LAB :: Secure HTTP traffic using SSL Certificate

- In this example we are using apnictraining.net as domain name.
- # super user command.
- $ normal user command.
- N replace with your group no.
- Username `apnic` and password `training`.

Topology

```
[group1.apnictraining.net] [192.168.30.1]
[group2.apnictraining.net] [192.168.30.2]
......
[group10.apnictraining.net] [192.168.30.10]
[group11.apnictraining.net] [192.168.30.11]
......
[group20.apnictraining.net] [192.168.30.20]
[group21.apnictraining.net] [192.168.30.21]
......
[group30.apnictraining.net] [192.168.30.30]
```

In this lab we will generate SSL certificated, signed it with our own CA server.

Step 1: Generate Your Certificate Signing Request (CSR)
Step 2: Send the CSR to the CA. CA will sign the CSR and generate certficate
Step 3: Enable SSL and configure Apache with the certificate

Requirements

1. Login to the server.
2. Check if openssl installed and check it's version `# openssl version`. Install if not present already:

   ```
   sudo apt-get update
   sudo apt-get install openssl -y
   ```

   -y option is non-interactive (yes to all)

Step 1

Generate Certificate Signing Request (CSR)

** CSR is a request to get your public key signed by the CA

To generate the keys for the Certificate Signing Request (CSR) run the following command from a terminal prompt (please replace N with your group no):

```
sudo su
cd /etc/ssl
openssl req -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/groupN.apnictraining.net.key \
-out /etc/ssl/groupN.apnictraining.net.csr
```

This will ask for few question:

```
Country Name (2 letter code) [AU]: NZ
State or Province Name (full name) [Some-State]: Queenstown
Locality Name (eg, city) [ ]: Queenstown
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Training
Organizational Unit Name (eg, section) [ ]: Development
Common Name (e.g. server FQDN or YOUR name) [ ]: groupN.apnictraining.net
Email Address [ ]: groupN@apnictraining.net

A challenge password [ ]:
An optional company name []:
```

You can now enter your passphrase. For best security, it should be long (length vs complexity). Also remember that your passphrase is case-sensitive. You can keep `An optional company name []:` blank.

Once you have re-typed it correctly, the server key is generated and stored in the two file in `/etc/ssl/` folder.

```
ls -alh /etc/ssl/
groupN.apnictraining.net.csr
groupN.apnictraining.net.key
```

`groupN.apnictraining.net.csr` is the CSR file which you will send to CA.
`groupN.apnictraining.net.key` the private key.

** To look at the contents of the CSR:

```
openssl req -in groupN.apnictraining.net.csr -text -noout
```

it contains your public key and name.

Step 2

Upload CSR to the CA server

```
cd /etc/ssl/
scp groupN.apnictraining.net.csr apnic@ca.apnictraining.net:/home/apnic/csr
```

password is `training`

STOP

**Now instructor will generate SSL certificate for you. Wait..... **

Step 3

Download your certificate to the server.

```
cd /etc/ssl/
sudo apt-get install wget -y
sudo wget http://ca.apnictraining.net/cert/groupN.apnictraining.net.crt
```

[replace N with your group no]

Now we have the certificate in `/etc/ssl` folder which has been send by CA.

Install APACHE & Enable SSL in APACHE

```
sudo apt-get update
sudo apt-get install apache2 -y
```

Enable SSL

```
sudo a2enmod ssl
```

Edit SSL configuration file as follows:

```
sudo vi /etc/apache2/sites-available/default-ssl.conf

SSLEngine on

# disable existing demo certificate
# SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
# SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

SSLCertificateFile /etc/ssl/groupN.apnictraining.net.crt
SSLCertificateKeyFile /etc/ssl/groupN.apnictraining.net.key
```

[replace N with your group no]

Copy default-ssl.conf file to /etc/apache2/sites-enabled/

```
cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-enabled/
```

Restart Apache server.

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

or

```
service apache2 restart
```

Now try to browse https://groupN.apnictraining.net. This will give you an error that certificate is not trusted. We need to import CA server root certificate.

