# PROTECTID

# Client Authenticated SSL Server Setup Guide for Apache Webservers

**Document:**
**MK-UM-02180405-01-ProtectIDclientAuthSSLsetupApache.doc**

SENTRY PM

**Before you use the protectID product, you must agree to the following terms.**

Any use or distribution of the protectID product requires that either you or your supplier have a licence from Sentry Project Management Pty Ltd.   Please contact your supplier or support@sentrypm.com for details.

Neither Sentry Project Management nor any other person who has been involved in the creation, production, or delivery of the Software shall be liable to the user or to any other person for any direct, incidental or consequential damages, even if Sentry Project Management has been advised of the possibility of such damages.

## Purpose

This document is intended to provide integration support for use of ProtectID smartcards or tokens (ref www.SENTRYpm.com) with client-authenticated SSL on Apache-based webservers.

This document describes setup of the Apache server and use of soft certificates at the client PC.  Once this setup is complete and the website access is satisfactory, contact Sentry for further advice on installation of Sentry's protectID smartcard- and USB token-based certificates.

The following procedures assume general familiarity with Microsoft Windows systems and the Apache webserver.

## Digital certificate client authentication on Apache web-server

This document assumed that you already downloaded Apache web-server on your Linux Red Hat 9 machine. You must logon as root or as a user with super-user privileges.  The following discussion is based on Apache V2.0.53.

To setup a digital certificate based client authentication on Apache web-server follow the instructions below:

1. Enable SSL on Apache web-server.
2. Install a server certificate on Apache web-server. You may obtain the certificate from an external Certification Authority or generate one using your own CA. The procedure to do the latter will be described in the document.
3. Configure Apache to request a client certificate for authentication.
4. Obtain client certificates from an external CA or generate your own client certificates.
5. Provide the certificate to a user in a .p12 file.
6. Install the CA certificate on a web-browser.
7. Install user/client certificate on a web-browser.

# 1 Enable SSL on Apache web-server

1. Build Apache web-server using "–enable-ssl" option among other options you wish to support. Follow the instructions in http://httpd.apache.org/docs-2.0/install.html.
2. Install Apache web-server. Follow the instructions in http://httpd.apache.org/docs-2.0/install.html.

# 2 Install a sever certificate on Apache web-server

Before you can install a server certificate you must obtain one from an external CA or generate a server cerificate using your own CA. The procedure to generate your own server certificate is described below.

1. Generate a self-signed CA certificate.
2. Generate a server certificate signed by own CA.
3. Configure Apache certificate store.
4. Start Apache web-server with SSL enabled

## 2.1 Generate a self-signed CA certificate

To generate a self-signed CA certificate do the followings:

1. Create a key-pair.

   ```
   # openssl genrsa –des3 –out ca.key 1024
   ```

   You will be asked to enter a pass phrase for protecting the key. You will be asked for it when you use it to sign a certificate request. Remember the pass-phrase! If you lost it, there is no way to retrieve the key.

2. Self-signing the CA key.

   ```
   # openssl req –new –x509 –days 365 –key ca.key –out ca.crt
   ```

   You will be asked to enter information you wish to appear on the certificate. It's worth noting that the common name CN is usually a fully qualified domain name. If you don't have a domain name, you may enter your computer name, the word "localhost" or even the IP address of your machine. If you enter an IP address in this field, make sure your machine's IP address stays the same.

The self-signed CA certificate is now generated. This certificate will be used to sign the server certificate request.

## 2.2 Generate a server certificate signed by own CA

To generate a server certificate do the followings:

1. Generate a server key pair.

   ```
   # openssl genrsa –des3 –out server.key 1024
   ```

   You will be asked to enter a pass phrase for protecting the key. Remember the pass-phrase! If you lost it, there is no way to retrieve the key.

2. Generate a certificate request.

   ```
   # openssl req –new –key server.key –out server.csr
   ```

   You will be asked to enter information you wish to appear on the certificate. See the section Generate a self-signed CA certificate for more details.

3. Sign the certificate request. This document assumed you already have a copy of sign.sh script located in the current directory[1].

   ```
   ./sign.sh server.csr
   ```

   You will be asked to enter the pass-phrase of the CA key. After you entered the pass-phrase you will be prompted a couple more times to confirm your intention to generate a certificate. Press ‘y’ to continue. After the signing was completed, the server certificate is generated and it is stored in a subdirectory called ca.db.certs. Do not delete this subdirectory or other files that start with “ca.db.”.

