

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.
- N replace with your group no.
- Username `apricot` and password `security` / You already have ssh key to login.

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]
.....
[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 certificate, 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 certificate

Step 3: Enable SSL and configure Apache with the certificate

Requirements

1. Your laptop can properly resolve groupN.apnictraining.net
2. Check apache server is installed and configured. please try browsing groupN.apnictraining.net
3. Check openssl installed and check its version `# openssl version`. If `openssl` is not present do the following:

```
sudo apt-get update
```

```
sudo apt-get install openssl
```

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 N with your group no}:

```
sudo su
cd /etc/ssl
sudo 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]: VN
State or Province Name (full name) [Some-State]: HCMC
Locality Name (eg, city) [ ]: Saigon
Organization Name (eg, company) [Internet Widgits Pty Ltd]: APRICOT2017
Organizational Unit Name (eg, section) [ ]: WORKSHOP
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 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/
groupN.apnictraining.net.csr
groupN.apnictraining.net.key
```

`groupN.apnictraining.net.csr` is the CSR file which we will send to CA.

`groupN.apnictraining.net.key` the private key.

Step 2

Upload CSR to the CA server

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

It's all key based authentication. You don't need any password. If required password is be `security`

STOP

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

Step 3

Download your certificate to the server.

```
cd /etc/ssl/  
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
```

Enable SSL

```
sudo a2enmod ssl
```

Edit SSL configuration file and enable it.ss

```
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
```

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

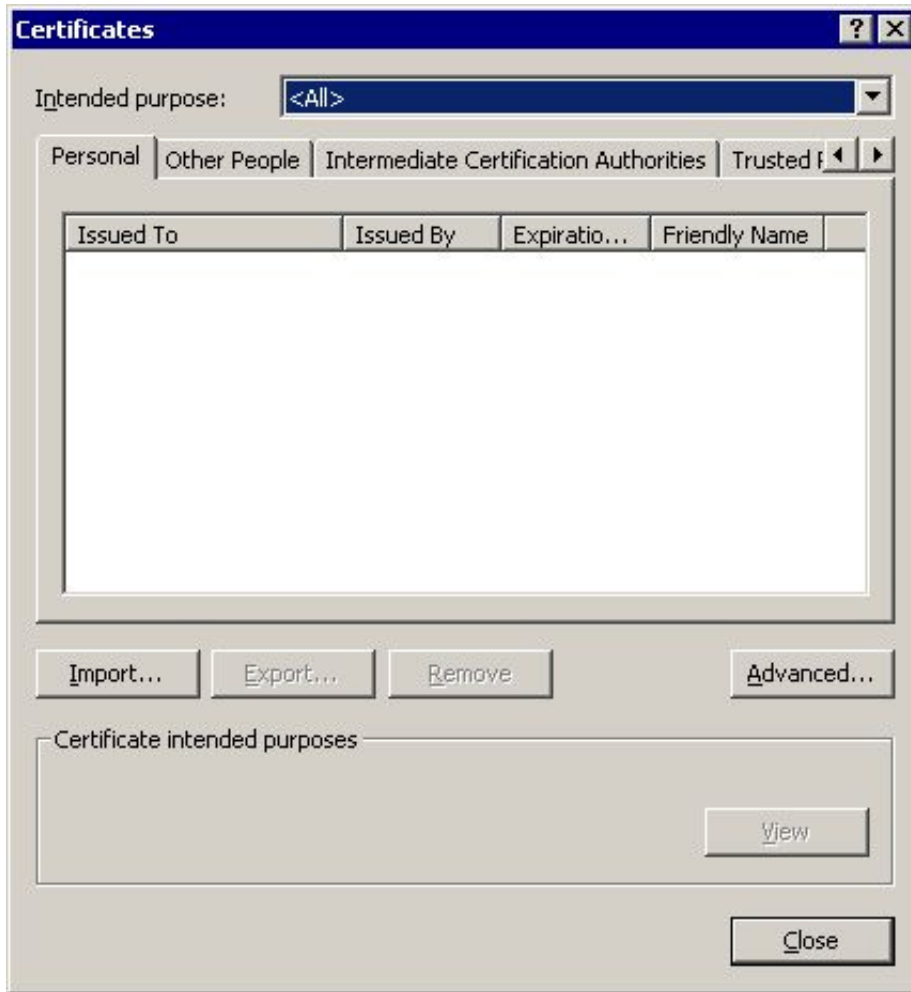
Import Certificate:

1. Internet Explorer:

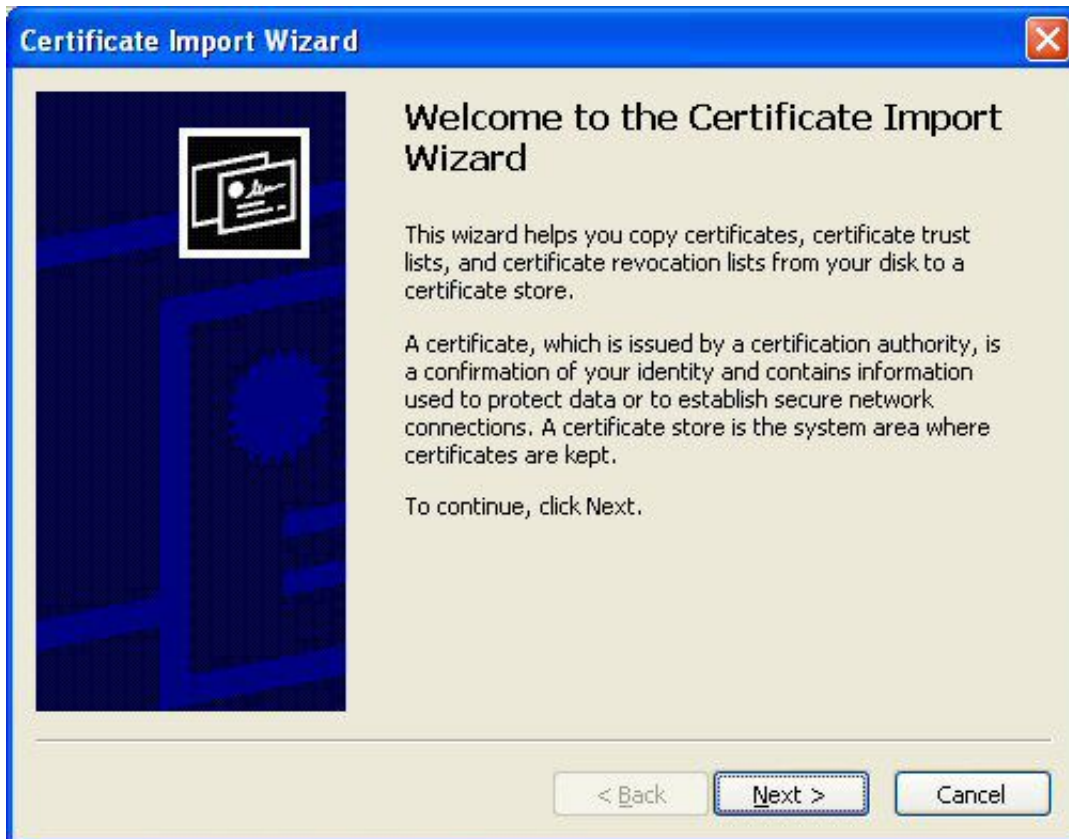
a. Run IE 9 and click the "Options" > "Internet Options" menu. The Internet Options dialog box shows up.