Step 4

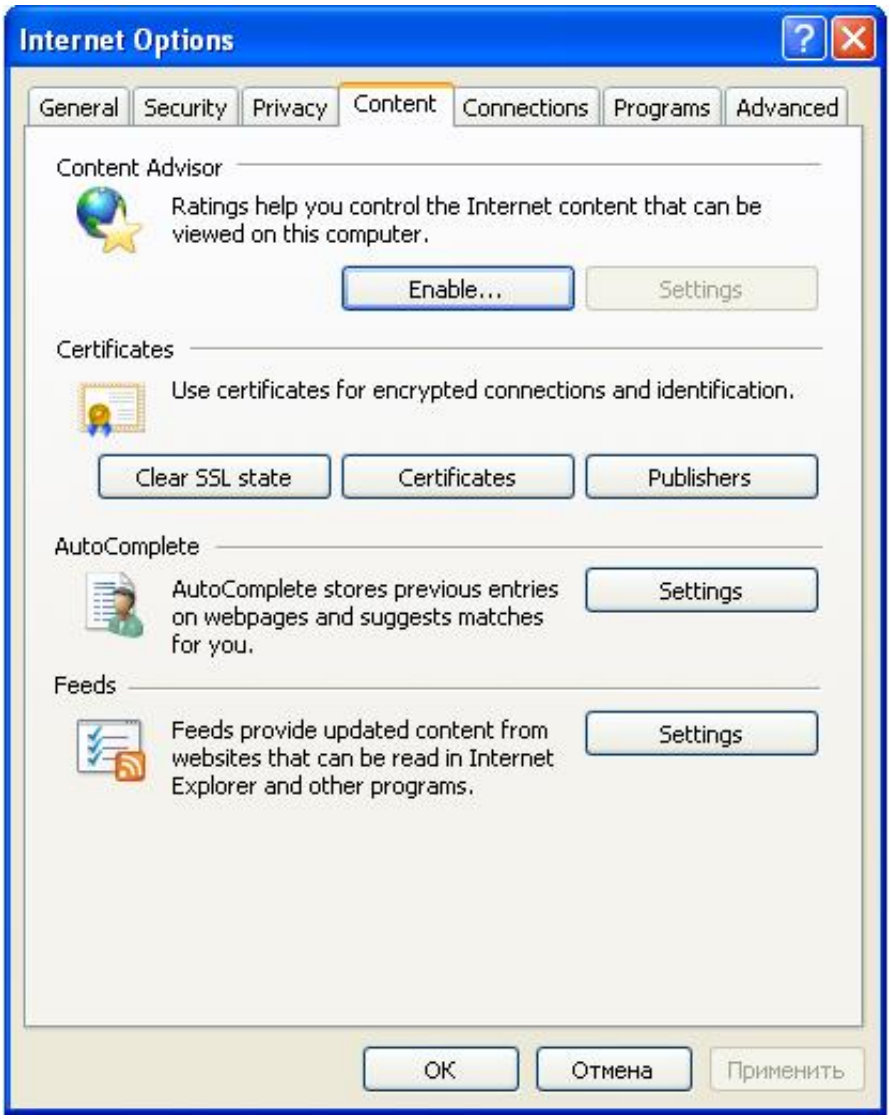
**Ask your instructor to provide you the CA server root certificate. **

Step 5

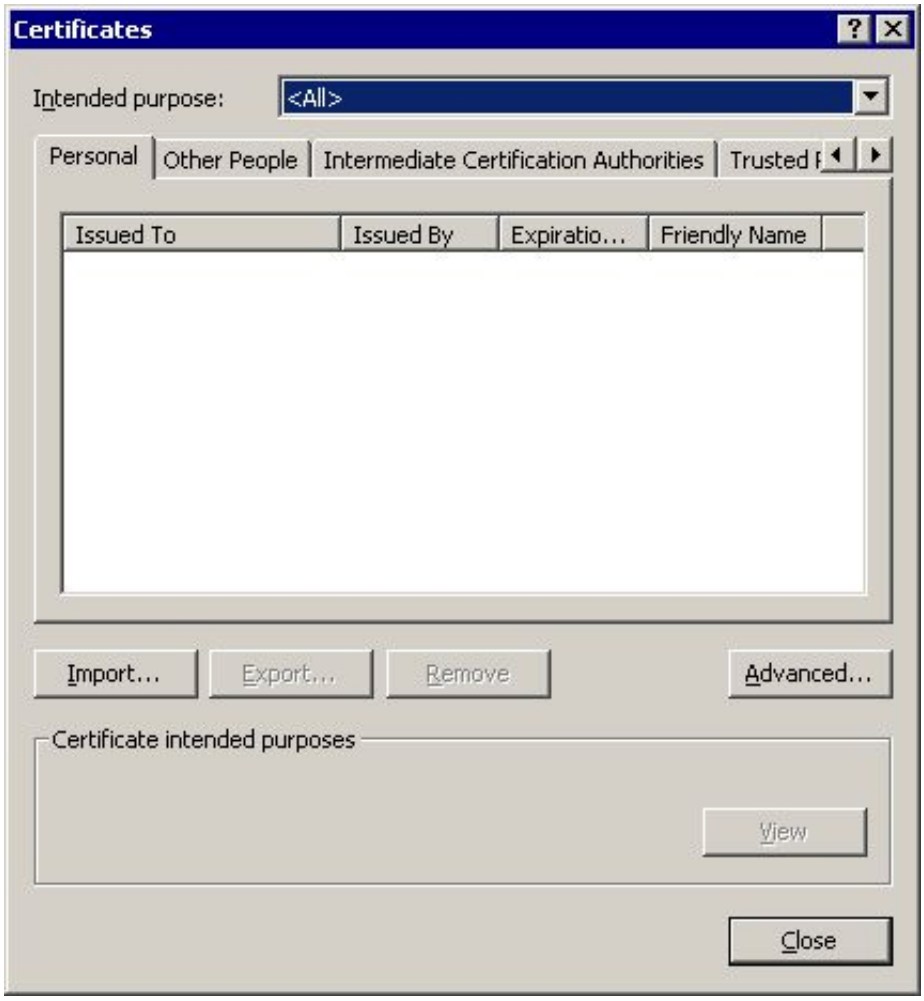
Import Certificate:

1. Internet Explorer:

a. Run IE 9 and click the "Options" > "Internet Options" menu. The Internet Options dialog box shows up.

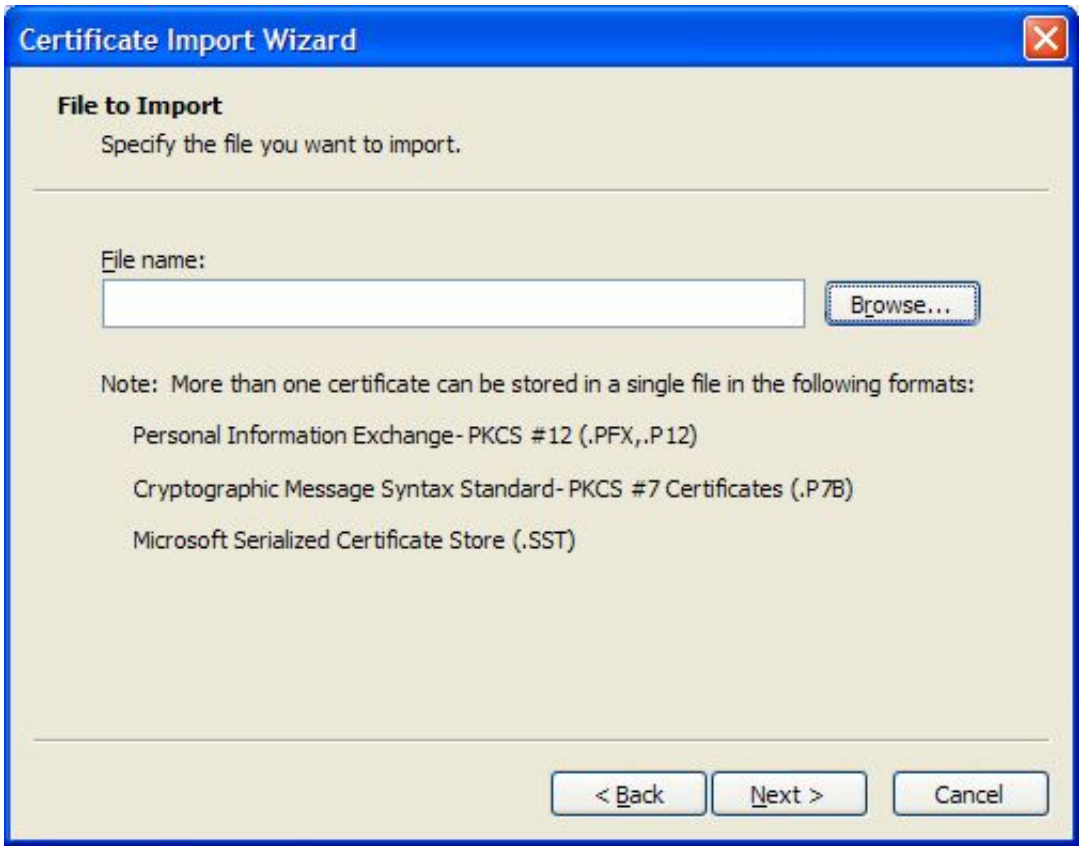


b. Click the "Content" tab and the "Certificates" button. The Certificates dialog box shows up.



