Generate Certificates with Hashicorp Vault

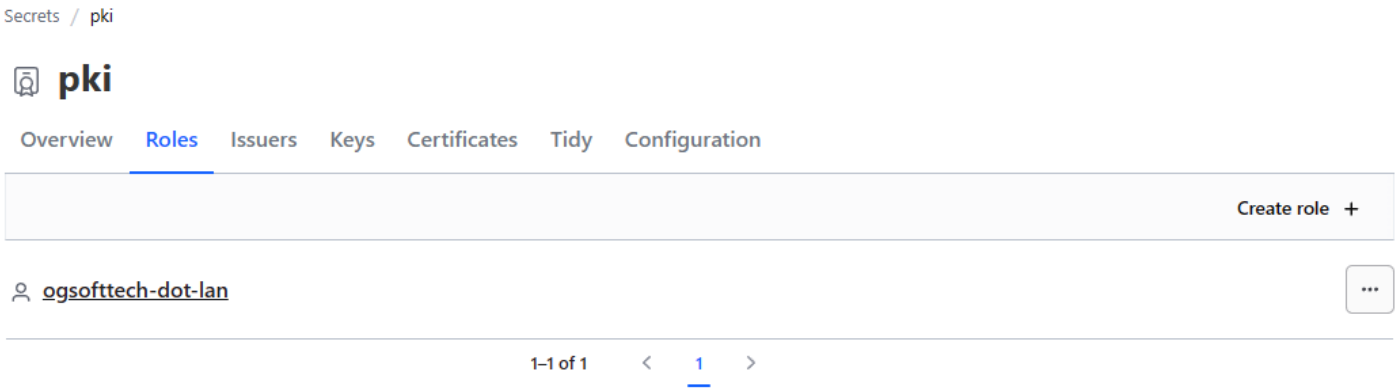
Here are steps to generate SSL certificates using HashiCorp Vault as an Intermediate CA.

NOTE: Be sure that you've setup a vault instance as an Intermediate CA.
See this page for how: Vault as Intermediate CA

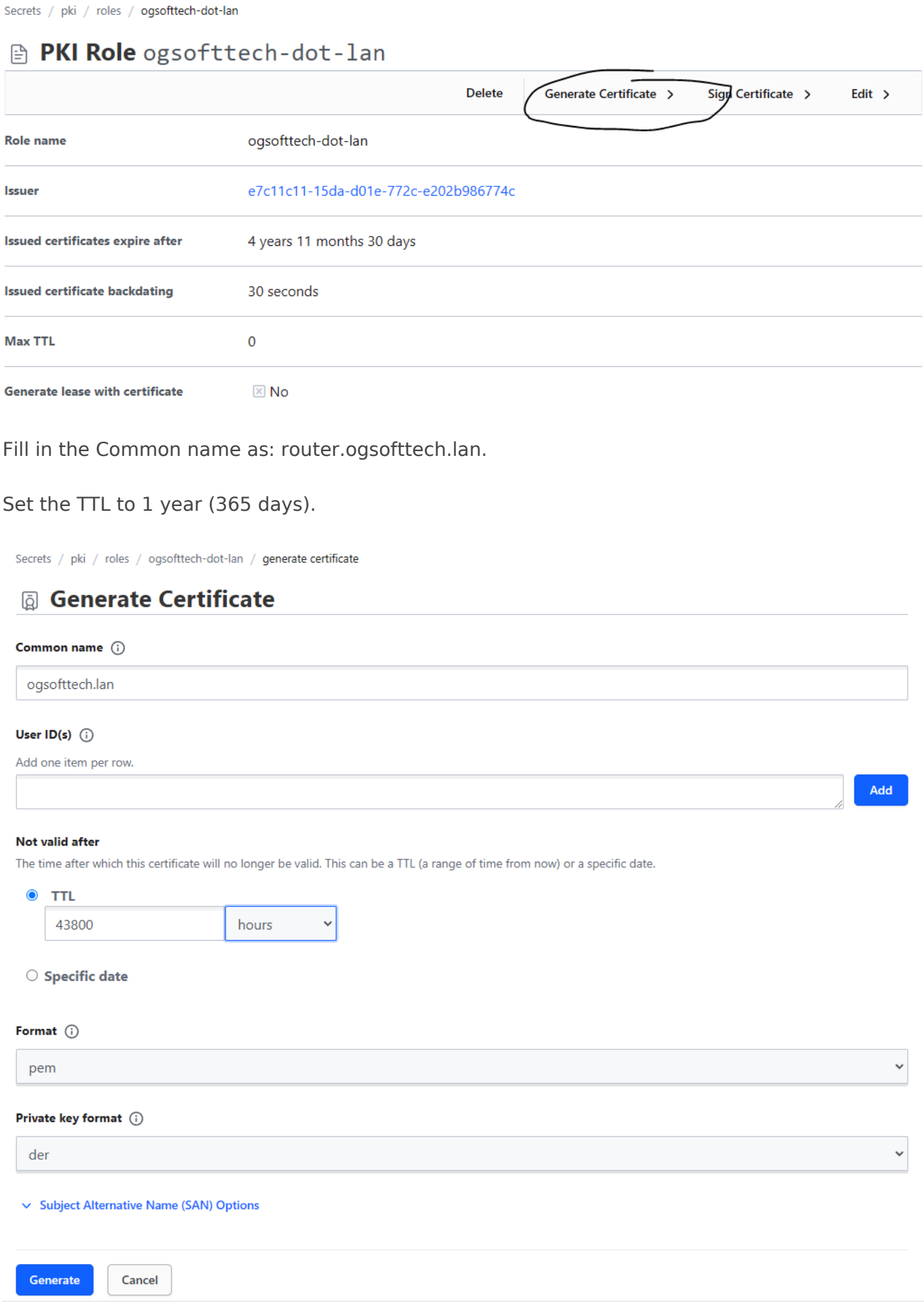
Login to the web UI of your intermediate CA, such as: https://vault02.ogsofttech.lan:8200/ui/
If DNS is down, use this: https://192.168.60.6:8200/ui/

For the latest intermediate CA url, see this page: Vault Services

Find the issuing role by navigating to Secrets/PKI/Roles.



