Dematerialized Securities System - Guidelines for client workstation setup

Version 1.0

10/03/2016

Contents

1. Requirements 3
1.1 Java Runtime Environment (JRE) 4
1.2 Browsers 5
1.3 Certificates 5
1.4 Adobe PDF Reader – Browser Plug-in 7
Appendix A - Installing ATHEX Certificates on Internet Explorer 8
Appendix B - Installing ATHEX Certificates on Firefox 26
Appendix C – Code Signing Certificates 41

1. Requirements

As a consequence of upgrading the DSS application in the new web-based environment (Oracle Forms 11gR2), user's access to the application is changing as well. The user interface is supported by means of a Java applet, which is accessible from a browser of the client workstation. Therefore, some configuration actions need to be performed on the workstation that is hosting the client application.

Prerequisites for supporting the application can be summarized in the following:

- Installing the Java Runtime Environment (JRE), a program that allows Java applications to be executed by a host computer.
- Installing one of the supported browsers.
- Installing the ATHEX certificates.
- Installing the Adobe PDF Reader and browser plug-in.

1.1 Java Runtime Environment (JRE)

According to the Oracle guidelines[1], for the supported setup of a client workstation that supports Forms 11gR2 applications, the minimum JRE edition that is applicable is version 1.6.0_10.

For installing the latest JRE edition, visit the Java download page and select the JRE Download option.

[1] http://www.oracle.com/technetwork/developer-tools/forms/oracle-forms-11gr2certmatrix-519680.xls

1.2 Browsers

The following browsers support the client application:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.6
- Firefox 5
- Safari 5

1.3 Certificates

The use of certificates[2], regarding the DSS application, spans over three layers of certification:

- Certification of the executable code, as well as the vendor of this code.
- Certification of the web server hosting the application (server authentication).
- Certification of the user of the application (client authentication), in cases where this is applicable.

Detailed instructions in order to install certificates for Internet Explorer are provided Appendix A and for Firefox in Appendix B of this document.

Certification of the executable code

The application's executable code is provided by two vendors, namely Oracle and ATHEXGroup, and is digitally signed certificates which are issued by VeriSign and Symantec

[2] For the well-functioning of certificates, communication between the client workstation and the certificate's vendor needs to be established, in order to confirm the non-revocation of a certificate by its issuer (certificate revocation list). As an indication, in the current implementation, the client workstation needs to have internet access to the following resources:
http://ocsp.verisign.com
http://s2.symcb.com
http://sv.symcd.com
http://sf.symcd.com
http://ocsp.athexgroup.gr
http://www.helex.gr
http://ocsp.geotrust.com
http://gtssl-ocsp.geotrust.com
http://crl.geotrust.com

respectively. Appendix C describes the process for permanently accepting the two certificates used by software vendors.

Certification of the web server (server authentication)

Communication between the client workstation and the DSS application incorporates the use of the Secure Sockets Layer (SSL) protocol, allowing the server's identity certification by the client workstation. In order to avoid security warning messages regarding the server's validity, it is required to install the Primary certification authority certificate (ROOT CA), as well as the Underlying Certificate Authority (Athex SSL Certificates CA), which can be retrieved from the following link http://www.helex.gr/en/web/guest/digital-certificates-pki-regulations.

Certification of the user of the application (client authentication) through ATHEXNet

In case the application is accessed from workstations within the closed proprietary network administered by ATHEXGroup (ATHEXNet)[3] or through the attached intranet network of the participant, it is not required to install a certificate that validates the identity of the user (client authentication).

Certification of the user of the application (client authentication) through the Internet

In case the application is accessed from the Internet, client authentication is mandatory, combined with the use of a secondary access password. Certificates for the intended users are issued by the Digital Certificates Division of ATHEXGroup, upon user request. The certificate provided to the user, needs to be installed in the browser that will access the application, under the personal certificates group.

[3] For the same reason as mentioned in the previous footnote, workstations connecting through ATHEXNet, need to configure their browsers in order to use the proxy athexsquid.athexnet.gr for connecting to non-local addresses. This proxy provides access to the aforementioned web resources. During proxy configuration, the DSS application url's need to be excluded explicitly.

1.4 Adobe PDF Reader – Browser Plug-in

For the correct display of Oracle Reports generated by the DSS application in PDF format, the following components must be installed:

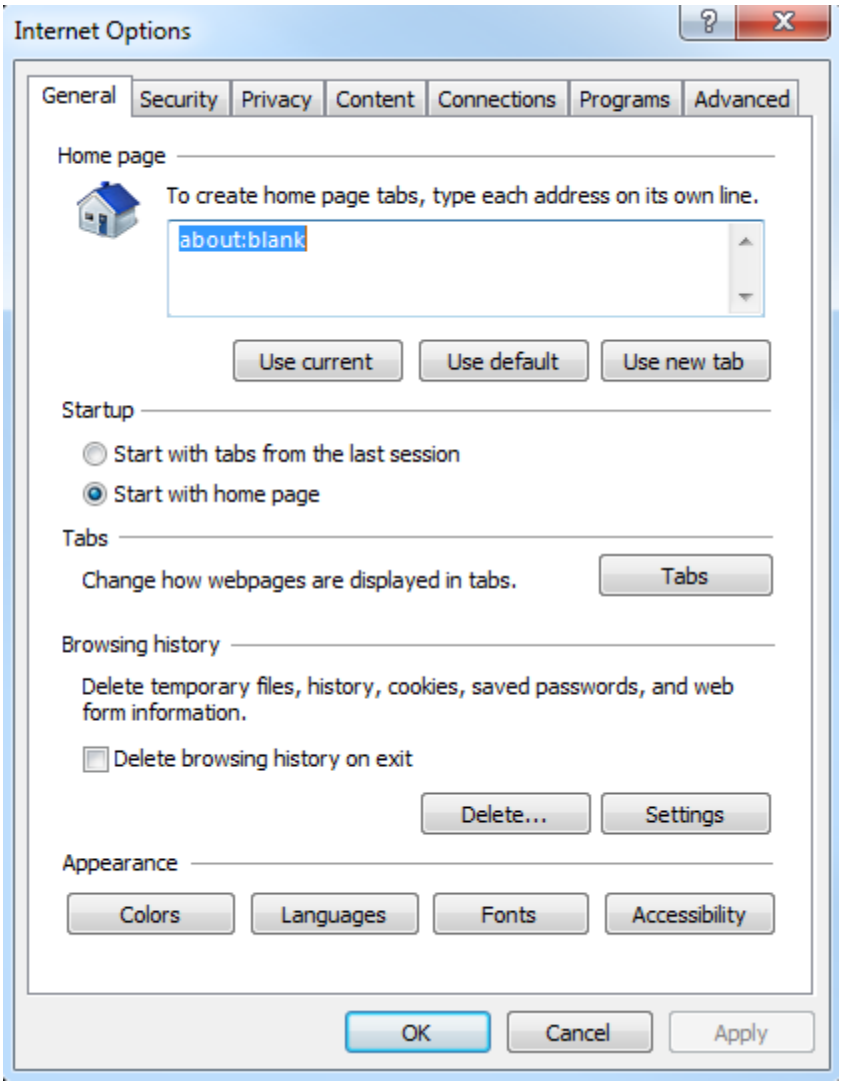
- Adobe Reader application, for reports saved locally in the client workstation (https://get.adobe.com/reader/).
- The appropriate Adobe PDF plugin for the browser, in order to support reports displayed through browser tabs (https://helpx.adobe.com/acrobat/using/display-pdf-in-browser.html).

Appendix A - Installing ATHEX Certificates on Internet Explorer

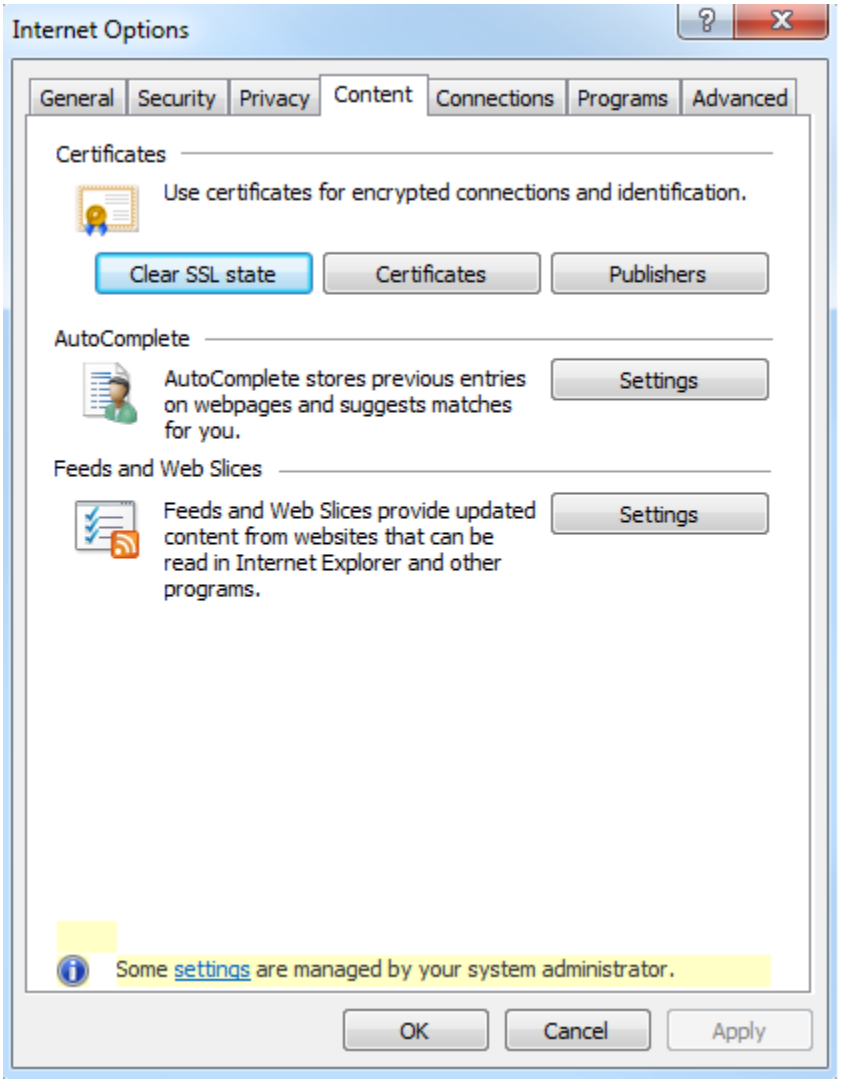
Installing ATHEX Certificates for server authentication

Below, are the steps required for installing the different types of certificates on Internet Explorer:

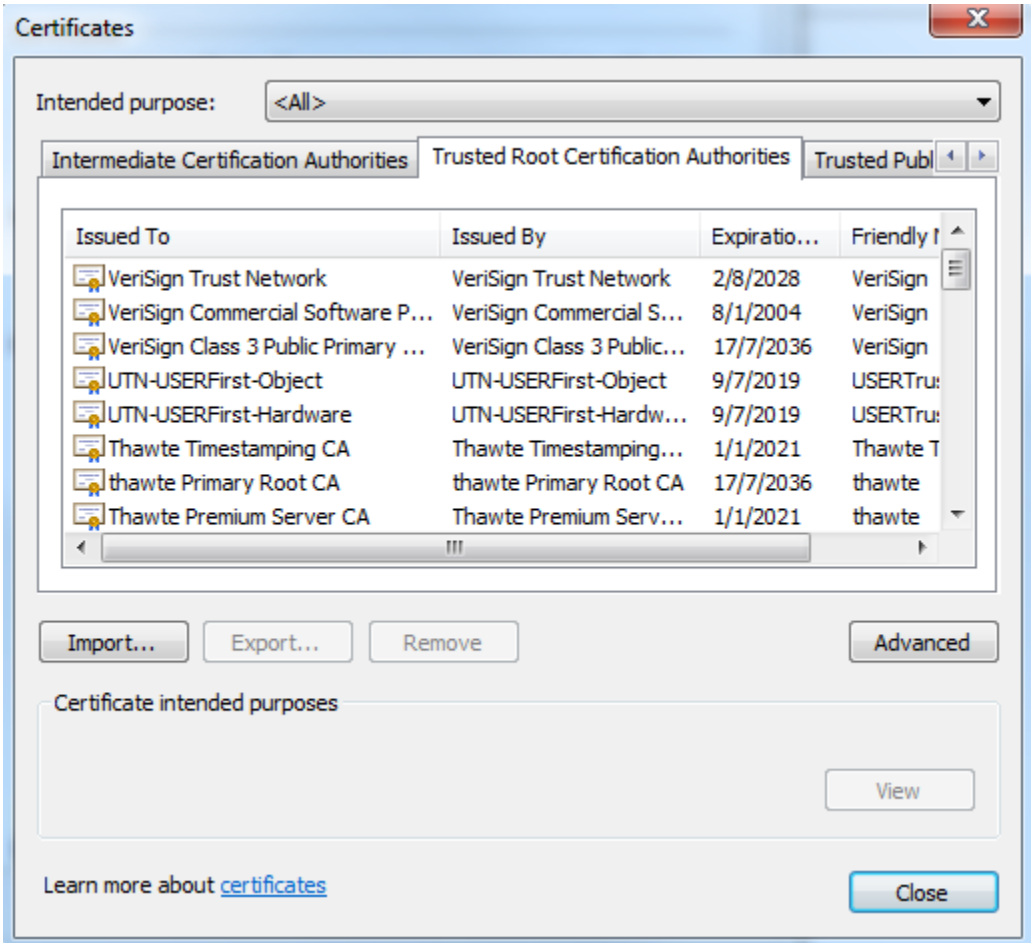
- From the Internet Explorer menu select: “Tools” -> “Internet Options”.



