OEF TLS met apache2

Karel de Grote
Hogeschool

Configuratie apache2

- Nieuw bestand /etc/apache2/sites-available/sslsite.conf

```
<VirtualHost *:443>|
DocumentRoot /var/www/
SSLEngine on
SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
</VirtualHost>
```

- Activeren

```
sudo a2ensite sslsite|
sudo systemctl restart apache2
```

Configuratie machine

- De hostname Common Name moet kloppen!
- Deze wordt gegarandeerd door de Certificate Authority
- Meestal geregistreerd bij een DNS server
- Bij de oefening toevoegen in je lokale /etc/hosts bestand zodat je dit niet moet registreren bij een DNS server

  127.0.0.1 localhost kdguntu www.mijnweb.local

Geheime private key maken

- **openssl genrsa -des3 -out server.key 4096**
- Generating RSA private key, 4096 bit long modulus (2 primes)

  ```
  ...............................++++
  ...............................................................++++
  e is 65537 (0x010001)
  Enter pass phrase for server.key:
  Verifying - Enter pass phrase for server.key:
  ```

Request voor de CA aanmaken

- **openssl req -new -key server.key -out server.csr**
-
  ```
  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) [AU]:BE
  State or Province Name (full name) [Some-State]:Antwerpen
  Locality Name (eg, city) []:Antwerpen
  Organization Name (eg, company) [Internet Widgits Pty Ltd]:KdG
  Organizational Unit Name (eg, section) []:MIT
  Common Name (e.g. server FQDN or YOUR name) []:www.mijnweb.local
  Email Address []:
  ```
- **Optional mag je leeg laten**
-
  ```
  Please enter the following 'extra' attributes
  to be sent with your certificate request
  A challenge password []:
  An optional company name []:
  ```

Request laten tekenen door CA (jezelf)

-
  ```
  openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
  ```

-
  ```
  Signature ok
  subject=C = BE, ST = Antwerpen, L = Antwerpen, O = KdG, OU = MIT, CN = www.mijnweb.local
  Getting Private key
  ```

CA tekent eigen request (self signed)

- **openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650**
- Generating a RSA private key

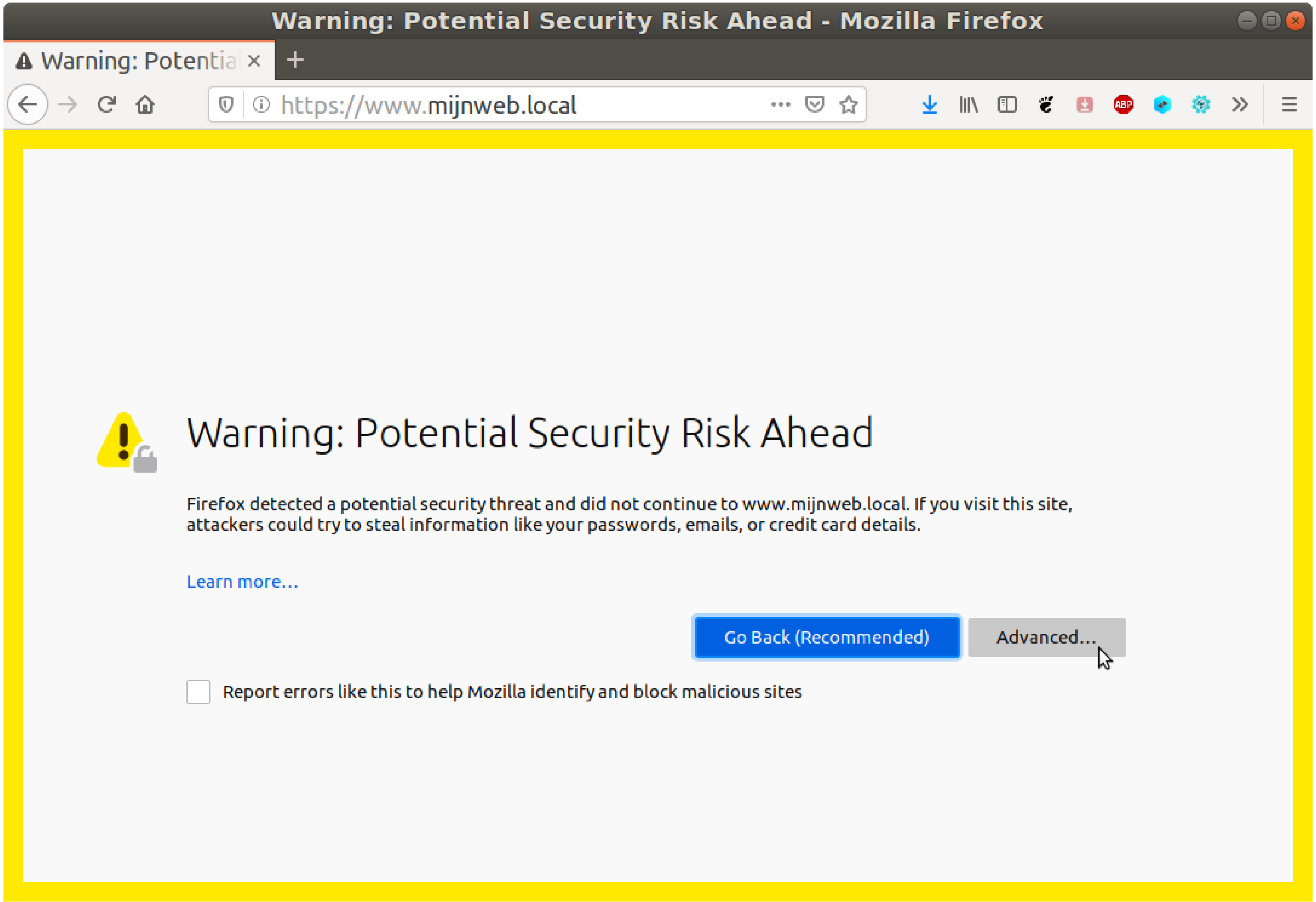
```
.................+++++
..................+++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called 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) [AU]:BE
State or Province Name (full name) [Some-State]:Antwerpen
Locality Name (eg, city) []:Antwerpen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:KdG
Organizational Unit Name (eg, section) []:MIT
Common Name (e.g. server FQDN or YOUR name) []:www.mijnweb.local
Email Address []:
```

