LAB :: Secure HTTP traffic using Secure Sockets Layer (SSL) Certificate

- In this example we are using apnictraining.net as domain name.
- # super user command.
- $ normal user command.
- X 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]
[group3.apnictraining.net] [192.168.30.3]
......
[group10.apnictraining.net] [192.168.30.10]
[group11.apnictraining.net] [192.168.30.11]     [group12.apnictraining.net] [192.168.30.12]
......
[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 wll 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. Your laptop can properly resolve groupX.apnictraining.net
2. Check apache server is installed and configured. please try browsing groupX.apnictraining.net
3. Check openssl installed and check it's version `# openssl version`

Step 1

Generate Certificate Signing Request (CSR)

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

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

This will ask for few question:

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

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

You can now enter your passphrase. For best security, it should at least contain eight characters. 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/
groupX.apnictraining.net.csr
groupX.apnictraining.net.key
```

groupX.apnictraining.net.csr is the CSR file which we will send to CA. groupX.apnictraining.net.key the private key.

Step 2

Send the groupX.apnictraining.net.csr file for CA. Wait for CA to reply back the signed certificate.

Ask your instructor for the email address. Instructor will sign your CSR and generate

certificate for you

Step 3

Download your certificate to the server.

```
# cd /etc/ssl/
# wget http://192.168.30.54/cert/groupXX.apnictraining.net.crt
```

[replace XX with your group no]

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

Enable SSL in APACHE

```
# sudo a2enmod ssl

# 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/groupX.apnictraining.net.crt
SSLCertificateKeyFile /etc/ssl/groupX.apnictraining.net.key
```

[replace X 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
```

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

Step 4

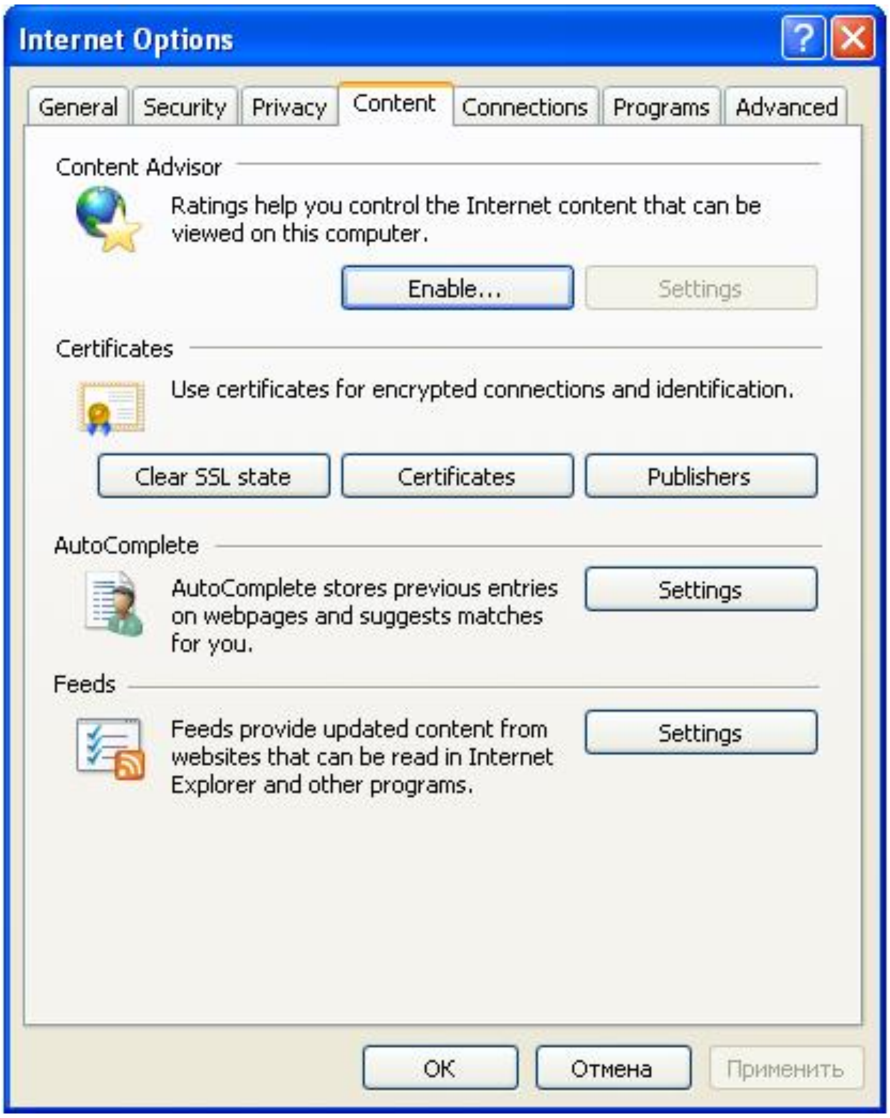
Ask your instructor to provide you the CA server root certificate.