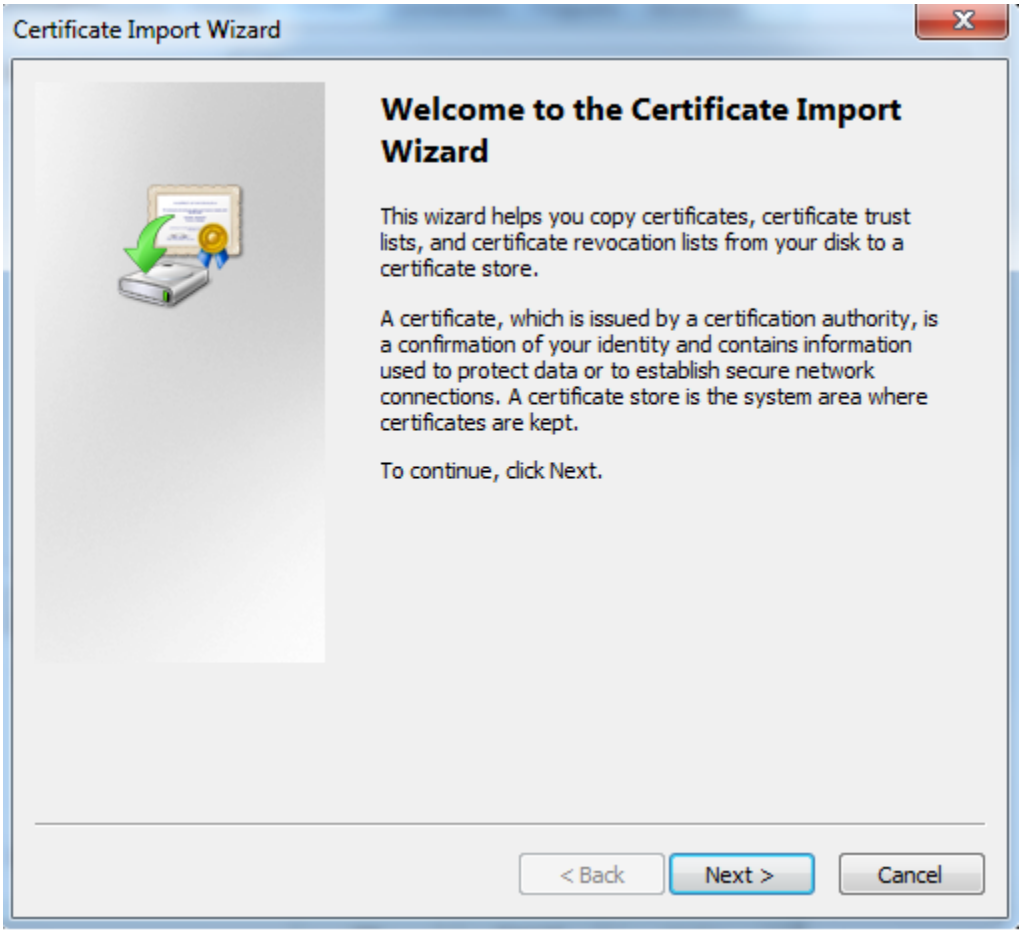
- Select the “Content” tab, click “Certificates”.



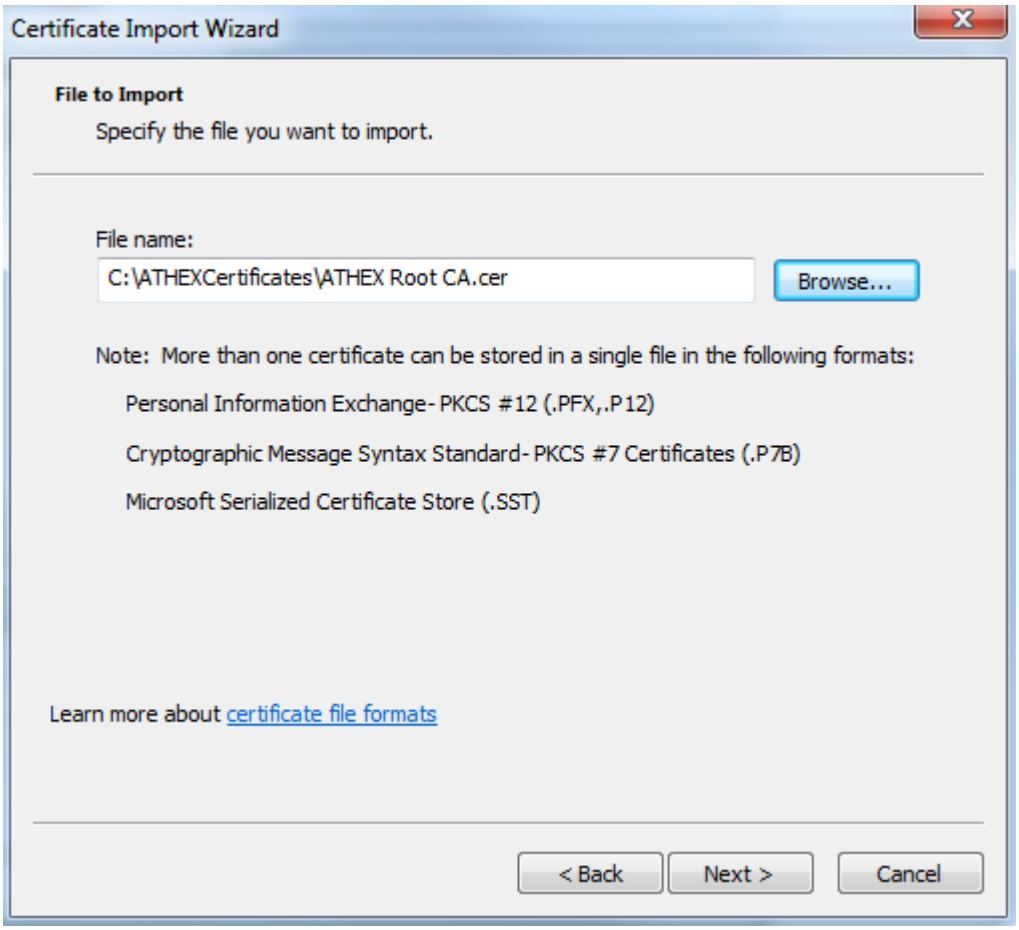
- Select the “Trusted Root Certification Authorities” tab, click “Import”.



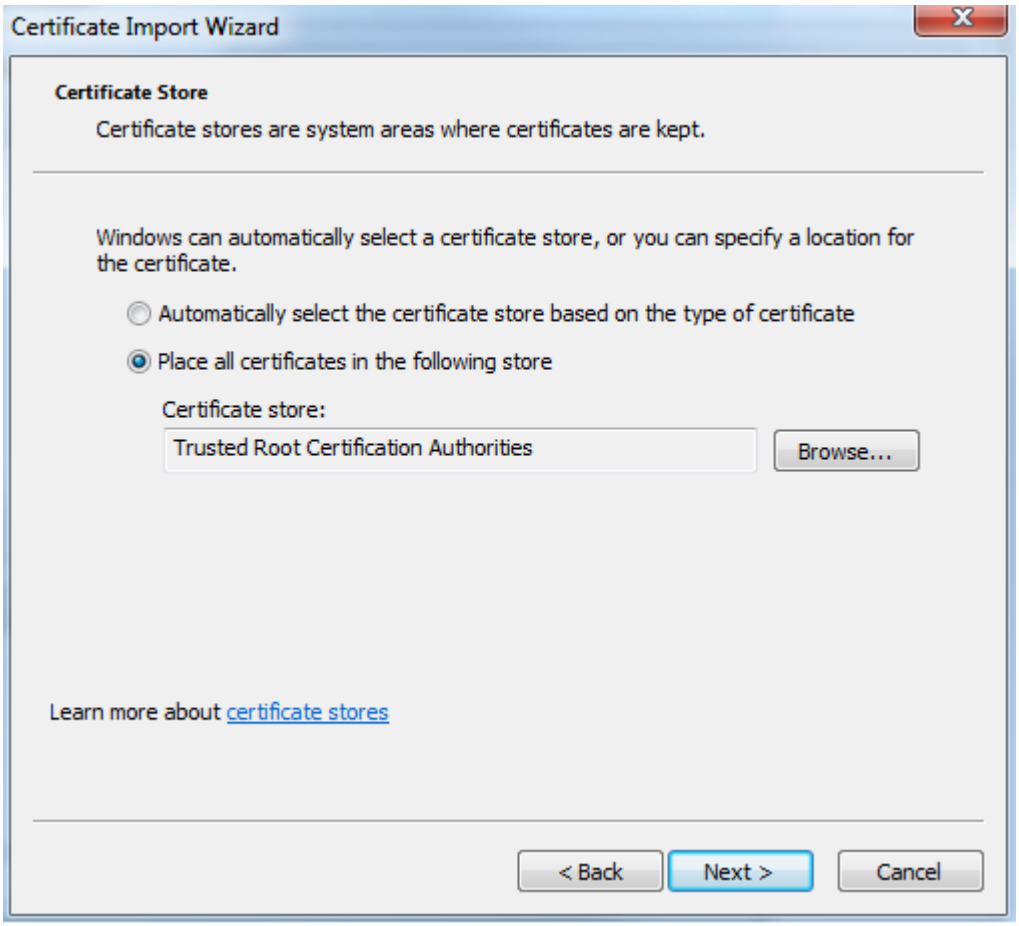
- The helper program “Certificate Import Wizard” appears. Click “Next”.



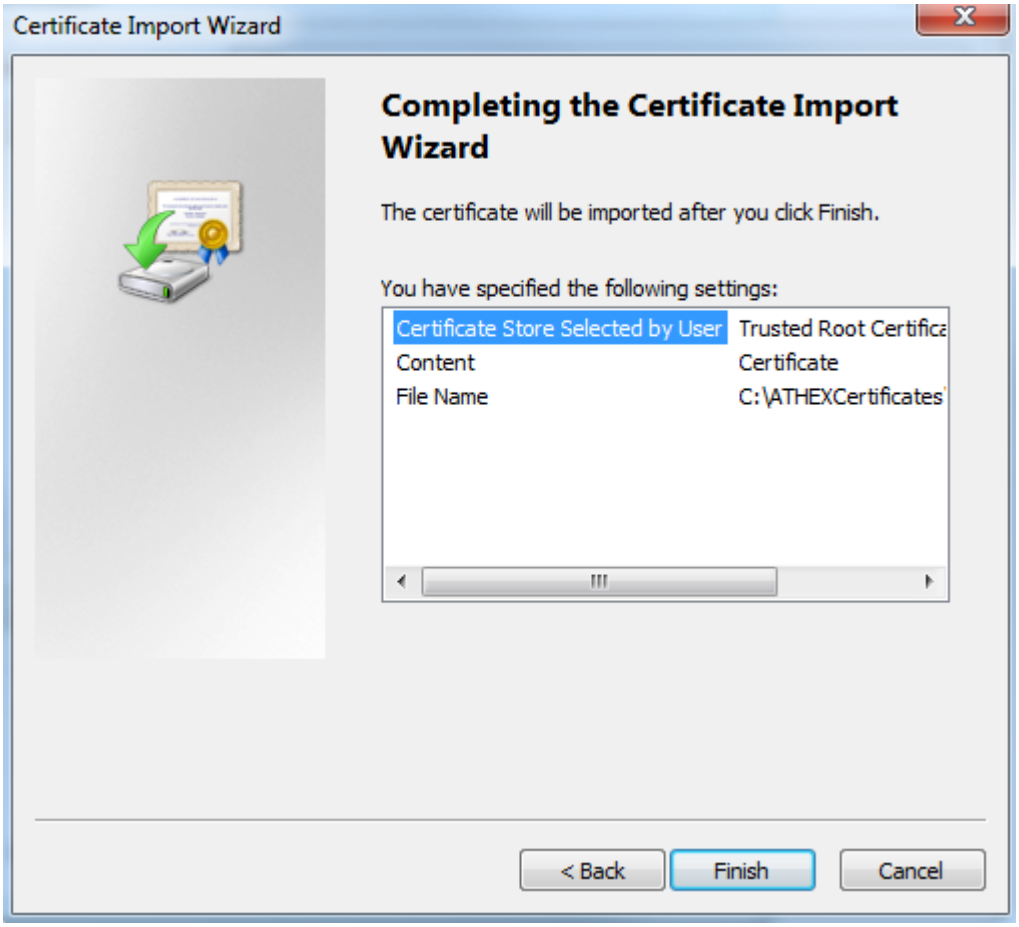
- Click “Browse” and locate the certificate “ATHEX Root CA.cer” from the directory where it is saved. Click “Next”.



