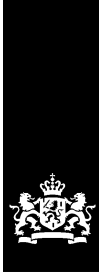


CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Het aanmaken en installeren van een servercertificaat onder Apache

Versie 1.4

Datum 10 Januari 2019
Status Definitief

Inhoud

Versiehistorie

Versie	Datum	Status	Toevoegingen en wijzigingen
1.0	30 mrt 09	definitief	Aanpassingen: Toevoegen G2 hiërarchie
1.1	8 apr 09	definitief	Aanpassingen: - Toevoeging testen SBV-Z testtool - Extra toelichting OpenSSL - Voorbeeldnamen PKCS#10 request hernoemd
1.2	10 apr 09	definitief	Aanpassingen: - Hoofdstuk X hernoemd (toevoeging UZI-pas) - Hoofdstuk 3 aangevuld met FQDN naam - Bijlage toegevoegd: Toelichting systeemnaam
1.3	23 apr 09	definitief	Aanpassingen: - Hoofdstuk 3 aangevuld met reden gebruik IIS - Hoofdstuk 6: Generen PFX - Aanvulling op Bijlage: Toelichting systeemnaam
1.4	10 jan 19	Definitief	Aanpassingen: - Omgezet naar ZOVAR

1 Werkwijze Apache

1.1 Wat heeft u nodig

Dit hoofdstuk omschrijft een mogelijke werkwijze voor het genereren van een RSA sleutelpaar en het bijbehorende PKCS#10-bestand (Certificate Signing Request) met behulp van OpenSSL. Deze stappen zijn nodig voor het aanvragen van een servercertificaat dat te gebruiken is voor bijvoorbeeld een webserver.

- Een werkende OpenSSL installatie;
- Informatie over het te genereren servercertificaat (zie lijstje hieronder).

Als u nog geen (werkende) OpenSSL installatie heeft, raadpleeg dan de documentatie van uw besturingssysteem hoe u deze kunt installeren.

Voordat u verder gaat heeft u enige informatie nodig over het te genereren servercertificaat. Tijdens het proces heeft u het volgende nodig:

- De landcode (NL);
- De volledige naam van de provincie;
- De naam van de stad;
- De naam van de organisatie (zorginstelling);
- Naam van de organisatie unit (De naam van de afdeling);
- De "Common Name"*;
- Een e-mailadres van de gemachtigde aanvrager of wettelijk vertegenwoordiger.

LET OP:
(*) De common name is een belangrijk deel. In het geval van een webserver certificaat MOET dit gelijk zijn aan de te gebruiken url (bijvoorbeeld: www.mijnsite.nl).

Afhankelijk van de gebruikte OpenSSL installatie kan u nog gevraagd worden om een:

- Challenge Password;
- Optional company Name.

U kunt deze leeg laten.

1.2 Stap voor stap

Het proces bestaat uit de volgende stappen:

1 Het genereren van een RSA sleutelpaar;
2 Het genererenvan een PKCS#10-bestand.

Het genereren van een sleutelpaar kunt u het beste doen op een locatie waar alleen de root gebruiker bij kan. *Normaliter is dit alleen de systeembeheerder*. Dit omdat het private deel van het sleutelpaar nooit in handen van derden mag komen. In het voorbeeld gaan we uit dat het genereren plaatsvindt in de home-directory van de root gebruiker.

1.2.1 Stap 1:

```
# cd /root
# mkdir newcerts
# cd newcerts
# openssl genrsa –des3 2048 > server.key
```

Dit genereert een RSA sleutelpaar, met een 2048 bit groot publiek deel. Het private deel wordt 3des (Triple Des) versleuteld. Type hiervoor een wachtwoord (de zogeheten passphrase) in.

Onthoud dit wachtwoord goed. Zonder dit wachtwoord kunt u niet verder met stap 2.

Datzelfde wachtwoord typt u uiteindelijk ook in om de webserver te kunnen starten. Het sleutelpaar wordt opgeslagen in een bestand onder de naam server.key.

1.2.2 Stap 2:

Hieronder ziet u de voorkomende vragen bij het genereren van een PKCS#10-bestand (Certificate Signing Request).

```
# openssl req –new –key server.key –out server.csr Enter pass phrase
for server.key:
-----
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
DN.
There are quite e 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)[AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organisation Name (eg, company) [Internet Widgidt Pty Ltd]:
Organisational Unit Name (eg, section []:
Common Name (eg, YOUR name)[]:
Email Address []:
Please enter the foillowing 'extra' attributes
to be send with your certificate request
A Challenge Password []:
An optional company name []:
```

Het registratiesysteem maakt geen gebruik van deze informatie in het PKCS#10 bestand. U kunt de standaard waarden gewoon laten staan en op enter drukken.

