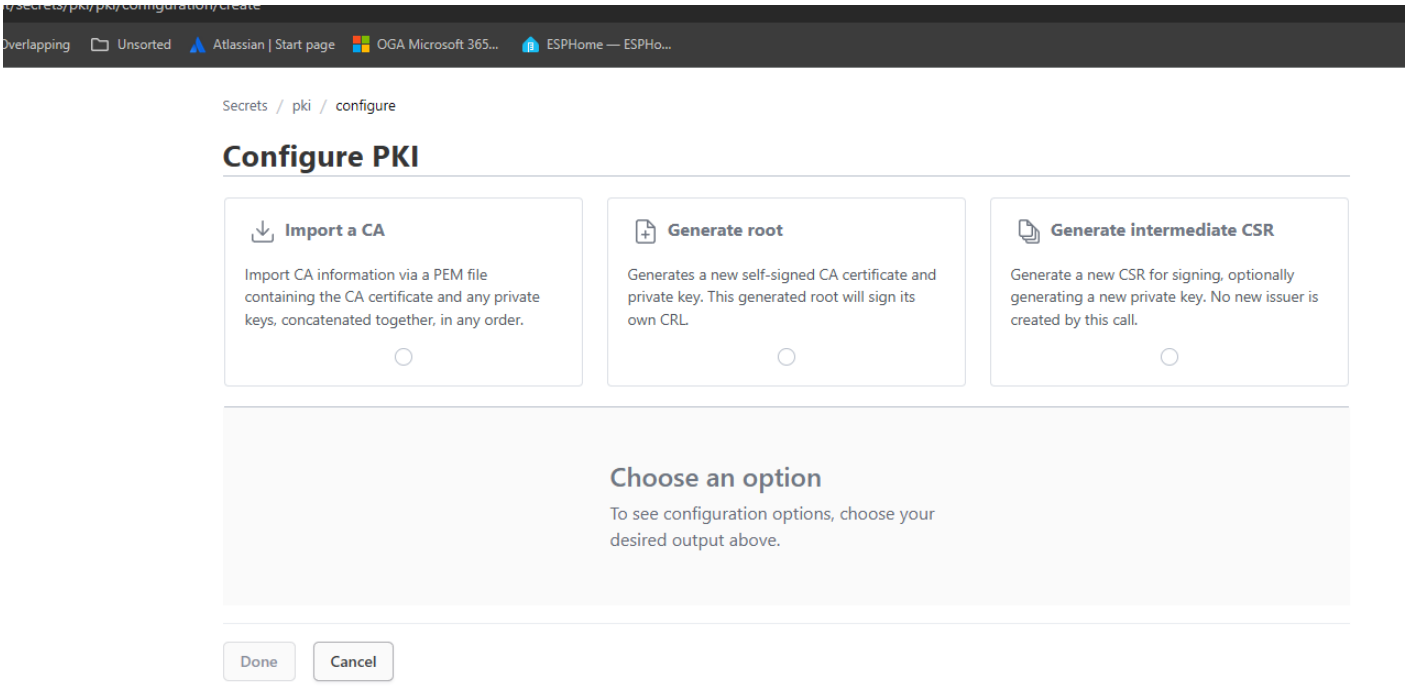


For a Root CA, set the Max lease time to as long as possible, as the root CA will be offlined after generation.

Once initialized, it will look like this:



For a root CA, click Configure PKI to begin setup.



