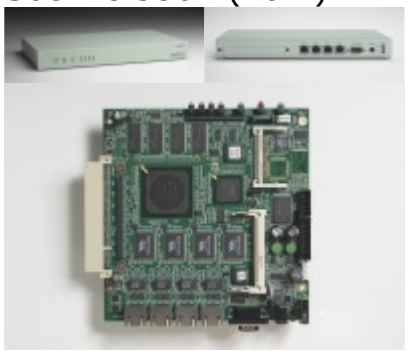
Hardware	=>	Soekris 5501 (10W)



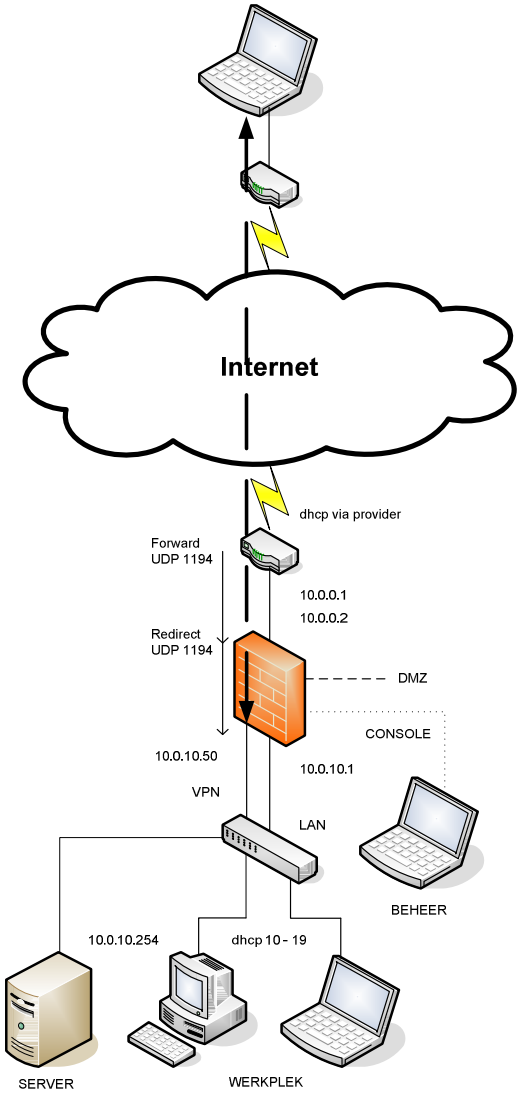
Tools	=>	USB Card Reader voor de CF USB naar Serial Adapter voor Console Een ouwe windows machine voor installatie op CF InfraRecorder voor branden ISO image Putty voor Terminal sessie middels USB Serial Adapter XCA voor sleutelbeheer
Operating System	=>	OpenBSD 4.8
Software	=>	OpenVPN

Inleiding:

Een VPN is een beveiligde verbinding naar een centrale computer, deze computer kan zorgen dat je gebruik kunt maken van de aanwezige resources, bv het LAN.
In ons geval installeren we OpenVPN op de Firewall.
De verbinding wordt opgezet middels een Client en een Server op basis van SSL/TLS met X.509 Keys.
Beheer van de Keys doen we middels XCA, andere tool mag ook naar keuze.

Is de 2.2.0 Client compatible met de 2.1.4 Server?

Schema:


Internet
dhcp via provider
Forward
UDP 1194
10.0.0.1
10.0.0.2
Redirect
UDP 1194
DMZ
CONSOLE
10.0.10.50
10.0.10.1
VPN
LAN
BEHEER
10.0.10.254
dhcp 10 - 19
SERVER
WERKPLEK

Pre-install:

De programmatuur bestaat uit een Client en een Server deel.
De Client haal je hier http://www.openvpn.net/index.php/open-source/downloads.html, in ons geval de Windows Installer.
Grafisch Sleutelbeheer op BeheerPC middels XCA
http://sourceforge.net/projects/xca/files/xca/0.9.0/setup_xca-0.9.0.exe/download

Houdt de ingevulde variabelenlijst van de **Bijlage Variabelen** in het inleidende document **HowTo OpenBSD Firewall met Secure Anonymous Access** bij de hand tijdens instalatie/configuratie.
Zodra je een variabele ziet, bv `%HOST%` vervang dit dan in zijn geheel door wat je had ingevuld, dus zeker geen %-tekens achterlaten.