Het PKCS#10-bestand wordt opgeslagen met de naam server.csr.

1.2.3 Combinatie van stap 1 + 2

Stap 1 en 2 kunt u eventueel combineren met het volgende commando:

```
# openssl req –nodes –newkey rsa:2048 –keyout server.key –out
server.csr
```

De werking is verder exact hetzelfde.

1.2.4 Aanvragen servercertificaat

Nu u een zogeheten PKCS#10-bestand (CSR) heeft kunt u deze gebruiken om het daadwerkelijke servercertificaat aan te vragen. Het servercertificaat kunt u aanvragen via www.zovar.nl Op de website vind u ook meer informatie over de procedure voor het aanvragen van het servercertificaat.

2 Installatie van de certificaten (Apache - OpenSSL)

2.1 Wat heeft u nodig

- Een geldig servercertificaat, uitgegeven door ZOVAR;
- Een werkende Apache webserver, inclusief de SSL toevoeging (mod_ssl).

In hoofdstuk 1.2 is een voorbeeld gegeven hoe u een servercertificaat kunt genereren.

Als u de mod_ssl niet geïnstalleerd heeft, raadpleeg dan de documentatie van uw besturingssysteem hoe u deze dient te installeren.
Zorg ervoor dat deze SSL toevoeging automatisch geladen wordt. Raadpleeg hiervoor de documentatie van uw besturingssysteem.

2.2 Plaatsing van de certificaten

Als u al een locatie heeft voor de plaatsing van de certificaten en private sleutels dan kunt u deze gebruiken.

Als u nog geen locatie heeft voor de plaatsing van de certificaten en private sleutels dan kunt u onderstaand voorbeeld volgen:

Zorg er altijd voor dat de certificaten en private sleutels buiten de webroot staan. Dat wil zeggen, ze mogen door derden niet direct opvraagbaar zijn.

Maak een directory aan voor alle SSL webpagina's:
```
# mkdir /var/www/ssl/
```

Maak ook een directory (als deze nog niet bestaat) voor de plaatsing van de Root CA certificaten:
```
# mkdir /var/www/ca/
```

Maak een directory aan voor de webpagina waarvan u de communicatie wilt beveiligen:
Stel dat u een webpagina heeft die www.mijnsite.nl heet, gebruik dan onderstaand commando:
```
# mkdir /var/www/ssl/www.mijnsite.nl/
```

In de zojuist gemaakte directory plaats u de volgende bestanden:
- Het PEM-encoded X.509 certificaat (deze heeft u gekregen van het ZOVAR);
- het PEM-encoded Private sleutel bestand (deze heeft u zelf gemaakt, bijv. in hoofdstuk 1).

De naamgeving van de certificaat- en private sleutelbestanden zijn vrij. In dit document gebruiken we de volgende naamgeving:
server.key: Het private sleutelbestand (RSA sleutelpaar)
server.pem: Het PEM-encoded X.509 certificaat
Als u een andere naamgeving heeft aangehouden, gebruik dan in alle voorbeelden uw eigen naamgeving.

Mocht u het certificaat in DER-encoded formaat hebben staan, dan kunt u dit middels de bijlage: "Het omzetten van en naar PEM encoding (Apache - OpenSSL)"