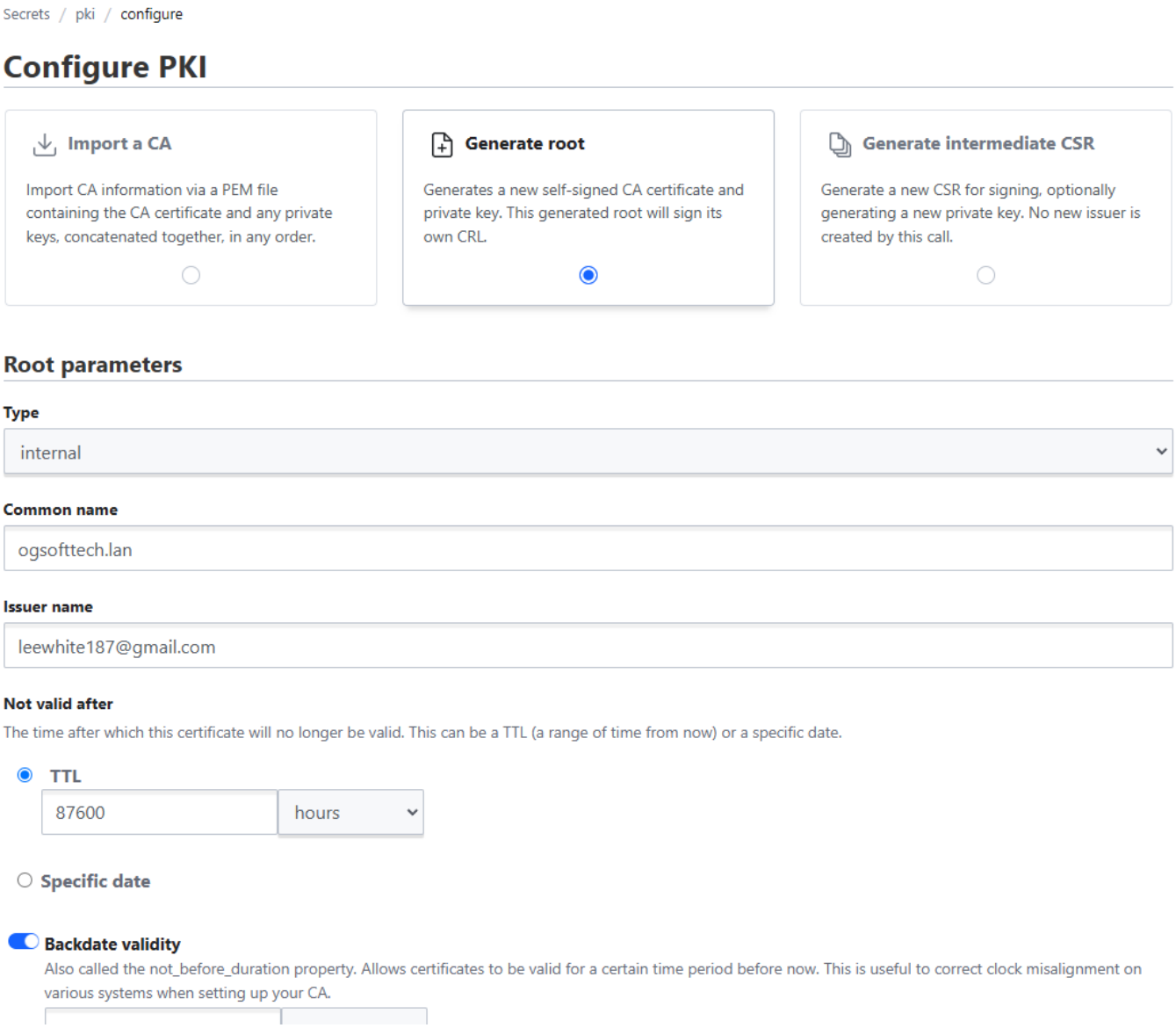
Choose the Generate Root option.

Set Type to Internal.

