Digital Certificates User Guide

Information Classification – Public

Table of Contents

Introduction

ASX utilises a Public Key Infrastructure (PKI) using Symantec's Managed PKI (MPKI) solution.

The MPKI is a cloud based service that provides access to internal and external facing applications and services and reduces the risk of fraud. This solution also provides an additional layer of protection beyond a standard user name and password.

MPKI uses digital certificates to protect information assets via the following mechanisms:

- **Authentication** – Authentication ensures the validation of machines and users.
- **Encryption** – By encoding data it ensures that information is only viewed by authorised machines and users.
- **Digital Signing** – Digital signing is equivalent to a hand written signature and enables ASX to verify integrity of data and identify any tampering intransit.
- **Access Control** – Access control determines what applications and information a user is authorised to access.
- **Non-repudiation** – This ensures all data exchanges, transactions and communications are legally valid and irrevocable.

The MPKI certificates can be enrolled via the PKI Client (advanced security template) or via a web browser (basic security template). By default certificates are provided via the basic security template. The Advanced security template is mainly for compatibility for users. Certificates will be provided via the Advanced security template on request only. Both templates provide certificates with 2056bit keys and SHA-256 signed.

Enrolling via the PKI Client (Advanced Security Template)

The default template uses the PKI client software to store and protect the client key as well automate a number of the certificate lifecycle processes.

Installing the PKI Client

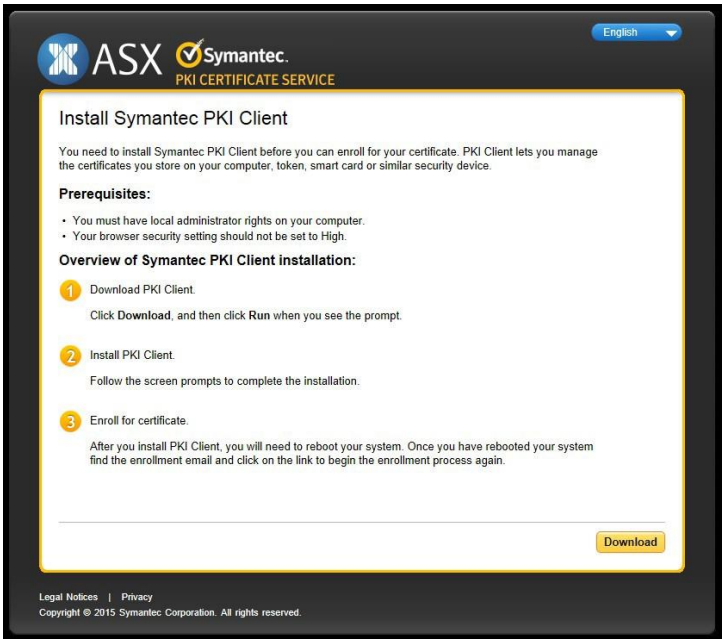
As part of the first installation, the Symantec PKI Client software automatically installs. If when installing a certificate the system blocks the installation, it can be manually downloaded by selecting Austraclear Digital certificate - Symantec PKI via https://asxonline.com/public/documents/austraclear-technical-documents.html his must be installed prior to the certificate being obtained.

To install the PKI client, the following prerequisites are required:

- Administrator rights for the computer
- Browser security settings – not set to High.

To install the PKI client manually:

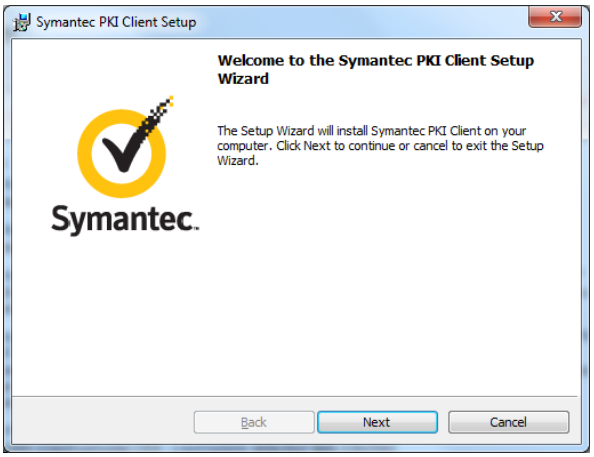
1. Click on the link provided in the email received from Symantec. This opens the Symantec screen where the PKI client can be downloaded.
2. Click **Download**.



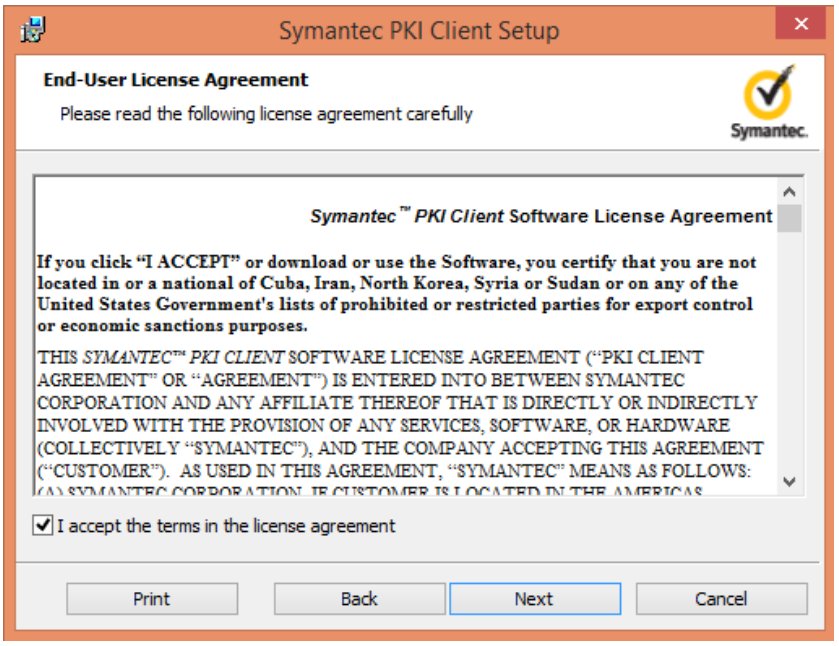
3. Click **Run**.

4. Enter the User name and Password for the Administrator in the *User Account Control* screen.

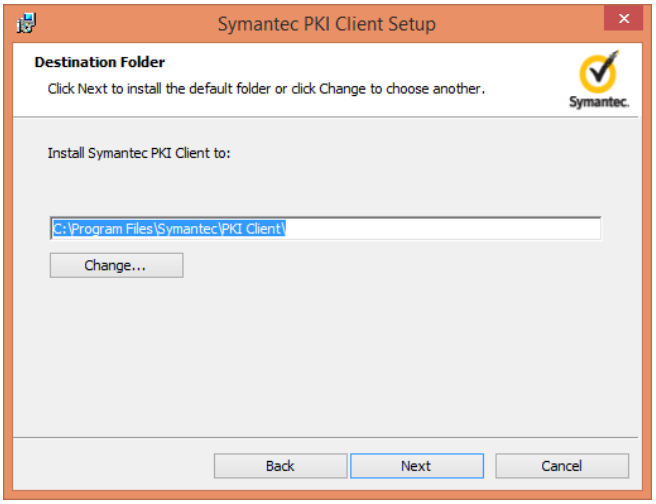
5. Click **Next**.



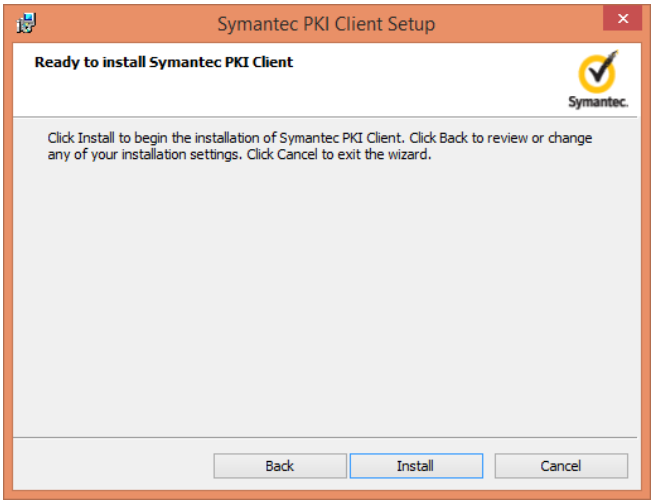
6. Select *I accept the terms in the license agreement* and click **Next**. Click **Cancel** if not in agreement with the terms and conditions.