Toevoegen server aan CA

-
  ```
  echo 01 > /etc/ssl/serial
  touch /etc/ssl/index.txt

  openssl ca -in server.csr -config /etc/ssl/openssl.cnf
  ```

-
  ```
  Using configuration from /etc/ssl/openssl.cnf
  Enter pass phrase for /etc/ssl/private/cakey.pem:
  Check that the request matches the signature
  Signature ok

  ......

  Sign the certificate? [y/n]:y

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

  ....
  -----END CERTIFICATE-----
  Data Base Updated
  ```

Melding in Firefox https niet Ok



Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potentia ×
https://www.mijnweb.local

Warning: Potential Security Risk Ahead

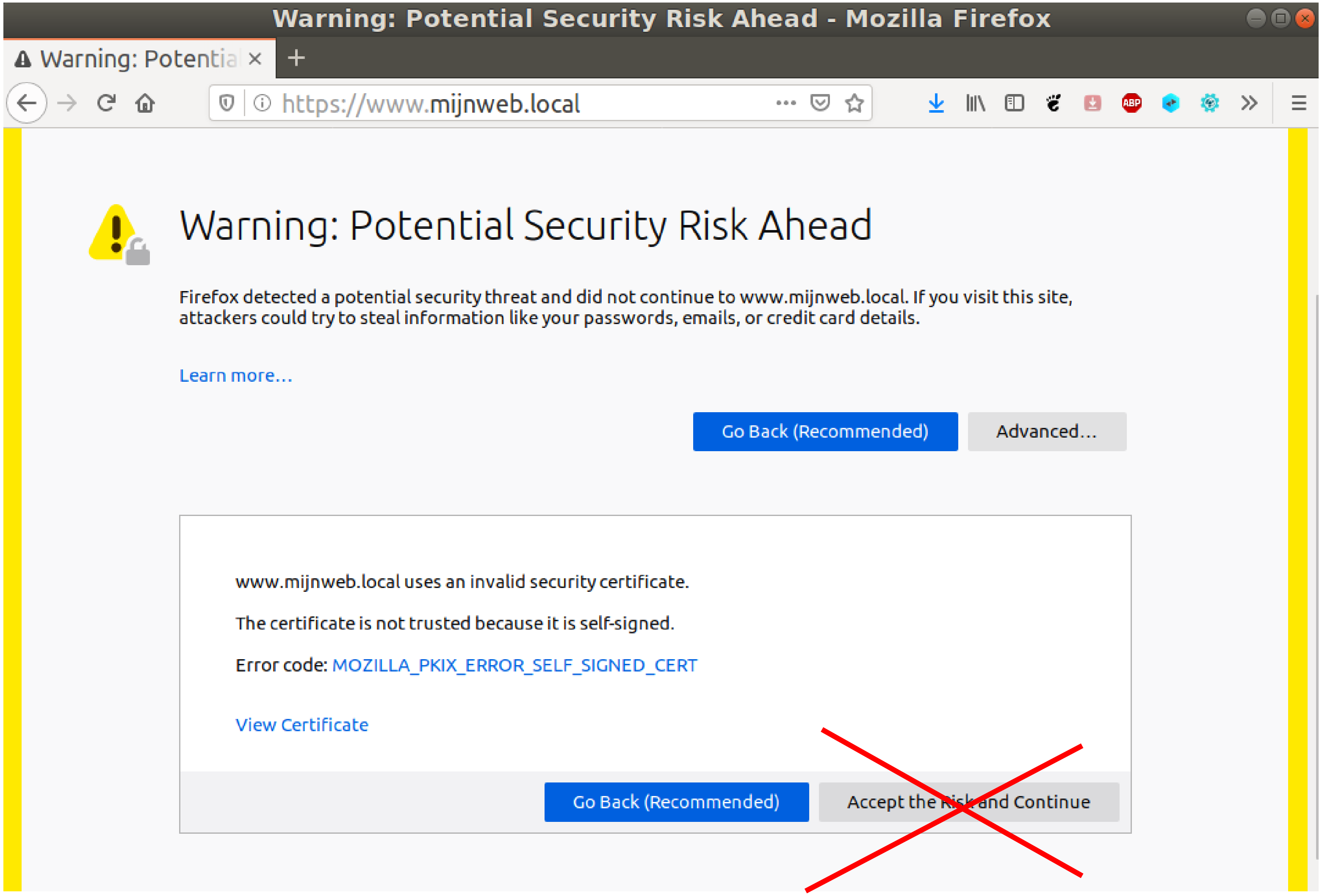
Firefox detected a potential security threat and did not continue to www.mijnweb.local. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

Go Back (Recommended)
Advanced…

□ Report errors like this to help Mozilla identify and block malicious sites

GEEN exception ingeven!



Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potentia ×
https://www.mijnweb.local

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to www.mijnweb.local. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

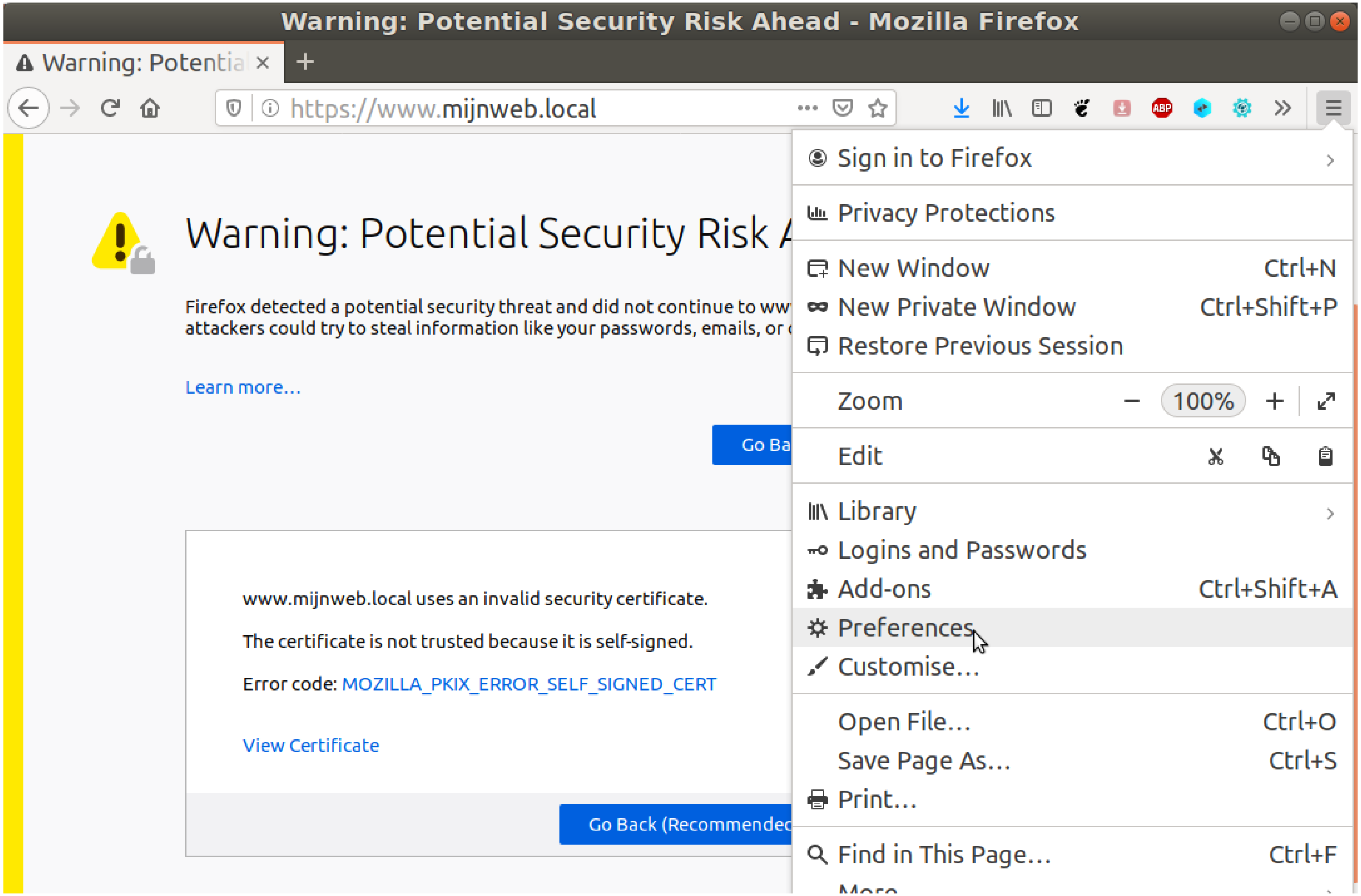
Learn more…
Go Back (Recommended)
Advanced…

www.mijnweb.local uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

WEL eigen CA toevoegen als Trust



Warning: Potential Security Risk A

Firefox detected a potential security threat and did not continue to ww
attackers could try to steal information like your passwords, emails, or c

Learn more…

Go Ba

www.mijnweb.local uses an invalid security certificate.