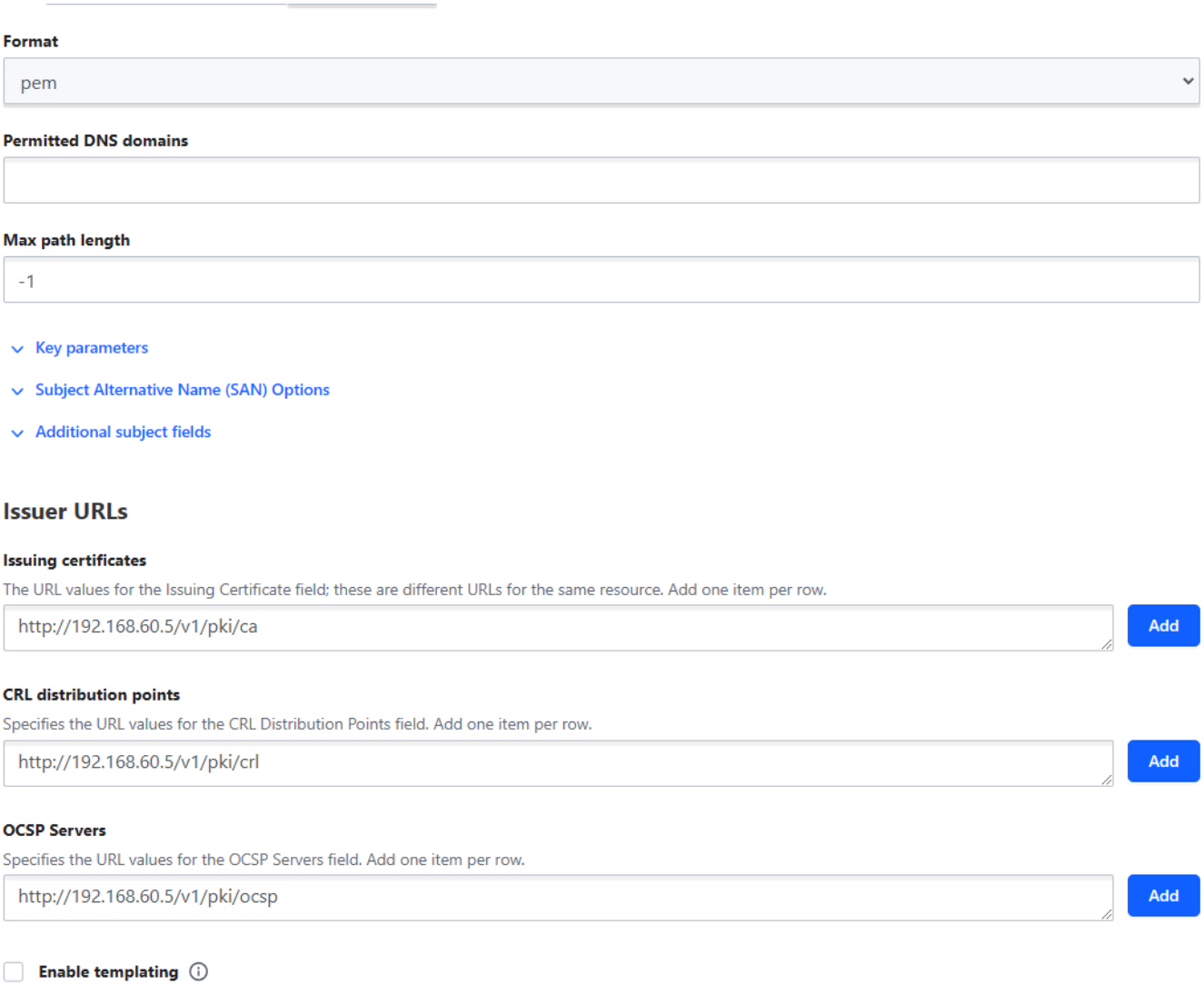
Set your Common name. Usually, this is a domain with a private TLD suffix.

Set the issuer name.

Set a TTL that is maxed out: 87600 hours.