Installatie OpenVPN Server:

Dependancies zullen tevens worden mee geïnstalleerd.

```
root @ 10.0.10.1 - PuTTY [ksh]
# pkg_add openvpn-2.1.4.tgz
```

Post-Installatie OpenVPN Server:

Dit onderdeel verschilt per type router die je van je provider heb gehad.
De bedoeling is dat je poort `1194` forward from `any` to `any` proto `udp`.
(mogelijk beter to `10.0.10.2`, echter de routers zijn middels cross cable direct verbonden)
Alle verkeer voor je VPN wordt dus doorgestuurd naar de Soekris, een PF Rule zorgt voor een redirect naar het juiste adres waarop OpenVPN actief is.

Additionele interfaces toevoegen.
Dit nummer 50 komt niet overeen met het nummerplan, dus aanpassen in 200 (ook schema's).

```
root @ 10.0.10.1 - PuTTY [vi /etc/hostname.vr2]
inet 10.0.10.50 255.255.255.0 NONE
```

Maak de noodzakelijke tunnel interface.
Tevens starten we van hieruit openvpn.

```
root @ 10.0.10.1 - PuTTY [vi /etc/hostname.tun0]
link0 up

!/usr/local/sbin/openvpn --daemon --config
/etc/openvpn/VPN_Server.conf
```

Werkt starten openvpn niet op bovenstaande manier haal dan de regel weg en doe als onderstaand.
Niet beide, want gestart is gestart, geeft dan rommel in logs.
Alles wat je lokaal wilt starten voeg je toe in `rc.local`.
Plaats het voor de regel met `echo '.'`

root @ 10.0.10.1 - PuTTY [vi /etc/rc.local]

```
if [ -x /usr/local/sbin/openvpn ]; then
    echo -n ' openvpn'
    /usr/local/sbin/openvpn --daemon --config
/etc/openvpn/VPN_Server.conf >/dev/null 2>&1
fi
```

Het VPN werkt middels een bridge, je zit direct 'in' het netwerk.
Vooral in een Windows omgeving is dit de juiste keuze.

root @ 10.0.10.1 - PuTTY [vi /etc/hostname.bridge0]

```
add vr2
add tun0
up
```

Packet Filter benodigt enkele aanpassingen.
Voeg dit toe onder bestaande entries bij navolgende kop:

```
######## Macro's
#
```

root @ 10.0.10.1 - PuTTY [vi /etc/pf.conf]

```
vpn_if    = "vr2"
tunnel_if = "tun0"
```

Deze rules tussenvoegen voor deze regel:

```
# Local Broadcast
```

```
root @ 10.0.10.1 - PuTTY [vi /etc/pf.conf]
# OpenVPN
pass in quick log inet proto udp from any to any port 1194 rdr-to
10.0.10.50 port 1194
pass quick on { $tunnel_if, $vpn_if } from any to any
```

Zie **Bijlage Sleutelbeheer** om Keys aan te maken op de BeheerPC.

Maak eerst de benodigde directory ...

```
root @ 10.0.10.1 - PuTTY [ksh]
# mkdir -p /etc/openvpn/keys
```

… en plaats hier een kopie van de aangemaakte Keys mbv WinSCP.

dh1024.pem
%EIGENAAR%_CA.crt
VPN_Server.crt
VPN_Server.pem (soms ook als .key bestand aangemaakt, rename deze dan)

Controleer of ze er staan.

```
root @ 10.0.10.1 - PuTTY [ksh]
# cd /etc/openvpn/keys
# ls -l
```

Dit is de server configuratie.