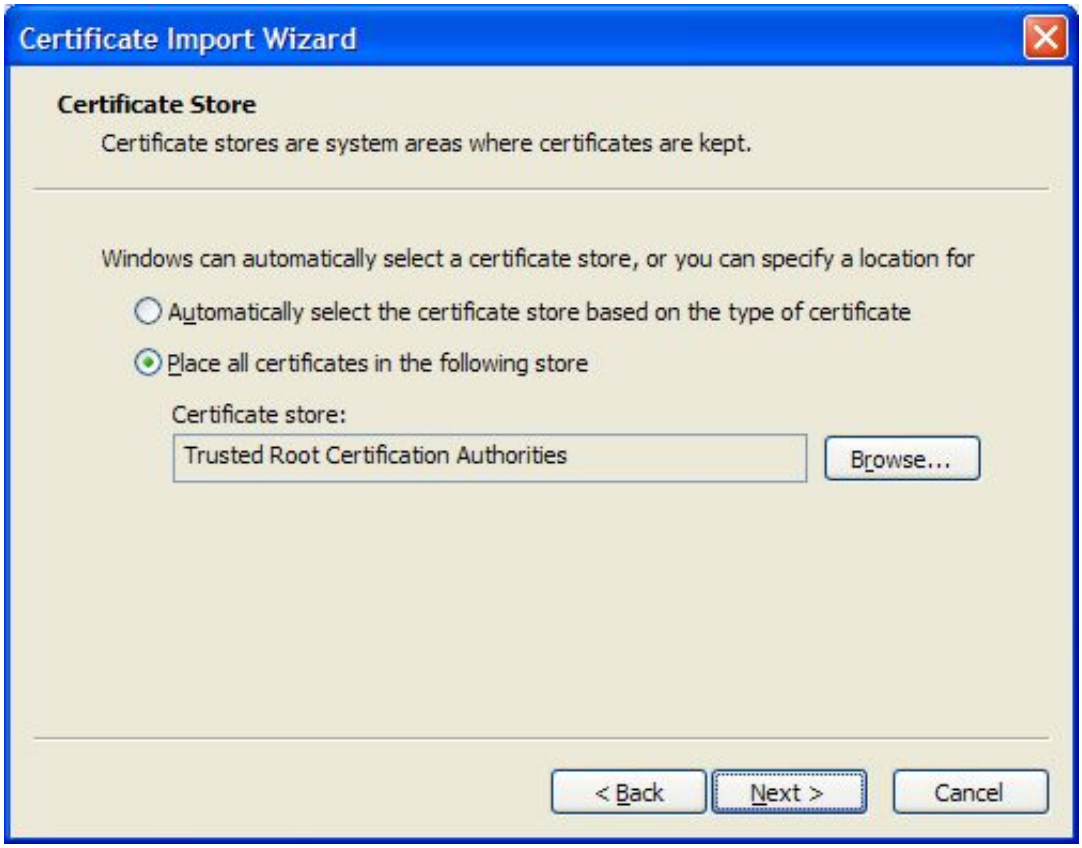
c. Click the "Trusted Root Certification Authorities" tab, and click the "Import..." button. The Certificate Import Wizard shows up.

d. Click the "Next" button. The File to Import step shows up.



e. Use the "Browse" button to find and select cacert.pem. Then click the "Next" button. The Certificate Store step shows up.

f. Keep the default certificate store selection: "Trusted Root Certificate Authorities", and click the "Next" button. The confirmation step shows up.