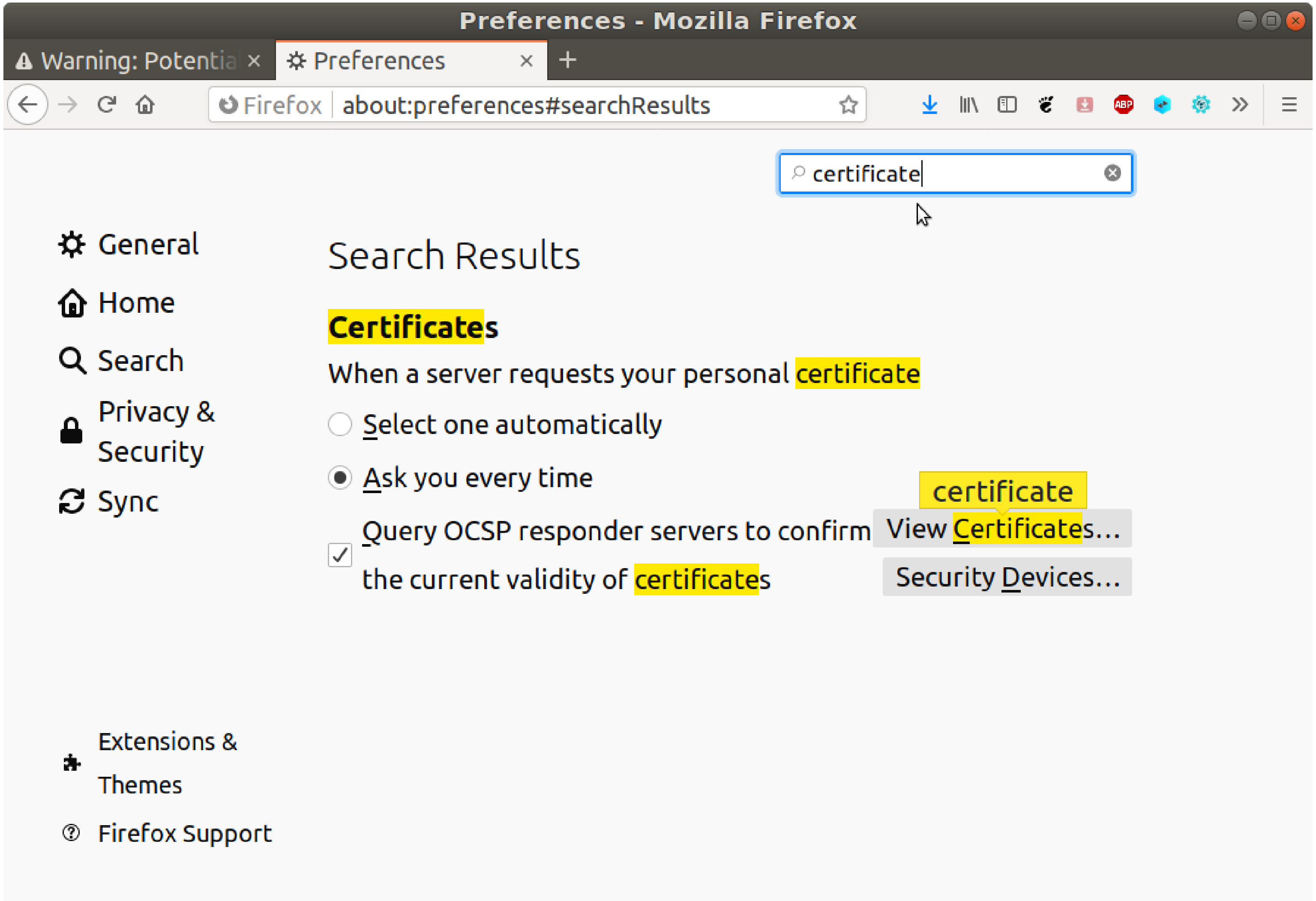
The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Go Back (Recommended

