

PFX maken op Mac OS (OpenSSL)

Als u een Certificate Signing Request (CSR) heeft aangemaakt op Mac OS en u wilt het certificaat op een andere systeem (bijv. een Windows Server) gebruiken dan is het nodig om een zogenaamd .pfx bestand te maken. In een .pfx bestand zijn het Servercertificaat en de bijbehorende private sleutel gecombineerd. Hieronder staan de stappen beschreven om een .pfx bestand te maken van de sleutel die u zelf hebt aangemaakt en het servercertificaat dat u van KPN ontvangt.

1. Start de Terminal op

Het maken van het .pfx bestand wordt gedaan in de Terminal. Druk op

```
[command ⌘] + [spatie]
```

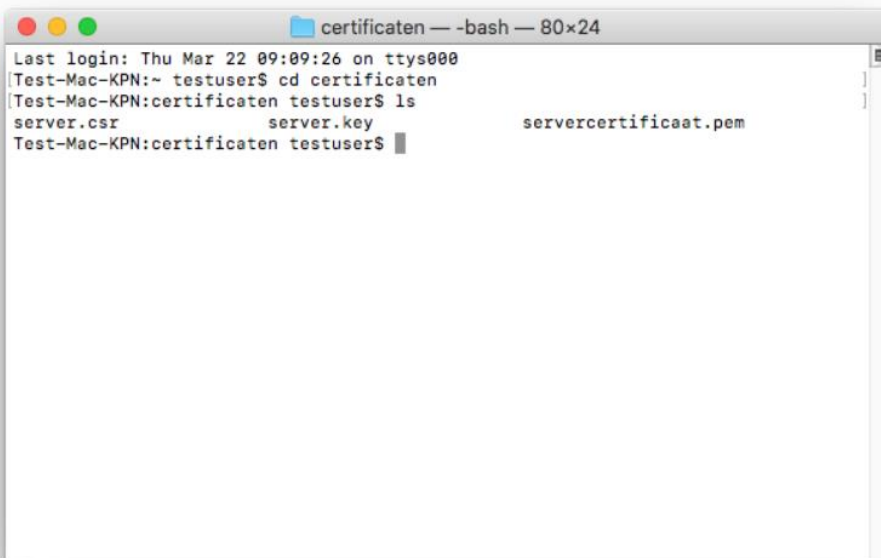
om de zoek functie te openen. Zoek op 'Terminal' en druk op [Enter]. De terminal wordt nu geopend.

2. Ga naar de map waarin het sleutelpaar en de csr is gemaakt

Tijdens het aanmaken van de CSR op de Mac heeft u een map "certificaten" aangemaakt. In deze map dient u het certificaat dat u per e-mail van KPN ontvangt op te slaan. Ga naar deze map en controleer de inhoud door de volgende commando's uit te voeren in de terminal:

```
cd certificaten
```

```
ls
```



```
certificaten — -bash — 80x24
Last login: Thu Mar 22 09:09:26 on ttys000
[Test-Mac-KPN:~ testuser$ cd certificaten
[Test-Mac-KPN:certificaten testuser$ ls
server.csr          server.key          servercertificaat.pem
[Test-Mac-KPN:certificaten testuser$
```

Zorg er voor dat de volgende bestanden in deze map aanwezig zijn (hoewel de server.csr niet meer nodig is na het aanvragen van het certificaat):

- server.key
- server.csr
- servercertificaat.pem

De 'server.key' en 'server.csr' zijn door u gemaakt tijdens de aanvraag. Het 'servercertificaat.pem' bestand is het certificaat dat u van KPN ontvangt als de aanvraag is goedgekeurd. Uiteraard kunt u gekozen hebben voor andere bestandsnamen. Die dient u dan te gebruiken in de vervolgstap.

3. Maak het .pfx bestand met OpenSSL

Op Mac OS is standaard het programma OpenSSL geïnstalleerd. Dit programma heeft u nodig om een .pfx file te maken van de key en het servercertificaat.

Voer het volgende commando uit:

```
openssl pkcs12 -export -out certificaat.pfx -inkey server.key -in servercertificaat.pem
```

Toelichting: Het commando vraagt eerst om de pass phrase in te voeren zodat u de server.key kan gebruiken. Deze pass phrase heeft u gekozen tijdens het aanmaken van de CSR op de Mac.

```
Enter pass phrase for server.key:
```

Vervolgens dient u tweemaal een Export password te kiezen om de .pfx te beveiligen. Dit mag hetzelfde zijn als de pass phrase van de server.key. De bestandsnaam van het nieuwe bestand is 'certificaat.pfx'.

```
Enter Export Password:  
Verifying - Enter Export Password:
```

Kies een sterk password voor het .pfx bestand. Het is belangrijk om het password van de .pfx te onthouden. Zonder dit password kunt u geen gebruik maken van het .pfx bestand voor installatie op een ander systeem.

De bestandsnaam van het nieuwe bestand is 'certificaat.pfx' en is zichtbaar als u opnieuw het commando 'ls' uitvoert in de terminal.



```
certificaten — -bash — 80x24  
Last login: Thu Mar 22 09:17:59 on ttys000  
[Test-Mac-KPN:~ testuser$ cd certificaten/  
[Test-Mac-KPN:certificaten testuser$ ls  
server.csr          server.key          servercertificaat.pem  
[Test-Mac-KPN:certificaten testuser$ openssl pkcs12 -export -out certificaat.pfx  
-inkey server.key -in servercertificaat.pem  
[Enter pass phrase for server.key:  
[Enter Export Password:  
[Verifying - Enter Export Password:  
[Test-Mac-KPN:certificaten testuser$ ls  
certificaat.pfx    server.key  
server.csr        servercertificaat.pem  
Test-Mac-KPN:certificaten testuser$
```