omzetten naar PEM-encoded. Het formaat kunt u verifiëren door het certificaat in notepad te openen. PEM/Base64 ziet er als volgt uit:

```
-----BEGIN CERTIFICATE-----
MIIFcDCCBFigAwIBAgIQPAWdivn/Lu2gyYthoNXenDANBgkqhkiG9w0BAQUFADB/
MQswCQYDVQQGEwJOTDFEMEIGA1UECgw7YWdlbnRzY2hhcCBDZW50cmFhbCBJbmZv
cm1hdGllcHVudCBCZXJvZXBlbiBHZXpvbmRoZWlkc3pvcmcxKjAoBgNVBAMMIVRF
U1QgVVpJLXJlZ2lzdGVyIFpvcmd2ZXJsZW5lciBDQTAeFw0wNTA3MjgxMzE4MDZa
Fw0wODA3MjcxMzE4MDZaMIGZMS8wLQYDVQQMDCZBcnRzIGFyYmVpZCBnZXpvbmQu
IC8gdmVyemVrZXJpbmdzYXJ0czESMBAGA1UEBRMJMDAwMDAwMjgzMSAwHgYDVQQD
DBdBZ25lcyBUZXN0em9yZ3ZlcmxlbmVyMjEjMCEGA1UECgwaVGVzdC1hY2FkZW1p
(10 lines deleted)
CCsGAQUFBwICMIGZGoGWQ2VydGlmaWNhYXQgdWl0c2x1aXRlbmQgZ2VicnVpa2Vu
IHRlbiBiZWhvZXZlIHZhbiBkZSBURVNUIHZhbiBoZXQgVVpJLXJlZ2lzdGVyLiBI
ZXQgVVpJLXJlZ2lzdGVyIGluIGdlZW4gZ2V2YWwgYWFuc3ByYWtlbGlqayB2
b29yIGV2ZW50dWVsZSBzY2hhZGUuMFoGA1UdHwRTMFEwT6BNoEuGSWh0dHA6Ly93
d3cudXppLXJlZ2lzdGVyLXRlc3QubmwvY2RwL3Rlc3RfdXppLXJlZ2lzdGVyX3pv
cmd2ZXJsZW5lcl9jYS5jcmwwDgYDVR0PAQH/BAQDAgeAMB0GA1UdDgQWBBTX9LqL
MwhhPMwm3W1agTN9WcYCAzANBgkqhkiG9w0BAQUFAAOCAQEAOTZNg48v94MmDZjs
9fdsZGhUVP+N59O0pBTLIL8aCgCFQY1zNOmRl3677lu01LirzQbnd9KKxMnbb69R
ne2umR6EDgP+E2TLvbpYCu0bdAwvzeWrRmuBqzxgzZ2yYU/INGJR7sePydOeItK1
JVCeeL5A2YwL+mdjKpIyaBqEbSvG8gv4WgYLP+QKAD8YMWWGrqJYn66YbpZsVy3w
ozAKY9gQ+Q7ODZeJdyG+0jEd1s63fsqMAgRSRW+tKzoJl2ZiGTGhLYXWX3We9dOV
lrdFAUZJA0QR2WpaYm0lqSfVm0tNu1nkJNP5dz9O8niZ2rz/kI1Gn9hgaSjiid0H
NPbFtw==
-----END CERTIFICATE-----
```

2.3 Plaatsing Root CA certificaten

Wanneer de Apache webserver een servercertificaat toestuurt aan de cliënt is het van belang dat ook de complete CA keten wordt meegestuurd. De cliënt heeft dan direct toegang tot de certificaten én kan dan het servercertificaat van de server controleren op validiteit. Een voorbeeld ziet u op de op één na laatste pagina in dit document.

De Root CA keten bestaat uit de volgende CA's en kan verschillen per generatie servercertificaat.
Voor de servercertificaten CA – G1 generatie:

-> Staat der Nederlanden Private Root CA - G1
->Staat der Nederlanden Private Services CA - G1
->UZI-register Private Server CA G1

U kunt de overige Root en Overheid CA certificaten hier downloaden:
https://cert.pkioverheid.nl/

De actuele ZOVAR CA certificaten kunt u altijd vinden op:
https://www.zorgcsp.nl/ca-certificaten
U moet hier het ZOVAR Server CA G1 en bovenliggende hiërarchie certificaten downloaden.

Pas wanneer u client authenticatie door middel van clientcertificaten wilt vereisen, zijn de andere CA certificaten noodzakelijk.

Voor test authenticatiemiddelen zijn afzonderlijke CA certificaten noodzakelijk. Deze kunt u downloaden via: https://acceptatie.zorgcsp.nl/ca-certificaten
LET OP:
Al deze certificaten zijn DER-Encoded (binair) X.509 certificaten. Apache kan hier niet mee overweg. Gebruik de handleiding "Het omzetten van en naar PEM encoding" om deze certificaten om te zetten naar een PEM-encoding (ASCII)

Al deze certificaten dienen in de volgende directory te staan.

```
/var/www/ca/
```

LET OP:
Apache gebruikt een vrij ingewikkeld systeem om te achterhalen welke certificaten hij mee dient te sturen. Dit gebeurt met bestandsnamen die gelijk zijn aan de HASH waarde van common name uit het certificaat.