Zoek bij Preferences op certificate



Preferences - Mozilla Firefox

Warning: Potentia × Preferences ×

Firefox about:preferences#searchResults

certificate

Search Results

Certificates

When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

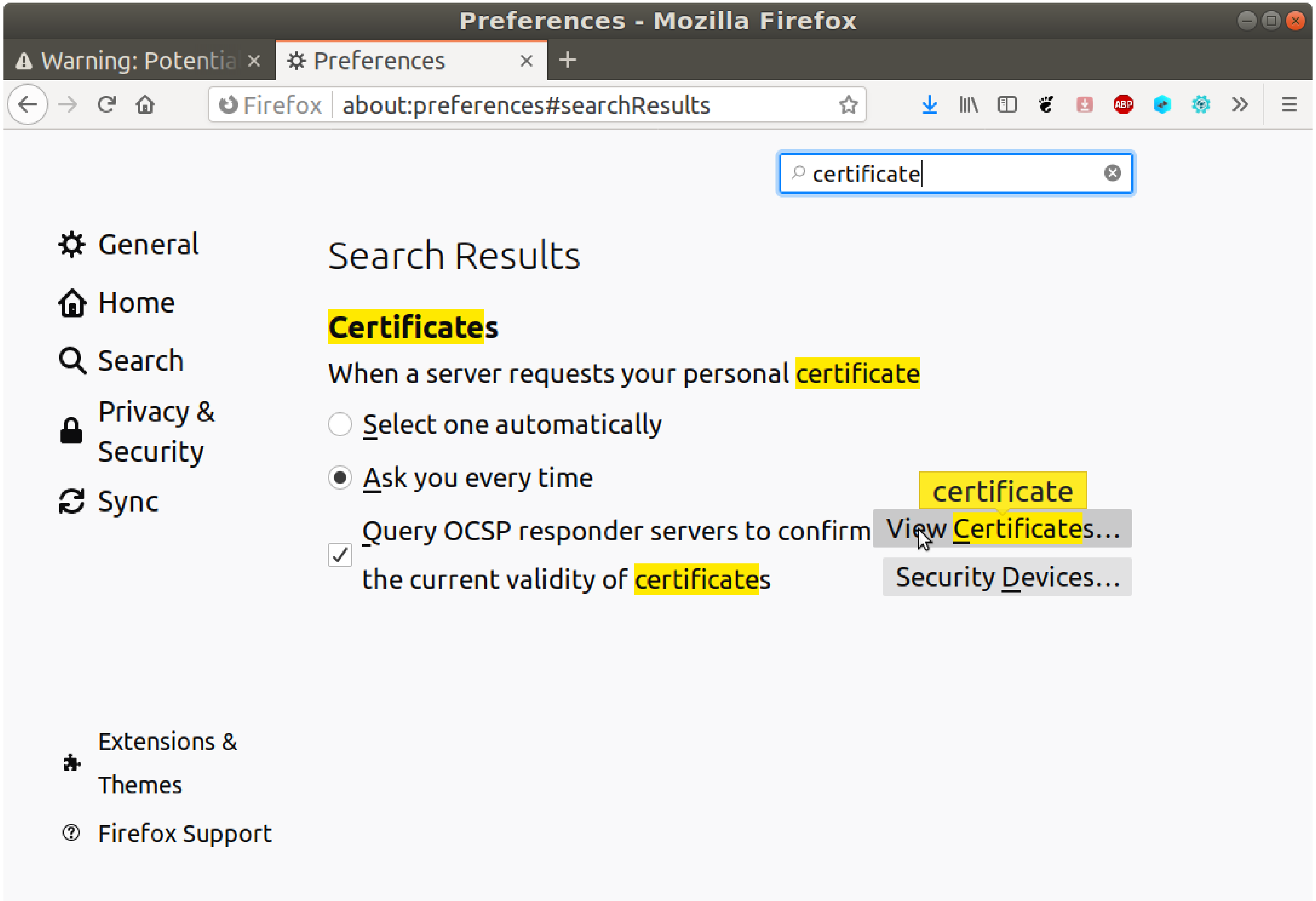
certificate

View Certificates…

Security Devices…

Karel de Grote Hogeschool

Kies: View Certificates



Search Results

Certificates

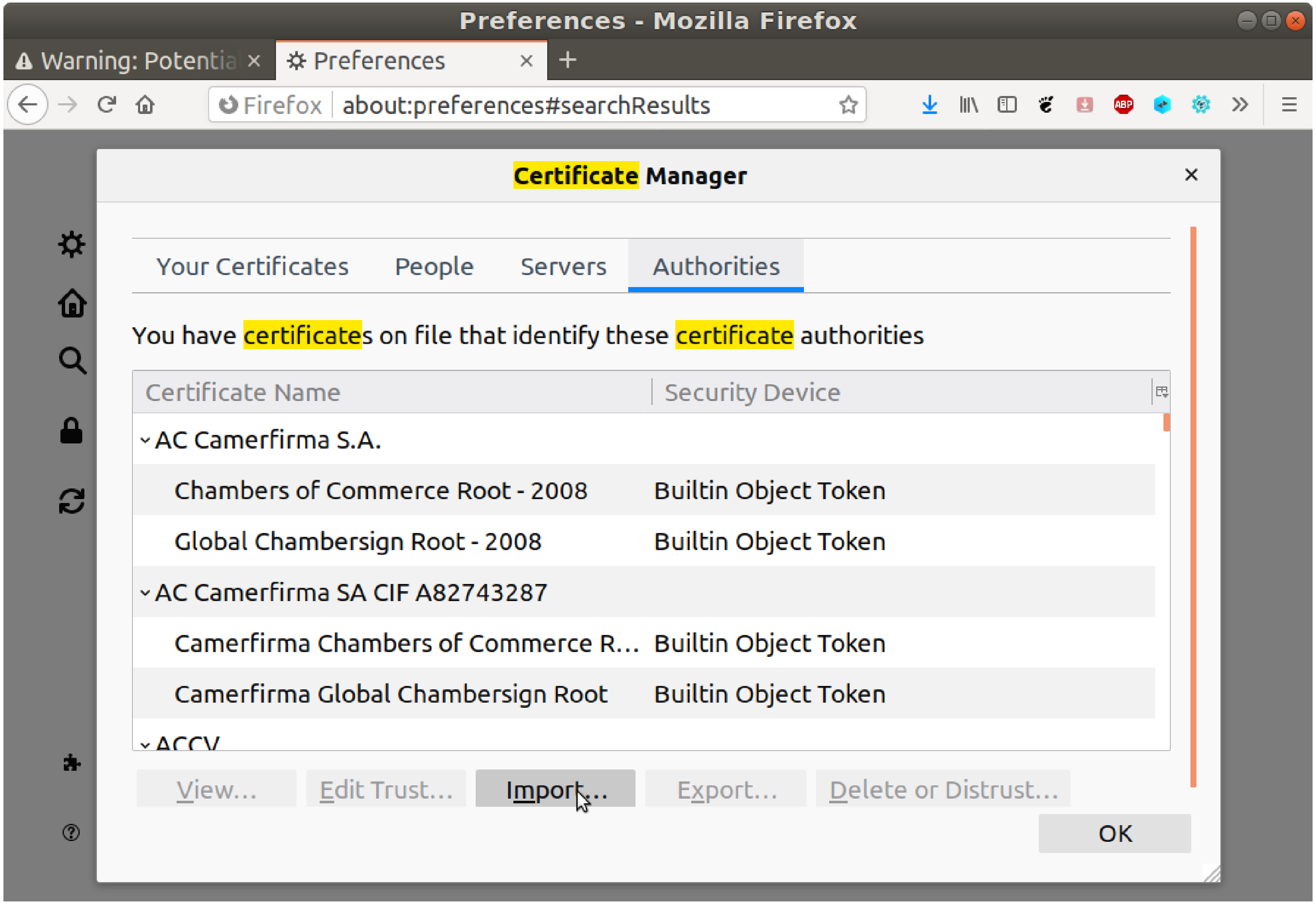
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Kies indien nodig: Import