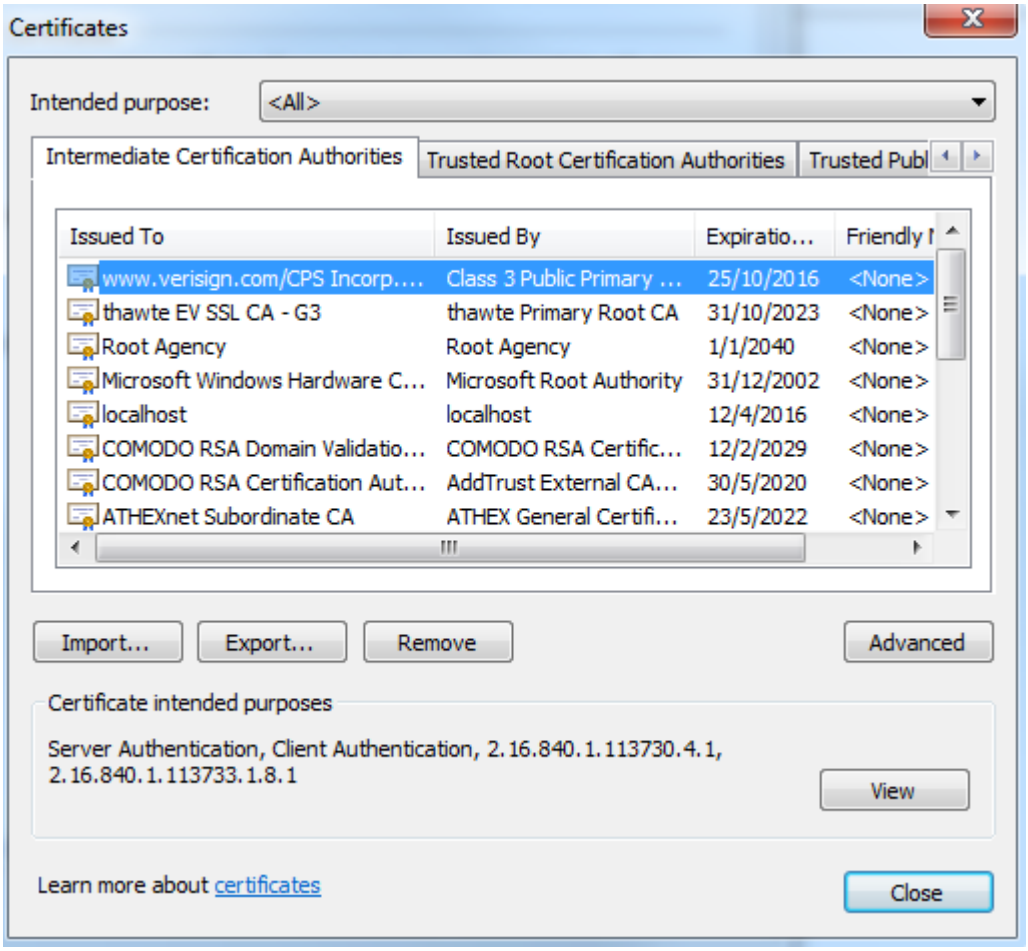
- Select “Place all certificates in the following store” with the “Certificate store” option set to “Trusted Root Certification Authorities”. Click “Next”.



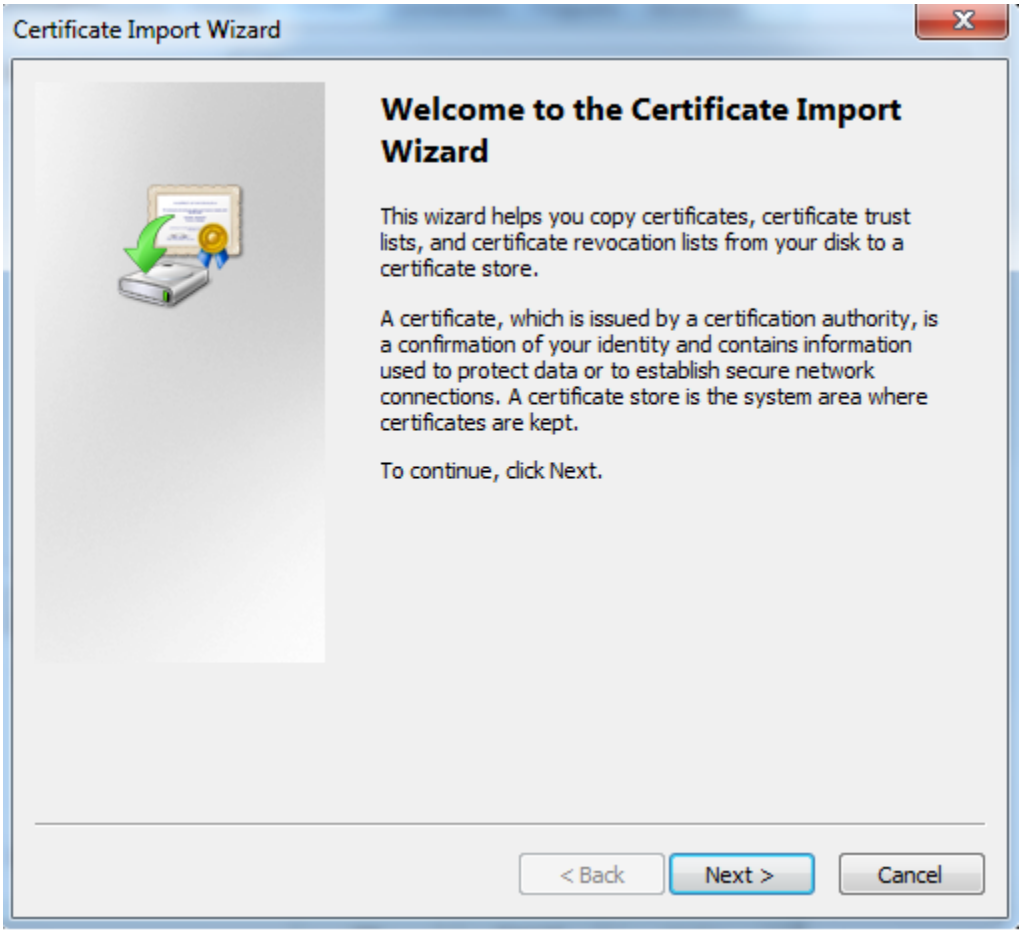
- In the summary tab, click “Finish”.



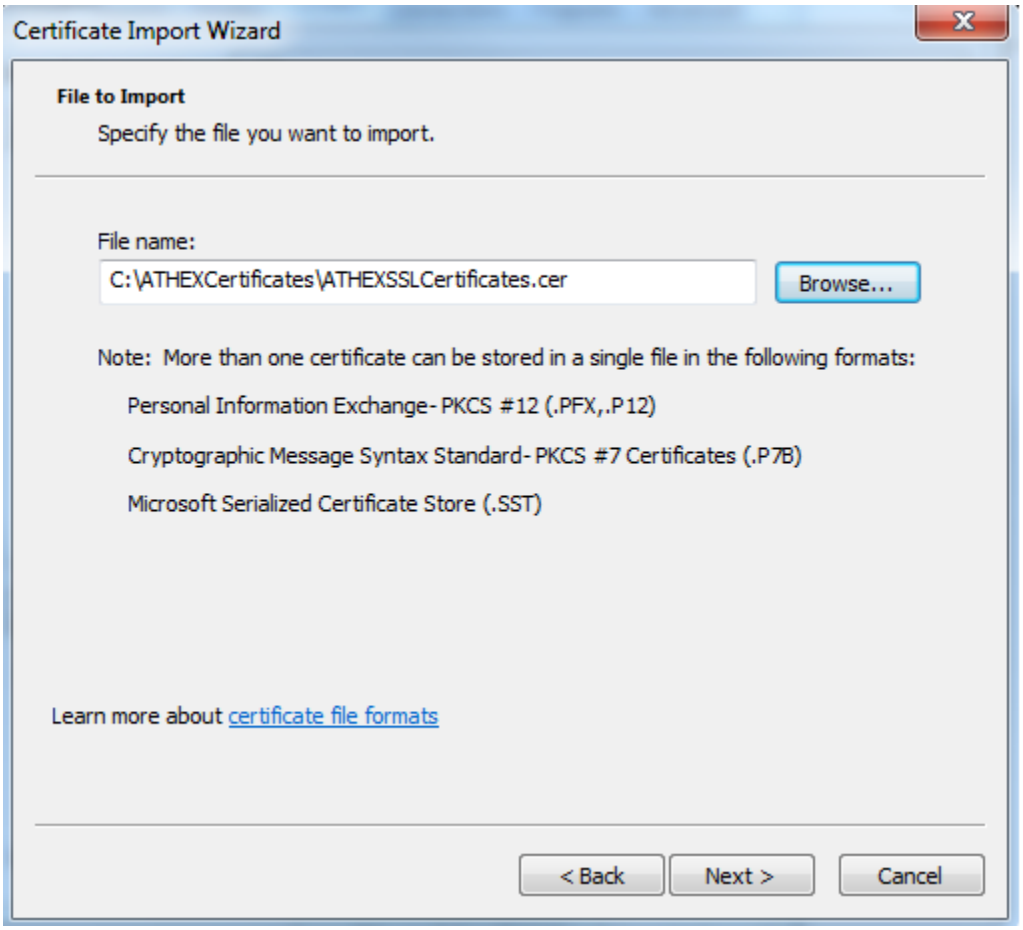
- Select the “Intermediate Certification Authorities” tab, click “Import”.



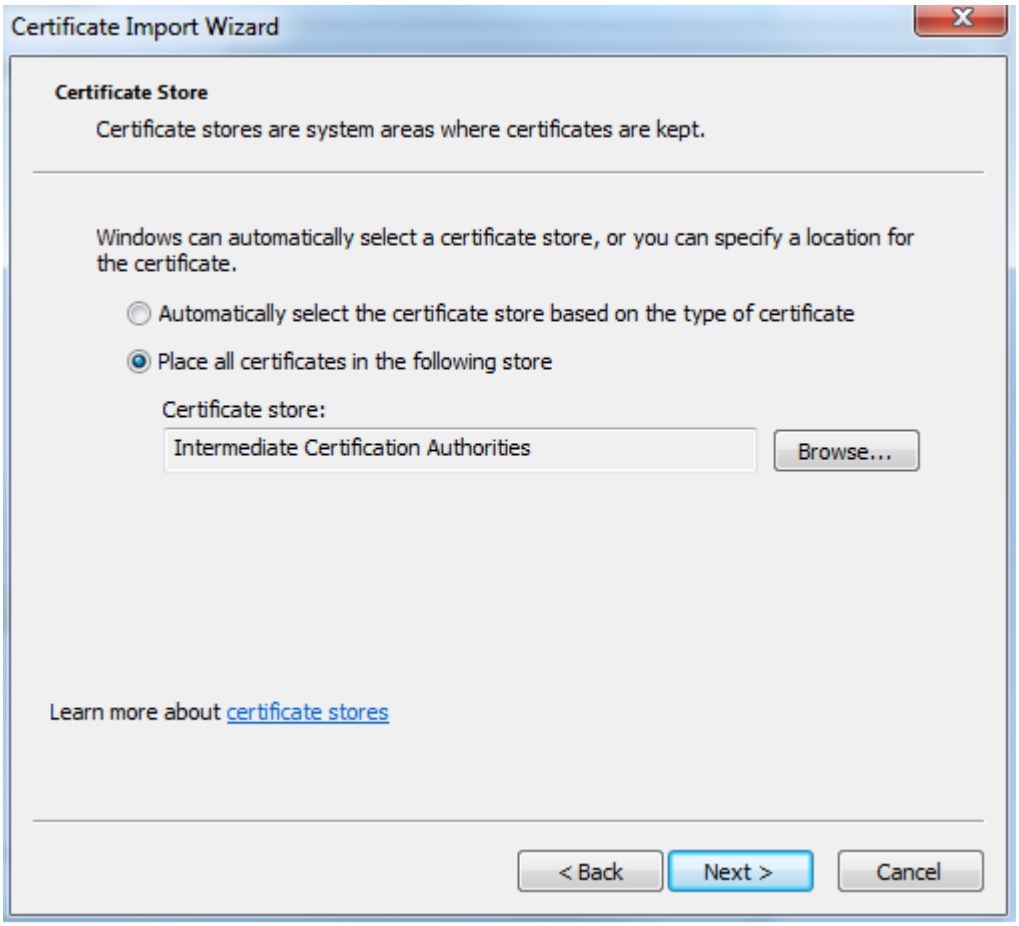
- The helper program “Certificate Import Wizard” appears. Click “Next”.



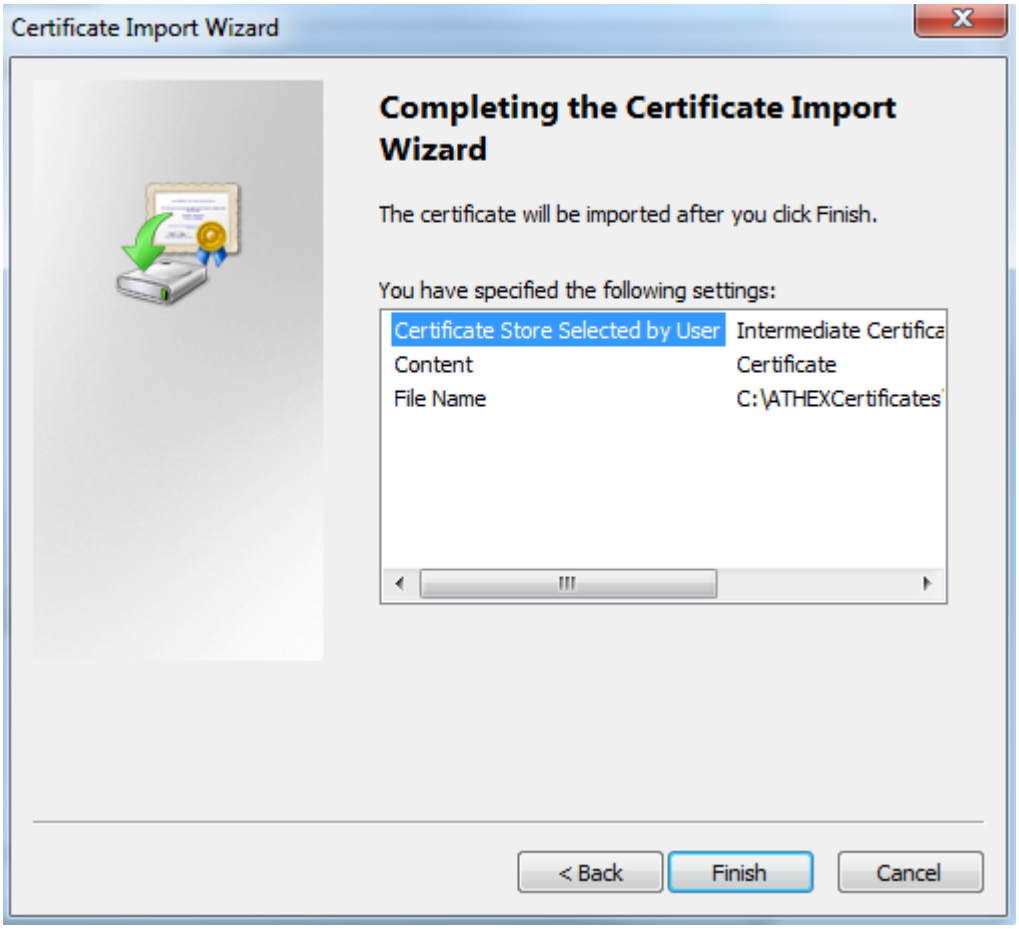
- Click “Browse” and locate the certificate “ATHEXSSLCertificates.cer” from the directory where it is saved. Click “Next”.