Gelukkig levert apache zelf een bestand aan om deze bestanden te creëren. Dit bestand (Makefile) dient u in de zelfde directory te zetten als de CA certificaten. Met het commando:

```
# make
```

worden er automatisch bestanden gemaakt (symbolic links) naar de certificaten met de correcte naam.

Heeft u deze Makefile niet, dan kan het nog op een andere manier. Deze is iets lastiger want u dient dit per certificaat te doen.

```
#ln -s my_ca.crt `openssl x509 -hash -noout -in my_ca.crt`.0
```

Dit creëert een symbolic link naar my_ca.crt met een naam als "dbed1725.0".

2.4 Toegang tot de bestanden voor de Apache gebruiker

Om er voor te zorgen dat de webserver ook daadwerkelijk leesrechten heeft op de directory en de bestanden, is het van belang dat we deze rechten goed zetten. Voor een correcte werking is leesrechten voldoende. De private sleutel van de webserver dient echter afgesloten te zijn voor toegang aan derden. Alleen de root gebruiker en de Apache-gebruiker mag hier bij komen.

Raadpleeg de documentatie van uw besturingsysteem om te achterhalen onder welke "user-group" de Apache webserver draait. Op veel systemen is dat apache of www-data.

Zet de rechten goed: (als de user-group apache heet)

```
# chown –R root:apache /var/www/ssl/ # chown –R root:apache
/var/www/ca/
# chmod 640 /var/www/ssl/* # chmod 640 /var/www/ca/*
```

3 Configuratie van de webpagina

3.1 Configuratie van de Virtual Host

Een website binnen apache staat meestal geconfigureerd in een configuratiebestand. Vaak wordt er per website een apart configuratiebestand gemaakt. In deze configuratiebestanden staat de configuratie van een zogeheten VirtualHost.

Een configuratie voorbeeld kan er zo uitzien:

```
<VirtualHost *:80>
   ServerAdmin admin@mijnsite.nl
   ServerName www.mijnsite.nl
   DocumentRoot /var/www/www.mijnsite.nl/

<Directory /var/www/www.mijnsite.nl/>
   AllowOverride none
   Order allow, deny
   allow from all
</Directory>

   ErrorLog /var/log/apache/www.mijnsite.nl_error.log

   LogLevel warn
CustomLog /var/log/apache/www.mijnsite.nl_access.log
…
</VirtualHost>
```

Om deze webpagina te voorzien van een SSL certificaat dient u enkele wijzigen door te voeren in de bestaande configuratie.

De configuratie van de website www.mijnsite.nl zou ongeveer zo uit moeten zien:

```
<VirtualHost *:443>
   ServerAdmin admin@mijnsite.nl
   ServerName www.mijnsite.nl
   DocumentRoot /var/www/www.mijnsite.nl/

## SSL PART
   SSLEngine On
   SSLCertificateFile /var/www/ssl/www.mijnsite.nl/server.pem
   SSLCertificateKeyFile
/var/www/ssl/www.mijnsite.nl/server.key
   SSLRequireSSL SSLLog /var/log/apache/www.mijnsite.nl_ssl.log
SSLLogLevel info

## SSL CA PART
SSLCACertificatePath /var/www/ca/

   <Directory /var/www/www.mijnsite.nl/>
      AllowOverride none
      Order allow, deny
      allow from all
   </Directory>

   ErrorLog /var/log/apache/www.mijnsite.nl_error.log

   LogLevel warn
CustomLog /var/log/apache/www.mijnsite.nl_access.log
…
</VirtualHost>
```

Om uw Apache webserver ook op de standaard SSL poort (tcp 443) te laten luisteren configureert u de Apache webserver.
Dit is meestal in het configuratiebestand “apache2.conf” te vinden.

```
Listen 80
Listen 443
```

Herstart hierna de Apache webserver.

Let er op dat het ook nodig kan zijn dat u de SSL poort open zet in de firewall.

3.2 Het herstarten van de Apache webserver

Na het veranderen van de configuratie start u de webserver opnieuw. Vaak kan dit met het commando:

```
# /etc/init.d/apache2 restart
```

Als dit voor uw besturingssysteem anders is, raadpleeg dan de documentatie voor de correcte manier van het herstarten van de webserver.
Als u tijdens het genereren van het sleutelpaar een beveiligde private sleutel heeft gemaakt dan wordt u bij het herstarten om het wachtwoord (passphrase) gevraagd.