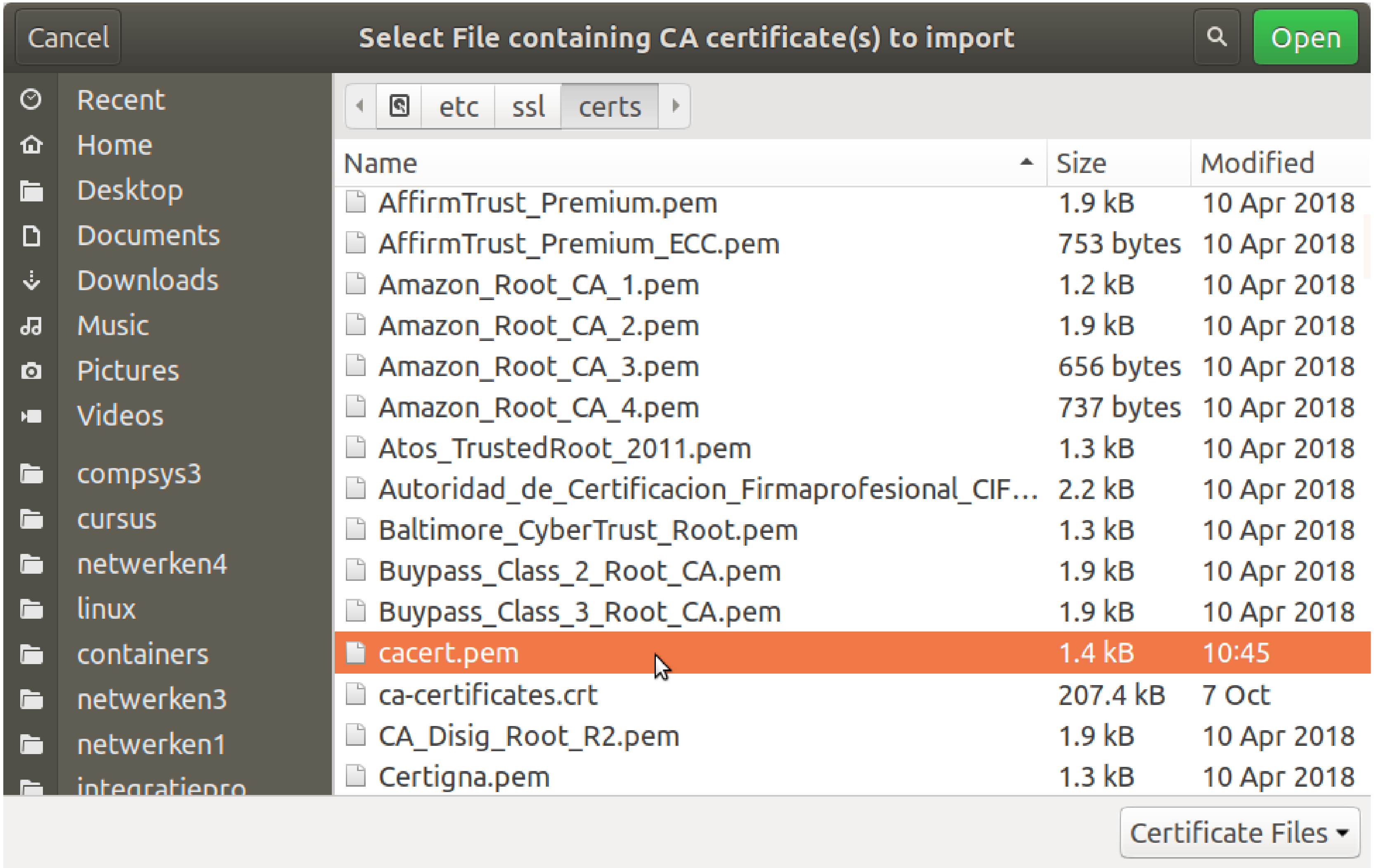
Preferences - Mozilla Firefox

Certificate Manager

You have certificates on file that identify these certificate authorities

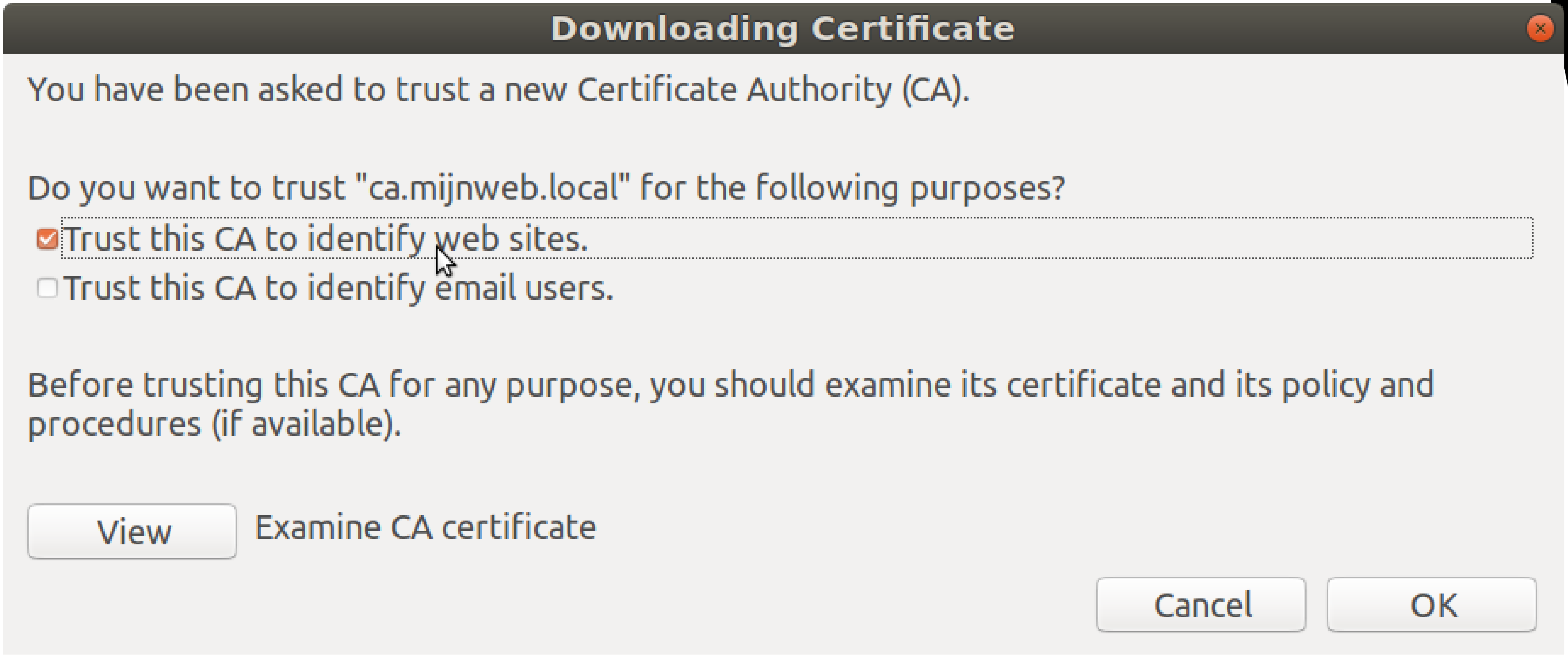
Certificate Name	Security Device
˅ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
˅ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
˅ ACCV	