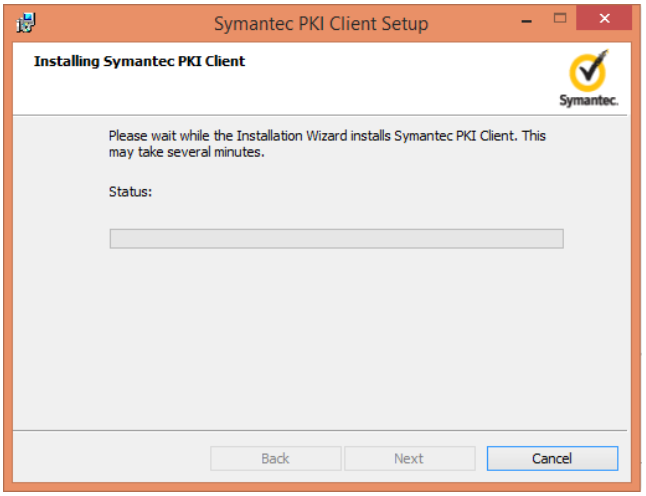


7. Click **Next**. Click **Change** to specify an alternative destination folder.

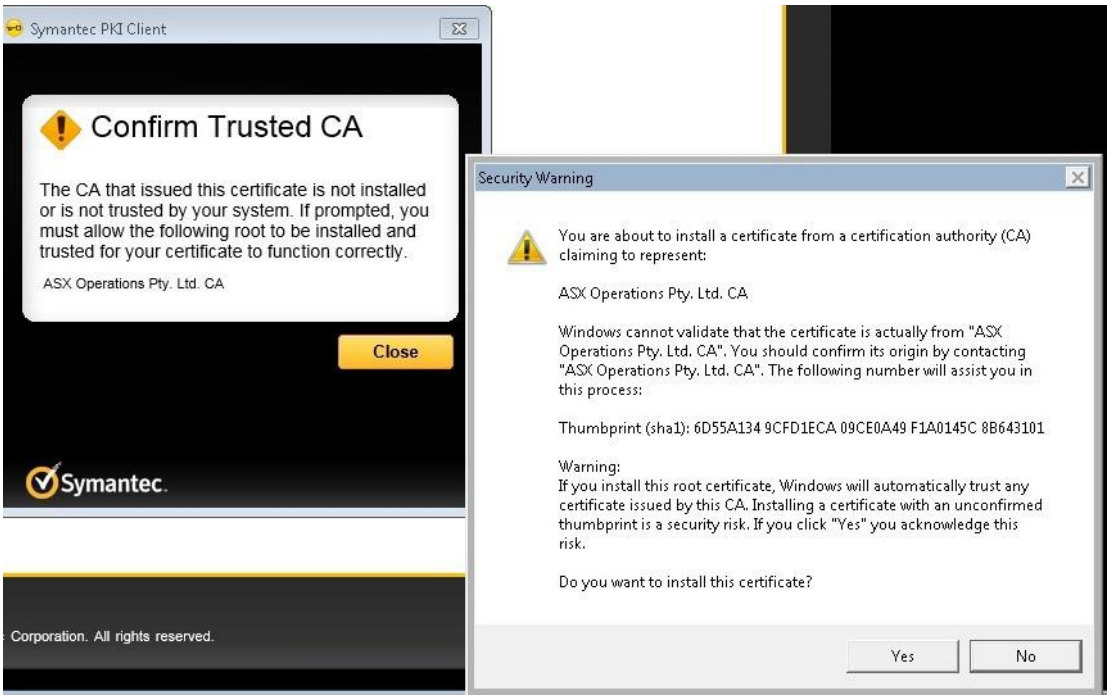


8. Click **Install** to begin the installation of the PKI client.

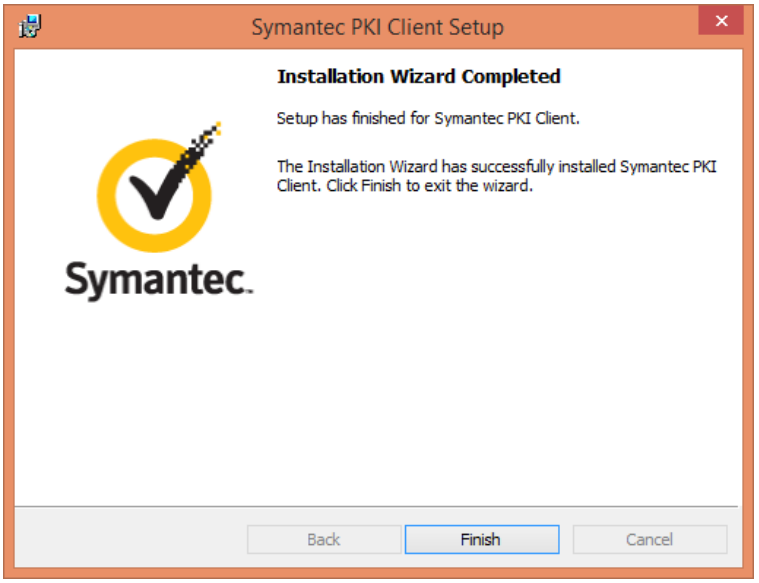




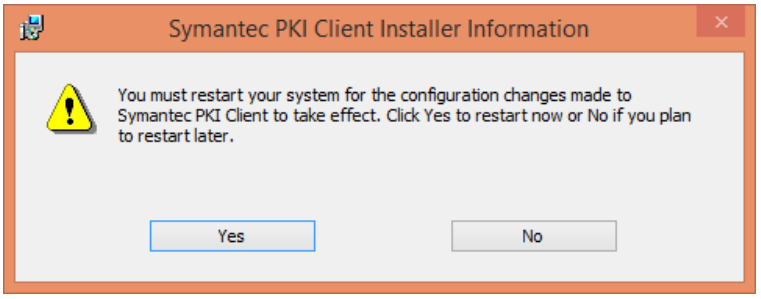
9. Confirm the installation of the Root CA. Click **Yes**.



10. Click **Finish**. Click **Finish** to complete the installation.



11. Click **Yes** to restart the system, or **No** to restart the system at a later date. In order for the configuration changes to take effect the system needs to be restarted.



Enrolling for a Certificate

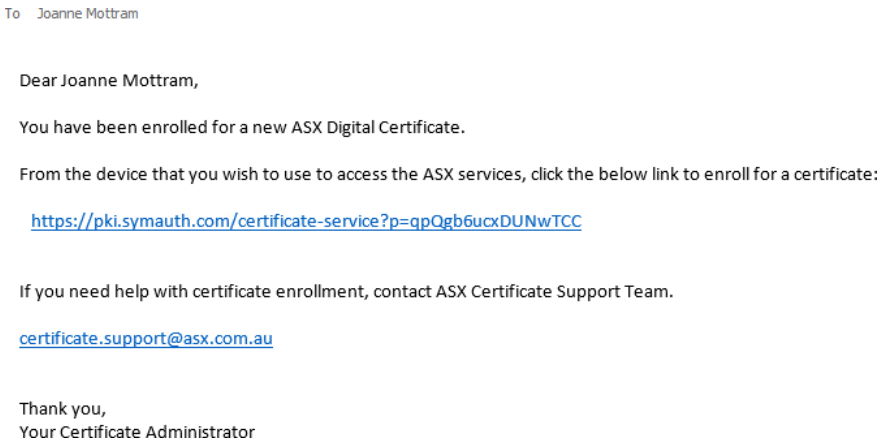
Once the PKI Client has been installed the certificate can be enrolled.

To enrol for a certificate:

1. Click the link in the provided email.

   To enrol for a new certificate or to replace an old or lost certificate, an email is required containing a specific link for enrolment.

2. Once the link has been selected, the Symantec PKI Certificate Service opens.


To Joanne Mottram

Dear Joanne Mottram,

You have been enrolled for a new ASX Digital Certificate.

From the device that you wish to use to access the ASX services, click the below link to enroll for a certificate:

https://pki.symauth.com/certificate-service?p=qpQgb6ucxDUNwTCC

If you need help with certificate enrollment, contact ASX Certificate Support Team.