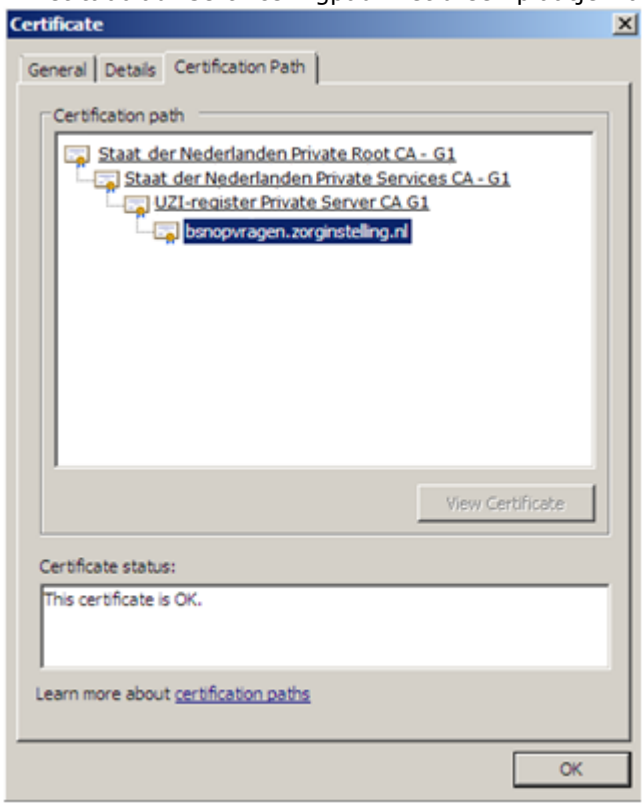
Dit is ook het geval bij een herstart.

3.3 Testen van de verbinding

Wanneer u uw servercertificaat in uw bezit heeft kunt u verder met hoofdstuk 4.
Ga met uw browser naar de zojuist geconfigureerd website. Vergeet dit niet met **https://** te doen.

U kunt een waarschuwing krijgen dat de certificeringinstantie niet vertrouwd is.
Wanneer u het Staat der Nederlanden Root CA of één van de onderliggende CA's al als vertrouwd heeft aangemerkt krijgt u geen melding.
In Internet Explorer ziet u onder in de statusbalk een geel slotje: Wanneer u daar op dubbelklikt ziet u de eigenschappen van het servercertificaat en zijn certificeringinstanties.

In het tabblad ‘Certificeringpad’ ziet u een plaatje wat lijkt op deze:



LET OP: Wanneer u het “Staat der Nederlanden Root CA G1” certificaat als vertrouwd heeft aangemerkt zijn alle onderliggende CA’s en servercertificaten ook vertrouwd.

4 Vereisen van clientcertificaten (Apache – OpenSSL)

4.1 Wat heeft u nodig

- Een werkende beveiligde webpagina voorzien van een geldig servercertificaat;
- De certificaten van volledige CA-Keten;
- een kopie van de Certificate Revocation List (CRL).

Als u nog geen werkende beveiligde webpagina heeft, raadpleeg dan de handleiding "Het installeren van een servercertificaat onder de Apache webserver".

4.2 Plaatsing van het servercertificaat

Voor de plaatsing van de volledige CA-keten kunt u een algemene locatie gebruiken. De webserver kan dit bestand voor meerdere webpagina's gebruiken.
Als u nog geen locatie heeft voor deze publieke sleutel, dan kunt u onderstaand voorbeeld volgen:

```
# mkdir /var/www/ca/
```

Plaats het PEM-encoded X.509 certificaat onder deze directory.

Ook voor de plaatsing van de CRL's kunt u een algemene locatie gebruiken. De webserver kan deze bestanden voor meerdere pagina's gebruiken. Wanneer u nog geen locatie heeft voor de CRL, dan kunt u onderstaand voorbeeld gebruiken:

```
# mkdir /var/www/crl/
```

Plaats de CRL's in de directory in een PEM-encoded X.509 formaat.

Wanneer de apache webserver een servercertificaat toestuurt aan de client is het van belang dat ook de complete CA keten wordt meegestuurd. De client heeft dan direct toegang tot de CA certificaten én kan dan het servercertificaat van de server controleren op validiteit. In het geval van Client Authenticiteit moet de server ook het client certificaat kunnen valideren. Hiervoor zijn de CA certificaten en CRL lijsten nodig.