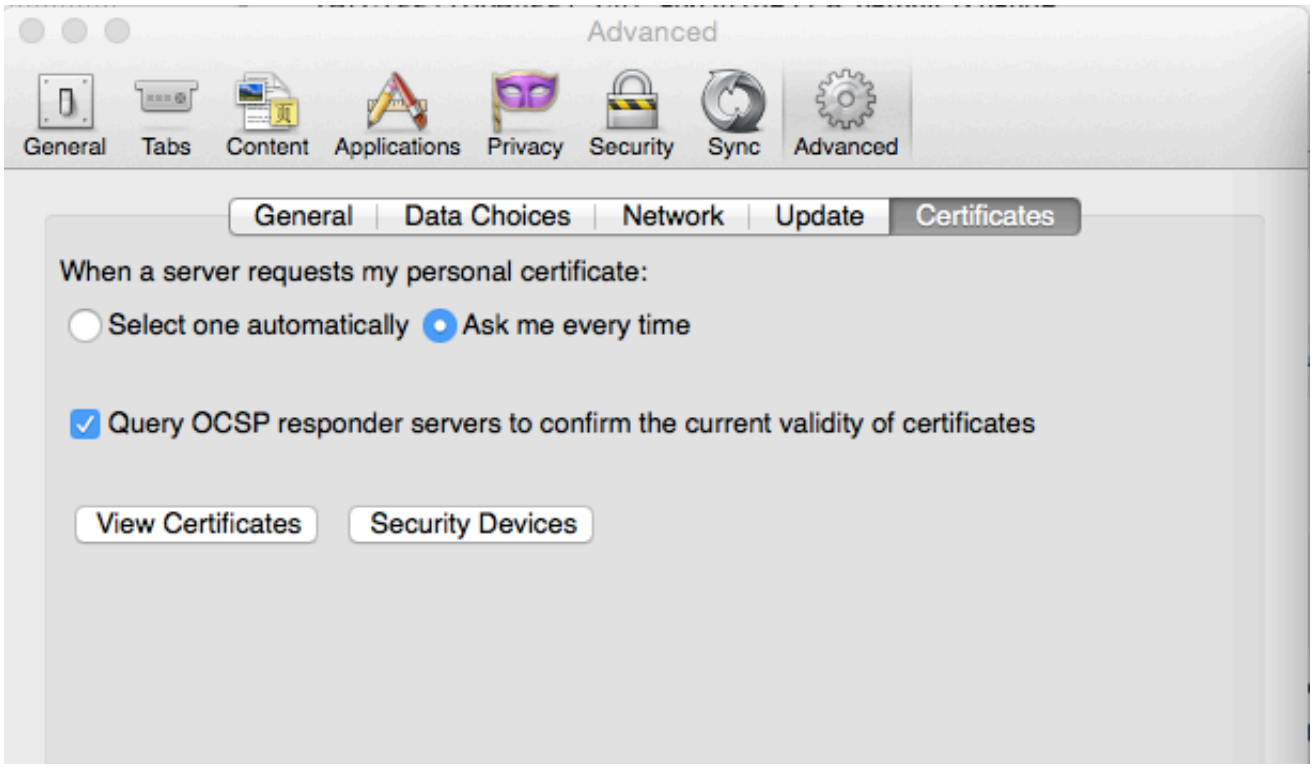


g. Click the "Yes" button. My self-signed certificate will be installed as a trusted root certificate.