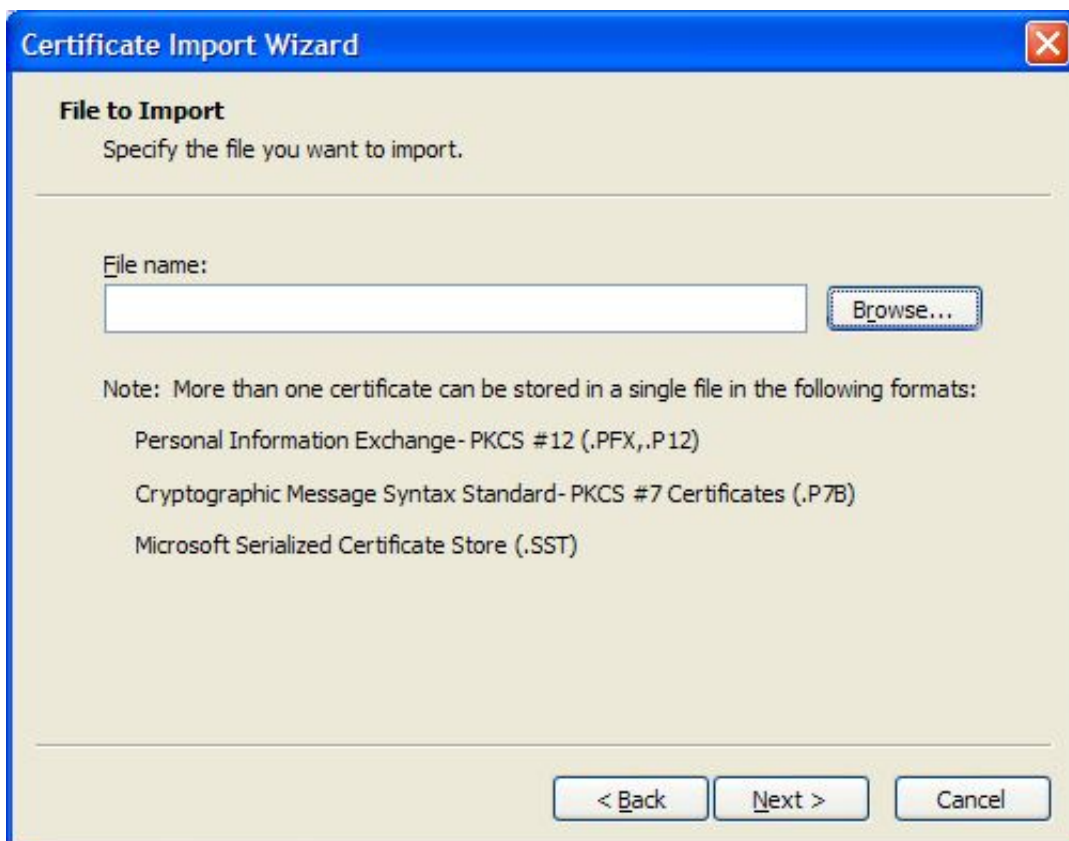
b. Click the "Content" tab and the "Certificates" button. The Certificates dialog box shows up.



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.