- Select “Place all certificates in the following store” with the “Certificate store” option set to “Intermediate Certification Authorities”. Click Next.

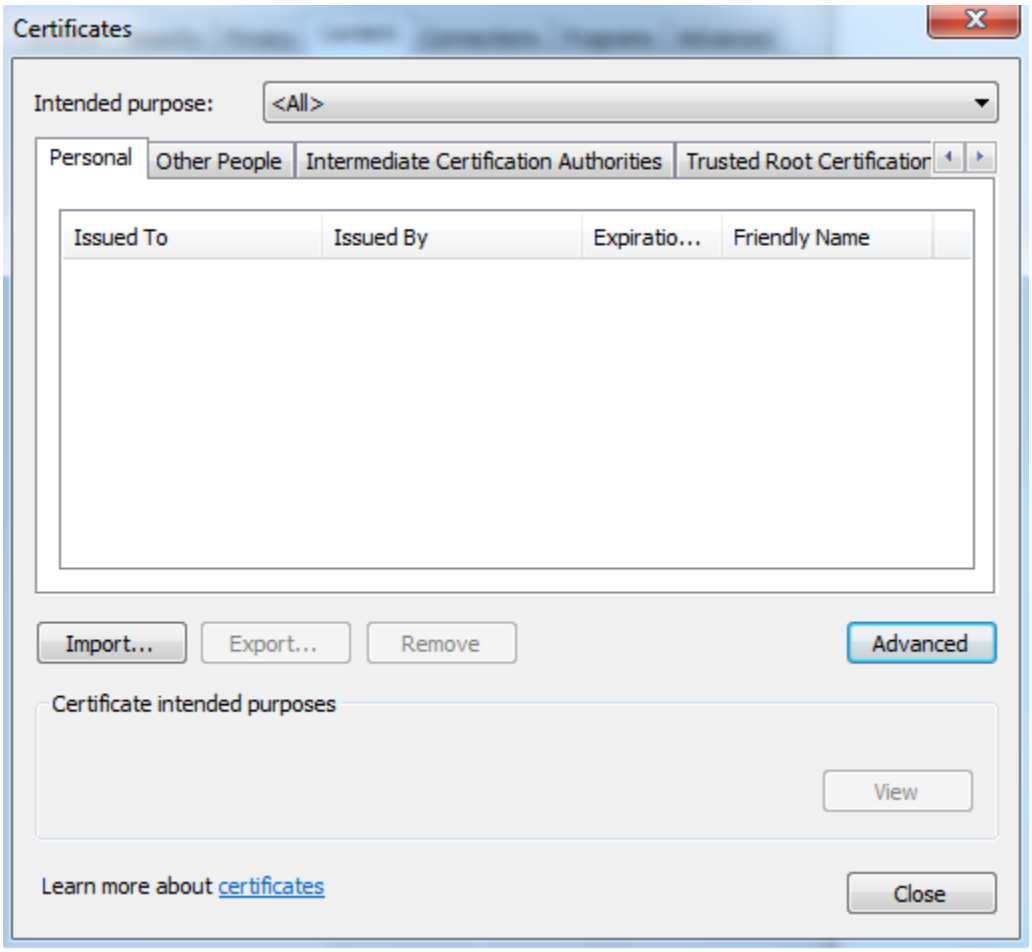


- In the summary tab, click “Finish”.

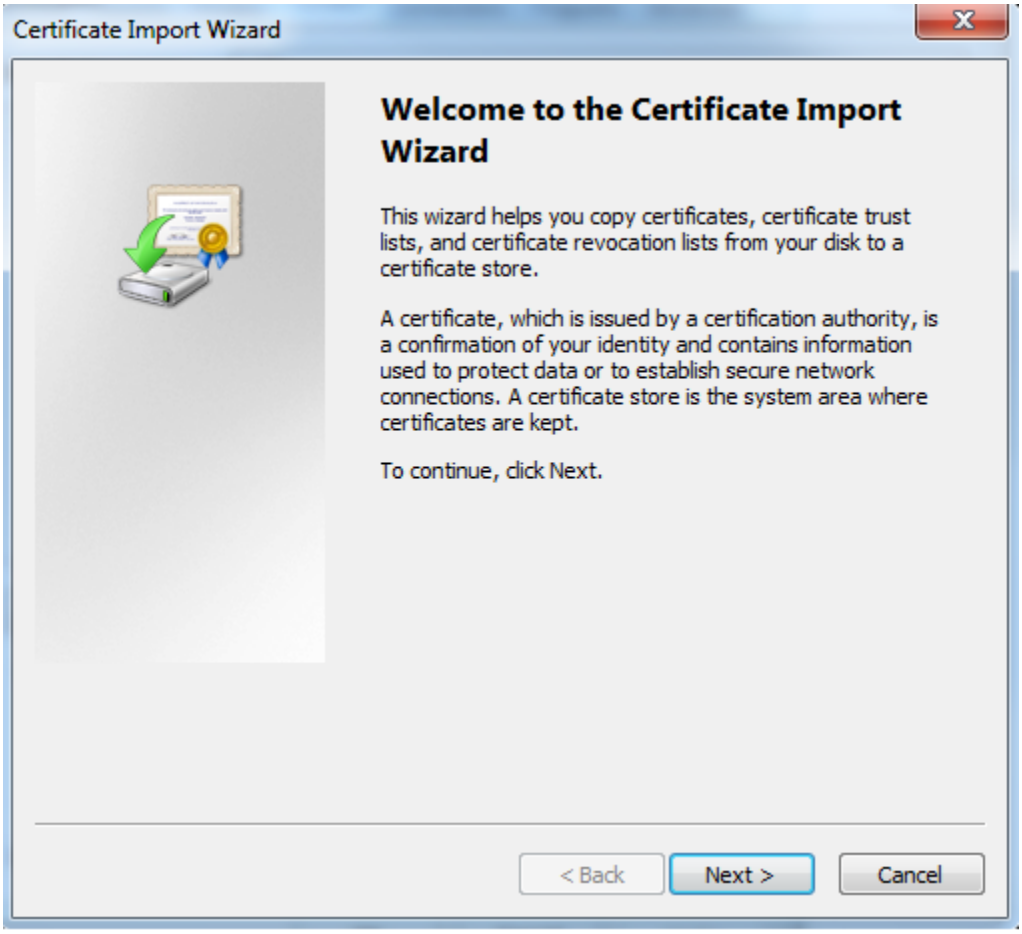


Installing ATHEX Certificates for client authentication

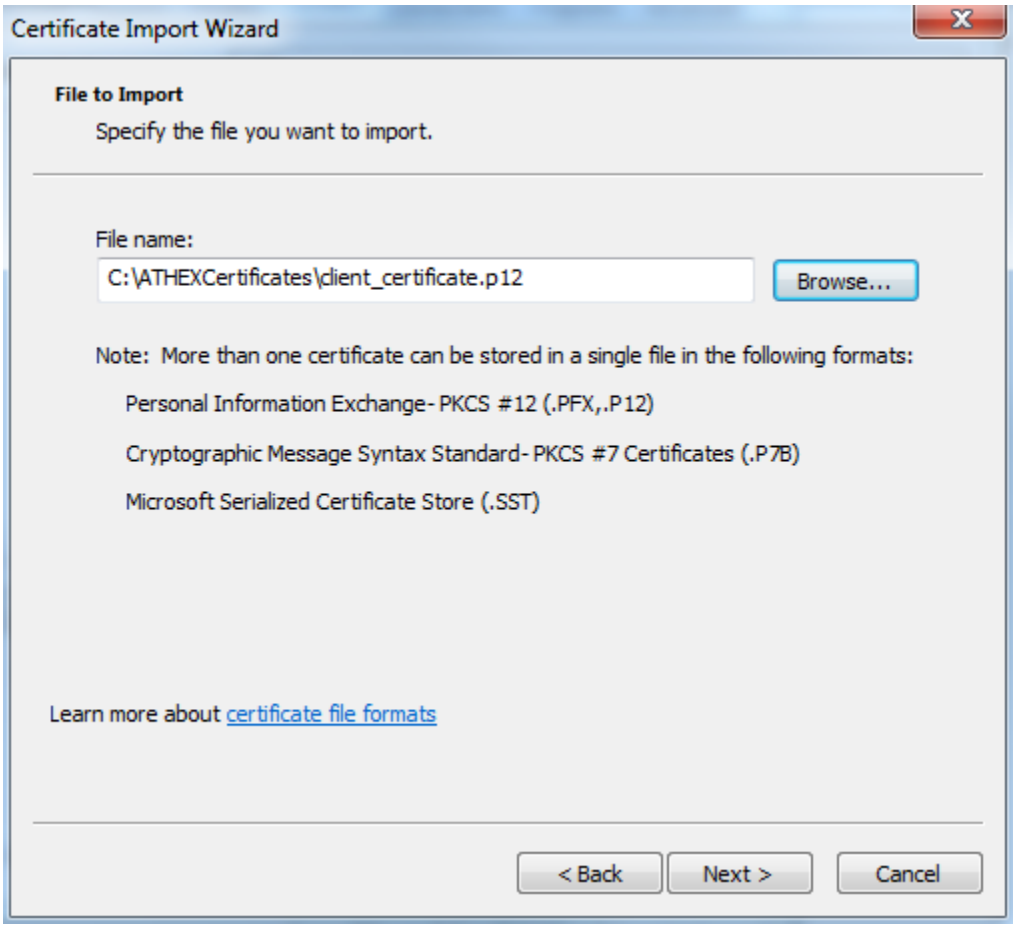
- Select the “Personal” tab, click “Import”.



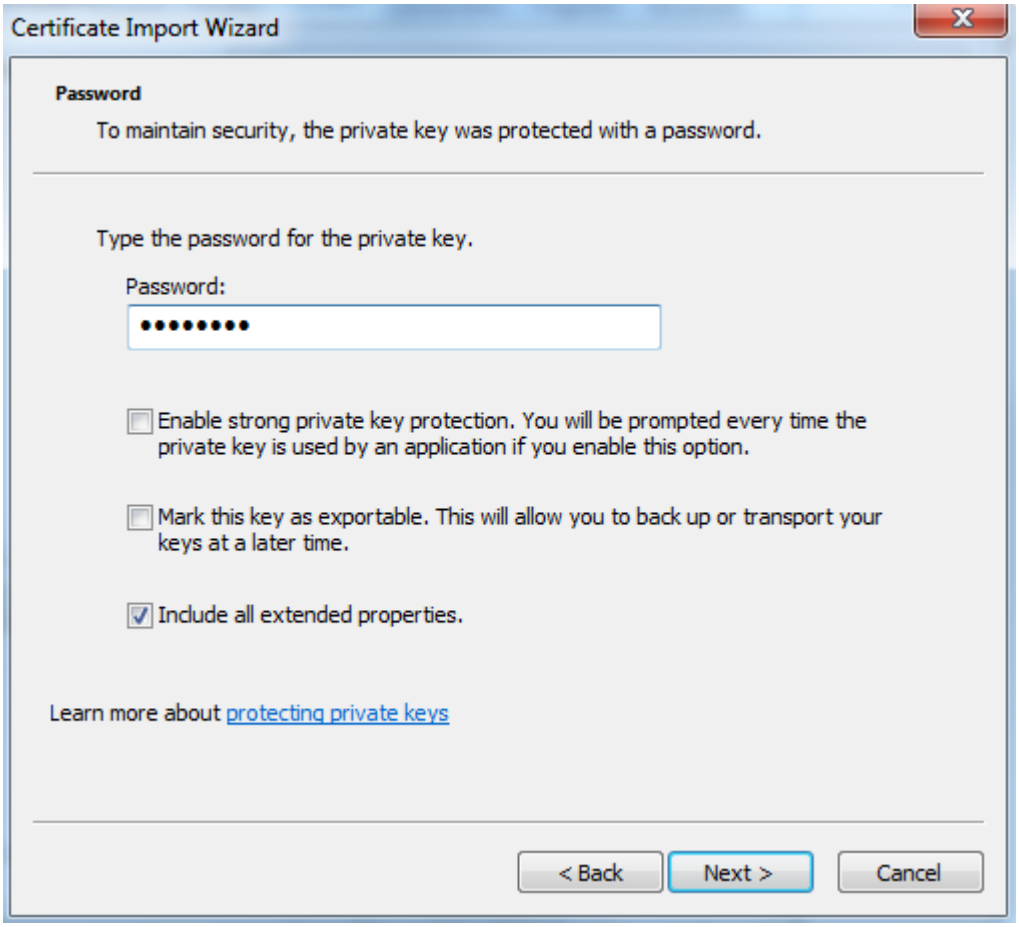
- The helper program “Certificate Import Wizard” appears. Click “Next”.