4. Move the CA certificate to a directory where you wish to keep it, let’s say /usr/ssl/cacert.crt subdir.

5. Move the CA key to a directory where you wish to keep it, let’s say /usr/ssl/cacert.key subdir.

6. Move the server certificate to a directory where you wish to keep it, let’s say /usr/ssl/ssl.crt subdir.

7. Move the server key to a directory where you wish to keep it, let’s say /usr/ssl/ssl.key subdir.

### 2.3 Configure Apache certificate store

To configure the certificate store you need to edit the ssl.conf file ( Under Apache V2.0.53 the SSL section is stored in a separate include file ssl.conf).

```
<VirtualHost _default_:443>

SSLEngine on

#   Server Certificate:
SSLCertificateFile /usr/ssl/ssl.crt/server.crt
#   Server Private Key:
SSLCertificateKeyFile /usr/ssl/ssl.key/server.key
#   Server Certificate Chain:
SSLCertificateChainFile /usr/ssl/cacert.crt/ca.crt
#   Certificate Authority (CA):
SSLCACertificatePath /usr/ssl/cacert.crt
SSLCACertificateFile /usr/ssl/cacert.crt/ca.crt

</VirtualHost>
```

[1] Note: sign.sh script is missing from the Apache distribution files. It can be found in mod_ssl distribution files under pkg.contrib/ subdir.

## 2.4 Start Apache web-server with SSL enabled

**To start Apache web-server with SSL enabled:**

1. Change to the directory where Apache is installed.
2. # bin/apachectl –DSSL –f conf/httpd.conf
   You will be asked to enter the pass-phrase for the server key.

# 3 Configure Apache to authenticate a client using a digital certificate

To configure Apache web-server to verify a client based on a digital certificate you need to edit the ssl.conf file in the following section.

```
<VirtualHost _default_:443>

#   Client Authentication (Type):
#   Client certificate verification type and depth.  Types are
#   none, optional, require and optional_no_ca.  Depth is a
#   number which specifies how deeply to verify the certificate
#   issuer chain before deciding the certificate is not valid.
SSLVerifyClient require
SSLVerifyDepth  1

</VirtualHost>
```

Restart Apache for the new configuration to take effect

Apachectl –k graceful

# 4 Obtain client certificates from an external CA or generate your own client certificates

This section describes the procedure to generate client certificates signed by your own CA.

To generate a client certificate follow the steps below:

1. Generate a key-pair.

   ```
   # openssl genrsa –des3 –out name.key 1024
   ```

   You will be asked to enter a pass phrase for protecting the key. Remember the pass-phrase! If you lost it, there is no way to retrieve the key.

2. Generate a certificate request

   ```
   # openssl req –new –key name.key –out name.csr
   ```

   You will be asked to enter information you wish to appear on the certificate. The common name is the name that will appear in the dialog box, when the browser asks you to select a certificate from the certificate store. Enter a name which clearly identifies the user to avoid any confusion in the future.

3. Sign the certificate request.

   ```
   ./sign.sh name.csr
   ```

   You will be asked to enter the pass-phrase of the CA key. Press ‘y’ when you are asked. After the signing was completed, the server certificate is generated and it is stored in a subdirectory called ca.db.certs. Do not delete this subdirectory or other files that start with “ca.db.”

   Note that the sign.sh script is missing from the Apache distribution files. It can be found in mod_ssl distribution files under pkg.contrib/ subdir.

4. Export the certificate into a PKCS#12 format file.

   ```
   # openssl pkcs12 –export –in name.crt –out name.p12 –inkey name.key
   ```

   You will be asked to enter the pass-phrase for the key and also a password to protect the exported certificate.