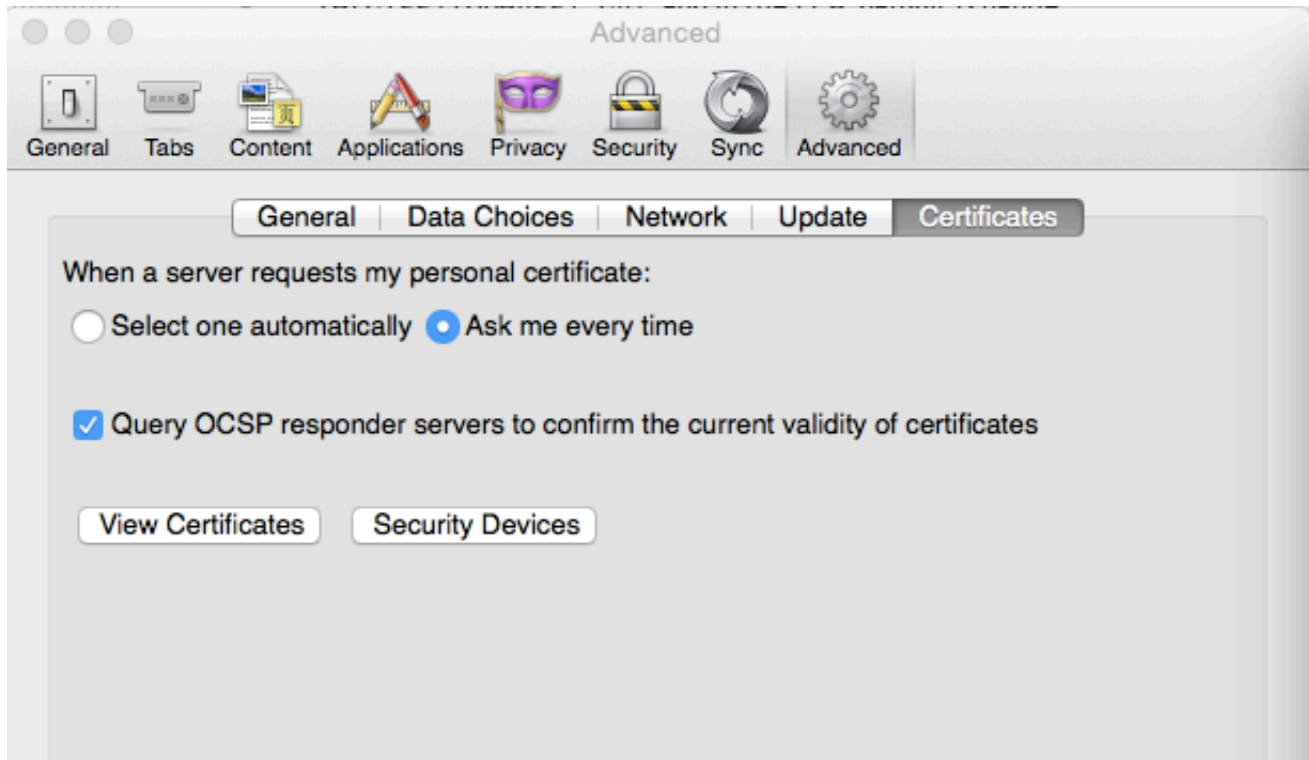
g. Click the "Yes" button. My self-signed certificate will be installed as a trusted root certificate.