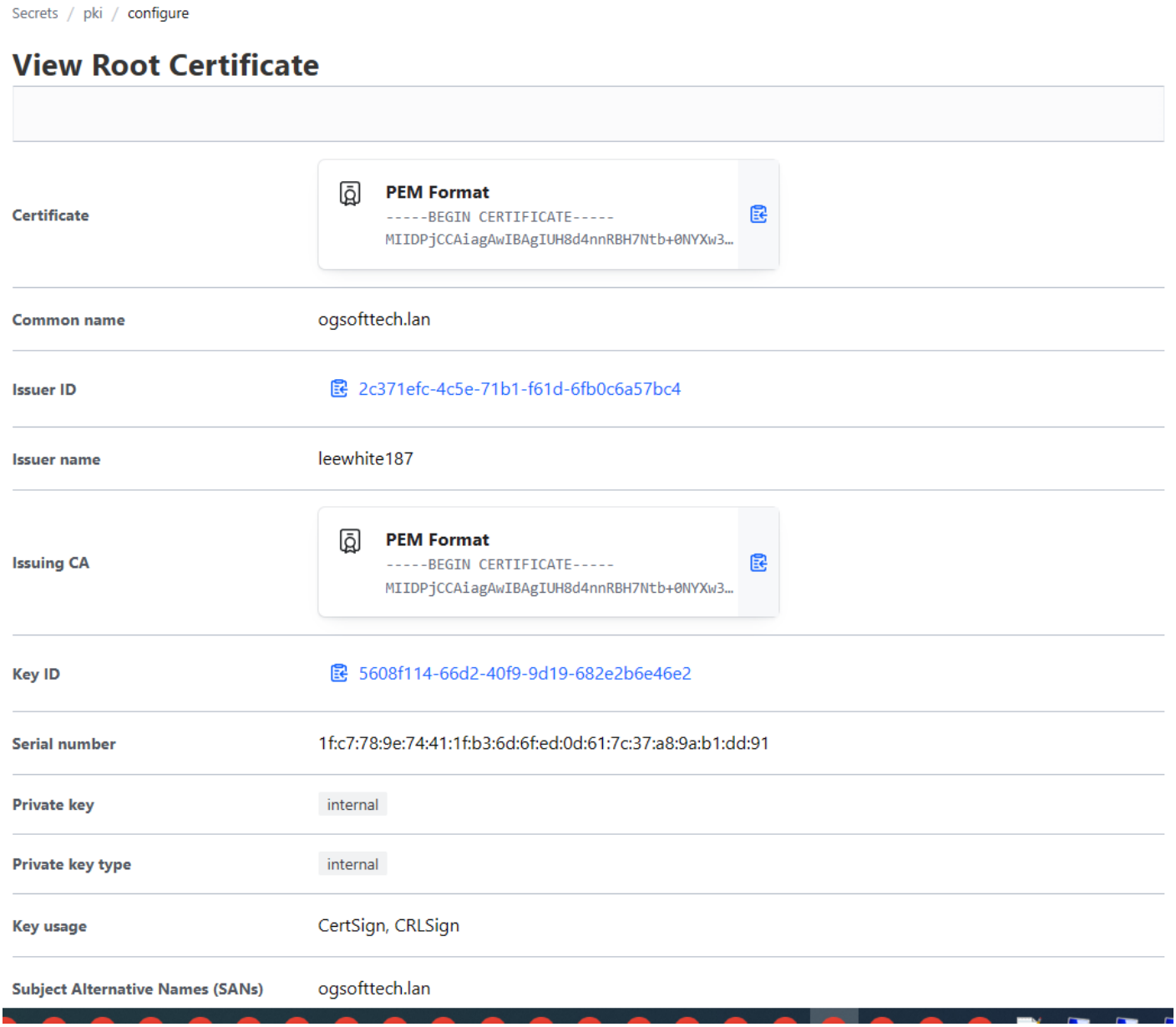


Scroll down and fill in the issuer URLs, matching the origin for your root CA host:



When finished, click Done, to generate the root CA key and certificate.

You will see a page like this:



Copy out the root CA certificate, and save it to a file, named: `ogsofttech.lan_ca.crt`

Install it on all machines of the local network, so they will recognized the signed SSL certs of hosts.

Current Intranet Root CA Certificate

The current root CA for the local intranet can be found in the secure share at this path:

```
\SecureShare git\oga\ogsofttech.lan\rootCA
```

> NOTE: This certificate should be installed on any host that will consume services signed by the root ca.

See this page for how to install it on an Ubuntu host: How to Add Root CAs to Ubuntu

Root CA Rotation

To make things easier, when it comes time to rotate your root CA key, add a role, now.

Click PKI.

Click Roles.

Click Create Role.

Give the new role a name that you will recognize as the root CA rotation role: CA_rotation_role

Leave the rest of the fields empty, and click Create.

Now, you have a working root CA key/cert for your network.

We will use it to sign the certificate of an Intermediate CA, that will do all the actual work.

And, we will offline the root CA.

Revision #7
Created 4 September 2025 02:55:37 by glwhite
Updated 23 September 2025 00:18:12 by glwhite