Selecteer /etc/ssl/certs/cacert.pem



Name	Size	Modified
AffirmTrust_Premium.pem	1.9 kB	10 Apr 2018
AffirmTrust_Premium_ECC.pem	753 bytes	10 Apr 2018
Amazon_Root_CA_1.pem	1.2 kB	10 Apr 2018
Amazon_Root_CA_2.pem	1.9 kB	10 Apr 2018
Amazon_Root_CA_3.pem	656 bytes	10 Apr 2018
Amazon_Root_CA_4.pem	737 bytes	10 Apr 2018
Atos_TrustedRoot_2011.pem	1.3 kB	10 Apr 2018
Autoridad_de_Certificacion_Firmaprofesional_CIF…	2.2 kB	10 Apr 2018
Baltimore_CyberTrust_Root.pem	1.3 kB	10 Apr 2018
Buypass_Class_2_Root_CA.pem	1.9 kB	10 Apr 2018
Buypass_Class_3_Root_CA.pem	1.9 kB	10 Apr 2018
cacert.pem	1.4 kB	10:45
ca-certificates.crt	207.4 kB	7 Oct
CA_Disig_Root_R2.pem	1.9 kB	10 Apr 2018
Certigna.pem	1.3 kB	10 Apr 2018

Vink aan: Trust this CA ...web sites



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "ca.mijnweb.local" for the following purposes?

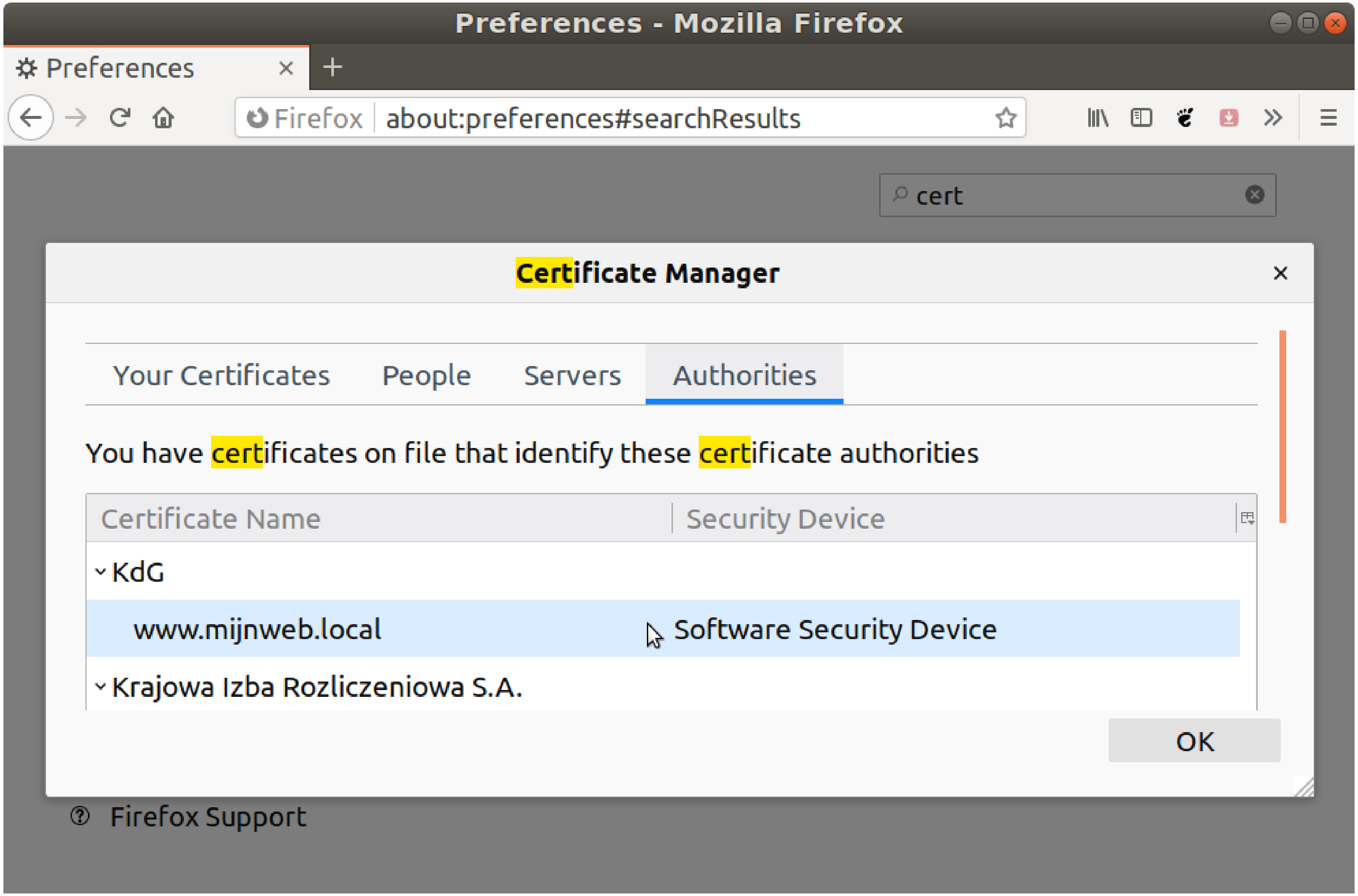
☑ Trust this CA to identify web sites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