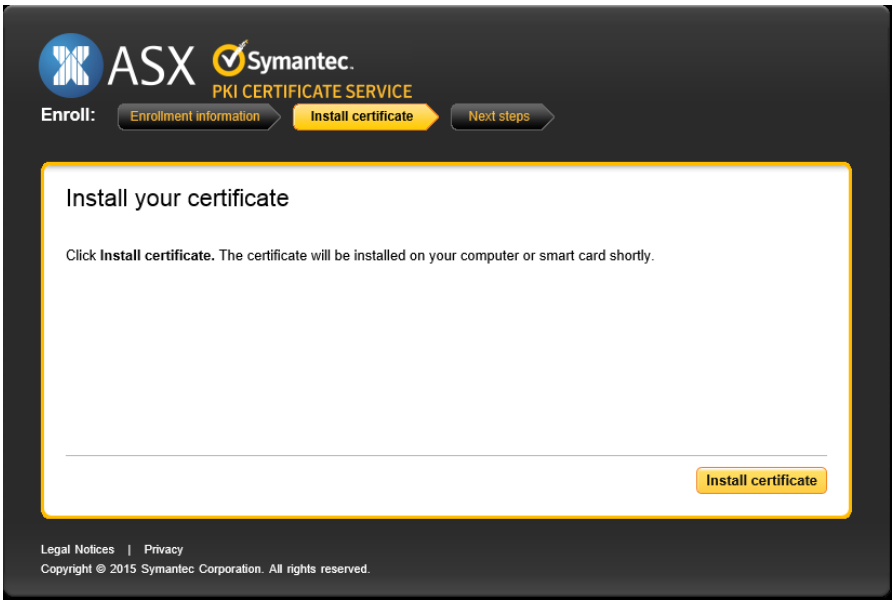
certificate.support@asx.com.au

Thank you,
Your Certificate Administrator

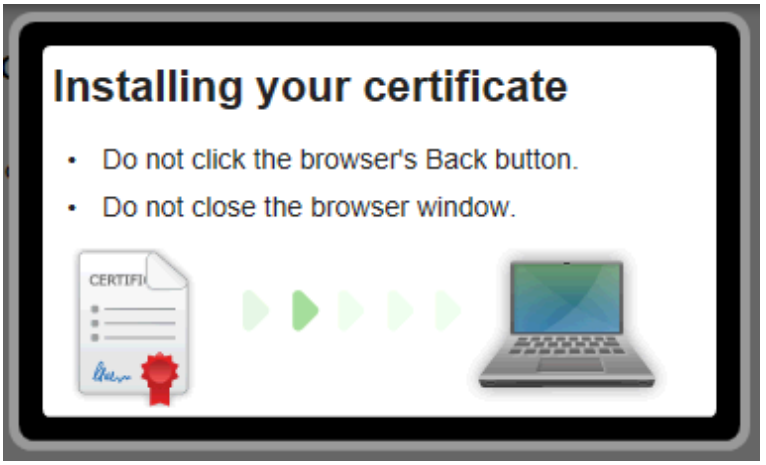
3. Check the details to verify that they are correct. Here you are given the opportunity to create a certificate nickname. The purpose of it is to be able to easily identify this certificate later.

4. Click **Continue**. This opens up a screen where the certificate can be installed.

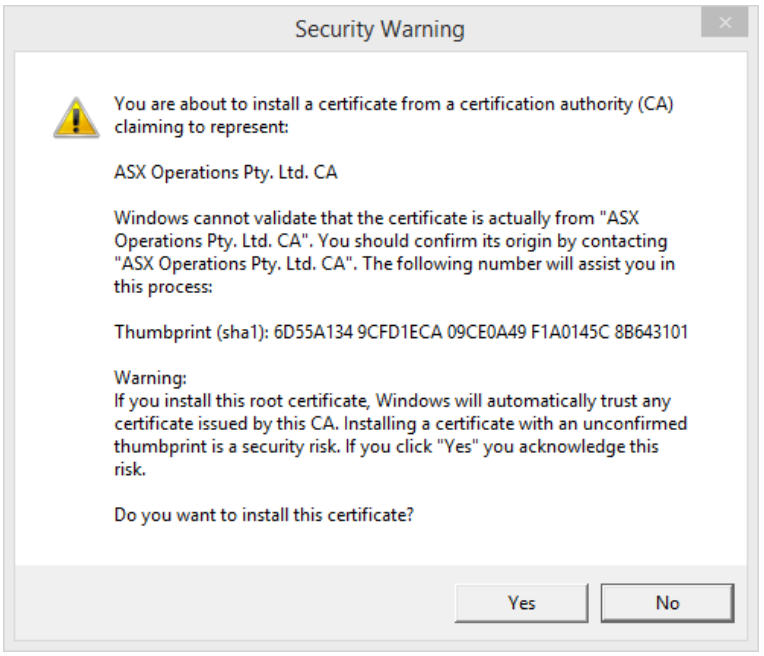
5. Click **Install Certificate**.



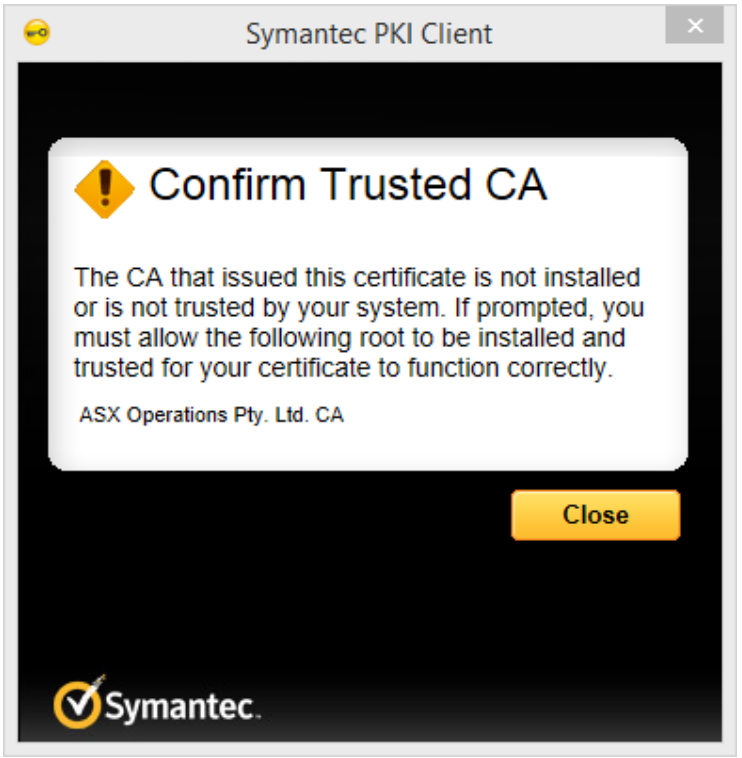
Once Install Certificate has been selected, the certificate starts installing.



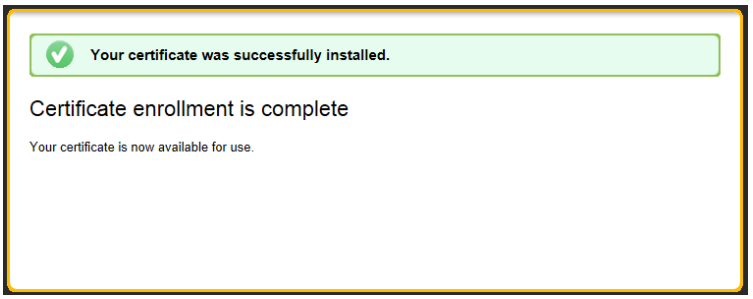
6. Click **Yes**



7. Click **Close**



Once the certificate is installed correctly, a confirmation message is displayed. The certificate can now be used for the required ASX Application.



Renewing Certificates

Using the PKI client automates the renewal of certificates.

When there are 30 days remaining on the current ASX certificate the system detects that the certificate is about to expire and the certificate is renewed automatically. A pop-up dialogue box will notify you when this happens.

Revoking Certificates

If a certificate is lost, compromised or no longer required, the certificate will need to be revoked. To revoke a certificate contact ASX (Austraclear@asx.com.au) who will revoke the certificate and if required will send back an email with new enrolment details.