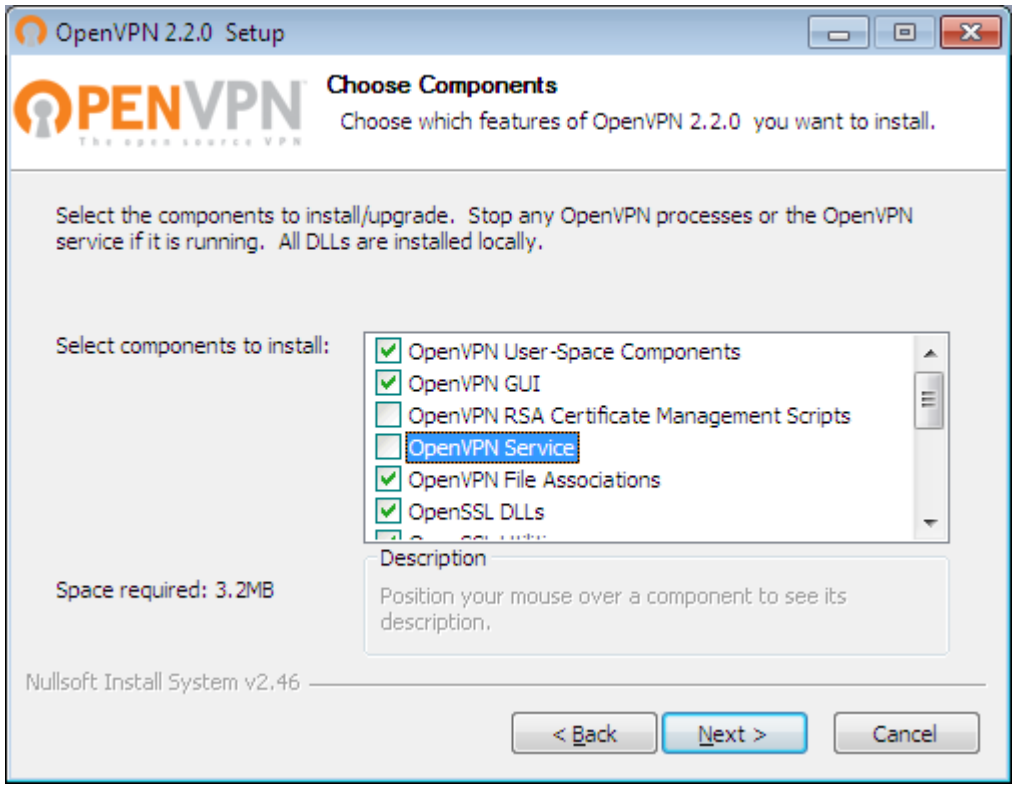
root @ 10.0.10.1 - PuTTY [vi /etc/openvpn/VPN_Server.conf]

```
#########################################################################
#######
###                           VPN_Server.conf
###
#########################################################################
#######

local 10.0.10.50                        # Aan deze Interface gekoppeld
port 1194                               # Luistert op deze Poort
proto udp                               # Transport Protocol

dev tun0                                # Tunnel Device
dev-type tap                            # Device Type

max-clients 2                           # Max Gelijktijdige
Verbindingen

# Elke Connectie krijgt Eigen IP binnen het Subnet
topology subnet

# X.509 Certifikaten
ca /etc/openvpn/keys/%EIGENAAR%_CA.crt
cert /etc/openvpn/keys/VPN_Server.crt
/etc/openvpn/keys/VPN_Server.pem

# Diffie-Hellman Key voor Secure Key Exchange
dh /etc/openvpn/keys/dh1024.pem

# Tijdelijk bestand voor toegewezen IP igv herstel connectie
ifconfig-pool-persist /var/log/openvpn/ipp.txt

# Bridge IP met Range voor toe te wijzen IP voor VPN Clients
server-bridge 10.0.10.50 255.255.255.0 10.0.10.240 10.0.10.250
```

```
# Alle Client verkeer gaat nu via VPN ipv eigen Default Gateway
push "redirect-gateway local def1"

# Te gebruiken Centrale DNS wordt doorgegeven
push "dhcp-option DNS 10.0.10.1"

# Alle verbonden Clients kunnen elkaar zien
client-to-client

# Controle of connecties in stand blijven
keepalive 10 120

# Gebruik van Compressie, tevens aangeven in Client Configuratie
comp-lzo

user _openvpn                           # chroot User
group _openvpn                          # chroot Group

persist-key                             # Behoudt Key na chroot
persist-tun                             # Behoudt Tun na chroot

# Status Huidige Connecties
status /var/log/openvpn/openvpn-status.log

# Voeg toe aan Bestaande Log
log-append  /var/log/openvpn/openvpn.log

verb 3                                  # Log Level
mute 20                                 # Max Gelijke Messages naar
Log
```

Installatie OpenVPN Client:

Installeer de Client die in vorige stap is gedownload.
De site is tamelijk onduidelijk en met verouderde info, vooral betreffende de Client.
Client en Server zitten in dezelfde executable, dat scheelt.
Het verschil maak je door kiezen van de opties om te installeren.
Als Client deselecteer je de RSA scripts en het draaien als service.



Zie volgende stap voor configuratie.

Post-Installatie OpenVPN Client:

Plaats hier een kopie van de aangemaakte keys:

C:\Program Files\OpenVPN\keys**%EIGENAAR%**_CA.crt

C:\Program Files\OpenVPN\keys\Patrick_Molier.crt # Specifieke Naam Client

C:\Program Files\OpenVPN\keys\Patrick_Molier.pem

Windows – KLADBLOK [C:\Program Files\OpenVPN\Patrick_Molier.ovpn]