De Root CA keten bestaat uit de volgende CA's en kan verschillen per generatie servercertificaat.
Voor de servercertificaten CA – G1 generatie:
-> Staat der Nederlanden Private Root CA - G1
->Staat der Nederlanden Private Services CA - G1
->UZI-register Private Server CA G1

U kunt de Root en Overheid CA certificaten hier downloaden:
https://cert.pkioverheid.nl/

De ZOVAR CA certificaten kunt u downloaden van:
https://www.zorgcsp.nl/ca-certificaten

De meest recente CRL's kunt u downloaden van:
https://www.zorgcsp.nl/certificate-revocation-lists-crl-s

4.3 Toegang tot de bestanden voor de Apache-gebruiker

Om er voor te zorgen dat de webserver ook daadwerkelijk leesrechten heeft op de directory en de bestanden is het van belang dat we deze rechten goed zetten. Voor een correcte werking zijn leesrechten voldoende. De private sleutel van de webserver moet echter afgesloten te zijn voor toegang aan derden. Alleen de root gebruiker en de Apache-gebruiker mogen hier bij komen.

Ook kunt u de private sleutel beschermen met een wachtwoord (een zogeheten passphrase). Alleen met behulp van deze passphrase kunt u de webserver herstarten. Raadpleeg de documentatie van uw besturingsysteem of apache installatie om te achterhalen onder welke "user-group" de apache webserver draait. Op veel systemen is dit apache of www-data.

Zet de rechten goed: (als de user-group apache heet)

```
# chown –R root:apache /var/www/ca
# chmod –R 640 /var/www/ca
# chown –R root:apache /var/www/crl
# chmod –R 640 /var/www/crl
```

4.4 Symbolic links van CA certificaten en CRL's

Apache gebruikt een vrij ingewikkeld systeem om te achterhalen welke root certificaten het mee moet sturen. Dit gebeurt met bestandsnamen die gelijk zijn aan de HASH waarde van common name uit het certificaat.
Hetzelfde geldt voor de Certificate Revocation Lists. Gelukkig levert mod_ssl zelf een bestand aan om deze bestanden te creëren. Dit bestand (Makefile) zet u in dezelfde directory als de CA certificaten.

Met het commando:

```
# make
```

worden er automatisch bestanden gemaakt (symbolic links) naar de certificaten met de correcte naam.

Wanneer u later een CA certificaat of CRL toevoegt of overschrijft met een nieuwere versie dan kunt u het commando:

```
# make update
```

gebruiken om de links te updaten.

Met het commando:

```
# make clean
```

worden alle links verwijderd.

Het Makefile bestand staat in de bijlage. Sla deze op met de naam "Makefile" in de directory waarin de CA certificaten en/of CRL's staan.

Het maken van linkfiles kan nog op een andere manier. Deze is iets lastiger want deze dient u per certificaat te doen.

```
#ln -s my_ca.crt `openssl x509 -hash -noout -in my_ca.crt`.0
```

Dit creëert een symbolic link naar my_ca.crt met een naam als "dbed1725.0".

<u>Doe dit voor zowel de CA's als de CRL's.</u>

5 Configuratie van de website

5.1 Configuratie van de Virtual Host

Open het configuratiebestand waarin de Virtual Host gedefinieerd staat voor de webpagina waarvoor u de clientidentificatie wilt configureren.

Een configuratie van een bestaande beveiligde webpagina kan er zo uitzien:

```
<VirtualHost *:443>
   ServerAdmin admin@mijnsite.nl
   ServerName www.mijnsite.nl
   DocumentRoot /var/www/www.mijnsite.nl/

   ## SSL PART
      SSLEngine On
      SSLCertificateFile /var/www/ssl/www.mijnsite.nl/server.pem
      SSLCertificateKeyFile
/var/www/ssl/www.mijnsite.nl/server.key
      SSLRequireSSL
   SSLLog /var/log/apache/www.mijnsite.nl_ssl.log
   SSLLogLevel info

   ## SSL CA PART
SSLCACertificatePath /var/www/ca/

<Directory /var/www/www.mijnsite.nl/>
   AllowOverride none
   Order allow, deny
   allow from all
</Directory>

ErrorLog /var/log/apache/www.mijnsite.nl_error.log

   LogLevel warn
CustomLog /var/log/apache/www.mijnsite.nl_access.log
…
</VirtualHost>
```

Er zijn enkele toevoegingen nodig om deze website zo te configureren, dat de client verplicht is een servercertificaat ter identificatie aan te bieden.