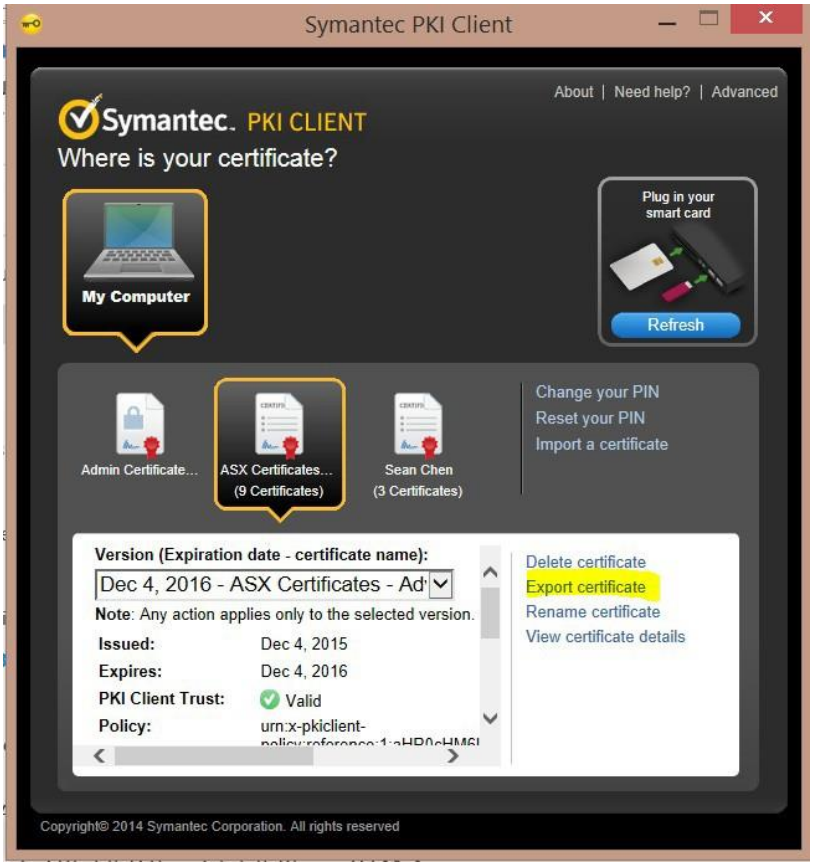
Export/Import certificates

In some cases it might be required to export the certificate from the computer where it was downloaded and to import it into another computer. Examples would be importing the certificate to BCP computers or to computers that connect to ASX via dedicated networks (e.g. ANNI) and don't have internet connectivity. When exporting the certificate it is important to ensure that the certificate file is kept safe and protected by a strong password as it represents part of your login credentials with ASX.

Export certificate

The example covers exporting a certificate enrolled via the PKI Client software (Advanced Security Profile).

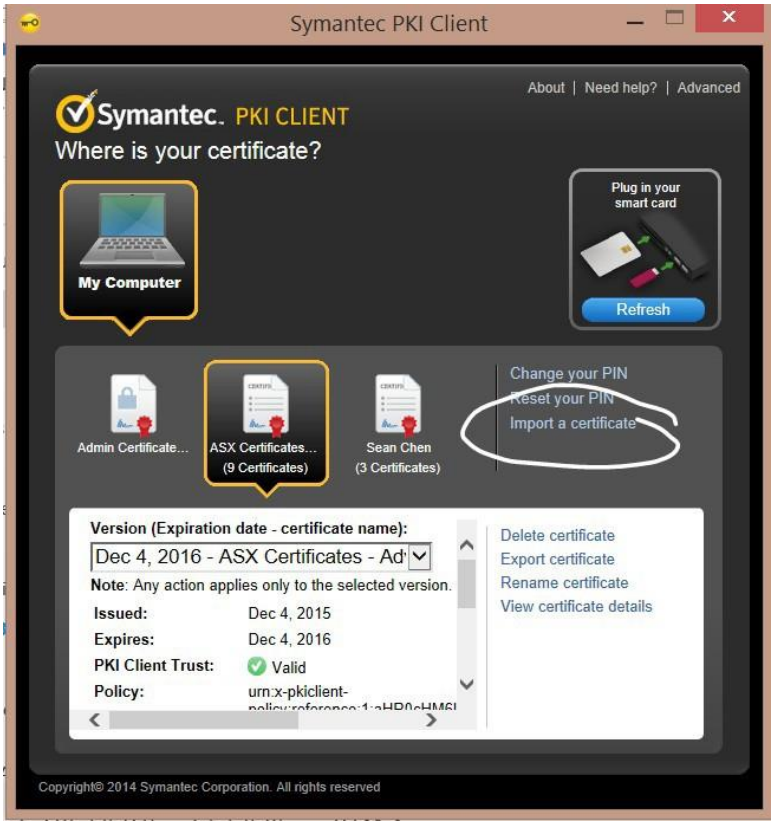
1. Open the Symantec PKI Client application
2. Select the certificate you would like to export
3. Click **Export Certificate**



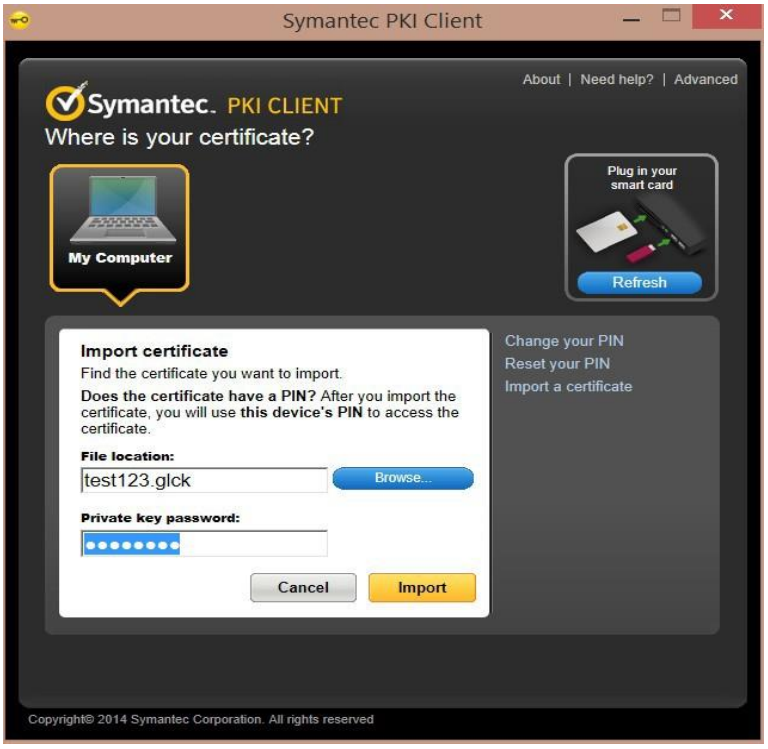
4. Select **Maximise compatibility with other systems** if you plan to install it on a computer that doesn't have PKI Client software installed. Or select **For import with PKI Client** if you plan to install the certificate on a computer that has PKI Client installed.
5. Type a strong password in the field named **Create private key password.** Note that this password will be required for importing the certificate at the destination computer.
6. Save the certificate file to a file location of your choice.

Import certificate to a computer with PKI Client software

1. Open the Symantec PKI Client application
2. Click on **Import Certificate**



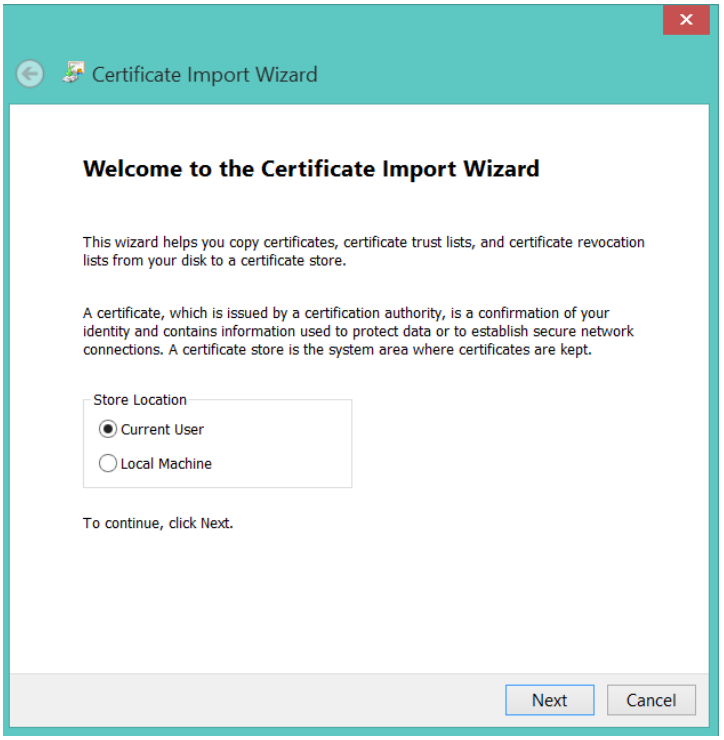
3. Point to the exported certificate .glck file
4. Type the password in the **Private key password** field
5. Click **Import**



Import certificate to a computer without PKI Client.