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.



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates for encrypted connections and identification.

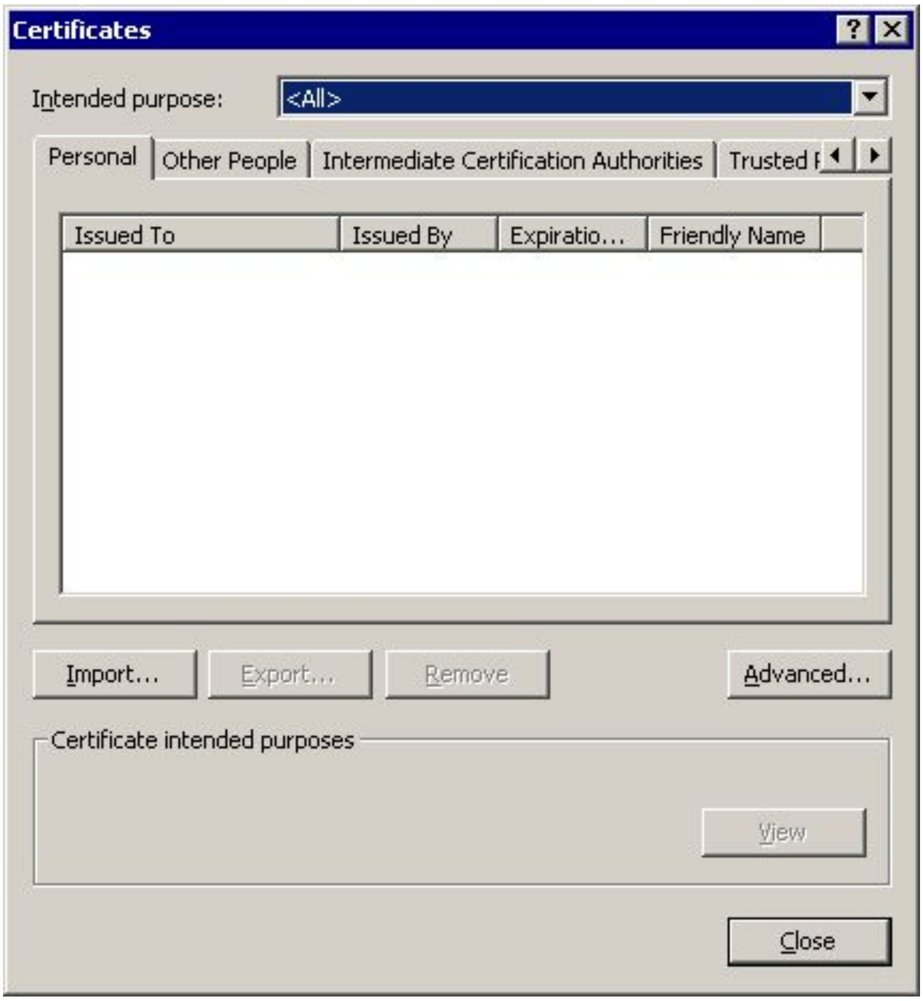
AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds