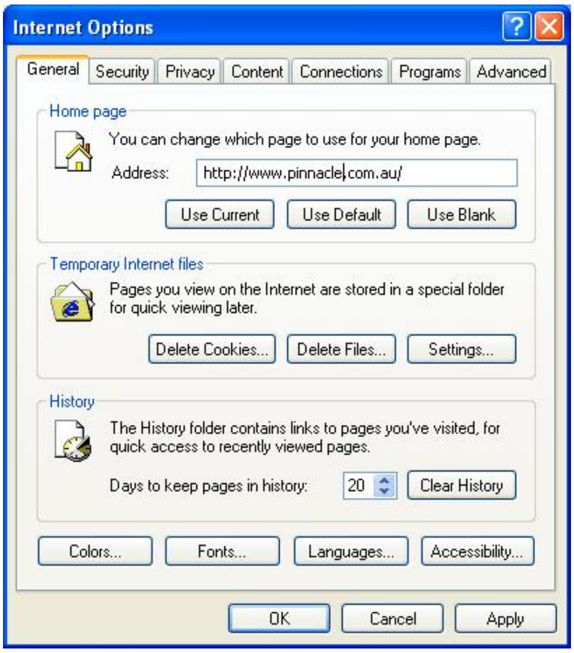
5. Provide this .p12 file to the user to be installed on his/her web-browser.

# 5 Install a CA root certificate on a web-browser

The following procedure assumed that you already obtained or generated a CA root certificate and it is stored in a .crt file. See section 2.1 for details on generating a self-signed CA root certificate.

## 5.1 Install a CA root certificate on MS-IE6

1. Start Internet Explorer
2. Click **Tools** menu and select **Internet Options…**
   Internet Options dialog box is opened.



You can change which page to use for your home page.

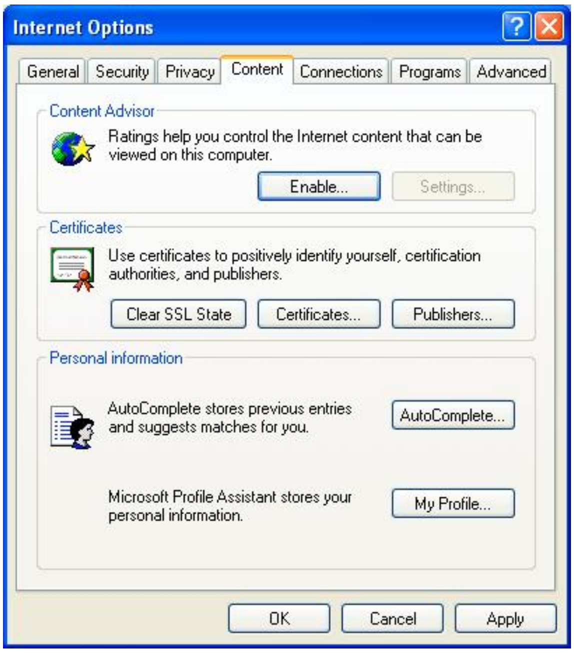
Address: http://www.pinnacle.com.au/

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

3. Click the **Content** tab.



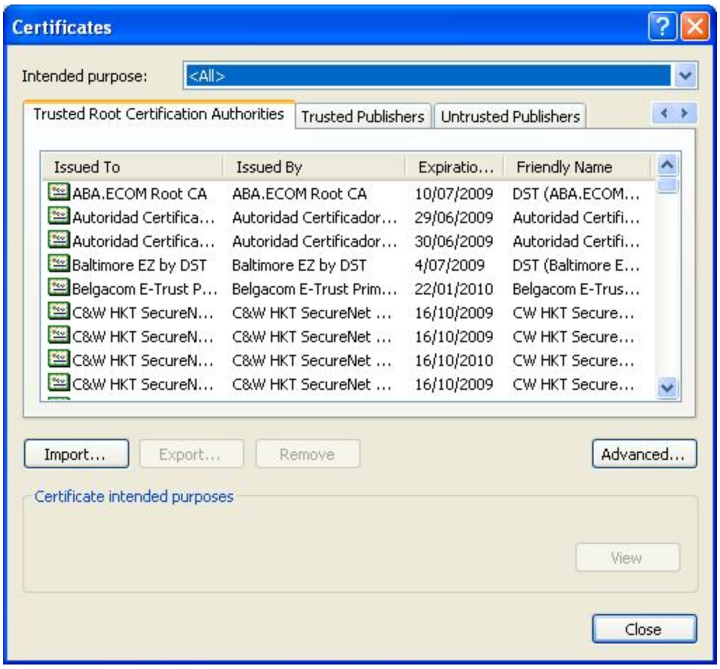
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