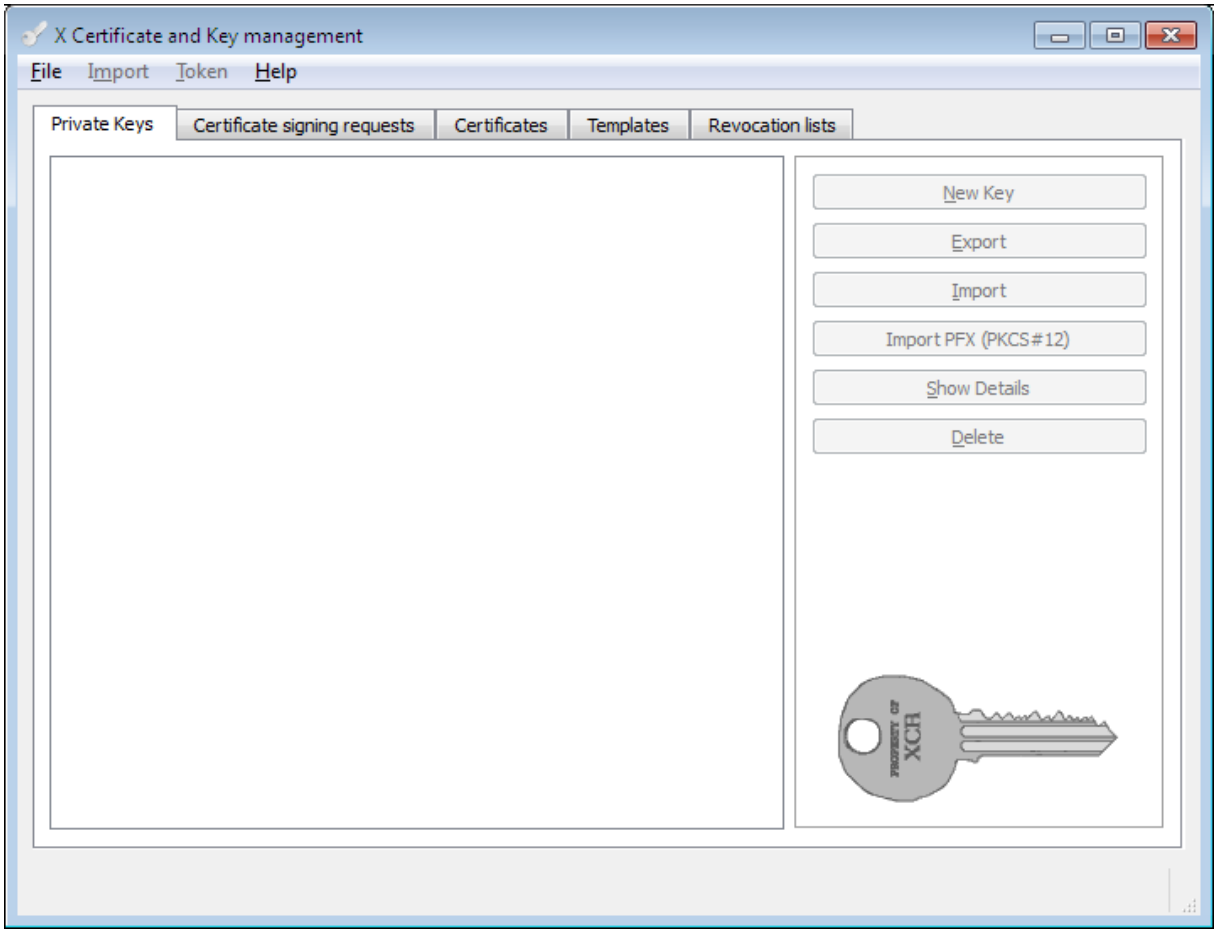
```
##############################################################################
#######
###                          Patrick_Molier.ovpn
###
##############################################################################
#######

# Geef aan dat we een Client zijn en Informatie van de Server
behoeven
client

proto udp                                  # Transport Protocol
nobind                                     # Geen Specifieke Poort
dev tap                                    # Device Type

remote %DOMEIN% 1194                       # Je Lokale IP middels
Provider

float                                      # Blijf Werken na Gewijzigd
Adres

# X.509 Keys
ca keys\\%EIGENAAR%_CA.crt
cert keys\\Patrick_Molier.crt
key keys\\Patrick_Molier.pem

persist-key                                # Behoudt Key na herstart
```

```
persist-tun                             # Behoudt Tun na herstart

mute-replay-warnings                    # Onderdruk Duplicate Warnings

ns-cert-type server                     # Controleer nsCertType =
Server

# Gebruik van Compressie, tevens aangeven in Server Configuratie
comp-lzo

verb 3                                  # Log Level
mute 20                                 # Max Gelijke Messages naar
Log
```

Aanpassen Client in %VOORNAAM%_%ACHTERNAAM%.

Bijlage Sleutelbeheer:

Sleutelbeheer bestaat uit verschillende onderdelen, er bestaan ook verschillende soorten sleutels.
Start XCA, dan lopen we ze achtereenvolgens af.