Example is provided with Windows 7. Similar process is followed for other Windows versions.

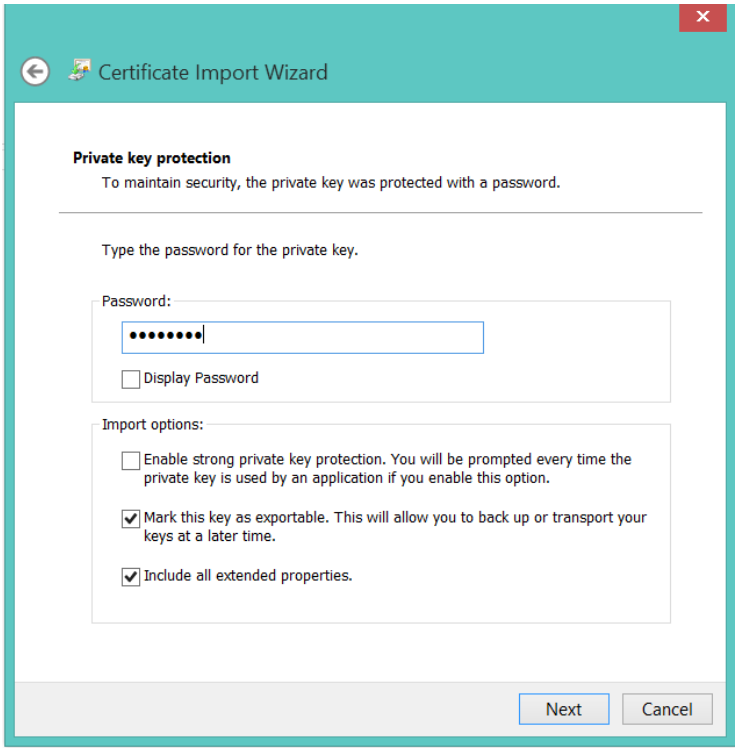
1. Double-click on the exported certificate .p12 file
2. Select **Current User**



3. Click **Next**

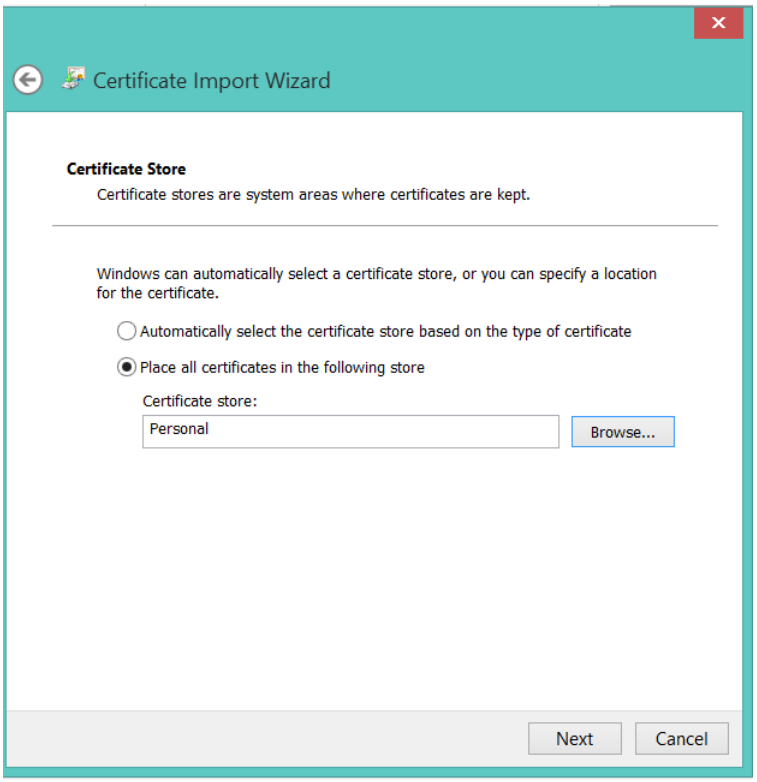
4. In the **File to import** window click **Next**

5. In the **Private key protection** window type the password and tick the **Mark this key as exportable** box if you would like to be able to export the certificate from this computer



6. Click **Next**

7. In the Certificate Store window select **Place all certificates in the following** store and select the **Personal** certificate store



8. Click **Next**
9. Click **Finish**

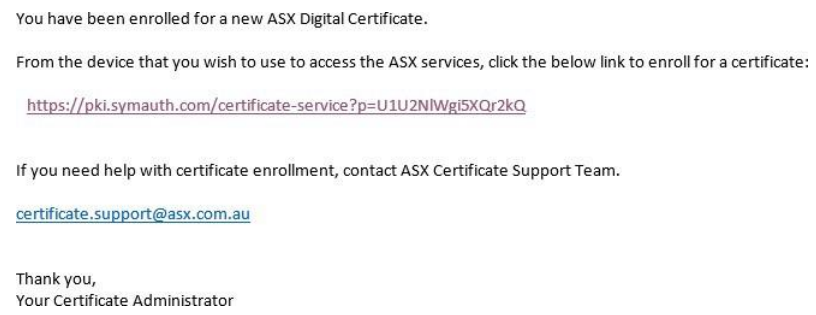
Enrolling Via a Browser (Basic Security Template)

The basic security template uses a web browser to download the certificate and Windows certificate store to store and protect the private key.

Enrolling for a Certificate

To enrol for a certificate:

1. Click the link provided in the email received from Symantec.


You have been enrolled for a new ASX Digital Certificate.

From the device that you wish to use to access the ASX services, click the below link to enroll for a certificate:

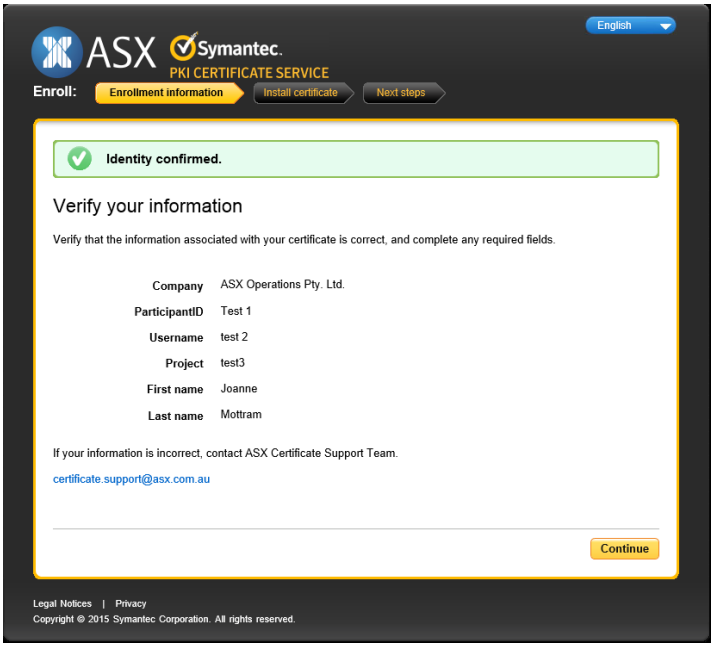
https://pki.symauth.com/certificate-service?p=U1U2NlWgi5XQr2kQ

If you need help with certificate enrollment, contact ASX Certificate Support Team.