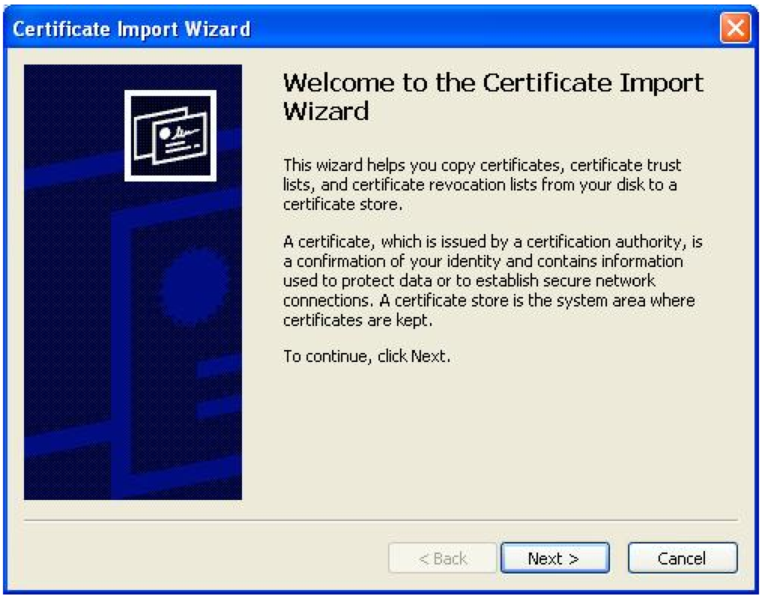
4. Click **Certificates..** button in the Certificates section. The Certificates… dialog box is opened.



Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| ABA.ECOM Root CA | ABA.ECOM Root CA | 10/07/2009 | DST (ABA.ECOM... |
| Autoridad Certifica... | Autoridad Certificador... | 29/06/2009 | Autoridad Certifi... |
| Autoridad Certifica... | Autoridad Certificador... | 30/06/2009 | Autoridad Certifi... |
| Baltimore EZ by DST | Baltimore EZ by DST | 4/07/2009 | DST (Baltimore E... |
| Belgacom E-Trust P... | Belgacom E-Trust Prim... | 22/01/2010 | Belgacom E-Trus... |
| C&W HKT SecureN... | C&W HKT SecureNet ... | 16/10/2009 | CW HKT Secure... |
| C&W HKT SecureN... | C&W HKT SecureNet ... | 16/10/2009 | CW HKT Secure... |
| C&W HKT SecureN... | C&W HKT SecureNet ... | 16/10/2010 | CW HKT Secure... |
| C&W HKT SecureN... | C&W HKT SecureNet ... | 16/10/2009 | CW HKT Secure... |

5. Click the **Trusted Root Certification Authorities** tab and click the **Import…** button. It starts the Certificate Import Wizard.



Welcome to the Certificate Import Wizard

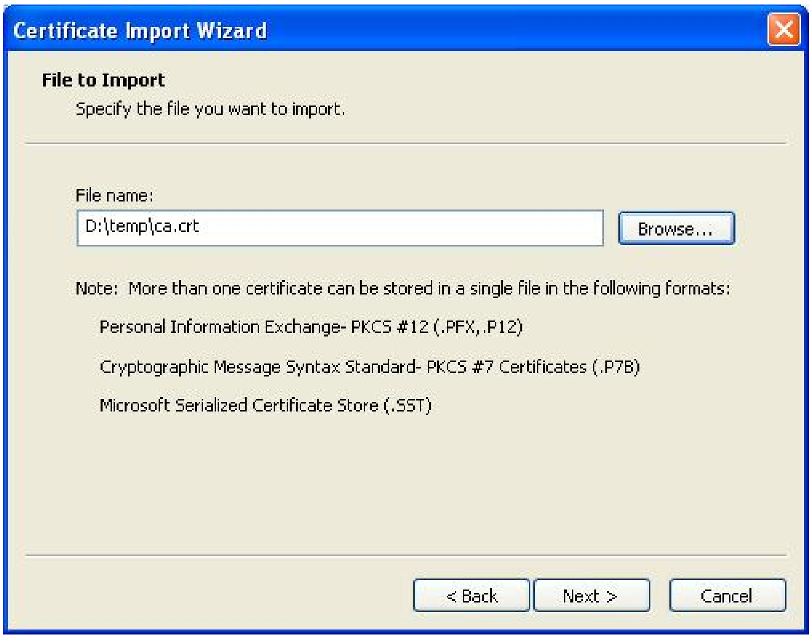
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

Click Next to go past the Welcome screen.