Er is nog niks te zien, maak eerst een nieuwe database om ze in op te slaan.
Selecteer File | New Database
Ga naar de directory waar je het wilt opslaan en geef de bestandsnaam, bv sleutels.
Er wordt direct om een password gevraagd, zorg dat dit een sterke is, maar dat zeggen we altijd natuurlijk, bv `TouwtjeUitBrievebusVraagOmInbrekers` (ben nostalgische hagenees).

Om keys veilig te kunnen uitwisselen tussen Client en Server wordt gebruik gemaakt van een Diffie-Hellman key.
Selecteer File | Generate DH Parameter
Accepteer de standard `1024 bits` (2048 of 4096 mag ook), de key wordt nu gegenereerd.
Sla `dh1024.pem` op in de directory waar ook de keys database staat.

Aanpassen key size in 2048 als minimum, net als ssh.
Aanpassen signature sha256 in de standaard sha1.

Nu gaan we een Certificate Authority (CA) aanmaken, vul je eigen gegevens in.

Selecteer Certificates | New Certificate
Selecteer Source
Signature Algorithm `SHA 256`
Template `[default] CA`
Druk op Apply All
Selecteer Subject
Internal Name **`%EIGENAAR%`** `CA` (automatisch ingevuld)
countryName `NL`
stateOrProvinceName `ZH`
localityName `Den Haag`
organizationName **`%EIGENAAR%`**
organizationalUnitName `CA`
commonName **`%EIGENAAR%`** `CA`
emailAddress `ca@`**`%EIGENAAR%`**`.nl` (evt ander TLD)
Druk op Generate a New Key
Accepteer default `1024 bit` (2048 of 4096 mag ook)
De Private Key wordt gegenereerd.
Het zal tevens het nog te genereren Certificaat ondertekenen.
Selecteer Extensions
Type `Certification Authority`
`Critical`
`Subject Key Identifier`
Time Range `6 Years` (langer dan server en clients)
Druk op Apply
Selecteer Key Usage `Certificate Sign`
`CRL Sign`
Selecteer Netscape `SSL CA`

S/MIME CA
Object Signing CA

Druk op OK rechts onder om het Certificaat te genereren.

Selecteer Export
Sla **%EIGENAAR%**_CA.crt op in de directory waar ook de keys database staat.

Selecteer Private Keys
Selecteer Export
Sla **%EIGENAAR%**_CA.pem op in de directory waar ook de keys database staat.

Eerst gaan we de VPN Server aanmaken, vul je eigen gegevens in.

Selecteer Certificates | New Certificate	
Selecteer Source	
Use Certificate for Signing	**%EIGENAAR%** CA
Signature Algorithm	SHA 256
Template	[default] HTTPS_server
Druk op Apply All	
Selecteer Subject	
Internal Name	VPN Server (automatisch ingevuld)
countryName	NL
stateOrProvinceName	ZH
localityName	Den Haag
organizationName	**%EIGENAAR%**
organizationalUnitName	Security
commonName	VPN Server
emailAddress	ca@**%EIGENAAR%**.nl (evt ander TLD)
Druk op Generate a New Key	
Accepteer default 1024 bit (2048 of 4096 mag ook)	
De Private Key wordt gegenereerd.	
Selecteer Extensions	
Type	End Entity Critical Subject Key Identifier
Time Range	5 Years
Druk op Apply	
Selecteer Key Usage	Digital Signature Non Repudiation Key Encipherment
Selecteer Netscape	SSL Server

Druk op OK rechts onder om het Certificaat te genereren.

Selecteer Export
Sla `VPN_Server.crt` op in de directory waar ook de keys database staat.

Selecteer Private Keys
Selecteer Export
Sla `VPN_Server.pem` op in de directory waar ook de keys database staat.

Nu gaan we VPN Client(s) aanmaken, vul je eigen gegevens in.

Selecteer Certificates | New Certificate	
Selecteer Source	
Use Certificate for Signing	**%EIGENAAR%** CA
Signature Algorithm	SHA 256
Template	[default] HTTPS_client
Druk op Apply All	
Selecteer Subject	
Internal Name	Patrick Molier (automatisch ingevuld)
countryName	NL
stateOrProvinceName	ZH
localityName	Den Haag
organizationName	**%EIGENAAR%**
organizationalUnitName	Security
commonName	Patrick Molier
emailAddress	patrick@**%EIGENAAR%**.nl
Druk op Generate a New Key	
Accepteer default 1024 bit (2048 of 4096 mag ook)	
De Private Key wordt gegenereerd.	
Selecteer Extensions	
Type	Certification Authority Critical Subject Key Identifier
Time Range	1 Years
Druk op Apply	
Selecteer Key Usage	Digital Signature Key Encipherment Data Encipherment
Selecteer Netscape	SSL Client

Druk op OK rechts onder om het Certificaat te genereren.

