TLS/SSL certificaten en signing

wordt aan gewerkt

Een eigen X.509 CA

Je kan natuurlijk een account nemen bij een club als StarSSL, maar mocht je self signed certificaten willen maken kan je ook een eigen CA opzetten.

Dit kan eventueel op de server zelf waar het certificaat gebruikt gaat worden.

instaleer open ssl: `yum install openssl`

pas de standaard configuratie aan door `vi /etc/pki/tls/openssl.cnf`

en daarin aan te passen:

```
req_extensions                  = v3_req
countryName_default             = NL
stateOrProvinceName_default     = Zuid Holland
localityName_default            = Den Haag
0.organizationName_default      = Boerema CI&ND
organizationalUnitName_default  = IT dept.
```

maak het CA certificaat en de CA private key aan:

`/etc/pki/tls/misc/CA -newca`

```
CA certificate filename (or enter to create)
```

druk op enter

```
Making CA certificate ...
Generating a 2048 bit RSA private key
.....................+++
........+++
writing new private key to '/etc/pki/CA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

vul een password in, het mag niet leeg zijn.

```
-----
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 a DN.
There are quite a 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) [NL]:
State or Province Name (full name) [Zuid Holland]:
Locality Name (eg, city) [Den Haag]:
Organization Name (eg, company) [DBoerema CI&ND]:Boerema CI&ND Certificate
Authority
Organizational Unit Name (eg, section) [IT Dept.]:
Common Name (eg, your name or your server's hostname) []:caserver.auriel.nl
Email Address []:webmaster@auriel.nl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

druk op enter

```
An optional company name []:
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:
```

en vul nogmaals het password in

Het hiermee aangemaakte certificaat maar een jaar geldig (je zou de default hiervoor kunnen veranderen in `/etc/pki/tls/openssl.cnf`). Verander dit nu naar 10 jaar door:

```
cd /etc/pki/CA/
openssl x509 -in cacert.pem -days 3650 -out cacert.pem -signkey
./private/cakey.pem
```

```
Getting Private key
Enter pass phrase for ./private/cakey.pem:
```

vul het eerder gemaakte password in.

De CA private key vindt je terug in `/etc/pki/CA/private/cakey.pem`

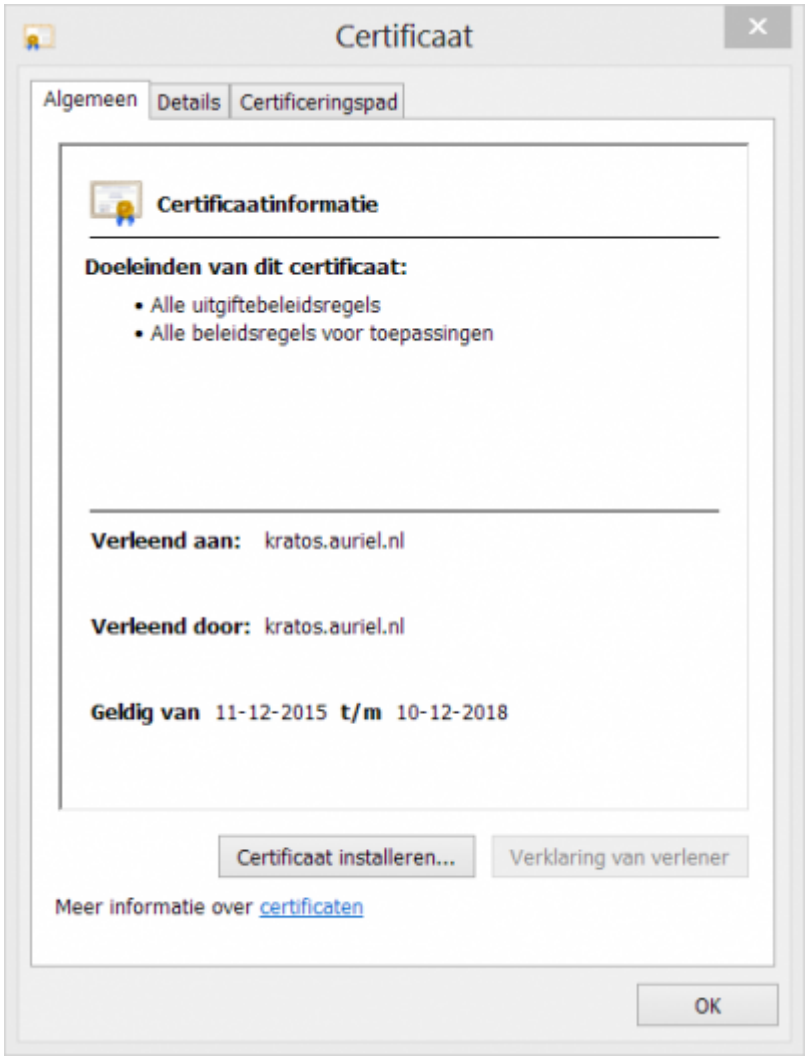
Het CA certificaat vindt je in `/etc/pki/CA/cacert.pem`