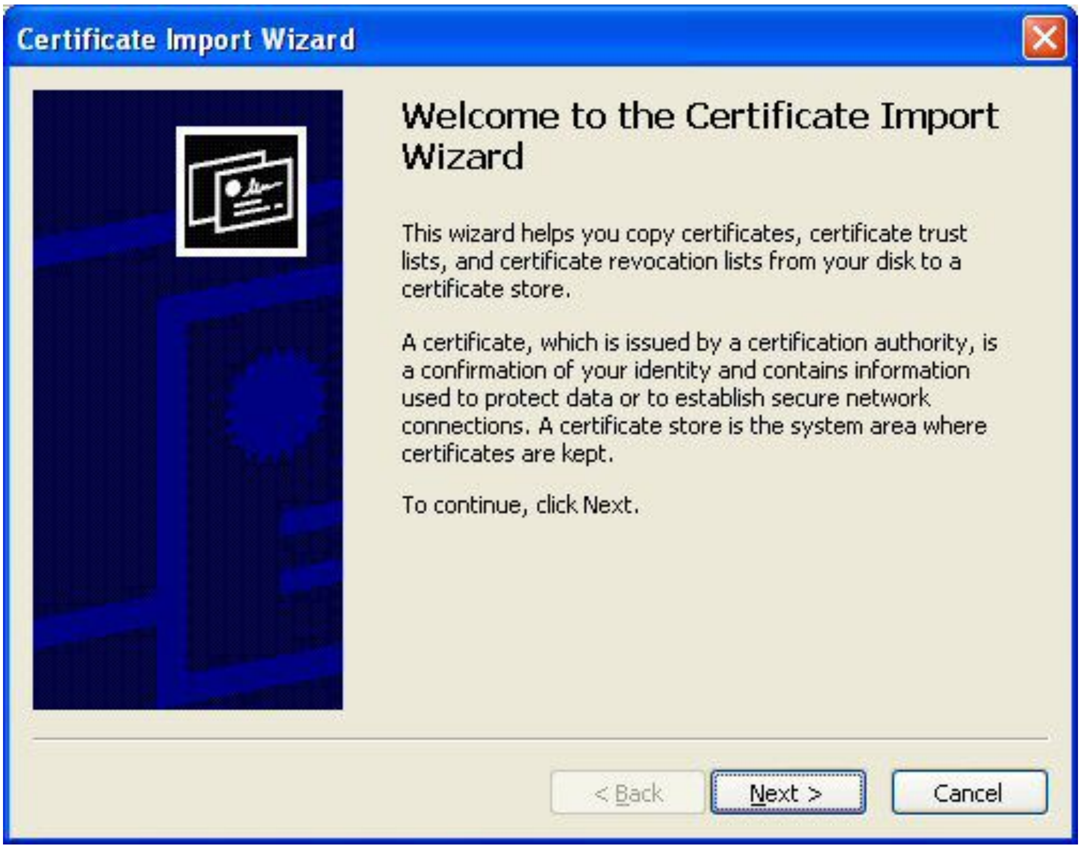
Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