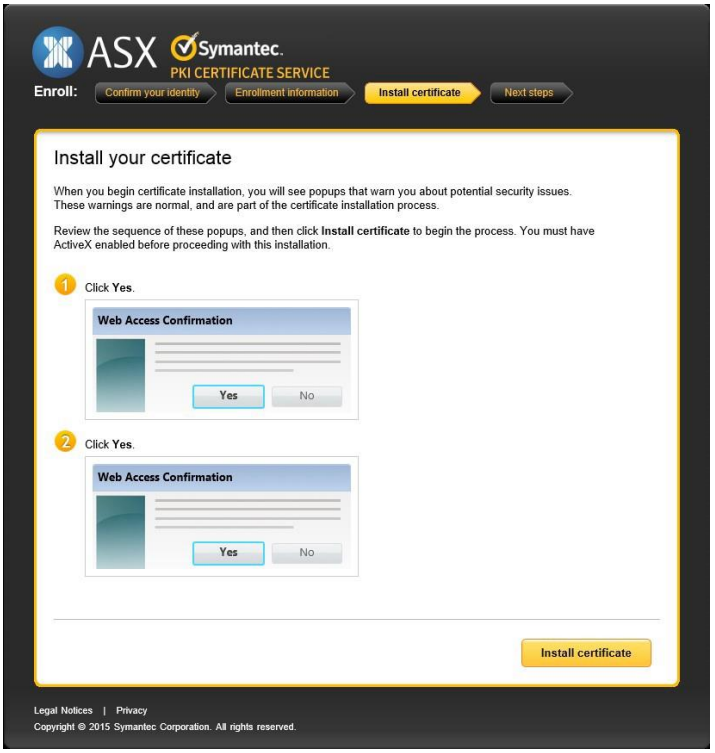
certificate.support@asx.com.au

Thank you,
Your Certificate Administrator

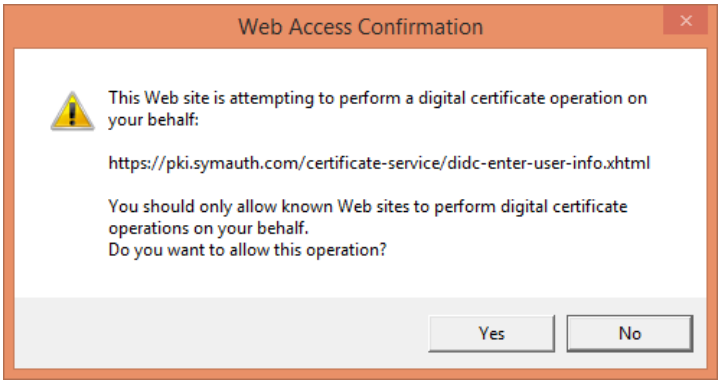
2. Verify the enrolment information and click **Continue**. If the enrolment information is incorrect, contact ASX Customer Support at Austraclear@asx.com.au.



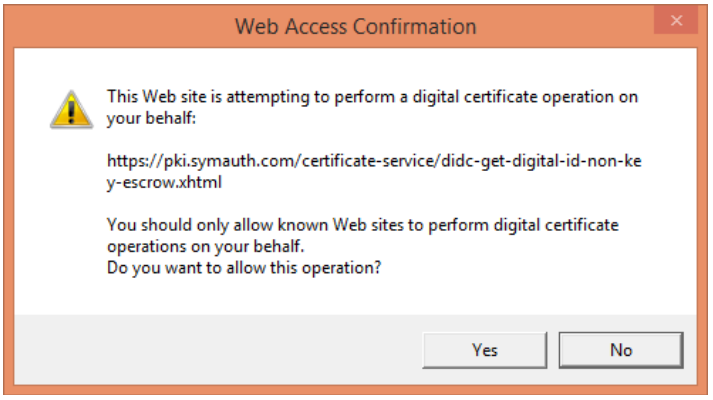
3. Click **Install Certificate**



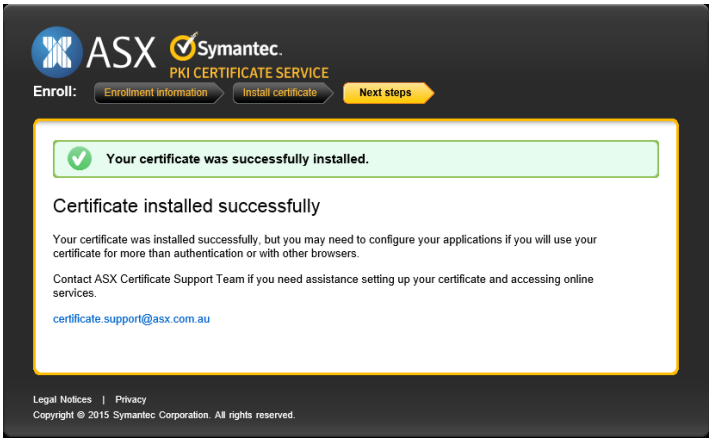
4. Click **Yes**



5. Click **Yes**



When the certificate has been successfully installed a confirmation message is displayed.



Renewing a Certificate

30 days prior to the ASX Certificate expiring an email is sent containing a link for renewing the certificate. Click the link and the certificate is automatically renewed.

Dear First Name1 Last Name,

Our records indicate that your ASX Digital ID (certificate) named ASX Certificates - Basic Security will expire in 29 days, at 11:59 PM UTC on Wednesday, April 15, 2015. To continue accessing company services, you need to renew your certificate before April 16, 2015.

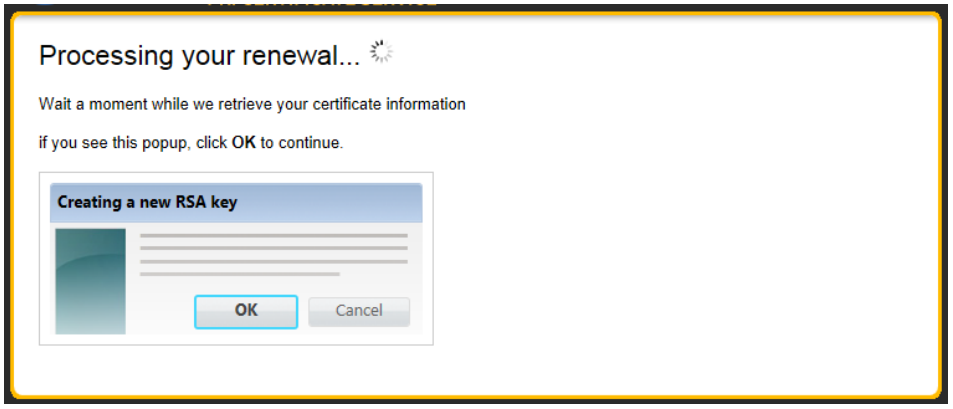
From the device you used to enroll for this certificate, access the following link to renew this certificate:

https://pki.symauth.com/certificate-service/renew/?id=

If you need help with certificate renewal, contact ASX Certificate Support Team.

certificate.support@asx.com.au

Thank you,
Your Certificate Administrator



Revoking a Certificate

If a certificate is lost, compromised or no longer required the certificate will need to be revoked. To revoke a certificate contact ASX (Austraclear@asx.com.au) who will revoke the certificate and if required will send back an email with new enrolment details.

Export/Import certificates

In some cases it might be required to export the certificate from the computer where it was downloaded and to import it into another computer. Examples would be importing the certificate to BCP computers or to computers that connect to ASX via dedicated networks (e.g. ANNI) and don't have internet connectivity. When exporting the certificate in is important to ensure that the certificate file is kept safe and protected by a strong password as it represents part of your login credentials with ASX.

Export certificate

The example covers exporting a certificate enrolled via browser (no PKI Client - Basic Security Profile).

1. Open Internet Explore --> Tools --> Internet Options --> Content --> Certificates
2. Select the certificate you want to export and click the **Export** button
3. In the **Welcome to the certificate export wizard** click **Next**
4. In the **Export private key** window click **Yes, export the privatekey**
5. Click **Next**
6. In the **Export file format** window select **Personal Information Exchange PKCS #12 (.pfx)**
7. Select **Include all certificates in the certificate path if possible** and **Export all extended properties**
8. In the **Security** window select the protection mechanism for your exported certificate. If the source and destination computer are part of the same Active Directory system, then

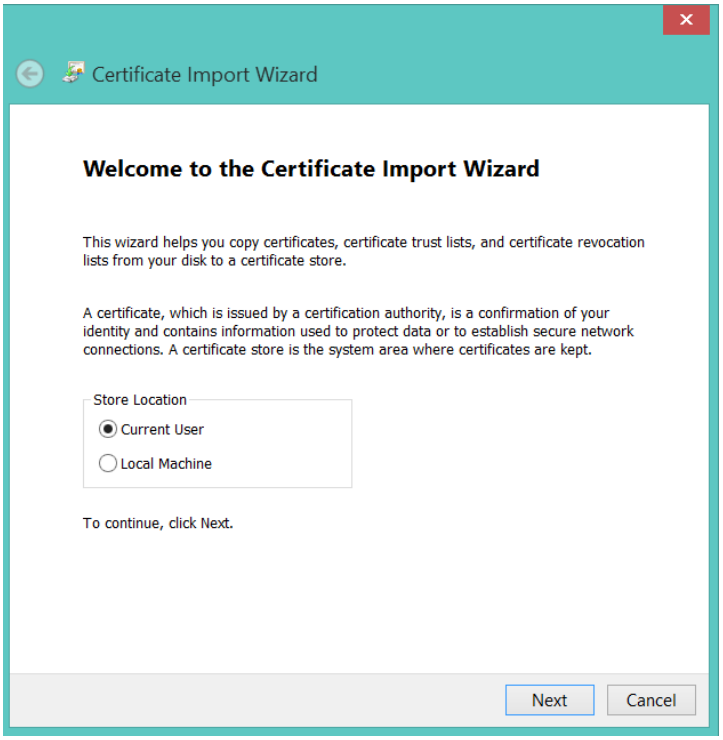
select **Group or usernames** and add the active directory group or usernames that need access to the exported certificate. Otherwise select **Password** and type and reconfirm the password that will be used to protect the certificate.