Selecteer Export
Sla `Patrick_Molier.crt` op in de directory waar ook de keys database staat.

Selecteer Private Keys
Selecteer Export
Sla `Patrick_Molier.pem` op in de directory waar ook de keys database staat.
Encrypt Key with Password (als voorbeeld 'geheim', moet natuurlijk sterker).
Elke keer dat de Client een verbinding opbouwt moet het password worden opgegeven.
Dit is niet gebruikersvriendelijk maar wel veiliger!

Intrekken Certficaat (Revoking).
Dit kan nodig zijn indien je denkt/weet dat een certificaat in verkeerde handen is gevallen.
Normaal gesproken is het slechts noodzakelijk als een medewerker ergens anders gaat werken.
In ieder geval wil je de toegang intrekken.

Selecteer in te trekken Certificaat
Right-click muis
Selecteer Revoke
Je kunt een tijdstip en reden aangeven
Er is een intrekverzoek aangemaakt
Selecteer `%EIGENAAR%` CA
Right-click muis
Selecteer CA | Generate CRL
Je kunt een termijn aangeven voor geldigheid lijst,
accepteer `1 maand`
Wat betekent slechts 1 maand?
Werken ze dan ineens weer?
Hashing Algoritm `SHA 256`
De `Certificate Revocation List` is aangemaakt
Selecteer Revocation Lists
Bekijk de aangemaakte details
De lijst moet nu naar de VPN Server
Selecteer Export | PEM
Kopieer bestand `crl.pem` naar `/etc/openvpn/keys` mbv WinSCP.

Toevoegen Certificate Revocation List na de entries onder deze kop:

