Convert SSL PFX for NGINX Usage

NGINX doesn’t natively use a pfx key file (pfx is what Windows IIS needs). So, it must be converted to a private key, removing the public key from it.

Folder Creation

Create the folder for storing SSL certificates:

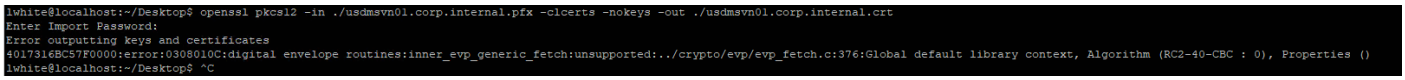
```
cd /etc/nginx/
mkdir ssl
cd ssl
chmod 700 /etc/nginx/ssl
```

Public Cert

From the pfx file, recover the public certificate:

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out public.crt
```

> NOTE: If you see an error, like the following, this means that the pfx was encoded with an old cipher.
> And, you must run the openssl command in legacy mode.



To work around the above error, add the '-legacy' switch to your statement, like this:

```
openssl pkcs12 -legacy -in cert.pfx -clcerts -nokeys -out public.crt
```

Private Key

From the pfx file, recover the encrypted private key:

```
openssl pkcs12 -in cert.pfx -nocerts -nodes -out private.rsa
```

> NOTE: Same as before. If you saw an error, when retrieving the public key, you will need to add the '-legacy' switch to the above statement.

Now, decrypt the encrypted private key:

```
openssl rsa -in private.rsa -out private.key
```

Moving Them

Move the public certificate and private key to the ssl folder, created earlier.

Set permissions on the ssl folder and files, so only root can access the certs and keys:

```
chmod 600 -R /etc/nginx/ssl/*
```

Revision #6
Created 10 June 2025 05:15:31 by glwhite
Updated 29 May 2026 19:37:35 by glwhite