

Server certificate management

There are two options for certificate management

- 1.** The easiest, fast and cheap one: Do not create any public or private key, nor enter any certificate chain. At first start up, Soffid Identity Provider will generate a new public/private key pair. Using this key, Soffid IdP will create a self-signed certificate and will store it on the certificate chain field.
- 2.** The secure one:
 - 2.1.** Create a public/private key.
 - 2.2.** Generate a PKCS#10 file. Use this file to ask for a certificate to a well known certificate authority.
 - 2.3.** After some paper work, the certificate authority will give you a valid certificate.
 - 2.4.** The certificate can be in PEM or DER format. If it's in PEM format, it will start with a line saying

```
-----BEGIN CERTIFICATE ----
```

In such a case, just paste its contents on certificate chain field.

If it's in binary DER format, you can use openssl to convert it from PEM to DER:

```
openssl x509 -in <DER-FILE> -inform DER -out <PEM-FILE> -outform PEM
```

Sometimes your CA will give you a base64 encoded DER file. In such a case, convert it to PEM using:

```
openssl base64 -d <DEF-FILE> | openssl x509 -inform DER -out <PEM-FILE> -outform PEM
```

Revision #2

Created 29 September 2021 08:51:53

Updated 27 September 2023 06:34:26