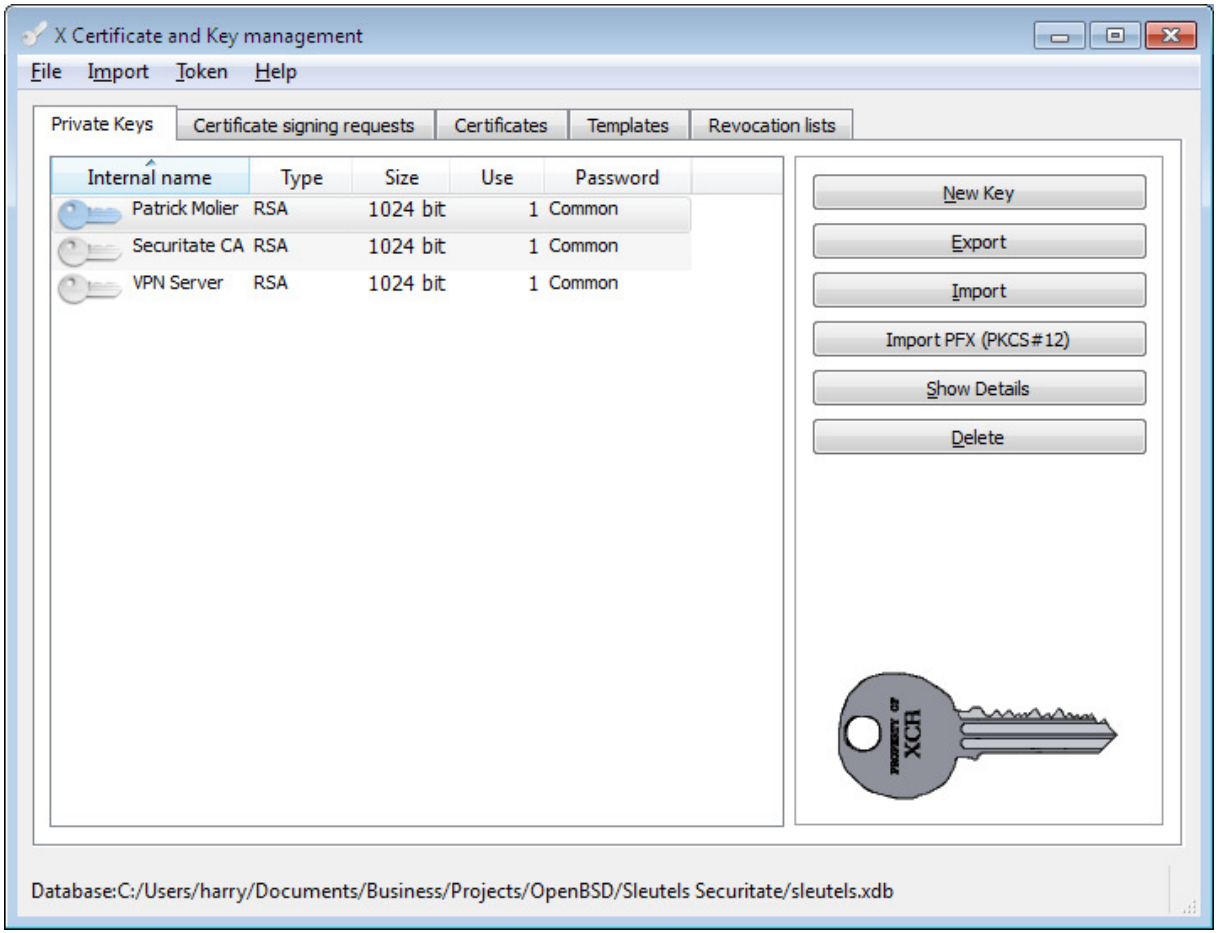
```
# X.509 Certificaten
```

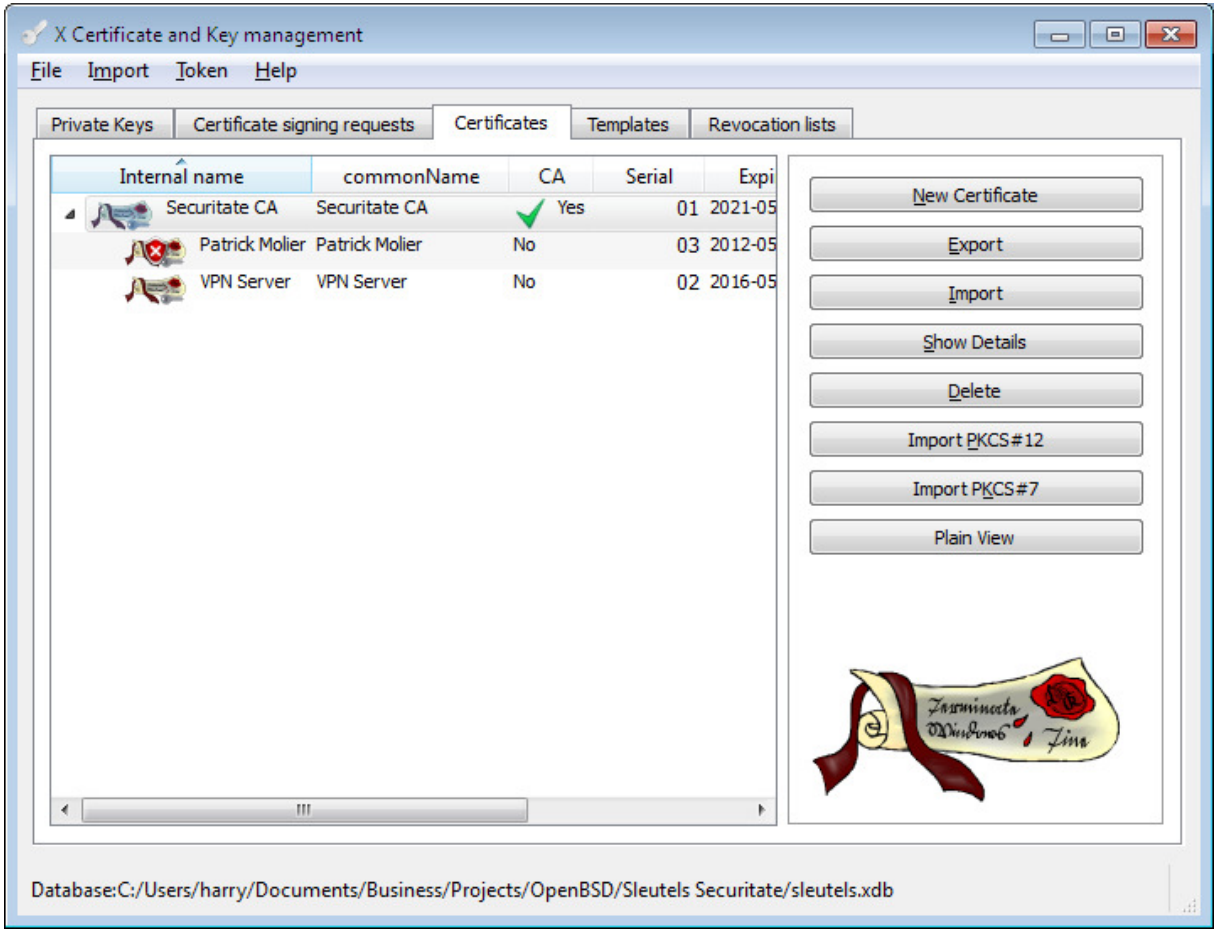
root @ 10.0.10.1 - PuTTY [vi /etc/openvpn/VPN_Server.conf]