De webpagina www.mijnsite.nl zou er dan ongeveer zo uit moeten zien:

```
   <VirtualHost *:443>
      ServerAdmin admin@mijnsite.nl
      ServerName www.mijnsite.nl
      DocumentRoot /var/www/www.mijnsite.nl/

## SSL PART
   SSLEngine On
   SSLCertificateFile /var/www/ssl/www.mijnsite.nl/server.pem
   SSLCertificateKeyFile
/var/www/ssl/www.mijnsite.nl/server.key
   SSLRequireSSL
SSLLog /var/log/apache/www.mijnsite.nl_ssl.log
SSLLogLevel info

## SSL CA PART
SSLCACertificatePath /var/www/ca/

## CERTIFICATE REVOCATION PART
SSLCARevocationPath /var/www/crl/

   #SSL CLIENT PART
SSLVerifyClient require
SSLVerifyDepth 4

   <Directory /var/www/www.mijnsite.nl/>
      AllowOverride none
      Order allow, deny
      allow from all
   </Directory>

   ErrorLog /var/log/apache/www.mijnsite.nl_error.log

   LogLevel warn
CustomLog /var/log/apache/www.mijnsite.nl_access.log
   …
   </VirtualHost>
```

5.2 Het herstarten van de Apache webserver

Na het veranderen van de configuratie start u de webserver opnieuw. Vaak kan dit met het commando:

```
# /etc/init.d/apache2 restart
```

Als dit voor uw besturingssysteem anders is, raadpleeg dan de documentatie voor de correcte manier van het herstarten van de webserver.

6 Voorbeeld script Apache

6.1 Voorbeeldscript voor het ophalen van CRL's

```
#!/bin/sh
CRL_DIR = /var/www/crl/
cd CRL_DIR
wget http://www.uzi-register.nl/cdp/uzi-register_csp_ca.crl
wget http://www.uzi-register.nl/cdp/uzi-register_zorgverlener_ca.crl
wget http://www.uzi-register.nl/cdp/uzi-register_medewerker_op_naam_ca.crl
wget http://www.uzi-register.nl/cdp/uzi-register_medewerker_niet_op_naam_ca.crl
make update
```

6.2 Crontab voor de root user

```
* */3 * * * /pad/naar/update-script
```

6.3 Makefile (zoals geleverd door mod_ssl)

```
##
## Makefile to keep the hash symlinks in SSLCACertificatePath up to
date
## Copyright (c) 1998-2001 Ralf S. Engelschall, All Rights Reserved.
##
SSL_PROGRAM=

update: clean
   -@ssl_program="$(SSL_PROGRAM)"; \
   if [ ".$$ssl_program" = . ]; then \
      for dir in . `echo $$PATH | sed -e 's/:/ /g'`; do \
         for program in openssl ssleay; do \
            if [ -f "$$dir/$$program" ]; then \
               if [ -x "$$dir/$$program" ]; then \
                  ssl_program="$$dir/$$program"; \
            break; \
                  fi; \
               fi; \
            done; \
            if [ ".$$ssl_program" != . ]; then \
         break; \
            fi; \
         done; \
      fi; \
      if [ ".$$ssl_program" = . ]; then \
         echo "Error: neither 'openssl' nor 'ssleay' program found"
      1>&2; \
         exit 1; \
   fi; \
   for file in *.crt; do \
      if [ ".`grep SKIPME $$file`" != . ]; then \
         echo dummy |\
         awk '{ printf("%-15s ... Skipped\n", file); }' \
         "file=$$file"; \
else \
   n=0; \
   while [ 1 ]; do \
      hash="`$$ssl_program x509 -noout -hash <$$file`"; \
      if [ -r "$$hash.$$n" ]; then \
         n=`expr $$n + 1`; \
      else \
         echo dummy |\
         awk '{ printf("%-15s ... %s\n", file, hash); }' \
         "file=$$file" "hash=$$hash.$$n"; \
         ln -s $$file $$hash.$$n; \
         break; \
      fi; \
   done; \
fi; \
done

clean:
-@rm -f [0-9a-fA-F]*.[0-9]*
```

Bijlage: Het omzetten van en naar PEM encoding (Apache - OpenSSL)

Wat heeft u nodig
Een werkende OpenSSL installatie;
een DER-encoded X.509 certificaat.

Een voorbeeld is het certificaat van de ZOVAR Services CA. Deze is nodig voor Cliënt authenticatie zoals beschreven in het document "Cliënt certificaat authenticatie voor Apache webserver". Dit is een DER-encoded (binair) certificaat. Een apache webserver kan hier echter niet mee overweg.