6. Enter the path and file name of the file that contains the response from the CA, and then click **Next**. The example below will read the certificate from D:\temp directory.



Certificate Import Wizard

**File to Import**

Specify the file you want to import.

File name:

D:\temp\ca.crt

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

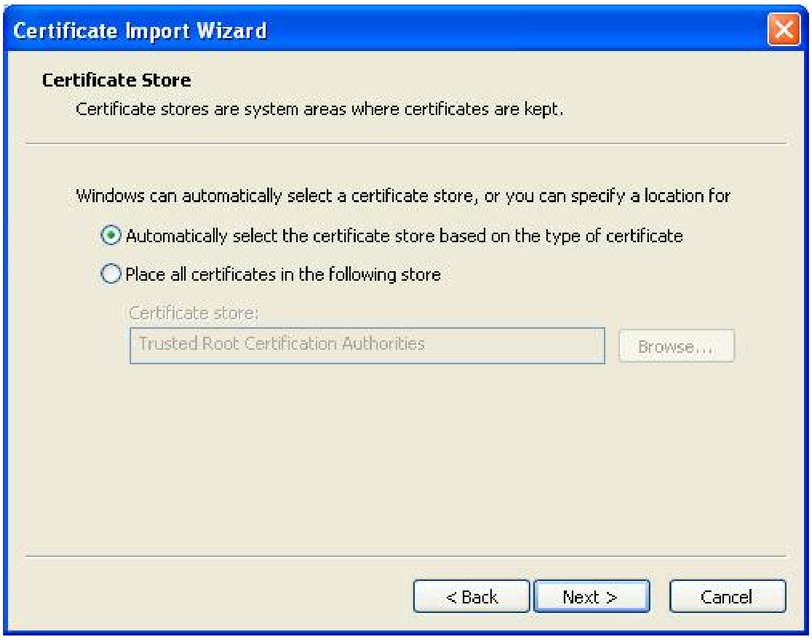
Personal Information Exchange- PKCS #12 (.PFX,.P12)

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

Microsoft Serialized Certificate Store (.SST)

Note: For certificates stored in PKCS#12 format, enter the password used to protect the exported certificate, not the pass-phrase that is used to protect the private key and click **Next**. In addition you may select to Enable strong private key protection and to mark this key as exportable. At the moment we just leave them unchecked.

7. On the next screen select Automatically select the certificate store…… and click **Next**.



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

8. Click **Finish** on the next screen to complete the Certificate Import Wizard.

### 5.2 Install a CA root certificate on Opera 7.54

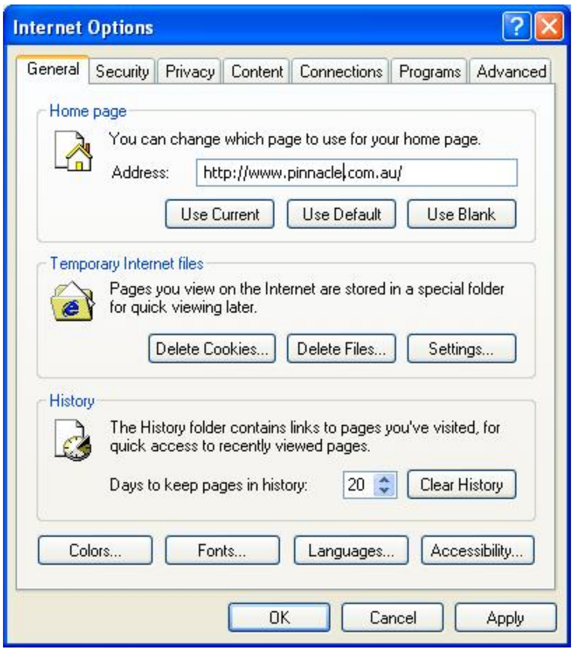
1. Start Opera web-browser
2. Click **Tools** menu and select **Preferences…**
3. In the left pane, select Security…
4. Click **Manage Certificates…** button. A dialog box is opened.
5. Click **Authorities** tab and click the **Import** button.
6. The Import certificates dialog box is opened. Select the CA certificate file that you wish to import and click **Open**.
7. The Install authority certificate dialog box is opened. Select the certificate from the list-box and click **Install** button.
8. You will be prompted to verify, whether you trust the CA. Click **Yes.**

# 6 Install client certificates on a web-browser

The section assumed that you have obtained a client certificate from an external CA or you have generated a client certificate from your own CA. It further assumed that the client certificate is stored in PKCS#12 format.