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



Intended purpose: <All>

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



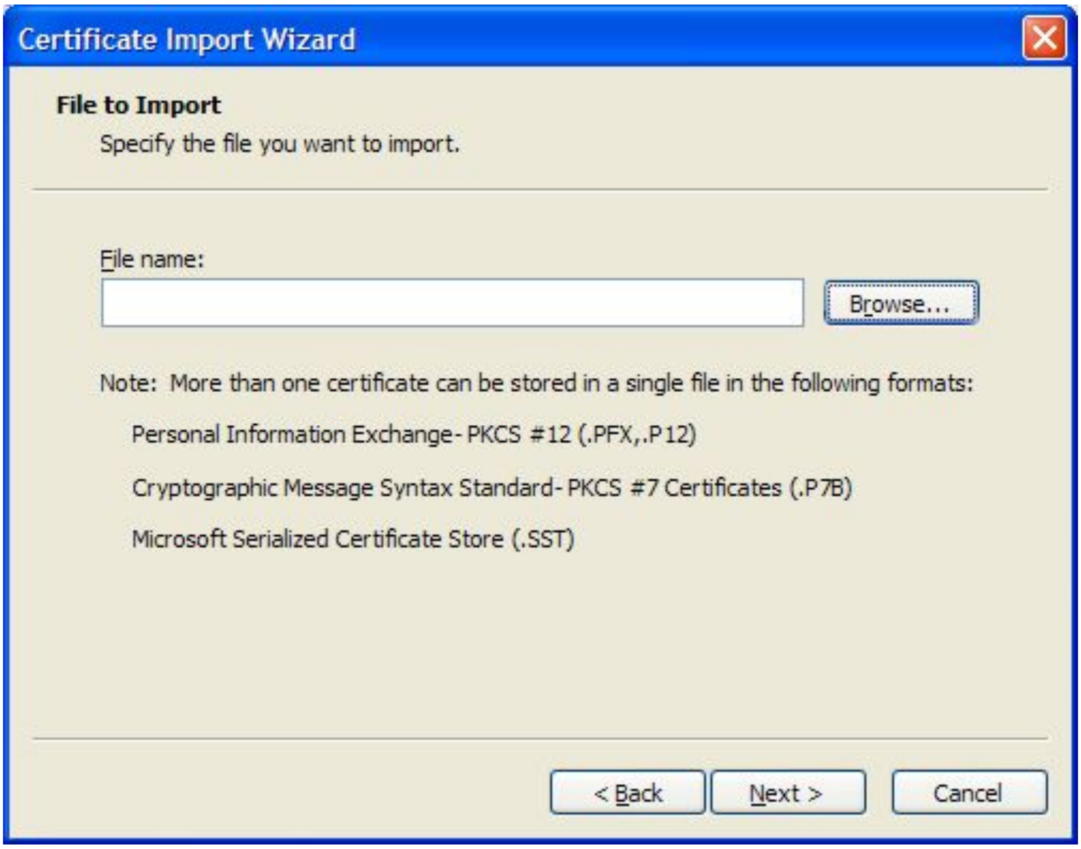
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

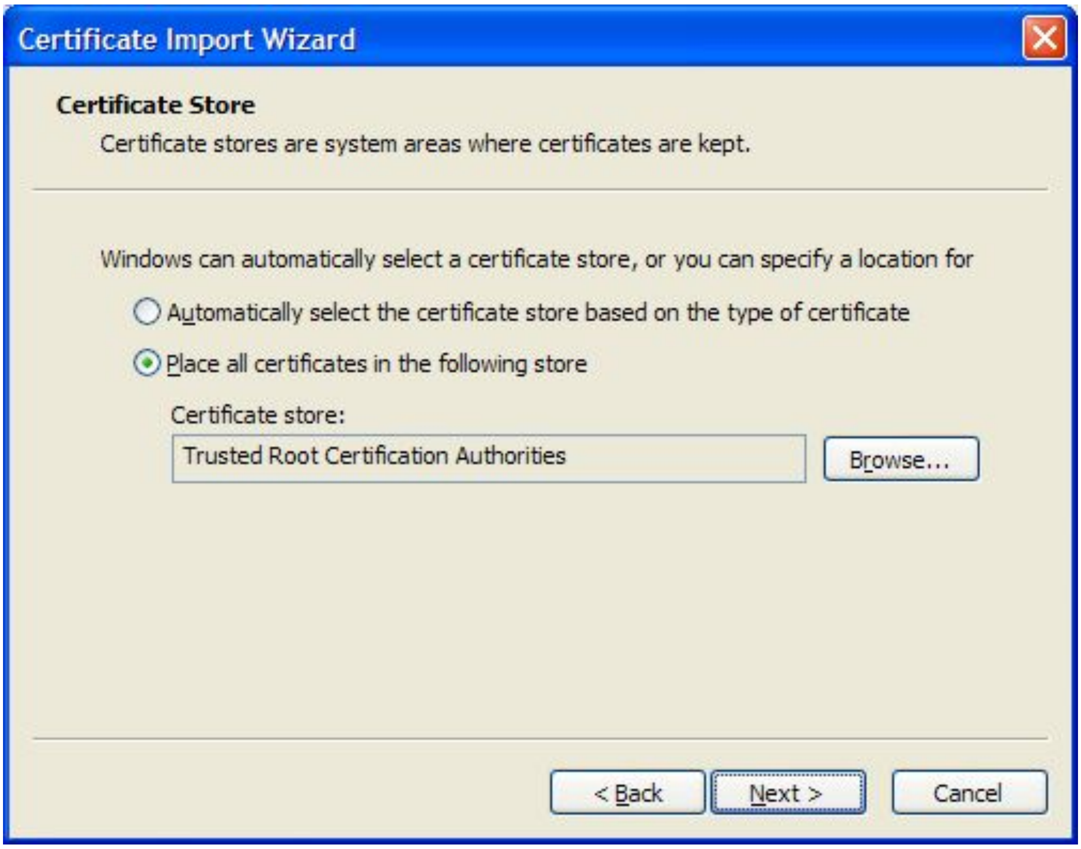
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