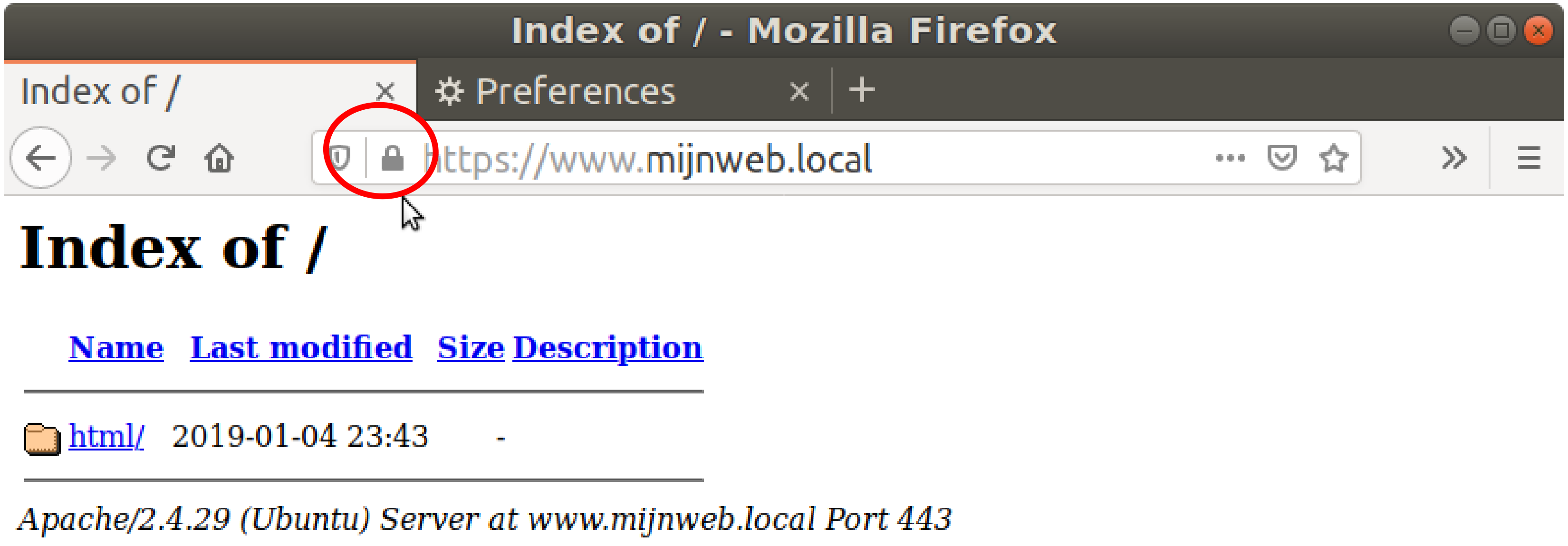
Jouw CA staat bij de Authorities



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
KdG	
www.mijnweb.local	Software Security Device
Krajowa Izba Rozliczeniowa S.A.	

HTTPS SLOT is OK!



Index of /

Name	Last modified	Size	Description
html/	2019-01-04 23:43	-	

Apache/2.4.29 (Ubuntu) Server at www.mijnweb.local Port 443

Fout bij opstarten apache2

- **root@kdguntu:/home/kdguntu# systemctl status apache2**
- ● apache2.service - The Apache HTTP Server

```
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: failed (Result: exit-code) since Thu 2019-11-14 15:37:21 CET; 51s ago
  Process: 25814 ExecStop=/usr/sbin/apachectl stop (code=exited, status=1/FAILURE)
  Process: 26132 ExecStart=/usr/sbin/apachectl start (code=exited, status=1/FAILURE)
 Main PID: 25760 (code=exited, status=0/SUCCESS)
Nov 14 15:37:20 kdguntu systemd[1]: Starting The Apache HTTP Server...
Nov 14 15:37:20 kdguntu apachectl[26132]: AH00526: Syntax error on line 4 of /etc/apache2/sites-enabled/sslsite.conf:
Nov 14 15:37:20 kdguntu apachectl[26132]: SSLCertificateFile: file '/etc/ssl/certs/server.crt does not exist or is empty
Nov 14 15:37:20 kdguntu apachectl[26132]: Action 'start' failed.
Nov 14 15:37:20 kdguntu apachectl[26132]: The Apache error log may have more information.
Nov 14 15:37:21 kdguntu systemd[1]: apache2.service: Control process exited, code=exited status=1
Nov 14 15:37:21 kdguntu systemd[1]: apache2.service: Failed with result 'exit-code'.
Nov 14 15:37:21 kdguntu systemd[1]: Failed to start The Apache HTTP Server.
```

- OPLS: kijk de locatie en inhoud van je bestanden na

Fout aanmaken CA certificaat

- **openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650**
- Generating a RSA private key

```
.....................+++++
.........................................................................................................................+++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
140558250865088:error:28078065:UI routines:UI_set_result_ex:result too
small:../crypto/ui/ui_lib.c:903:You must type in 4 to 1024 characters
140558250865088:error:2807106B:UI routines:UI_process:processing
error:../crypto/ui/ui_lib.c:543:while reading strings
140558250865088:error:0906406D:PEM routines:PEM_def_callback:problems
getting password:../crypto/pem/pem_lib.c:59:
140558250865088:error:0907E06F:PEM routines:do_pk8pkey:read
key:../crypto/pem/pem_pk8.c:83:
```

- **OPLS: pass phrase NIET leeg laten!**