## 6.1 Install client certificates on MS-IE6

1. Start Internet Explorer
2. Click **Tools** menu and select **Internet Options…**
   Internet Options dialog box is opened.



You can change which page to use for your home page.

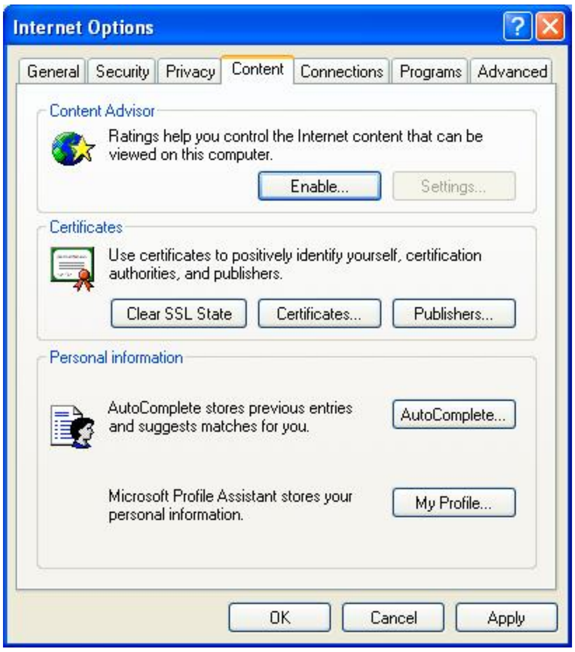
Address: http://www.pinnacle.com.au/

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

3. Click **Content** tab



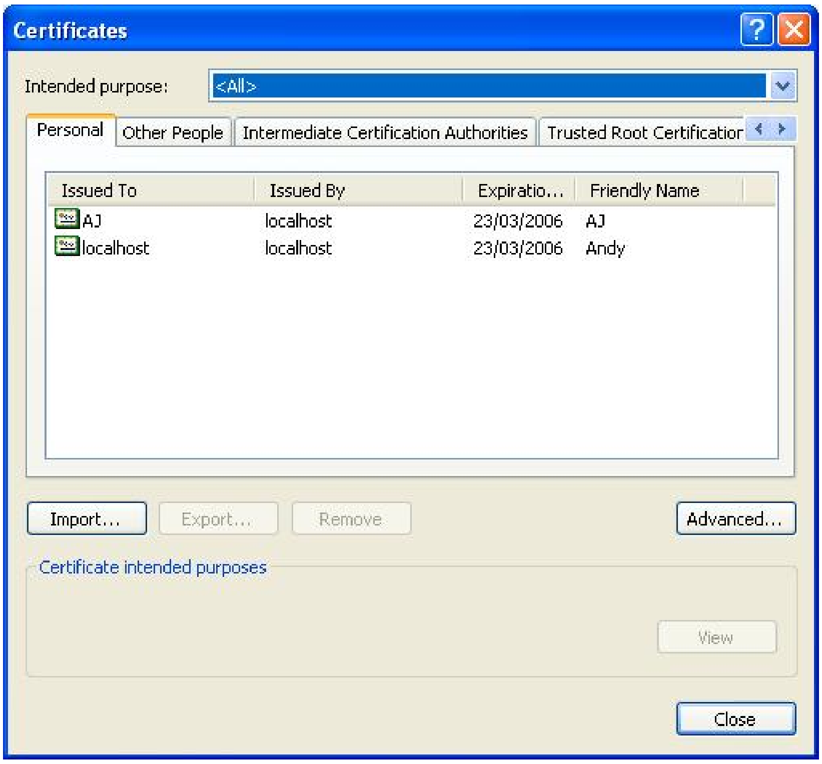
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