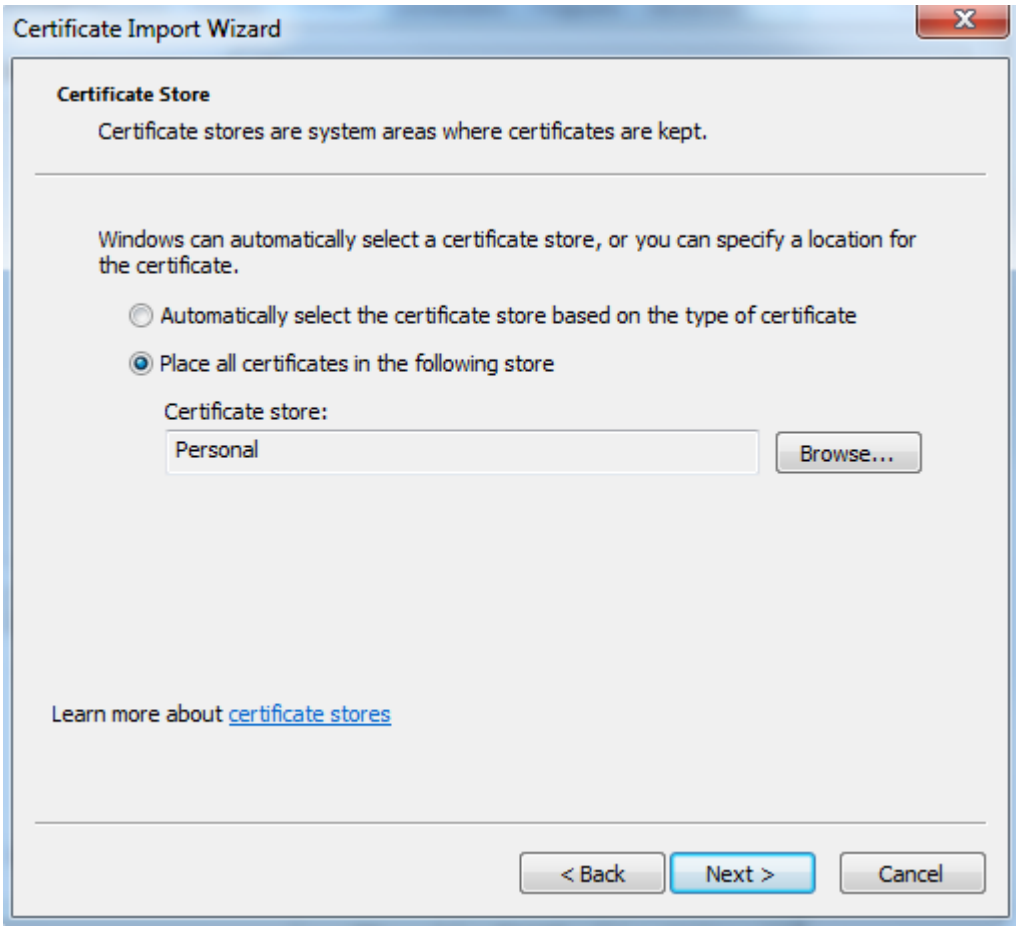
- Click “Browse” and locate the user certificate issued by ATHEXGroup (file having “.p12“ extension) from the directory where it is saved. Click “Next”.



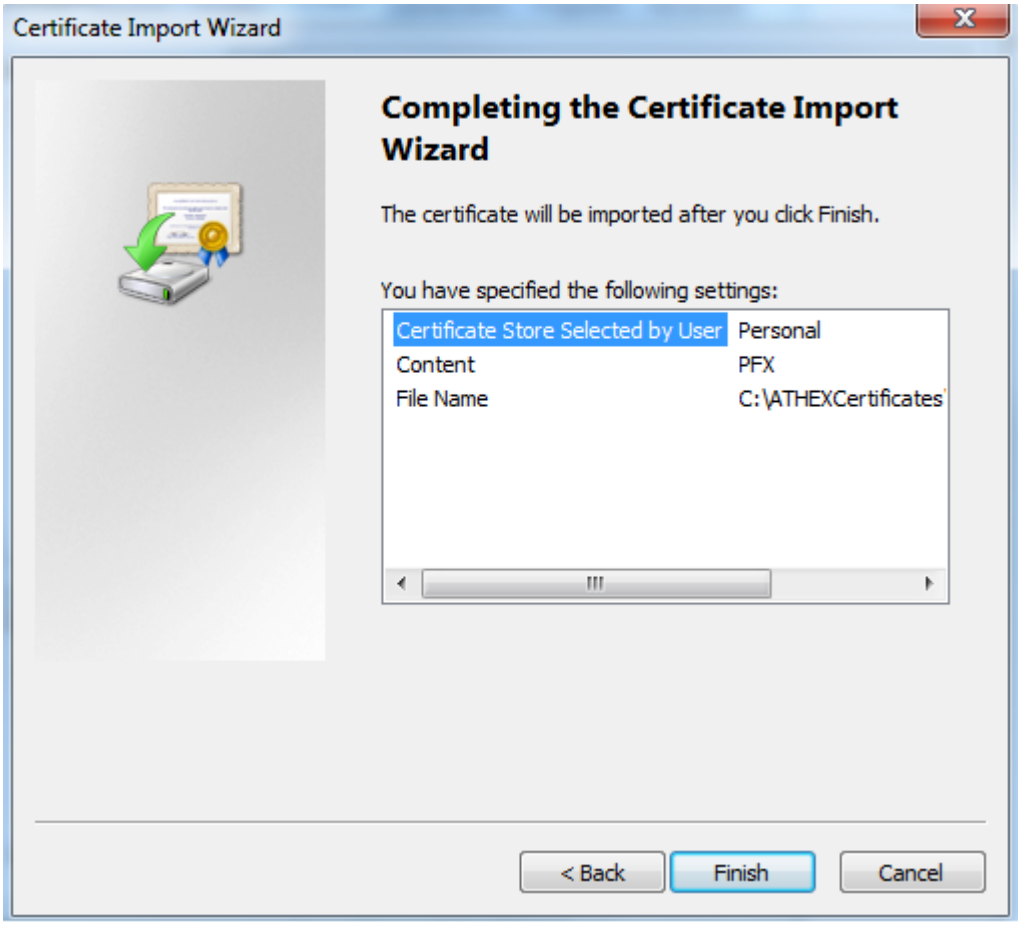
- Enter the provided password for this certificate. Click “Next”.



- Select “Place all certificates in the following store” with the “Certificate store” option set to “Personal”. Click “Next”.



- In the summary tab, click “Finish”.

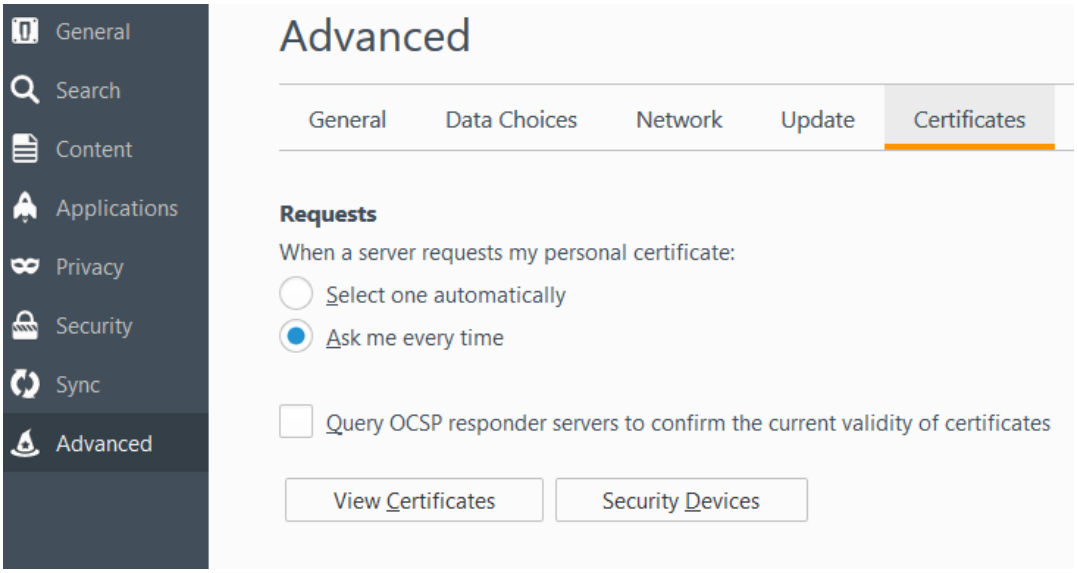


Appendix B - Installing ATHEX Certificates on Firefox

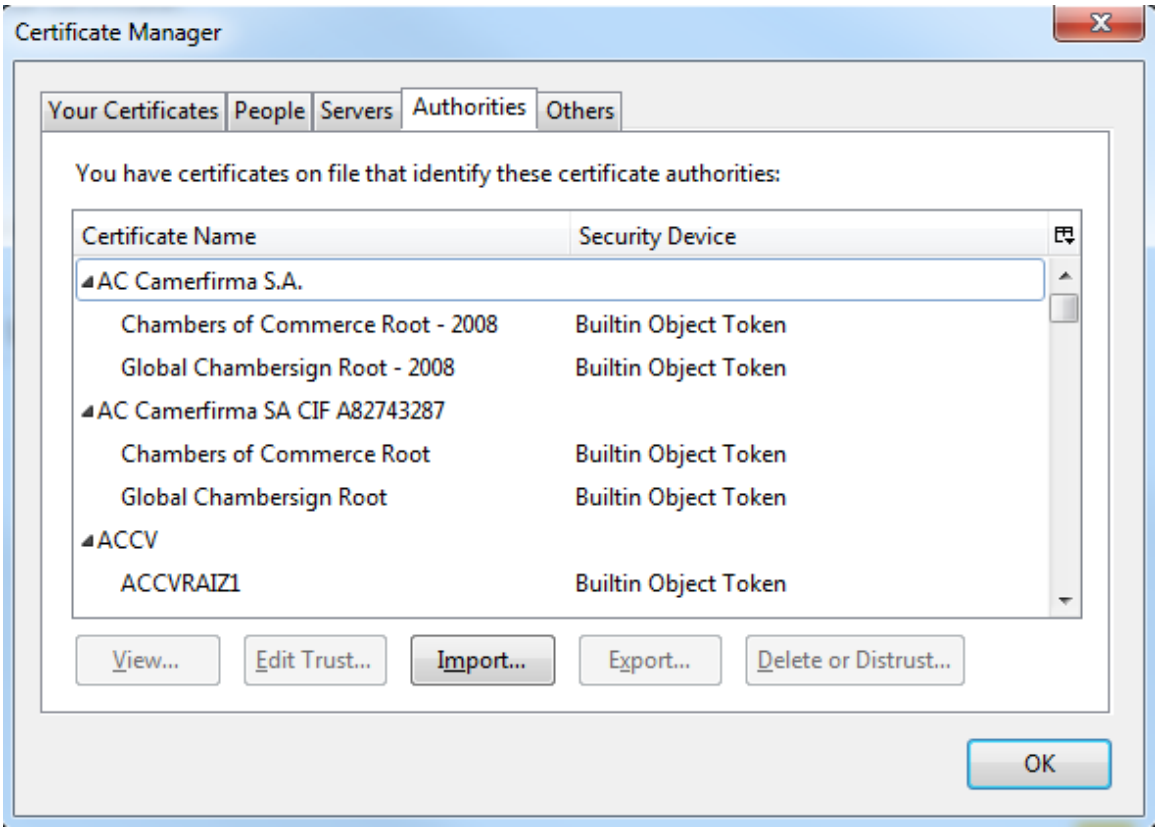
Installing ATHEX Certificates for server authentication

Below, are the steps required for installing the different types of certificates on Firefox:

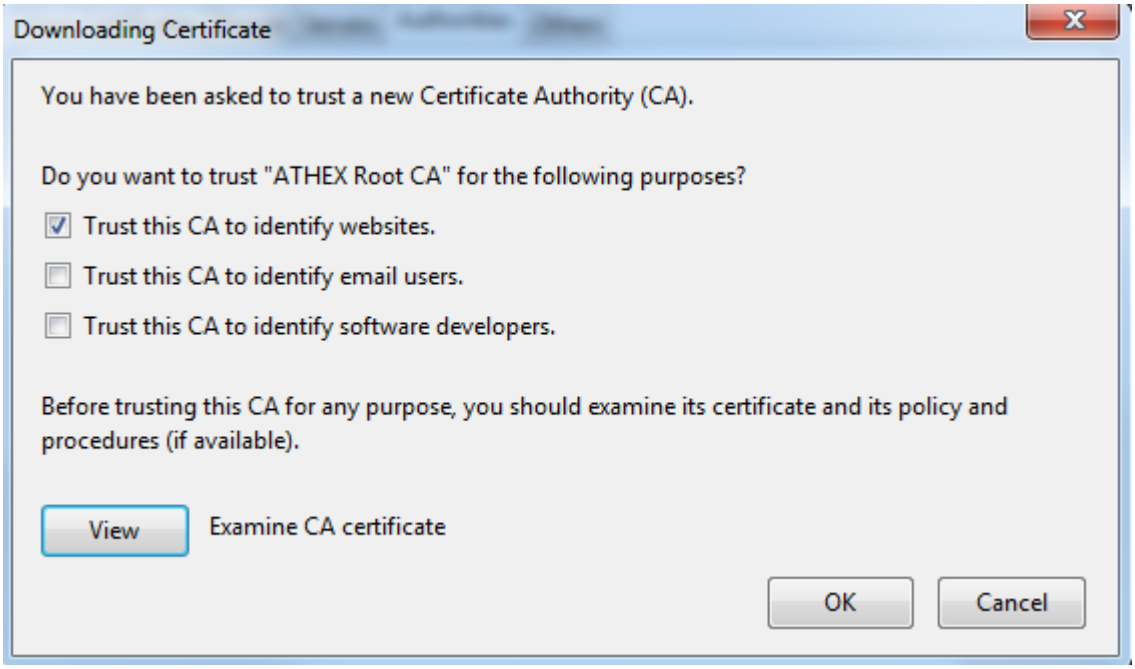
- From the Firefox menu select: “Options” -> “Advanced” -> “Certificates”. Click “View Certificates”.



