

Digital Certificates User Guide



Information Classification – Public

Table of Contents

TABLE OF CONTENTS	
INTRODUCTION	
ENROLLING VIA THE PKI CLIENT (ADVANCED SECURITY TEMPLATE)	4
INSTALLING THE PKI CLIENT	4
ENROLLING FOR A CERTIFICATE	
Renewing Certificates	
Revoking Certificates	
Export/Import certificates	
Export certificate	
Import certificate to a computer with PKIClient software	
Import certificate to a computer without PKI Client	
ENROLLING VIA A BROWSER (BASIC SECURITY TEMPLATE)	19
ENROLLING FOR A CERTIFICATE	
Renewing a Certificate	
Revoking a Certificate	
Export/Import certificates	
Export certificate	22
Import certificate to a computer without PKI Client	23
TROUBLESHOOTING	26
ERROR GENERATING THE CSR	
INVALID ENROLLMENT LINK	
YOUR BROWSER IS NOT SUPPORTED	

REQUENTLY ASKED QUESTIONS

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 <u>https://asxonline.com/public/documents/austraclear-technical-documents.html</u> 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.

Ins	tall Symantec PKI Client
You the c	need to install Symantec PKI Client before you can enroll for your certificate. PKI Client lets you manage ertificates you store on your computer, token, smart card or similar security device.
Pre	requisites:
• Ye	ou must have local administrator rights on your computer. our browser security setting should not be set to High.
Ove	rview of Symantec PKI Client installation:
1	Download PKI Client
	Click Download, and then click Run when you see the prompt.
2	Install PKI Client.
	Follow the screen prompts to complete the installation.
3	Enroll for certificate.
	After you install PKI Client, you will need to reboot your system. Once you have rebooted your system find the enrollment email and click on the link to begin the enrollment process again.
23	Download

3. Click Run.

Do you want to run or save Symantec-PKI-Client-2.13.0.exe (24.7 MB) from pki.symauth.com?	Run	Save	-	Cancel	×

- 4. Enter the User name and Password for the Administrator in the User Account Control screen.
- 5. Click **Next**.

Bymantec PKI Client Setup		
	Welcome to the Symantec PKI Client Setup Wizard	
	The Setup Wizard will install Symantec PKI Client on your computer. Click Next to continue or cancel to exit the Setup Wizard.	
Symantec.		
	Back Next Cancel	

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

B Symantec PKI Client Setup	×			
End-User License Agreement Please read the following license agreement carefully Sym	antec.			
Symantec [™] PKI Client Software License Agreeme	nt			
If you click "I ACCEPT" or download or use the Software, you certify that you are not located in or a national of Cuba, Iran, North Korea, Syria or Sudan or on any of the United States Covernment's lists of prohibited or restricted parties for export control or economic sanctions purposes.				
THIS SYMANTEC TH PKI CLIENT SOFTWARE LICENSE AGREEMENT ("PKI CLIENT AGREEMENT" OR "AGREEMENT") IS ENTERED INTO BETWEEN SYMANTEC CORPORATION AND ANY AFFILIATE THEREOF THAT IS DIRECTLY OR INDIRECTLY INVOLVED WITH THE PROVISION OF ANY SERVICES, SOFTWARE, OR HARDWARE (COLLECTIVELY "SYMANTEC"), AND THE COMPANY ACCEPTING THIS AGREEMENT ("CUSTOMER"). AS USED IN THIS AGREEMENT, "SYMANTEC" MEANS AS FOLLOWS:				
\blacksquare I accept the terms in the license agreement				
Print Back Next Cancel				

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

iii 🗄	Symantec PKI C	lient Setup	×
Destination Click Next t	Folder o install the default folder or click Cha	nge to choose another.	Symantec.
Install Syma	intec PKI Client to:		
C:\Program	n Files\Symantec\PKI Client\		
Chan	je		
	Pade	Neut	Cancel

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

國		Symantec PKI C	lient Setup	×
Ready to	install Symante	ec PKI Client		Symantec.
Click Inst any of yo	all to begin the in: uur installation set	stallation of Symantec F tings. Click Cancel to e	KI Client. Click Back to xit the wizard.	review or change
		Back	Install	Cancel
₿		Symantec PKI CI	ient Setup	- • ×
Installing	Symantec PKI (Client		Symantec.
	Please wait while may take severa	the Installation Wizard I minutes.	installs Symantec PKI (Client. This
	Status:			

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



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

遇	Symantec PKI Client Setup	×
₽ Symantec	Symantec PKI Client Setup Installation Wizard Completed Setup has finished for Symantec PKI Client. The Installation Wizard has successfully installed Symantec P Client. Click Finish to exit the wizard.	ж
	Back Finish Cancel	

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:

<a href="https://pki.symauth.com/certificate-service?p=qpQgb6ucxDUNwTCC">https://pki.symauth.com/certificate-service?p=qpQgb6ucxDUNwTCC</a>

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

<a href="mailto:certificate.support@asx.com.au">certificate.support@asx.com.au</a>

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.