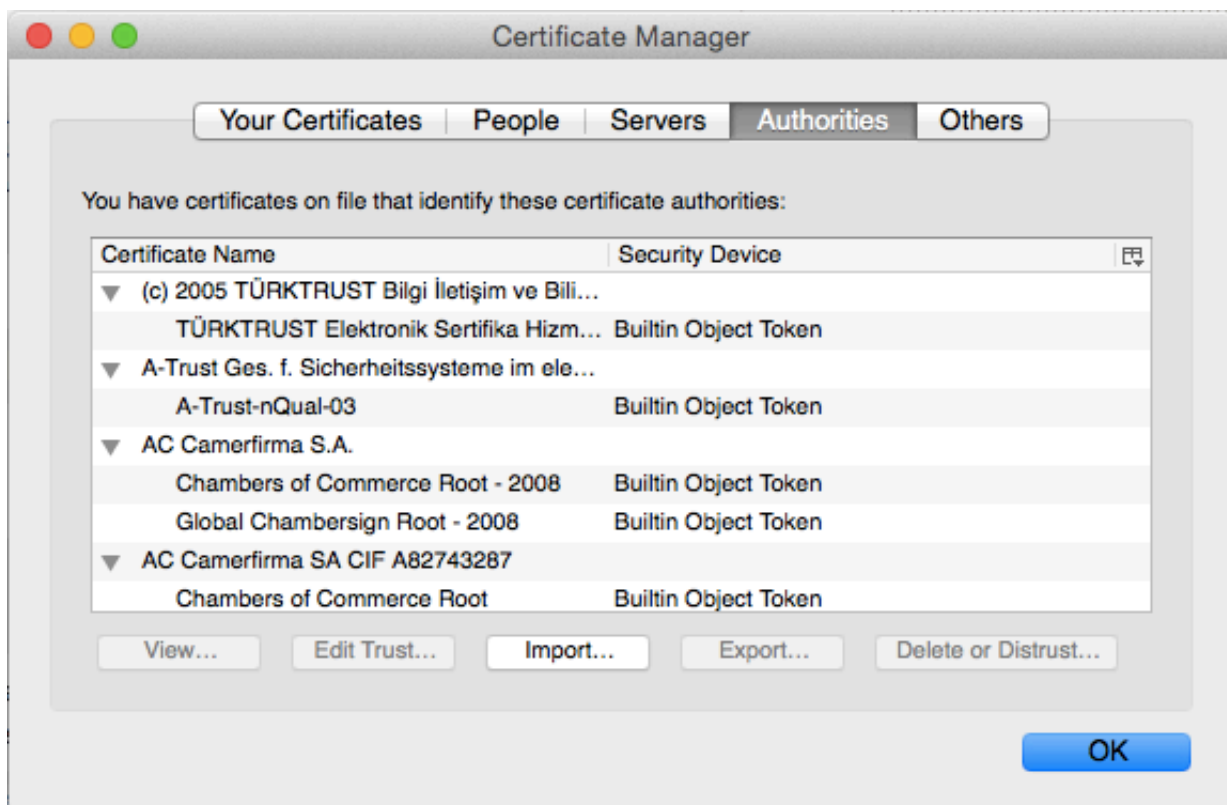
2. Mozilla Firefox:

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

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

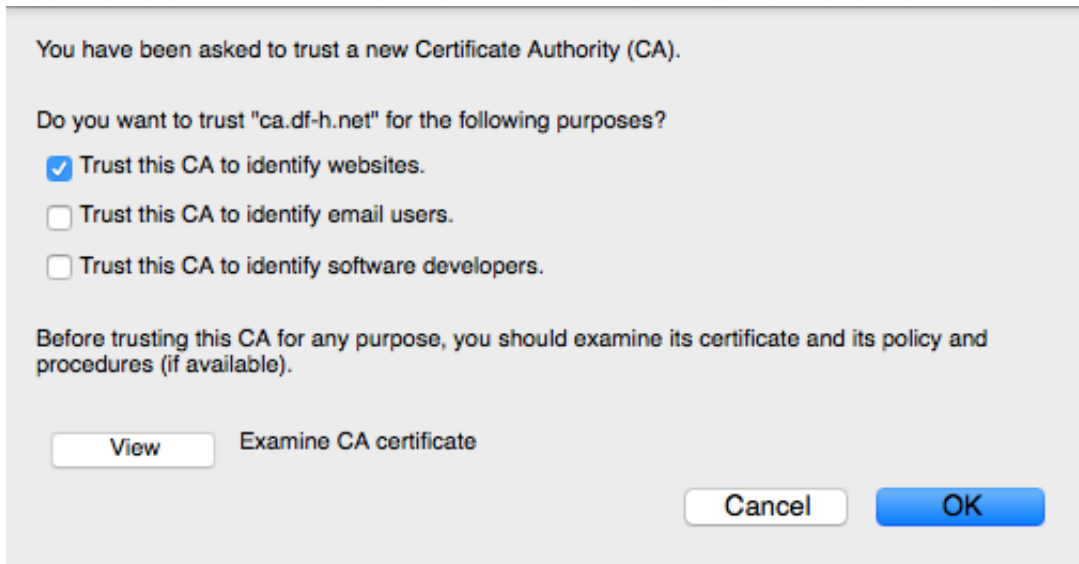


c. Click the "View Certificates" > "Authorities".



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