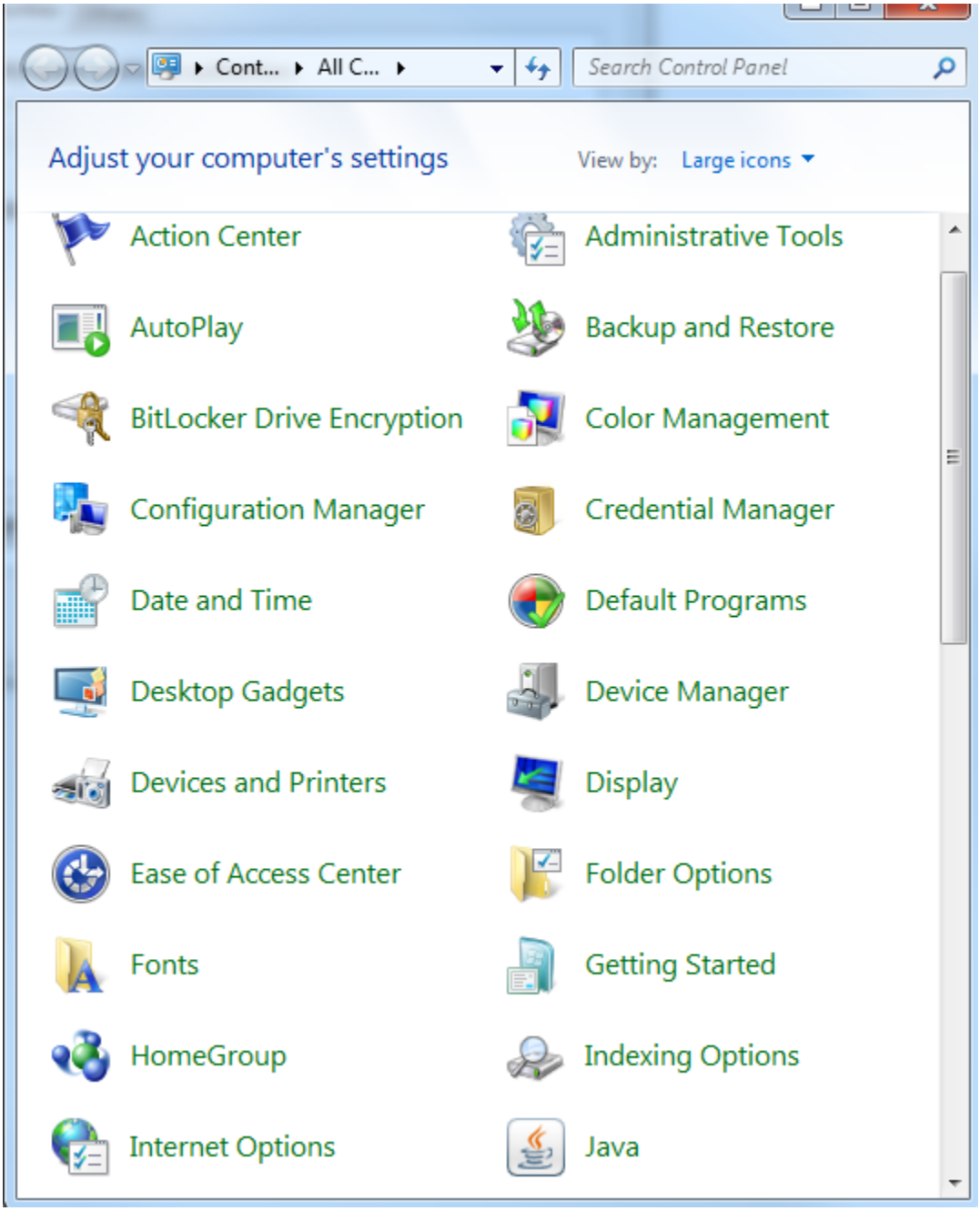
- The “Certificate Manager” appears. Select “Authorities” tab, click “Import”.



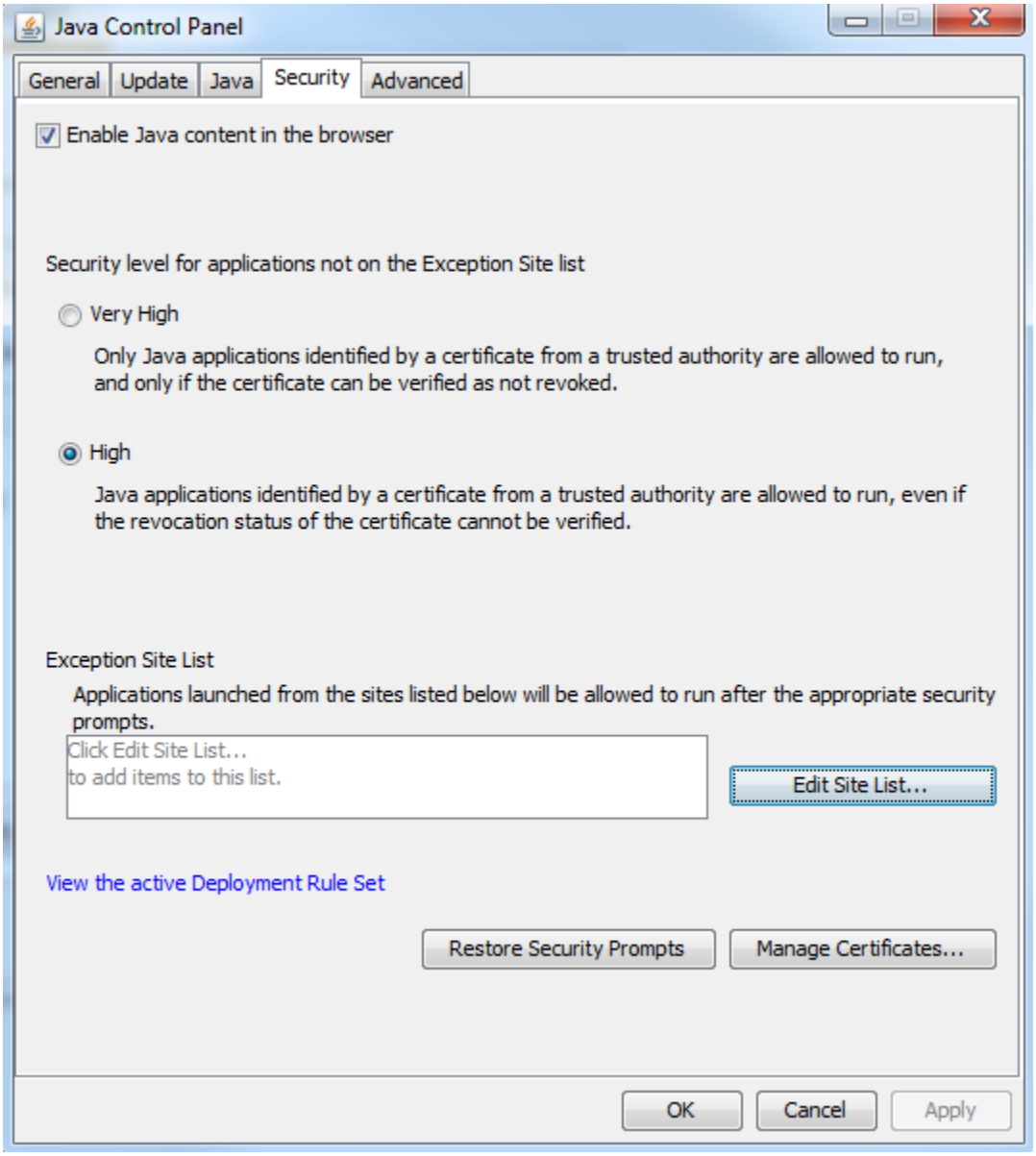
- Locate the certificate “ATHEX Root CA.cer” from the directory where it is saved. Click “Open”. The “Downloading Certificate” dialog appears. Select option “Trust this CA to identify websites”. Click “OK” in order to import the certificate.



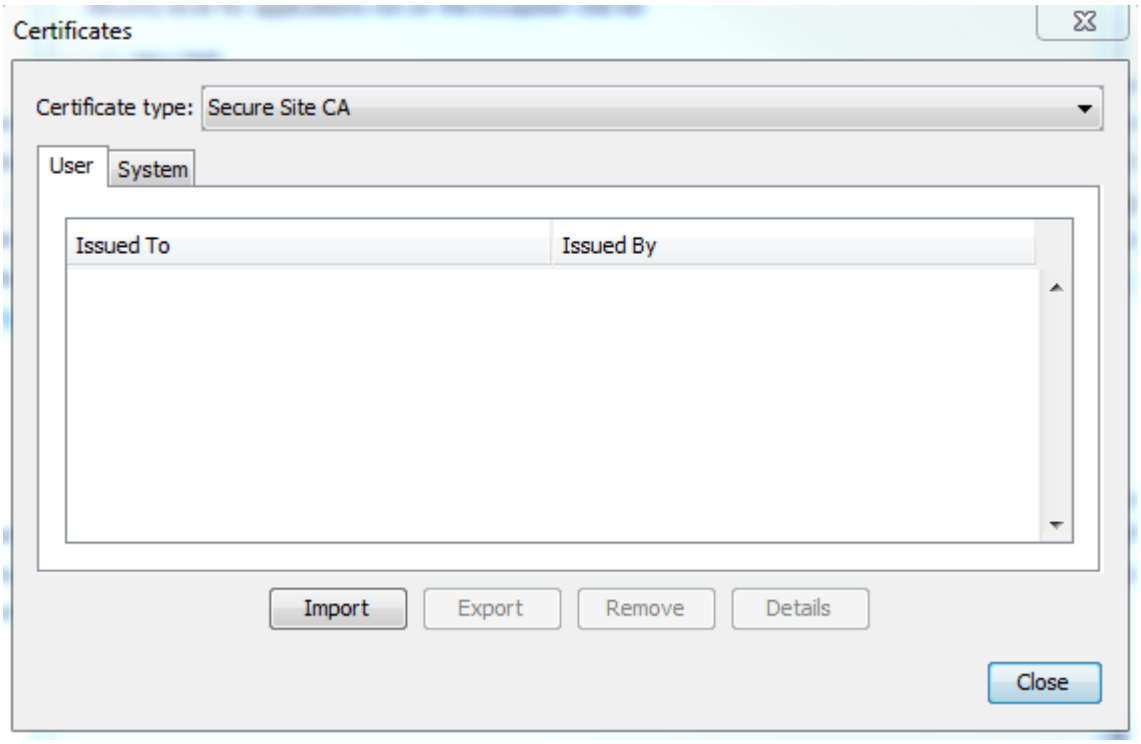
- For Firefox, it is required that the “ATHEX Root CA” certificate is also imported through Java’s Control Panel.
  On Windows, select “Start”->”Control Panel”.



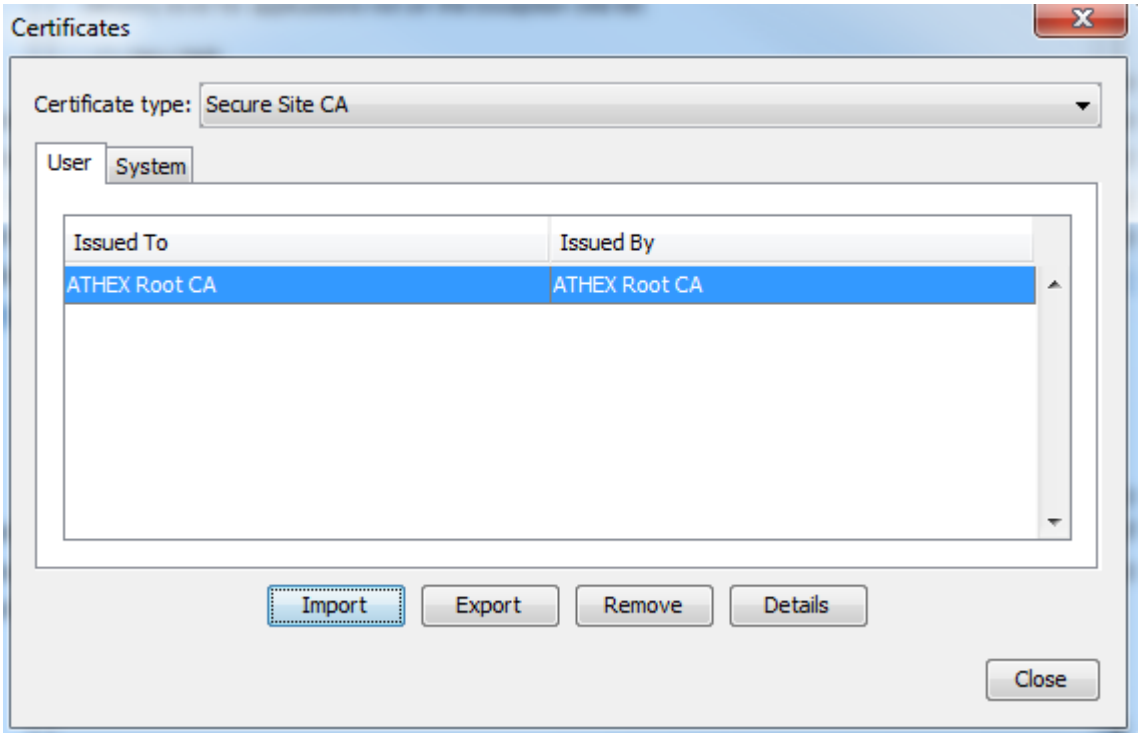
- Select “Java”. The “Java Control Panel” appears. Select tab “Security”.