9. Click **Next**
10. In the **Filename to export** window type select the location for the file export and type the filename for the exported certificate.
11. Click **Next**
12. Click **Finish**

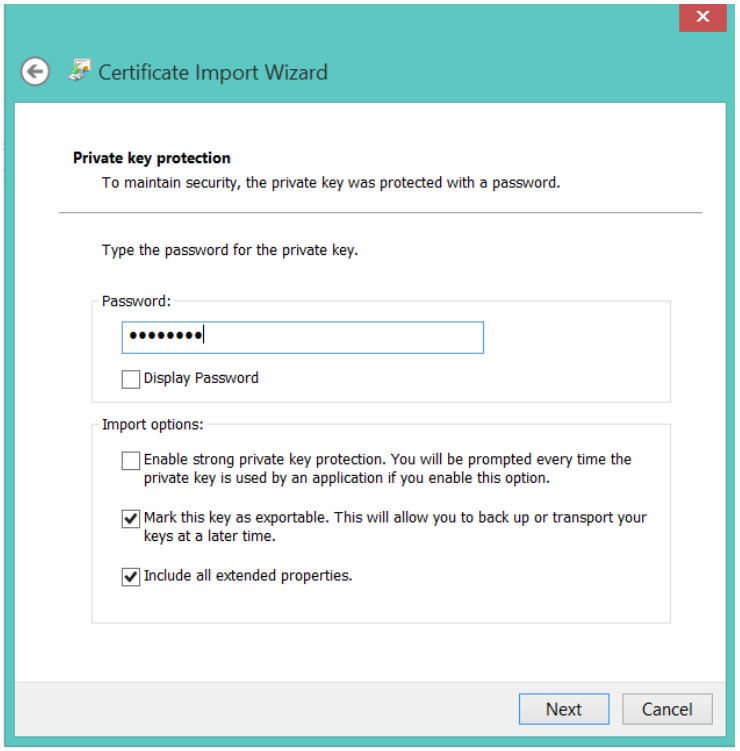
Import certificate to a computer without PKI Client.

Example is provided with Windows 7. Similar process is followed for other Windows versions.

13. Double-click on the exported certificate .p12 file
14. Select **Current User**

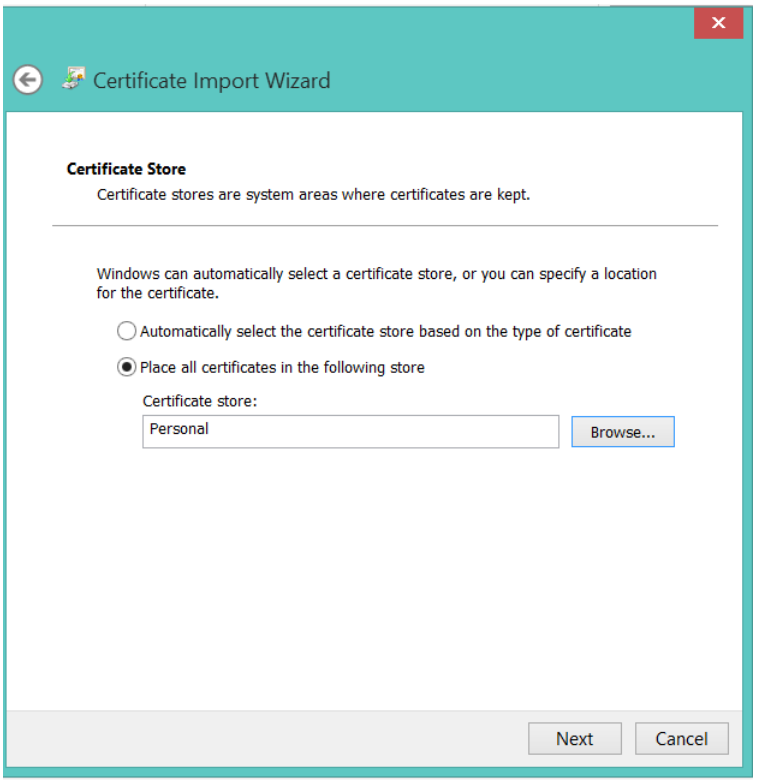


15. Click **Next**
16. In the **File to import** window click **Next**
17. In the **Private key protection** window type the password and tick the **Mark this key as exportable** box if you would like to be able to export the certificate from this computer



18. Click **Next**

19. In the Certificate Store window select **Place all certificates in the following** store and select the **Personal** certificate store



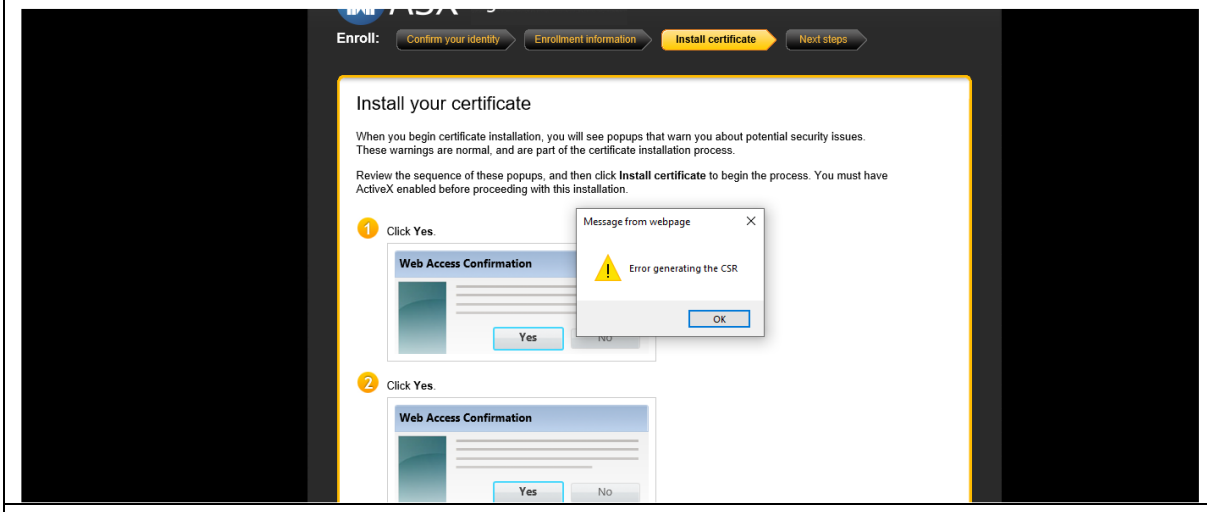
20. Click **Next**

21. Click **Finish**

Troubleshooting

Error generating the CSR

What does the screen look like?



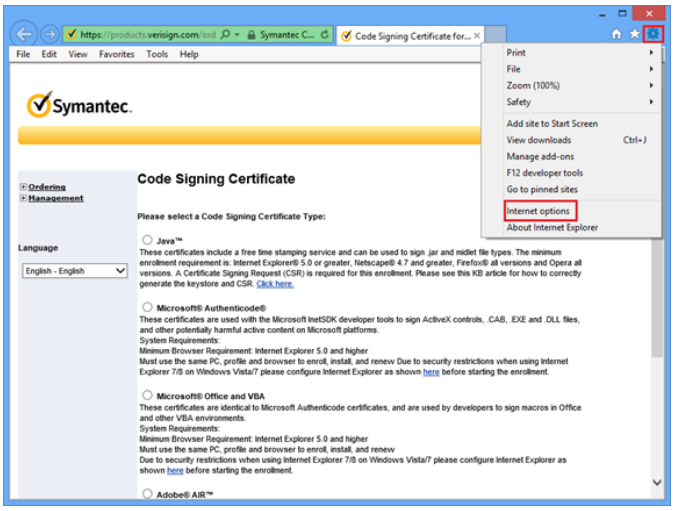
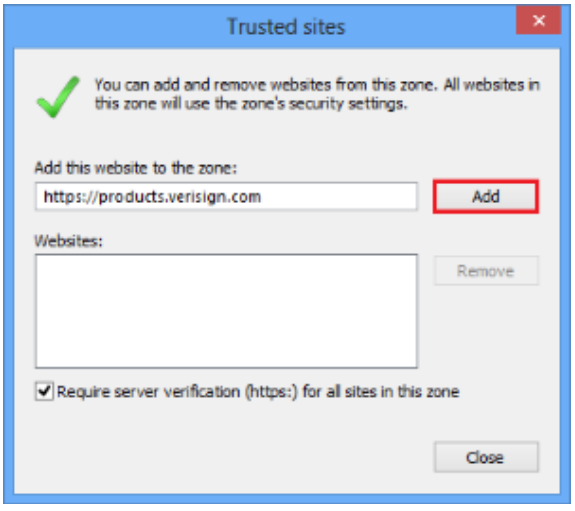
What does this code mean?