U kunt dit certificaat downloaden via onderstaande link:
https://www.zorgcsp.nl/ca-certificaten
N.B. Servercertificaten worden in beide formaten aangeleverd.

Als u geen (werkende) OpenSSL installatie heeft, raadpleeg dan de documentatie van uw besturingssysteem hoe u deze kunt installeren.

Het omzetten van DER naar PEM

Plaats het om te zetten DER-encoded certificaat in een willekeurige directory. In dit voorbeeld is uitgegaan van de directory /tmp.

```
# cd /tmp
# openssl x509 –inform der –outform pem < zovar_services_ca.cer >
zovar_services_ca.pem
```

Het omzetten van PEM naar DER
Natuurlijk is het ook mogelijk om een PEM-encoded bestand om te zetten naar een DER-encoding. Plaats het om te zetten PEM-encoded bestand in een willekeurige directory. In het voorbeeld is weer uitgegaan van de directory /tmp.

```
# cd /tmp
# openssl x509 –inform pem –outform der < zovar_services_ca.pem >
zovar_services_ca.cer
```

Bijlage: Toelichting systeemnaam (FQDN)

Voor het aanvragen van een servercertificaat moet de aanvrager een systeemnaam opgeven. Deze komt in het servercertificaat te staan. Deze systeemnaam moet een 'Fully Qualified Domain Name' zijn en aan een aantal eisen voldoen.

Beleid
Als de aanvraag voor een servercertificaat is ontvangen voert het ZOVAR een aantal controles uit. ZOVAR stelt vast of de bestanden correct zijn en of de opgegeven systeemnaam (URL) bij de Stichting Internet Domeinregistratie Nederland (www.sidn.nl) is geregistreerd. De aanvrager kan via de website vaststellen welke gegevens SIDN heeft geregistreerd. Als deze gegevens niet overeenkomen met de aan het ZOVAR geleverde gegevens dan is het nodig dat u eerst de informatie bij SIDN laat actualiseren, of ter alternatief, een verklaring/factuur van de houder van de domeinnaam kunt overleggen waaruit blijkt dat u gebruik mag maken van de opgegeven domeinnaam. Voor andere extensies kunt u gebruik maken van www.iana.org. Voorbeelden zijn: *.com & *.org.

De opgegeven domeinnaam moet uniek zijn en mag niet worden gebruikt bij een andere organisatie.

Het ZOVAR adviseert om in de systeemnaam voor de productieomgeving geen test te vermelden, het mag echter wel als de klant dit wenst. De systeemnaam die u in productie gebruikt, mag al gebruikt zijn in de testomgeving. Onze ervaring leert echter dat dit door gebruik van dezelfde systeemnaam lastiger te beheren is.

Systeemnamen die eindigen op .local zijn niet te toetsen voor ZOVAR: een aanvrager kan in principe iedere naam opgeven die hij wenst. ZOVAR kan er nu niet zeker van zijn of het systeem onder het domein van de abonnee hangt. Het ZOVAR accepteert dus geen systeemnamen die eindigen op .local.

Het gebruiken van een servercertificaat voor aansluiting op het Landelijk Schakel Punt (LSP) kan alleen als de systeemnaam eindigt op .aorta-zorg.nl.

Technisch
In een systeemnaam mogen alleen letters, cijfers en het minteken voorkomen, met de volgende beperkingen:
- de systeemnaam mag alleen uit kleine letters bestaan, tekens in de reeks van 0 t/m 9, a t/m z en het koppelteken: "–". Een underscore mag niet;
- de systeemnaam mag niet bestaand uit diakrieten;
- er moet tenminste één letter in de naam staan;
- een minteken mag alleen tussen twee letters en/of cijfers staan.

Voorbeelden van juiste systeemnamen
- webservice.zorginstelling.nl is een juiste systeemnaam.
- systeemnaam1.ziekenhuis.nl is een juiste systeemnaam.
- webmail.afdelinga.ziekenhuis.nl is een juiste systeemnaam.

Voorbeelden van onjuiste systeemnamen
- www.zorginstelling/.sbvzbevraging.nl is een onjuiste systeemnaam.
- www.intrekking.zovar.local is een onjuiste systeemnaam.
- ziekenhuis.nl is een onjuiste systeemnaam.
- *.ziekenhuis.nl is een onjuiste systeemnaam.