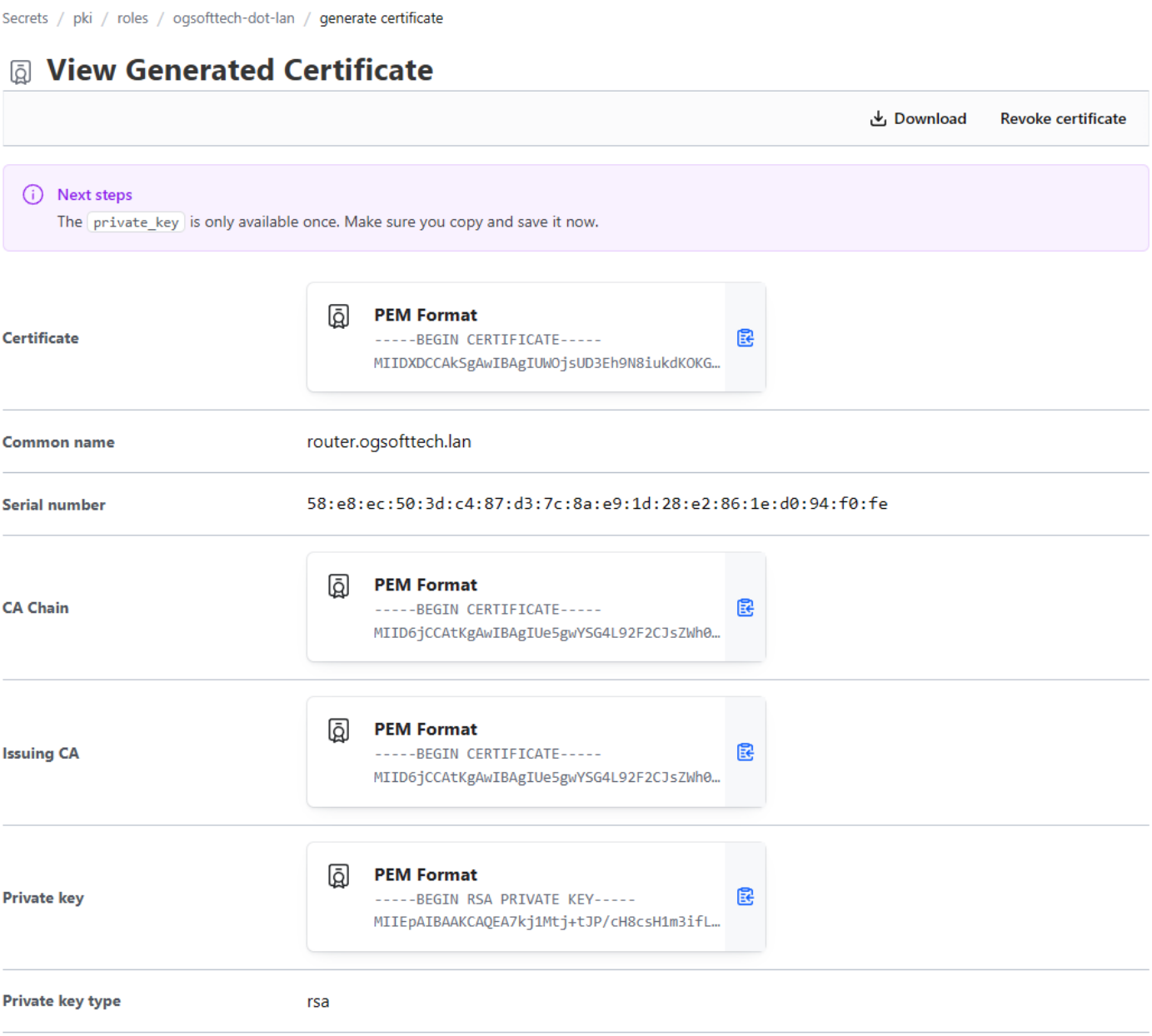
Select the role, and click Generate Certificate:



Fill in the Common name as: router.ogsofttech.lan.

Set the TTL to 1 year (365 days).

Click Generate, to create the key and certificate, and you'll see this:



Download the private key as: router.ogsofttech.lan-key.pem

Download the certiticate as: router.ogsofttech.lan-cert.pem

Download the CA chain as: router.ogsofttech.lan-cabundle.pem

> NOTE: We are calling the downloaded CA chain file a "ca bundle".
> CA bundle is the standard naming convention for this file type.
> Specifically, a cert is often concatenated with the CA bundle that signed it, to create a chain certificate file.

Now, you can copy the cert, ca bundle, and private key to the host, for usage.

If generating a pair for a linux host, you will need them as .crt and .key files.

Follow this: Converting PEM to crt and key

If generating a pair for an Nginx host, you will need

Revision #6
Created 1 September 2025 01:36:18 by glwhite
Updated 4 September 2025 03:24:34 by glwhite