- Click “Manage Certificates”. The “Certificates” window appears. In the “Certificate type” option, select “Secure Site CA” from the drop-down list.

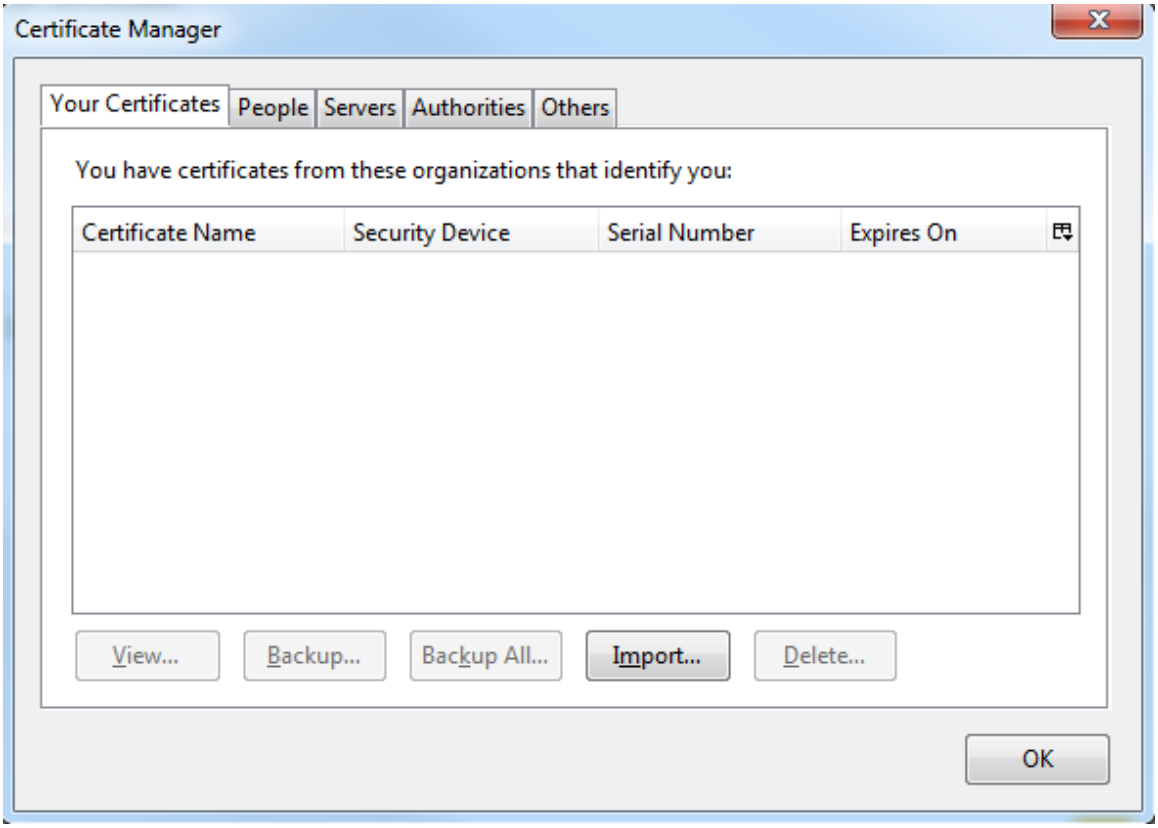


- Click “Import”. Locate the certificate “ATHEX Root CA.cer” from the directory where it is saved. Click “Open”. On success, the certificate is shown in tab “Secure Site CA”.

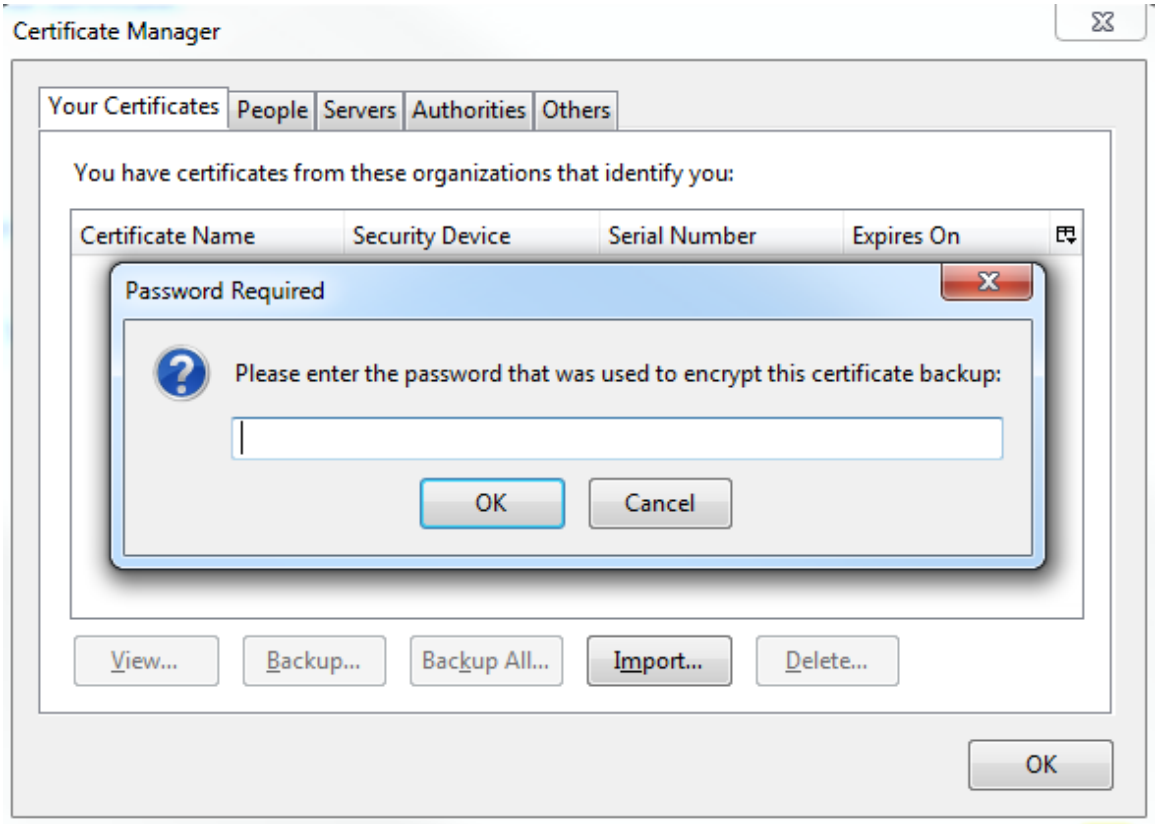


Installing ATHEX Certificates for client authentication

- In the “Certificate Manager” select “Your Certificates” tab, click “Import”.

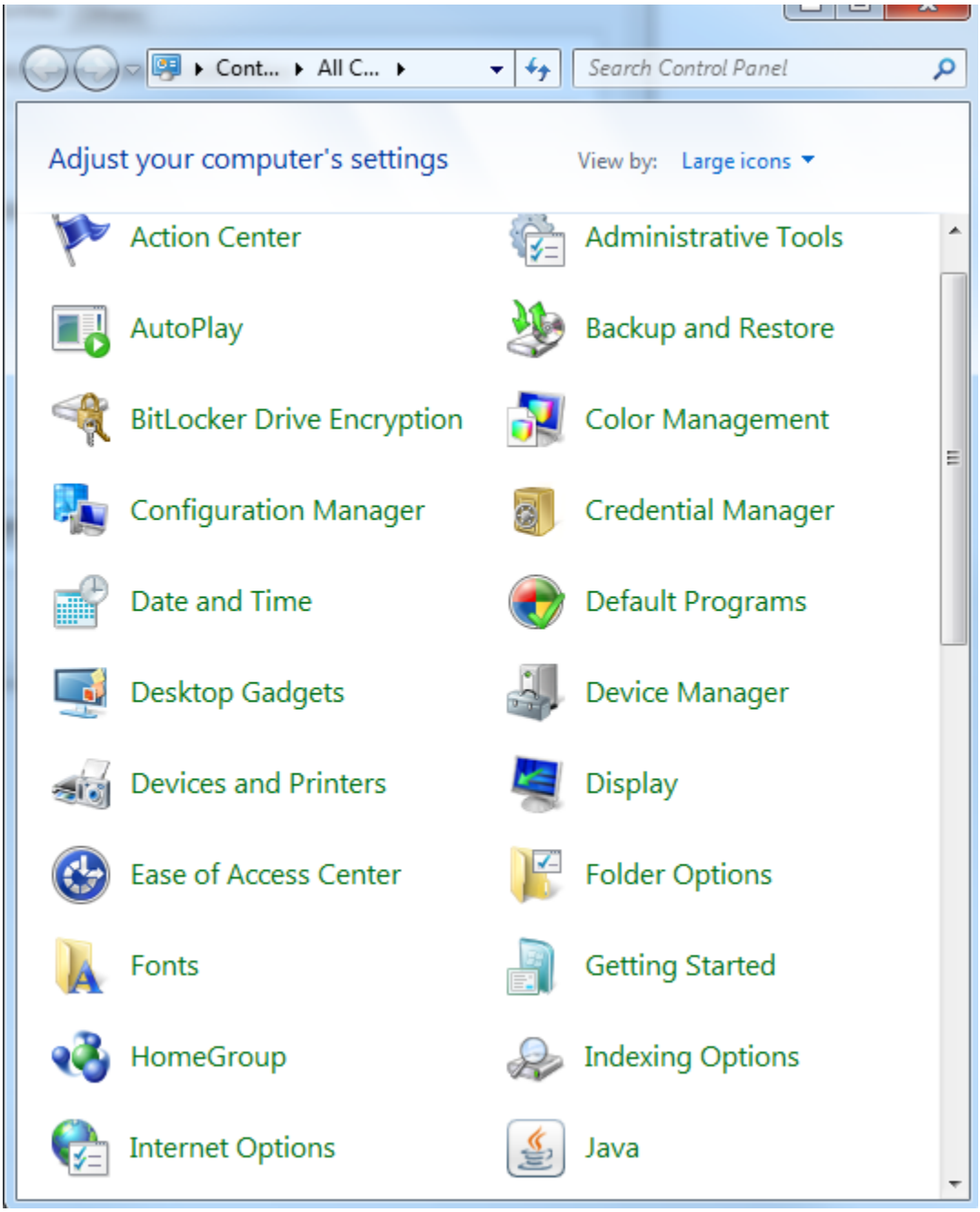


- Locate the user certificate issued by ATHEXGroup (file having ".p12" extension) from the directory where it is saved. Click "Open". Enter the provided password for this certificate. Click "OK".

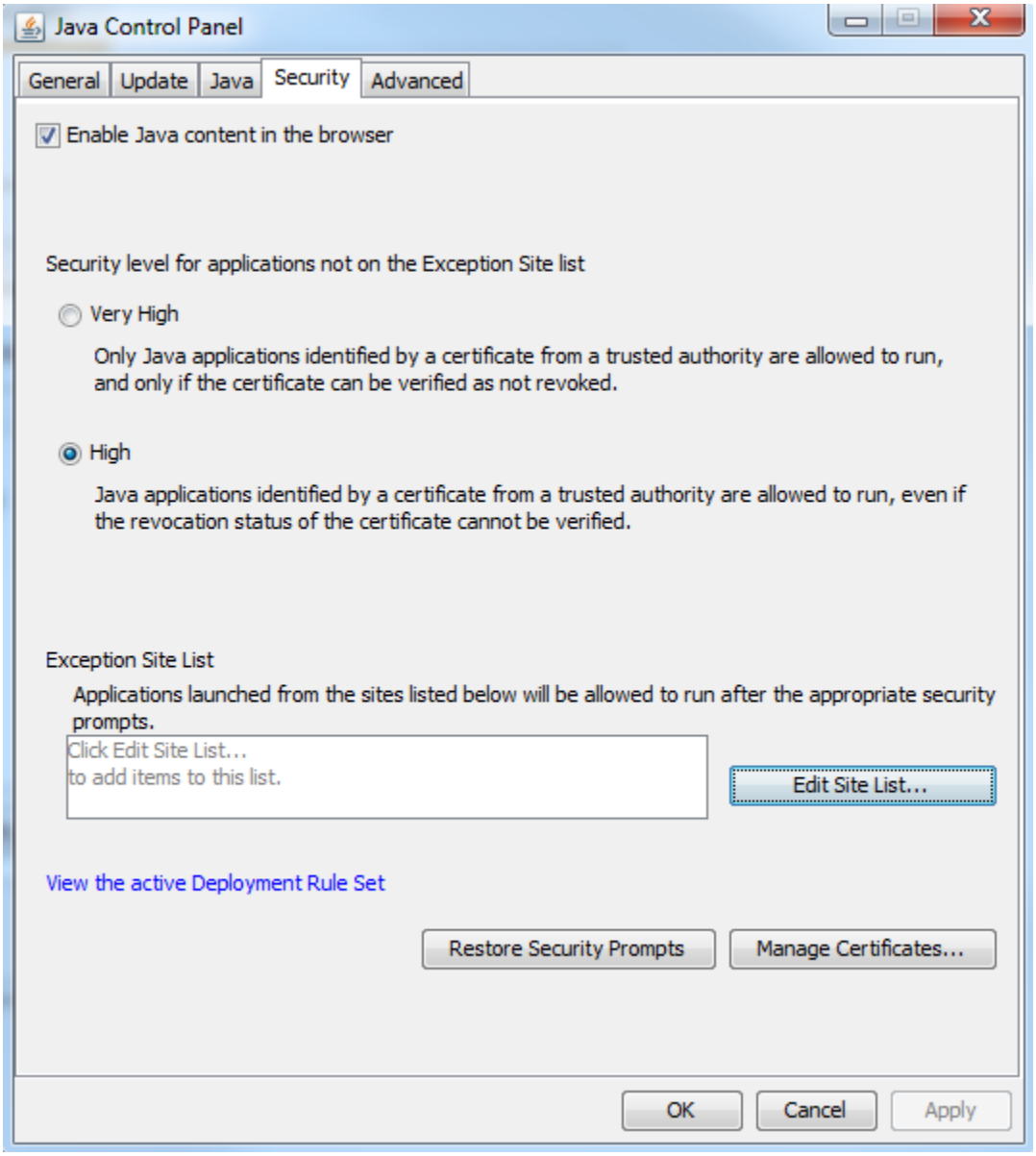


- For Firefox, it is required that the client certificate is also imported through Java's Control Panel. This will also create a Java personal keystore, if there isn't one already in the workstation.