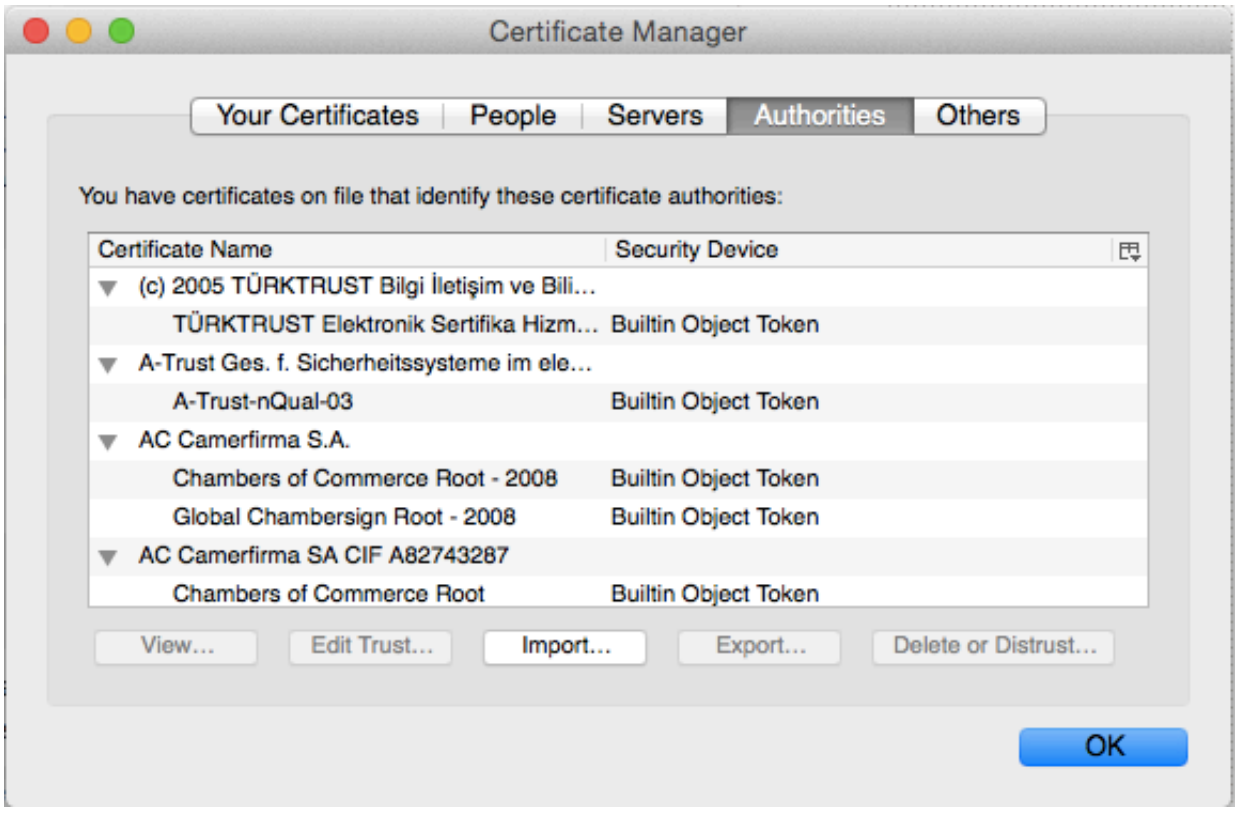
2. Mozilla Firefox:

a. 1. Run Mozilla Firefox and click the "Preference" menu. The Preferiece Options dialog box shows up.

b. Click the "Advanced" > "Certificates" tab. The Certificates dialog box shows up.

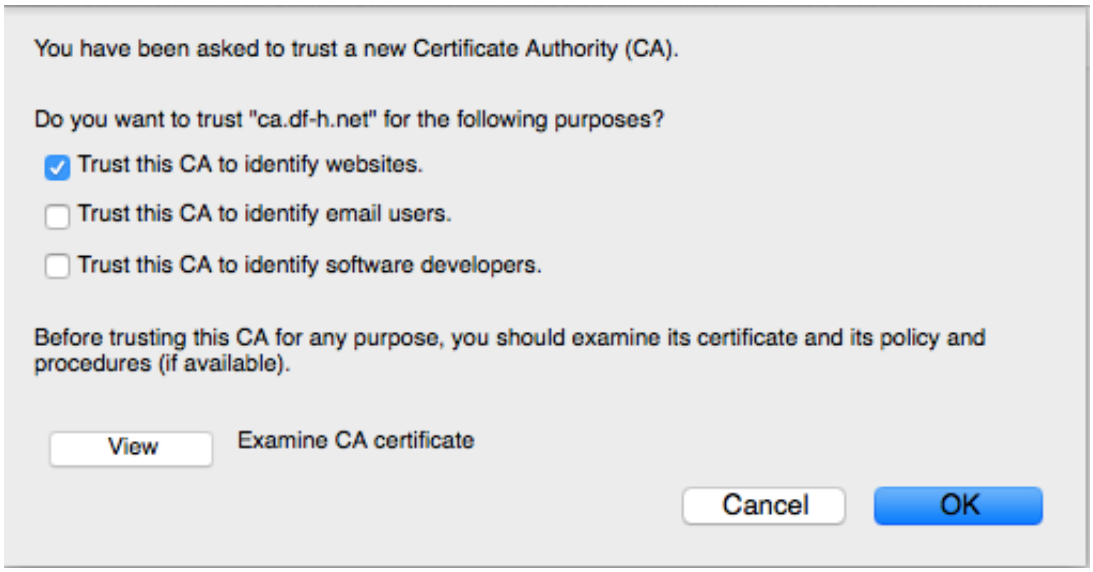


c. Click the "View Certificates" > "Authorities".



d. Use the "Import" button to find and select cacert.pem. Then click the "Next" button. The Certificate Store step shows up.

e. Select "Trust this CA to identify websites" and click ok.



Try to browse the site over https. Now it should not give any certificate error as you trust the CA.

```
***END OF EXERCISE***
```