trusted CA certificaten toevoegen

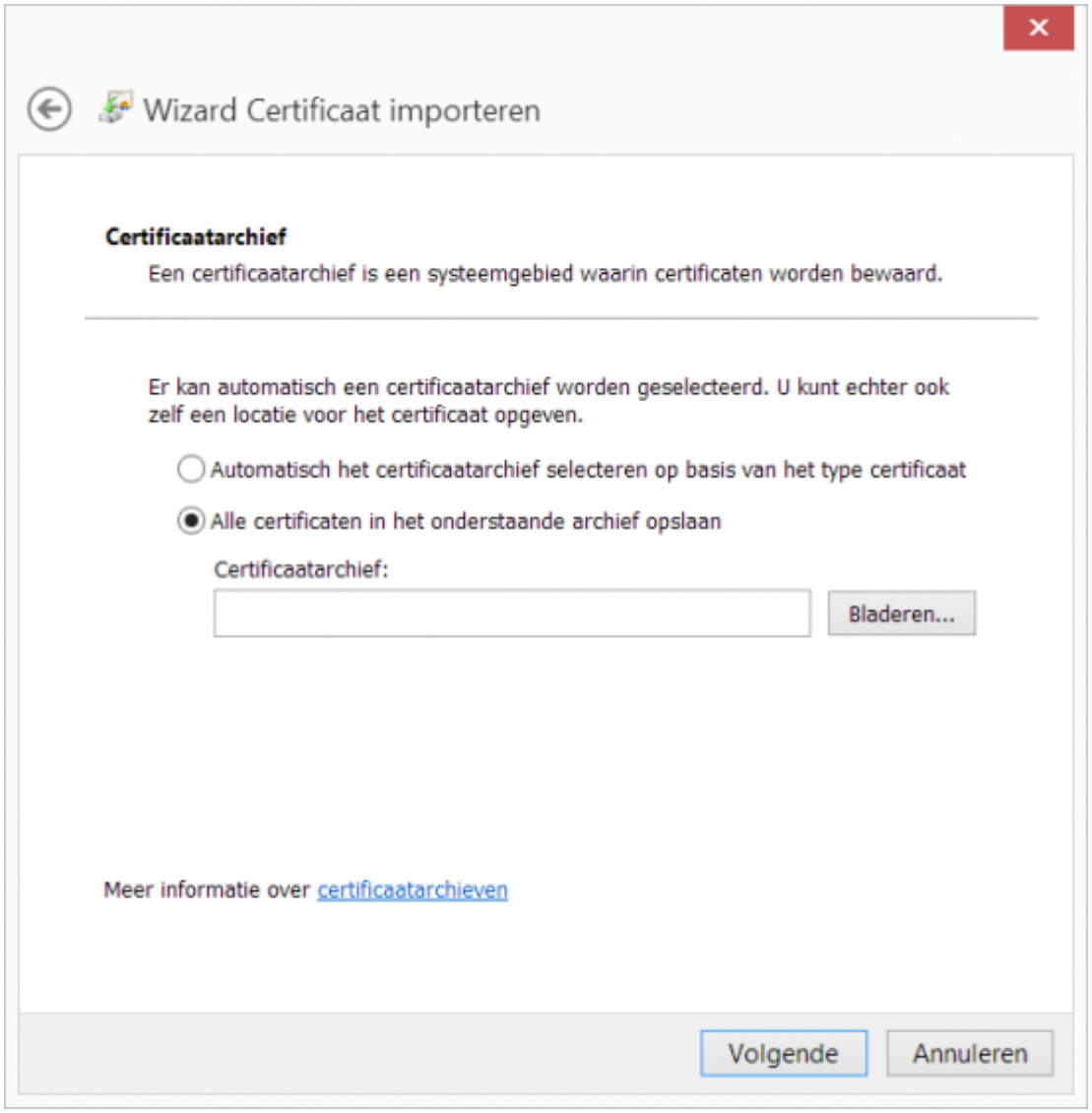
op Windows

Om zonder uitzonderingen per gebruikte webserver aan te maken in browsers en andere software is het belangrijk je eigen CA certificaat toe te voegen aan de vertrouwde certificaat authoriteiten op je werkplek.

