OpenSSL-only NetIQ Certificate Server SUB CA

18.10.23

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

OpenSSL-only NetIQ Certificate Server SUB CA

This is a quick step-by-step guide on how to create a SUB CA to NetIQ Certificate Server (eDirectory) with external certificate authority using only OpenSSL commands. This is much more straightforward process than done with iManager and allows more flexibility.

Overview

What we need to do:

- Create a new private key
- Make a certificate signing request
- Get signed certificate along with the chain from CA
- Create pfx from all of the above
- Delete NetIQ Certificate Server CA object
- Import pfx into a new CA in NetIQ Certificate Server using iManager
- Create default certificates

Create a new private key

First we need to create the private key with command

```
openssl genrsa -aes256 -out /path/to/mysubca.key 8192
```

Give a sufficient pass phrase when prompted.

Make a certificate signing request

Then we proceed to making the csr with openssl:

```
openssl req -sha256 -new -key /path/to/mysubca.key -out /path/to/mysubca.csr
```

Then answer the questions:

```
Enter pass phrase for /path/to/mysubca.key: <your pass phrase here>
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

```
Country Name (2 letter code) [FI]:
State or Province Name (full name) []:
Locality Name (eg, city) []:Lappeenranta
Organization Name (eg, company) []:My Org
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:myhost.domain
Email Address []:helpdesk@domain

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Issue certificate

Send the csr file /path/to/mysubca.csr to the CA authority to be signed and request also the CA certificate to be included in the chain of our SUB CA.

Create pfx

Now we can create the pfx file that will be used to import our SUB CA to eDirectory. Use command:

```
openssl pkcs12 -export -out /path/to/mysubca.pfx -inkey /path/to/mysubca.key
-in /path/to/mysubca.crt -certfile ca_cert.crt
```

The ca_cert.crt is the CA certificate you received from the issuer.

Delete CA

Use iManager, go to “Roles and Tasks”, select “eDirectory maintenance” and “Delete Object”. Browse to the CA object and press OK.

Import pfx as new SUB CA

In iManager go to “Roles and Tasks”, “NetIQ Certificate Server”, “Configure Certificate Authority”. Now that CA is deleted you should be presented with CA configuration wizard.

- Select “Import” and click “Next”
- Select PKCS12, click “Browse”, locate /path/to/mysubca.pfx and give the pass phrase
- Click OK, Next, Next and Finish

Create default certificates

Using iManager select “Roles and Tasks”, “NetIQ Certificate Server”, “Create Default Certificates”, select the first server and force the generation of new default certificates. Repeat for each server.

Comments

All comments and corrections are welcome.