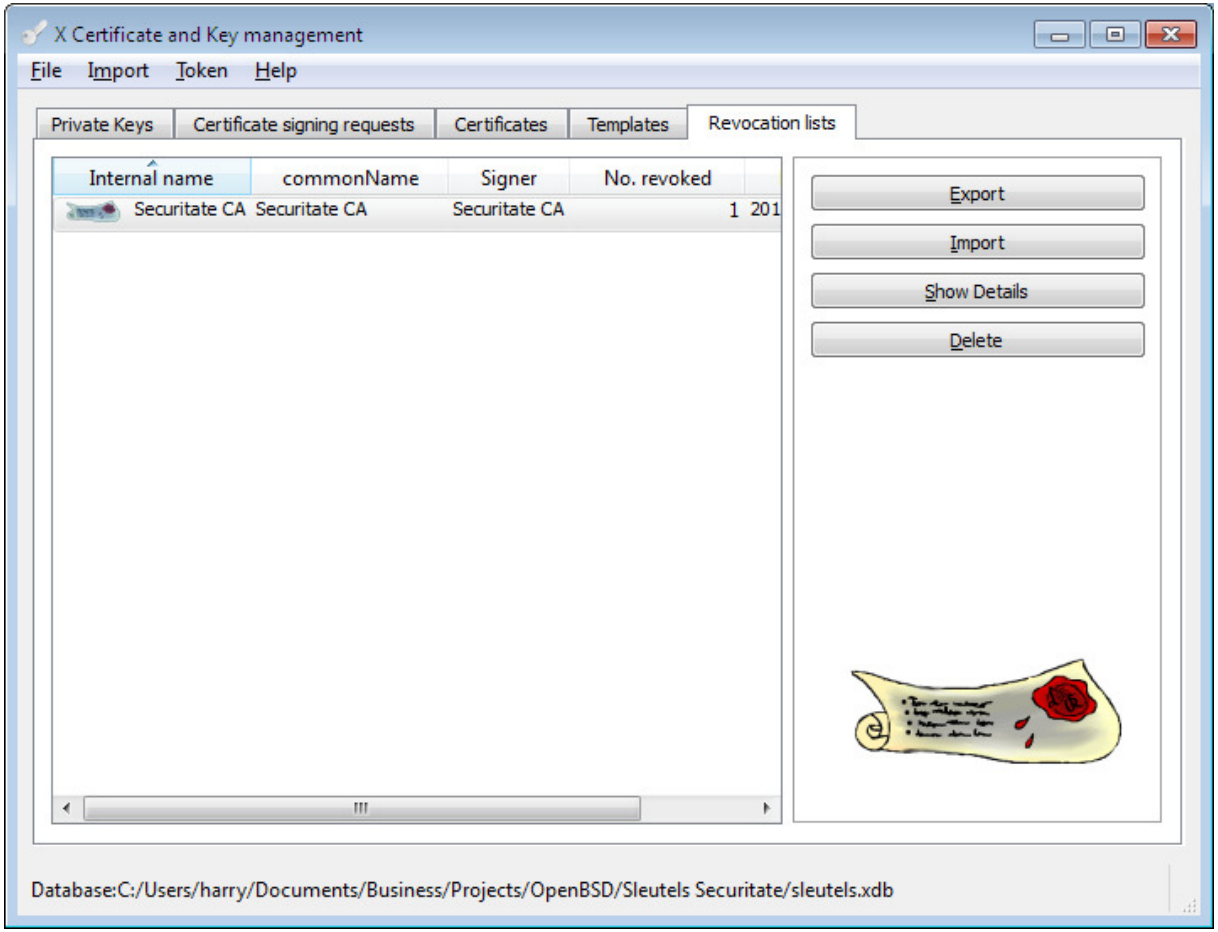
```
crl-verify /etc/openvpn/keys/crl.pem
```

Controleer dit laatste => nog niet gedaan en accepteert vervallen certificaat!!!

Resultaten.
Met Show Details zie je meer.




X Certificate and Key management
File
Import
Token
Help
Private Keys
Certificate signing requests
Certificates
Templates
Revocation lists
Internal name
commonName
CA
Serial
Expi
Securitate CA
Securitate CA
Yes
01
2021-05
Patrick Molier
Patrick Molier
No
03
2012-05
VPN Server
VPN Server
No
02
2016-05
New Certificate
Export
Import
Show Details
Delete
Import PKCS#12
Import PKCS#7
Plain View
Database:C:/Users/harry/Documents/Business/Projects/OpenBSD/Sleutels Securitate/sleutels.xdb



Bewerk plaatjes zodat mijn dir minder duidelijk wordt.

Links:

http://www.openbsd.org/
http://www.openvpn.net/index.php/open-source.html
http://www.chiark.greenend.org.uk/~sgtatham/putty/
http://xca.sourceforge.net/

Boeken:

Beginning OpenVPN 2.0.9