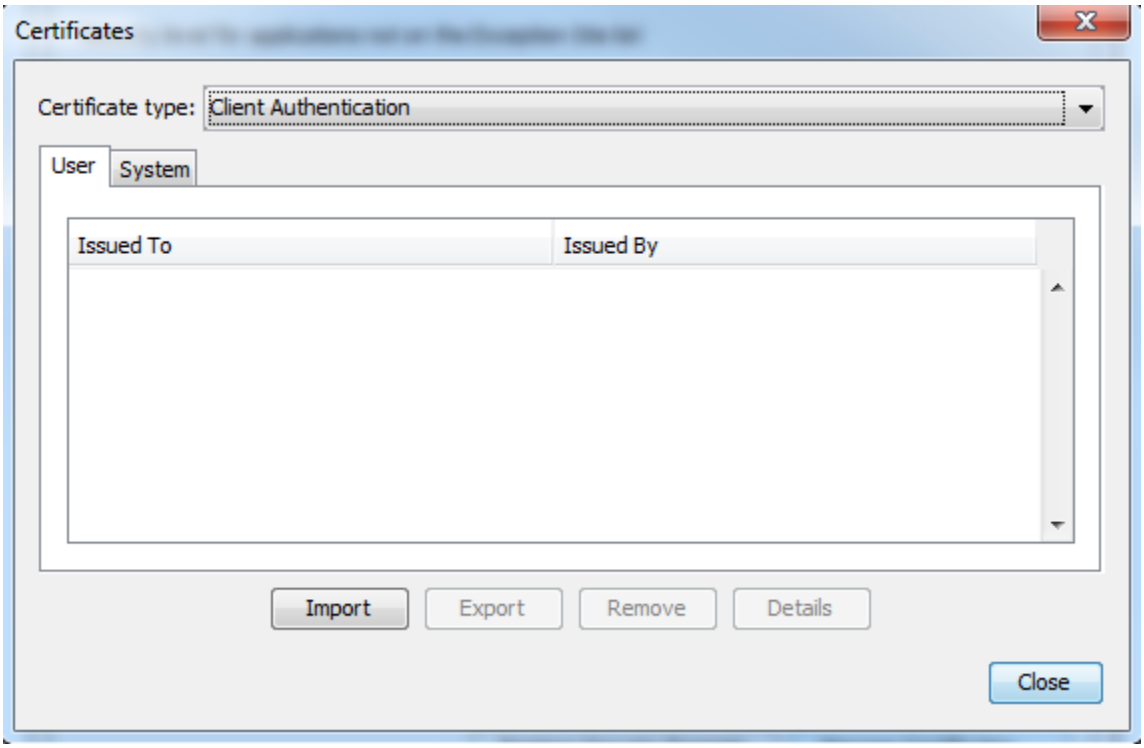
  On Windows, select "Start"->"Control Panel".



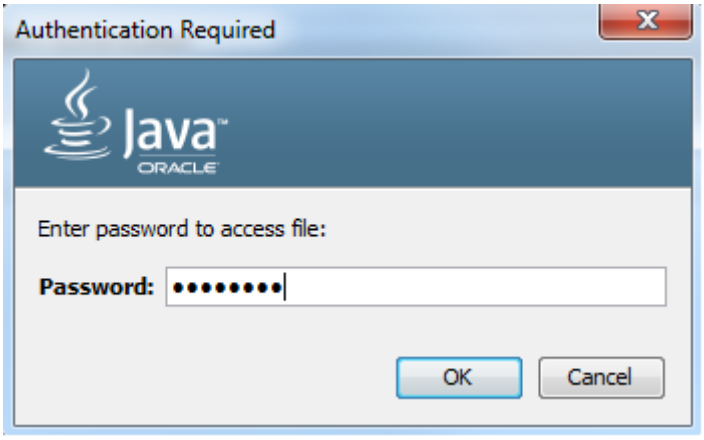
- Select “Java”. The “Java Control Panel” appears. Select tab “Security”.



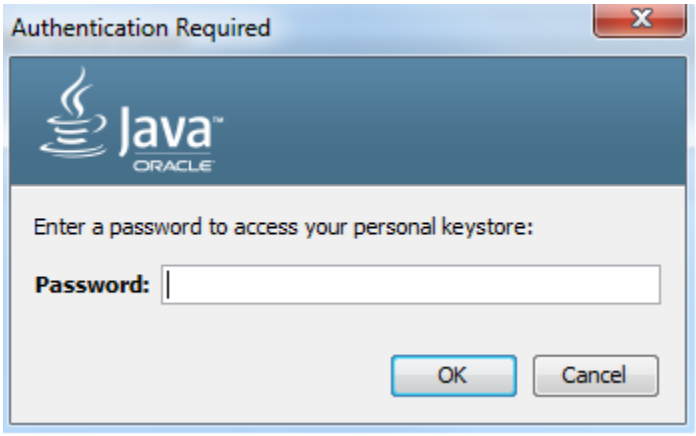
- Click “Manage Certificates”. The “Certificates” window appears. In the “Certificate type” option, select “Client Authentication” from the drop-down list.



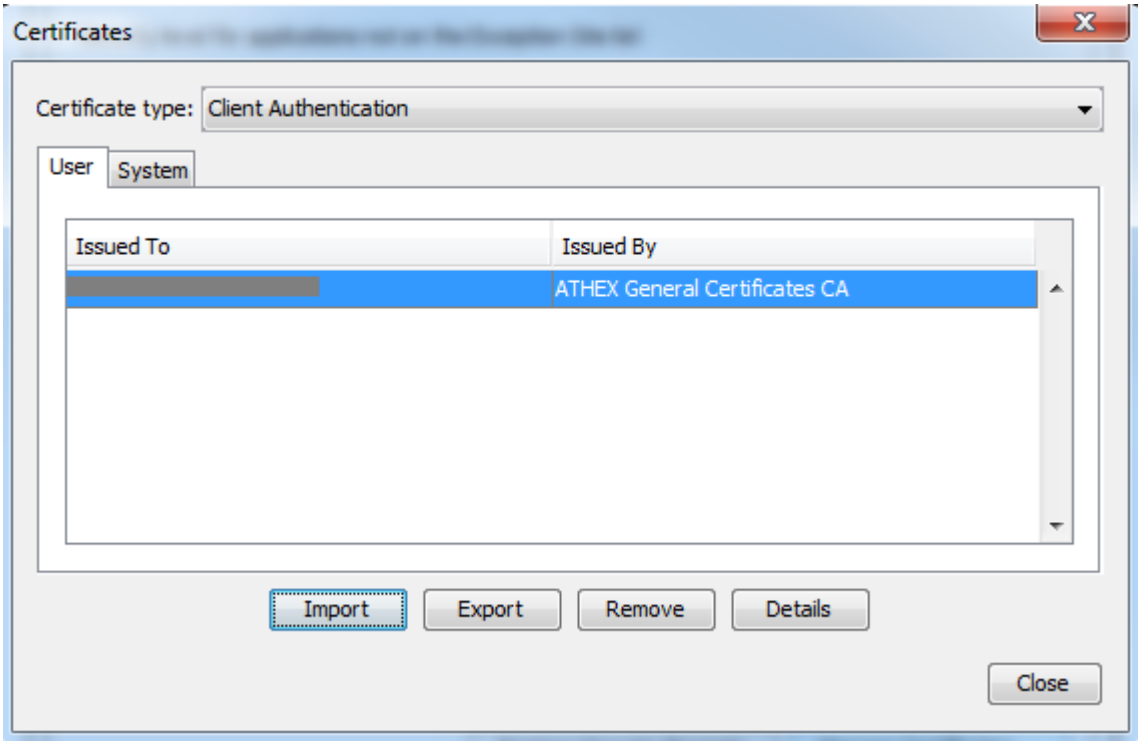
- Click “Import”. Locate the user certificate issued by ATHEXGroup (file having “.p12“ extension) from the directory where it is saved. Click “Open”. Enter the provided password for this certificate. Click “OK”.



- If a personal Java keystore already exists, the password for the existing keystore is required. If a personal Java keystore doesn't exist, Java will ask for a password in order to create a new keystore. Be sure to take a note of the keystore password, as it will be required for subsequent use. This password is not to be confused with the client's certificate password used in the previous step.



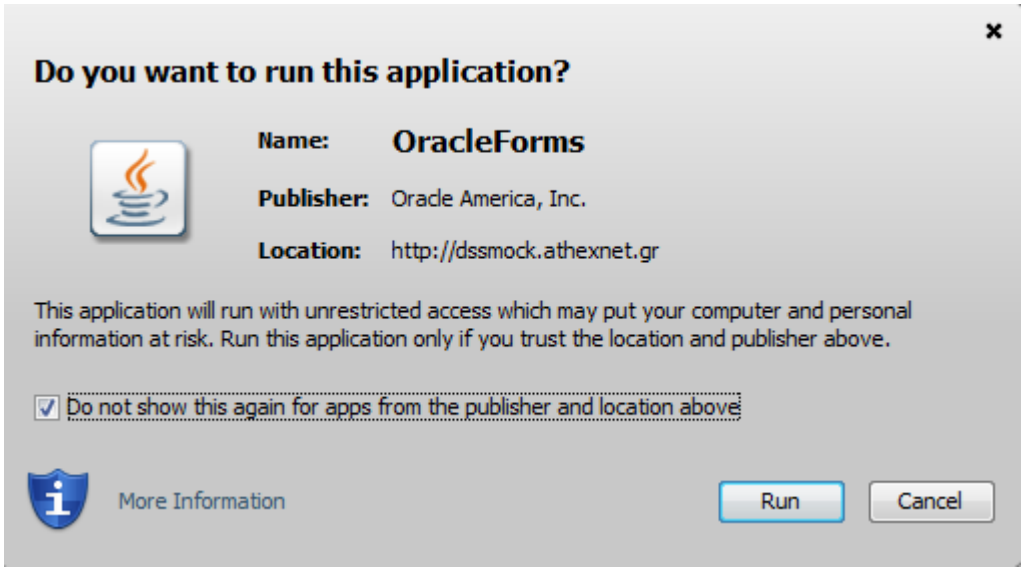
- On success, the certificate is shown in tab “Client Authentication”.

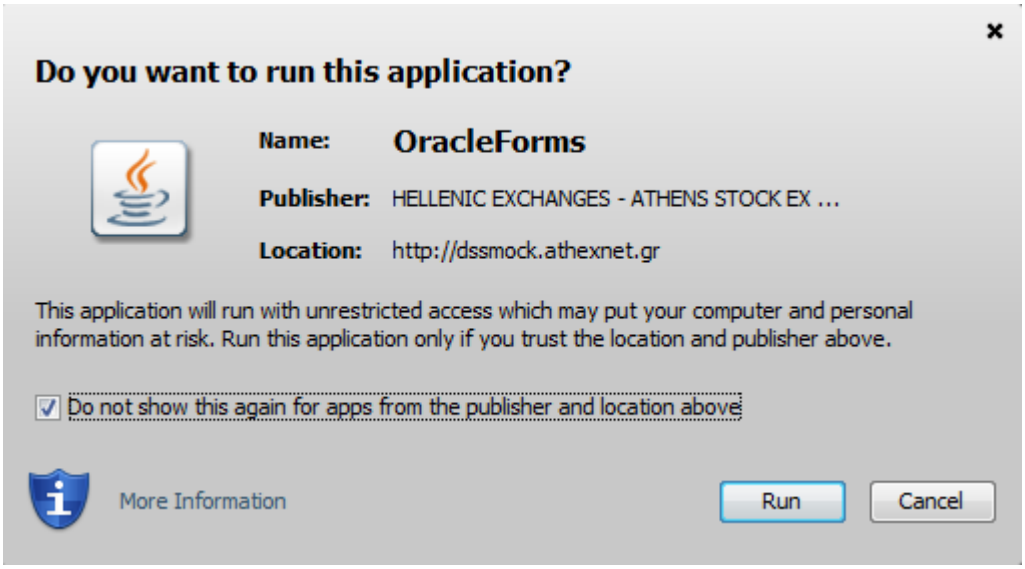


Appendix C - Code Signing Certificates

When the application is executed for the first time, the Java Runtime will issue warnings about the acceptance of the publishers of the code. Two dialogs will be presented, one regarding code that is signed by Oracle and another one regarding code that is signed by ATHEXGroup.

It is advised to select option “Do not show this again for apps from the publisher and location above” and click “Run”. Certificates for both publishers will be automatically imported in the trusted certificates store of Java.





After acceptance, the two certificates will be imported in the Java Control Panel, under the Trusted Certificates category.