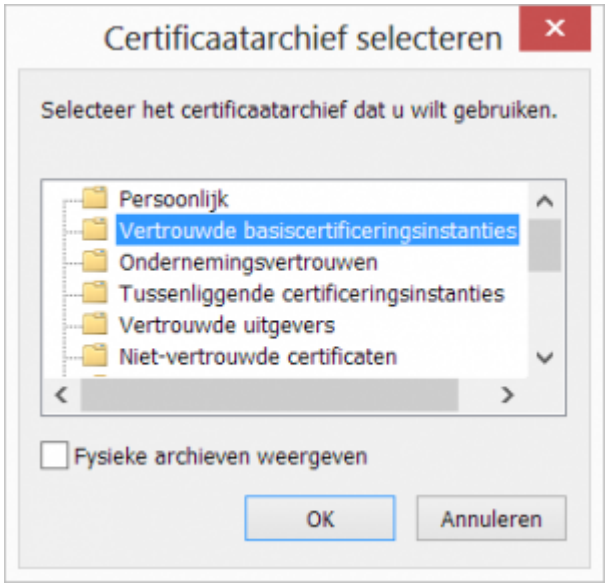
op windows doe je dat door te dubbelklicken op het CA certificaat wat je hebt opgehaald van je CA server. Er verschijnt een venster:



druk op `Certificaat installeren…`



Selecteer ⊗*Alle certificaten in het onderstaande archief opslaan* en kies `Bladeren…`



Kies *Vertrouwde basiscertificeringsinstanties* en druk in het vorige venster waar we in terug zijn op `Volgende` en `Voltooien`

Op Linux

Fedora sinds versie 19 & RHEL/CentOS 7

Kopieer je CA certificaat in PEM formaat naar `/etc/pki/ca-trust/source/anchors/` Of, als jee certificaat in OpenSSL's extended BEGIN TRUSTED CERTIFICATE formaat is, zet je het in /etc/pki/ca-trust/source.

En run `update-ca-trust`.

On RHEL 6, you have to activate the system with update-ca-trust enable.

Ubuntu & Debian

zet je ca certificaat in de trusted CA directory:
`cp foo.crt /usr/local/share/ca-certificates/foo.crt`

Update de CA store:
`update-ca-certificates`

Verwijderen gaat precies omgekeerd; rnm het certificaat en run:
`update-ca-certificates –fresh`

X.509 signing request maken

Je kan deze op de betreffende server aanmaken of op de CA,

- Op de betreffende server door:

```
openssl req -nodes -days 1000 -newkey rsa:2048 -keyout [FQDN].key -sha256 -out [FQDN].csr
```

Met dit commando wordt zowel het signing request als de server key aangemaakt.

Het programma vraagt je om enkele gegevens, waarvan de belangrijste de "`Common Name`" is. Vul hier je FQDN in

- Op de CA server.

Bij servers waar je geen locale ssl software tot je beschikking hebt en sommige devices zul je de certificaten en keys op de CA server moeten maken. In dat geval moet je ook de serverkey naar de server transporteren.

```
openssl req -nodes -days 1000 -newkey rsa:2048 -keyout [FQDN].key -sha256 -out [FQDN].csr
```

Met dit commando wordt zowel het signing request als de server key aangemaakt.

Het programma vraagt je om enkele gegevens, waarvan de belangrijste de "Common Name" is. Vul hier je FQDN van de server waar je een certificaat voor maakt in, **LET GOED OP!** de default waarden kunnen verkeerd staan.

X.509 Certificaten signen

Haal het request over naar de CA server. Overigens, het request is niets anders dan de public key ingepakt in een certificaat die alleen de signing mist.

sign het request, bijvoorbeeld die van de LDAP server:

```
openssl ca -days 3650 -out LDAPcert.pem -keyfile
/etc/pki/CA/private/cakey.pem -cert /etc/pki/CA/cacert.pem -policy
policy_anything -infiles LDAPreq.pem
```

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 11529081143652653341 (0x9fff86376a12191d)
        Validity
            Not Before: Dec  4 14:58:17 2015 GMT
            Not After : Dec  1 14:58:17 2025 GMT
        Subject:
            countryName               = NL
            stateOrProvinceName       = Zuid Holland
            organizationName          = Boerema CI&ND
            organizationalUnitName    = IT Dept.
            commonName                = ldap.auriel.nl
            emailAddress              = webmaster@auriel.nl
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                0A:90:79:34:2B:0C:AB:20:B4:EE:B9:5E:B2:71:0D:ED:E4:F4:A4:BF
            X509v3 Authority Key Identifier:
keyid:54:BB:6E:02:D7:AD:9E:D7:AD:30:FF:85:29:5B:FA:A8:7E:43:68:88

Certificate is to be certified until Dec  1 14:58:17 2025 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Zend het resulterende certificaat én het CA certificaat naar de betreffende server, in dit geval:

```
LDAPcert.pem
cacert.pem
```

Bronnen

http://www.zytrax.com/tech/survival/ssl.html#ssl

http://serverfault.com/questions/306345/certification-authority-root-certificate-expiry-and-renewal

https://sites.google.com/site/amitsciscozone/home/security/digital-certificates-explained

http://www.ipsec-howto.org/x595.html

https://www.linode.com/docs/security/ssl/ssl-apache2-centos

http://wiki.cacert.org/HowTo/InstallCAcertRoots

http://kb.kerio.com/product/kerio-connect/server-configuration/ssl-certificates/adding-trusted-root-certificates-to-the-server-1605.html

https://www.happyassassin.net/2015/01/14/trusting-additional-cas-in-fedora-rhel-centos-dont-append-to-etcpkitlscertsca-bundle-crt-or-etcpkitlscert-pem/