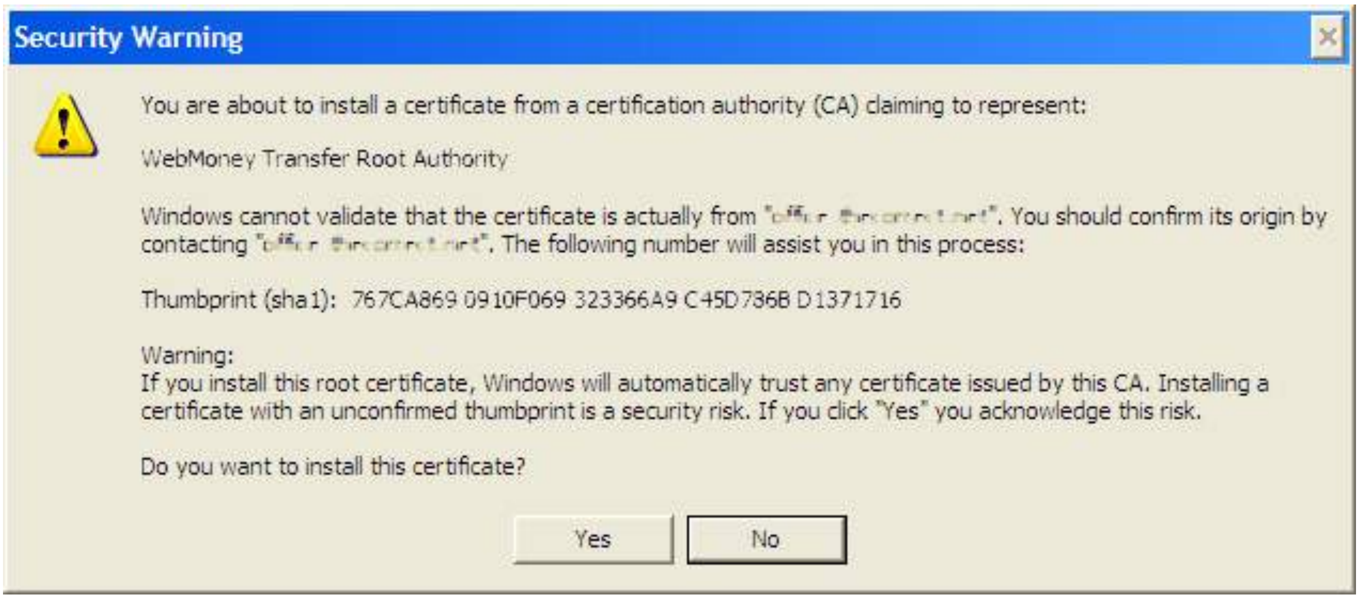
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

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



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

WebMoney Transfer Root Authority

Windows cannot validate that the certificate is actually from "[illegible]". You should confirm its origin by contacting "[illegible]". The following number will assist you in this process:

Thumbprint (sha1): 767CA869 0910F069 323366A9 C45D786B D1371716

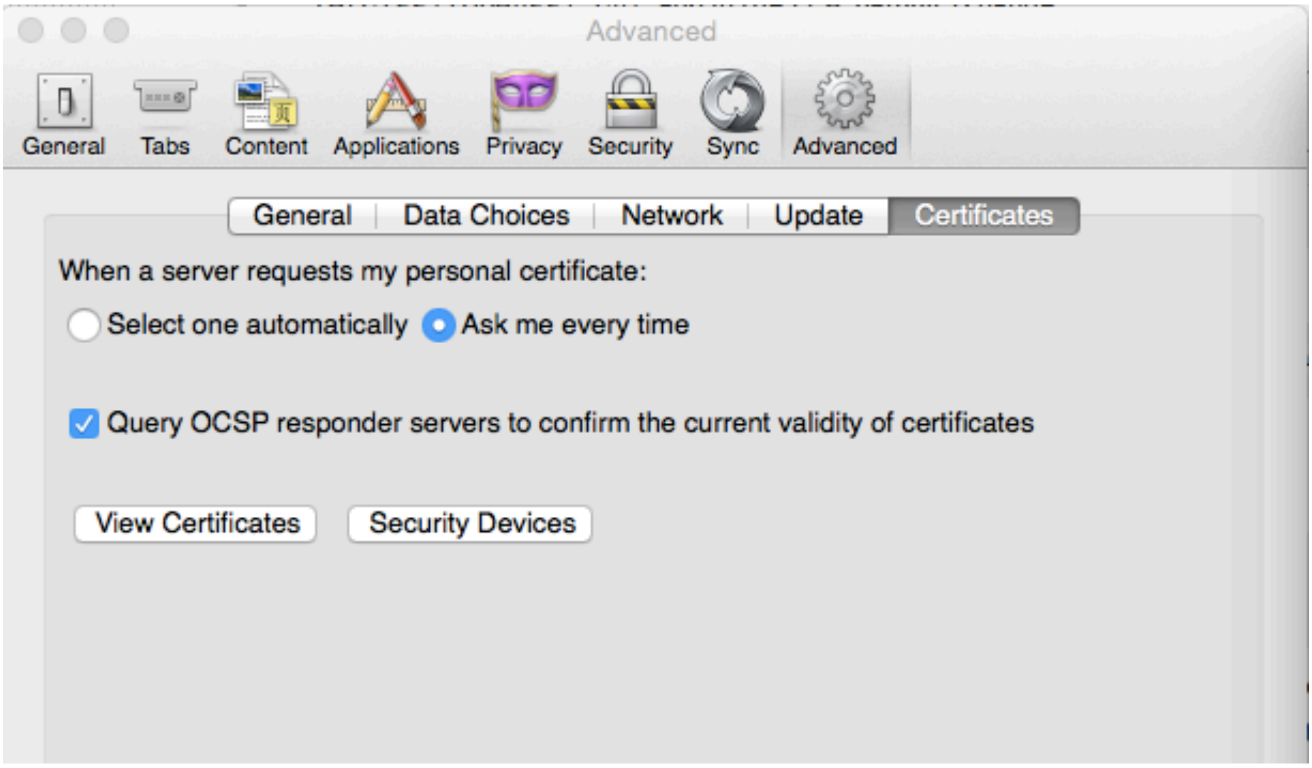
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this 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.