4. Click **Certificates..** button in the Certificates section. The Certificates… dialog box is opened.

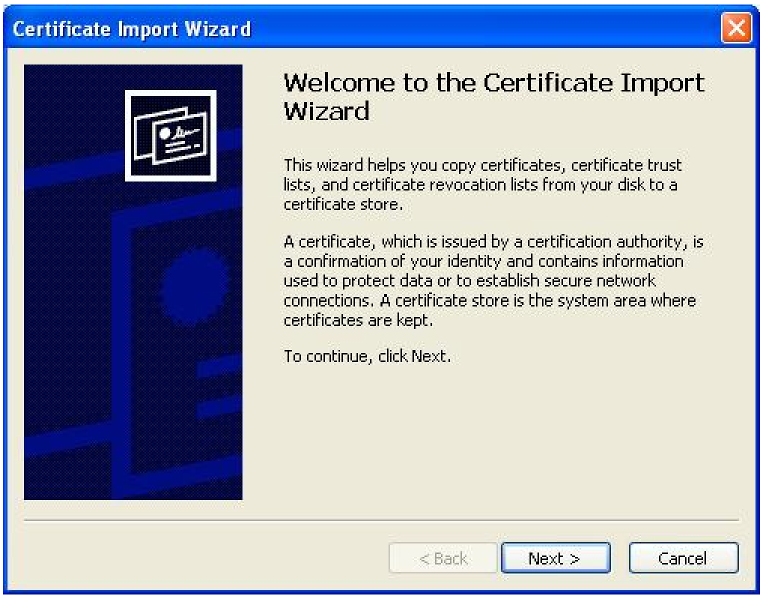


Certificates
Intended purpose:
<All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import…
Export…
Remove
Advanced…
Certificate intended purposes
View
Close

| Issued To | Issued By | Expiratio… | Friendly Name |
|---|---|---|---|
| AJ | localhost | 23/03/2006 | AJ |
| localhost | localhost | 23/03/2006 | Andy |

Click **Personal** tab and click the **Import…** button. It starts the Certificate Import Wizard.

5. Click Next to go past the welcome screen.



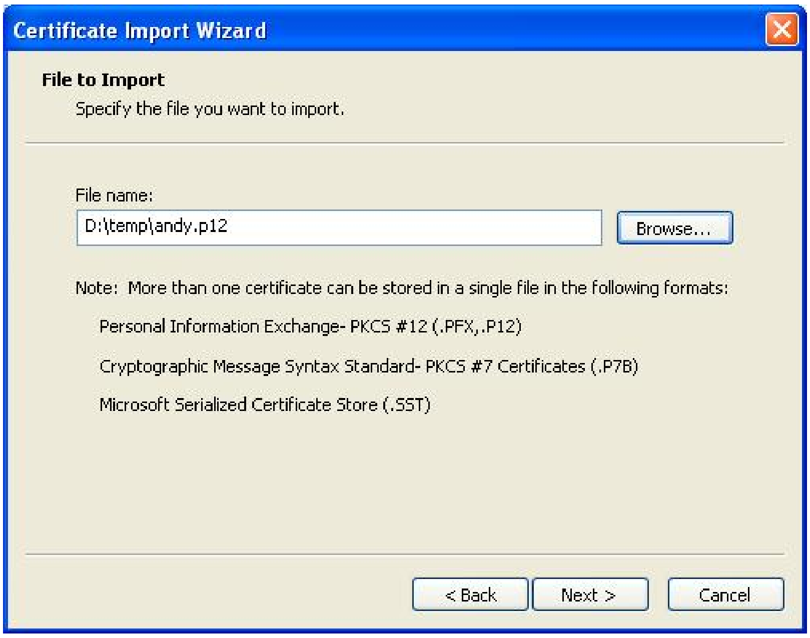
Welcome to the Certificate Import Wizard

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.

6. Enter the path and file name of the file that contains the client certificate, and then click **Next**. The example below will read the certificate from D:\temp directory.



Certificate Import Wizard

**File to Import**

Specify the file you want to import.