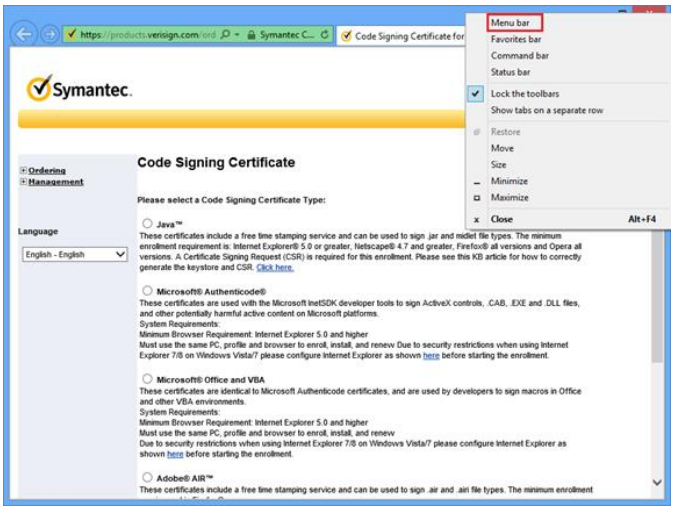
	The basic Digital Certificate was not installed. **This does not occur for advanced certificates.**

What do you need to do?

Please follow the steps below:

Step	Basic Certificate	
1	**Add web site as trusted sites by:**	
1.1	Opening Internet Explorer	

1.2	From the menu bar, click **Tools** > **Internet Options**	
1.3	Click **Security** tab select > sites	
1.4	Click **Add** and type in URL https:/products.verisign.com	
1.5	Click **Close** > **OK**	
2	**Enable Compatibility Mode by:**	
2.1	Opening Internet Explorer	

2.2	Right click on the top bar - select **Menu bar**	

Invalid Enrollment Link

What does the screen look like?
What does this code mean?
The basic Digital Certificate was not installed.
What do you need to do?
Please complete a new Digital Certificate form requesting a new digital certificate and attach as an Email austraclear@asx.com.au. The form can be located here <Link>

Your Browser is not supported at this time

What does the screen look like?

What does this code mean?
The basic Digital Certificate was not installed. An unsupported browser was used to access your unique enrollment link.
What do you need to do?
The an unsupported browser was used. We recommend accessing the link via Internet Explorer 9, 10 or 11.

Frequently Asked Questions

Q1: What are the benefits of using PKI Client?

A: PKI Client software provides additional security for the downloaded client certificates and provides user friendly certificate management (enrolments and renewals).

Q2: What port is used by the PKI client?

A: 443

Q3: What URLs does the PKI client require access to?

A: http://liveupdate.symantec.com; https://pki.symauth.com/ ; http://sr.symcb.com/ ; https://pki-ra.symauth.com; http://pki-ocsp.symauth.com; http://pki-crl.symauth.com

Table C1 (page 56) in the PKI Client Admin Guide lists all the access that the PKI Client needs.

pki-client-std-admin-guide.pdf

guide.pdf

Q4: What are the Symantec Managed PKI service IP Address range?

A: Symantec Managed PKI Service IP Address Range

pki-client-std-script
s-guide.pdf

Q5: Is the PKI Client software digitally signed?

A: Yes, the name of the signing organisation is "Symantec Corporation"

Q6: How do I download the Symantec PKI Client?

A: You'll be prompted to download it when you receive the enrolment link from ASX or alternatively you can manually download it by selecting Austraclear Digital certificate - Symantec PKI via https:// www.asxonline.com/public/documents/austraclear-technical-documents.html .

Q7: What operating system permissions are required for the installation of the Symantec PKI client?

A: Windows Administrator permissions are required to install the Symantec PKI Client. Where the users do not have Administrator permissions the PKI Client can be centrally deployed. Link to the client download pages is included in this FAQ.

Q8: What is the size of the Symantec PKI client?

A: The installer package is about 17MB.

Q9: What is the platform support for the PKI client?

A: For PKI Client version 8.14 the certified operating system and browser platform support is as follows. Check the Symantec PKI client Administrator Guide for the latest list of supported OS and browsers. Notably Windows XP is not supported.

Windows 7 SP1 (32-bit and 64-bit)

IE 9 (32-bit), IE 10 (32-bit), and IE 11

Firefox 38

Chrome 43

Windows® 8.1 (32-bit and 64-bit)

IE 11

Firefox 38

Chrome 43

Mac OS X v10.9.5a

Safari 7.1.6

Firefox 38

Chrome 43

Mac OS X v10.10.3b

Safari 8.0.6

Firefox 38

Chrome 43

Q10: What if my company's policy doesn't allow for installing the PKI Client software?

A: ASX can provide a more "traditional" browser based (no PKI Client) certificate enrolment on request. This method requires more user interactions around enrolment and renewals and specific browser settings to be enabled (ActiveX installation, EPM to be turned off). Please contact the Austraclear Helpdesk (Austraclear@asx.com.au) if you would require browser based enrolment for your client certificates.

Q11: Is the new CA publicly trusted?

A: No. It is an ASX private CA. The Root CA certificate will get automatically delivered to your computer as part of the initial enrolment.

Q12: What is the certified platform support for browser enrolments (no PKI Client)?

A: For MPKI version 8.14 the operating system and browser platform support is as follows:

Windows 7 Enterprise edition SP1

(32-bit and 64-bit)

IE 8 (32-bit), IE 9 (32-bit), IE 10 (32-bit), IE 11a

Firefox 38

Windows 8.1 (32-bit and 64-bit)

IE 11a

Firefox 38

Mac OS X v10.9.5

Safari 7.1.6

Firefox 38

Mac OS X v10.10.3

Safari 8.0.6

Firefox 38

Q13: What Internet Explorer settings are required to install a certificate (no PKI Client)?

A: Active-X needs to be enabled in order for the enrolment to work. The renewal plug-in is not supported in IE 11 if Enhanced Protection Mode (EPM) is enabled. EPM is disabled by default in IE 11.

Q14: Are SHA-256 certificates supported on Windows XP platform?

A: While Windows XP SP3 supports SHA-256 certificates, the PKI Client based certificates provided by ASX are not compatible with Windows XP. The PKI client will not install on this operating system. Where Windows XP has to be used, the browser based enrolment (no PKI Client) is recommended. Please contact the ASX Certificate Support Team (certificate.support@asx.com.au) if you would require browser based enrolment for your client certificates.

Q15: Are certificates exportable? Can I transfer the certificate to a computer that is not connected to Internet or to a BCP computer?

A: Yes - the downloaded certificates can be exported and transferred to another computer. For details refer to the ASX Digital Certificates User Guide. At expiry of the transferred certificates, the certificate should be renewed on the original Internet connected computer and then exported and moved to the destination computer.

Q16: Where do I find more details around how to enrol, renew, export certificates?

A: For these details refer to the ASX Digital Certificates User Guide.

Information Classification – Public

Disclaimer

This document provides general information only and may be subject to change at any time without notice. ASX Limited (ABN 98 008 624 691) and its related bodies corporate ("ASX") makes no representation or warranty with respect to the accuracy, reliability or completeness of this information. To the extent permitted by law, ASX and its employees, officers and contractors shall not be liable for any loss or damage arising in any way, including by way of negligence, from or in connection with any information provided or omitted, or from anyone acting or refraining to act in reliance on this information. The information in this document is not a substitute for any relevant operating rules, and in the event of any inconsistency between this document and the operating rules, the operating rules prevail to the extent of the inconsistency.

ASX Trade Marks

The trade marks listed below are trademarks of ASX. Where a mark is indicated as registered it is registered in Australia and may also be registered in other countries. Nothing contained in this document should be construed as being any licence or right to use of any trade mark contained within the document.

ASX®