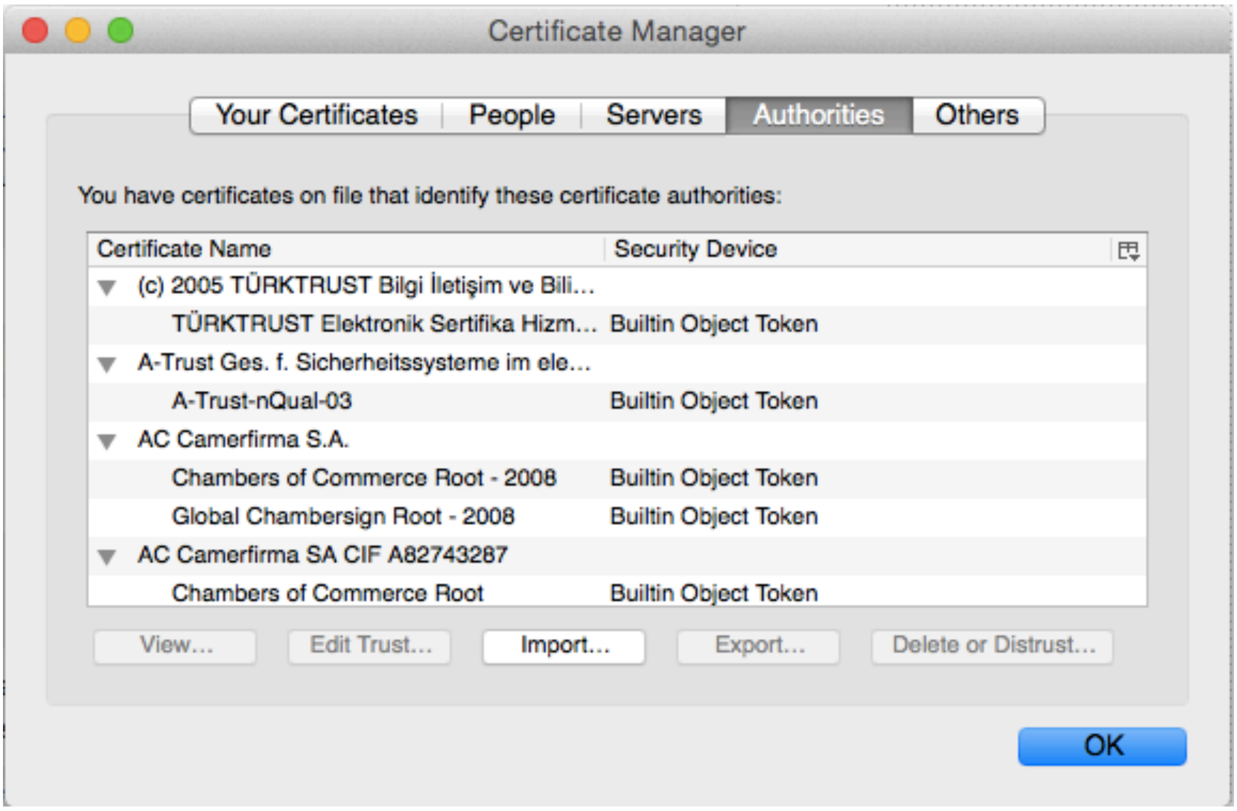


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

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

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

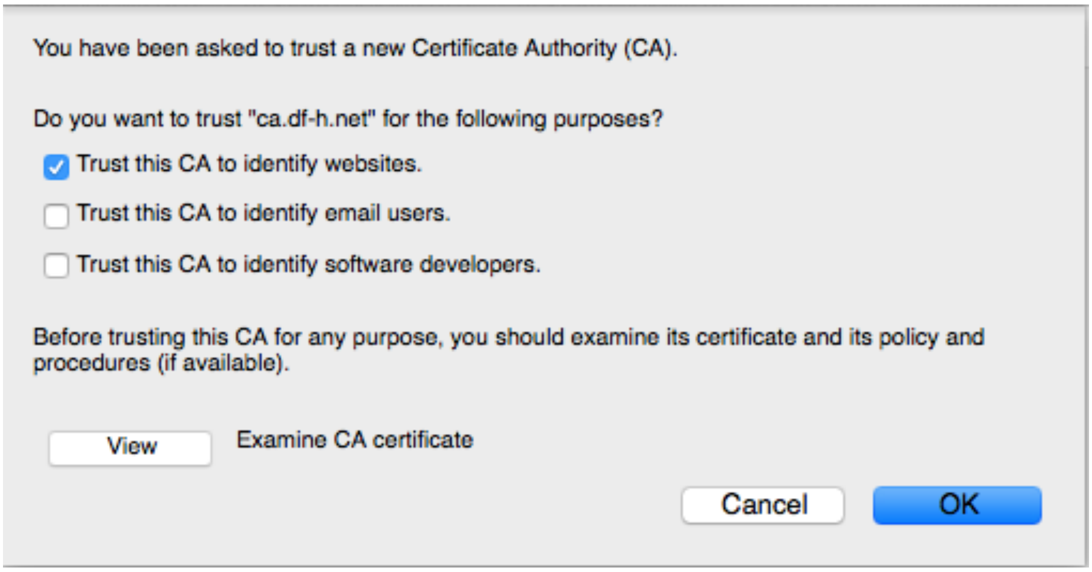


You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
▼ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bili…	
TÜRKTRUST Elektronik Sertifika Hizm…	Builtin Object Token
▼ A-Trust Ges. f. Sicherheitssysteme im ele…	
A-Trust-nQual-03	Builtin Object Token
▼ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▼ AC Camerfirma SA CIF A82743287	
Chambers of Commerce Root	Builtin Object Token

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.



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

Do you want to trust "ca.df-h.net" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

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

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

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