File name:

D:\temp\andy.p12

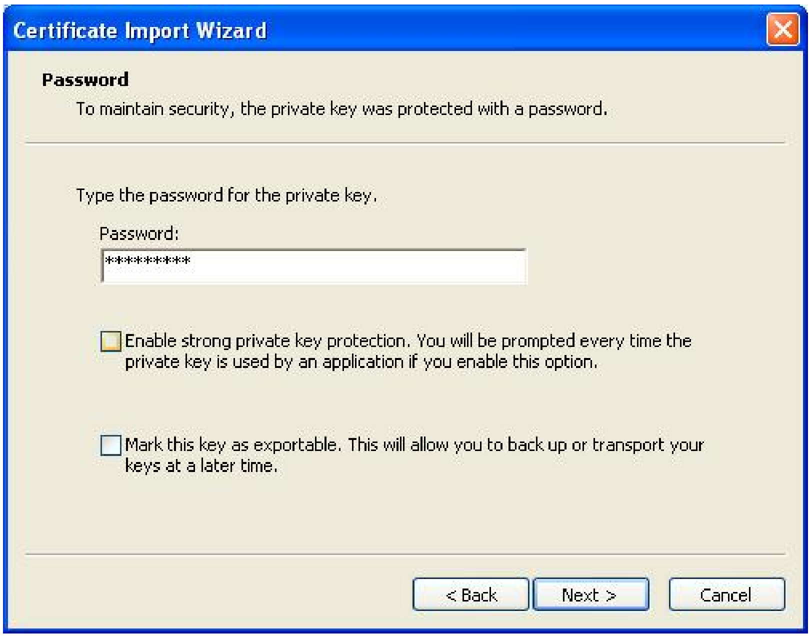
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

7. Enter the password used to protect the exported certificate, not the pass-phrase that is used to protect the user key and click **Next**.



Certificate Import Wizard

**Password**

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

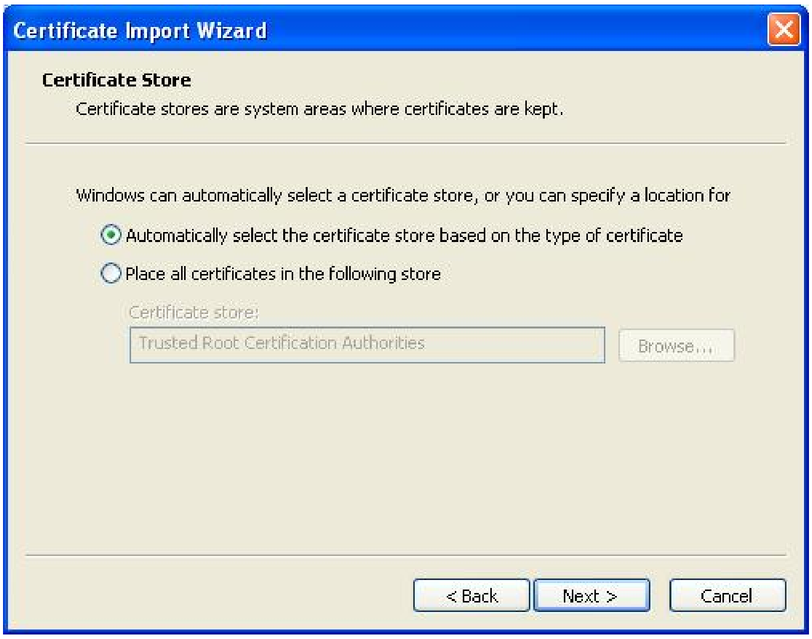
**********

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

In addition you may select to Enable strong private key protection and to mark this key as exportable. At the moment we just leave them unchecked.

8. On the next screen select **Automatically select the certificate store based on the type of certificate** and click **Next**.



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

9. On the next screen click **Finish** to complete the Certificate Import Wizard.

## 6.2 Install client certificates on Opera 7.54

1. Start Opera web-browser
2. Click **Tools** menu and select **Preferences…**
3. In the left pane, select **Security…**
4. Click **Manage Certificates…** button.
5. The **Certificate Manager** dialog box is opened. Click **Personal** tab and click the **Import** button.
6. The Import certificates dialog box is opened. Select the user.p12 file and click **Open.**
7. You will be prompted to enter a password. Enter the password used to protect the exported certificate and click **OK**.
8. The **Import key and certificate** dialog box is opened. Select the certificate you wish to import, if it hasn’t been selected and click **OK**.
9. You will be prompted to enter a security password. Enter the master password as previously set in Opera browser and click OK.

To see your certificate, close the **Certificate Manager** dialog box and re-open the **Certificate Manager** dialog box by clicking **Manage Certificates…** button. I suspect this is a bug in Opera.