ASX Øs PKI CEI Enroll: Enrollment informati	ymantec. RTIFICATE SERVICE on Install certificate Next steps	English
V Identity confirme	d.	
Verify your informa	tion	
Verify that the information assoc	ciated with your certificate is correct, and complete any required fields.	
Company	ASX Operations Pty. Ltd.	
First name	Joanne	
Last name	Mottram	
Project	Test 1	
Username	test 2	
ParticipantID	test3	
Certificate nickname	ASX Certificates - Advanced Security	0
If your information is incorrect, c	contact ASX Certificate Support Team.	
		Continue

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

Security Warning	×
You are about to install a certificate from a certification authority (CA) claiming to represent: ASX Operations Pty. Ltd. CA Windows cannot validate that the certificate is actually from "ASX Operations Pty. Ltd. CA". You should confirm its origin by contacting "ASX Operations Pty. Ltd. CA". The following number will assist you in this process: Thumbprint (sha1): 6D55A134 9CFD1ECA 09CE0A49 F1A0145C 8B643101 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?	
Yes No	
	Security Warning You are about to install a certificate from a certification authority (CA) claiming to represent: ASX Operations Pty. Ltd. CA Windows cannot validate that the certificate is actually from "ASX Operations Pty. Ltd. CA". You should confirm its origin by contacting "ASX Operations Pty. Ltd. CA". The following number will assist you in this process: Thumbprint (sha1): 6D55A134 9CFD1ECA 09CE0A49 F1A0145C 8B643101 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?

7. Click Close

•	Symantec PKI Client		×
	Confirm Trusted C	A	1
The or i mu tru: AS	The CA that issued this certificate is not installed or is not trusted by your system. If prompted, you must allow the following root to be installed and trusted for your certificate to function correctly. ASX Operations Pty. Ltd. CA		
		Close	
Ø	Symantec.		

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

Vour certificate was successfully installed.
Certificate enrollment is complete
Your certificate is now available for use.

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 (<u>Austraclear@asx.com.au</u>) 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 .p12file
- 2. Select Current User

	×
📀 🕭 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.	
Store Location	
Current User	
Uccal Machine	
To continue, click Next.	
Next Can	icel

- 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

	×
< 🕭 Certificate Import Wizard	
Private key protection	
To maintain security, the private key was protected with a password.	
	-
Type the password for the private key.	
Password:	
••••••	
Display Password	
Import options:	
Enable strong private key protection. You will be prompted every time the	
private key is used by an application in you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
✓ Include all extended properties.	
Next Cancel	
Next	

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

Certificate Sto Certificate	stores are system a	reas where cer	tificates are kept.		
Windows of for the cer	can automatically sel tificate.	lect a certificate	store, or you can	specify a	location
Auto	matically select the	certificate store	based on the typ	e of certi	ficate
Place	e all certificates in th	he following sto	re		
Cert	tificate store:				
Per	rsonal			E	Browse

- 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=U1U2NIWgi5XQr2kQ
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 <u>Austraclear@asx.com.au</u>.

Verify your information Verify that the information associate Company	DD ed with your certificate is correct, and comp SX Operations Pty. Ltd.	plete any required fields.	
Verify your information Verify that the information associat Company	DD ed with your certificate is correct, and comp .SX Operations Pty. Ltd.	plete any required fields.	
Verify that the information associate	ed with your certificate is correct, and comp	plete any required fields.	
Company A	SX Operations Pty. Ltd.		
	-		
ParticipantID T	est 1		
Username te	est 2		
Project te	est3		
First name J	oanne		
Last name	fottram		
If your information is incorrect, con'	act ASX Certificate Support Team.		
certificate.support@asx.com.au			
			Continue
gal Notices Privacy			

3. Click Install Certificate

nstall your	certificate				
/hen you begin c hese warnings ar	artificate installation, you w e normal, and are part of th	vill see popups tha he certificate insta	t warn you about p Illation process.	otential securit	/ issues.
eview the sequer ctiveX enabled b	ice of these popups, and the efore proceeding with this it	hen click Install c installation.	ertificate to begin	the process. Yo	ou must have
Click Ve-					
Ulick Yes.	an Caufinnation				
Web Acc	ss commation				
	Yes	No			
2 Click Yes.					
Web Acc	ess Confirmation				
_					
	Yes	No			

4. Click Yes

	Web Access Confirmation	
Â	This Web site is attempting to perform a digital certificate operation on your behalf: https://pki.symauth.com/certificate-service/didc-enter-user-info.xhtml You should only allow known Web sites to perform digital certificate operations on your behalf. Do you want to allow this operation?	
	Yes No	

5. Click Yes



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

MSX Symantec. PKI CERTIFICATE SERVICE Enroll: Enrolment information Instat certificate Next steps	
Vour certificate was successfully installed.	
Certificate installed successfully	
Your certificate was installed successfully, but you may need to configure your applications if you will use your certificate for more than authentication or with other browsers.	
Contact ASX Certificate Support Team if you need assistance setting up your certificate and accessing online services.	
certificate.support@asx.com.au	
ogal Nolices Privacy apyright 6 2015 Symanice Corporation. All rights reserved.	

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

Processing your renewal 🧩					
Wait a moment while we retrieve your certificate information if you see this popup, click OK to continue.					
Creating a new RSA key OK Cancel					

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 .p12file
- 14. Select Current User

📀 🔗 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 ceruncate store is the system area where ceruncates are kept.
Store Location
To continue, click Next.
Next Cancel

- 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

	x
📀 👼 Certificate Import Wizard	
Private key protection	
To maintain security, the private key was protected with a password.	
Type the password for the private key.	-
Password:	
••••••	
Display Password	
Import options:	
Enable strong private key protection. You will be prompted every time the	
I Mark this key as expertable. This will allow you to back up or transport your	
keys at a later time.	
✓ Include all extended properties.	
Next Cancel	

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

Certificato Certifi	: Store cate stores are system a	areas where certi	ficates are kept.	
Windo for the	ws can automatically se e certificate.	elect a certificate	store, or you can sp	ecify a location
0	Automatically select the	certificate store	based on the type of	certificate
۲	Place all certificates in t	the following store	9	
	Certificate store:			
	Personal			Browse

- 20. Click Next
- 21. Click Finish

Troubleshooting

Error generating the CSR

What does the screen look like?					
	Errol: Content woor identity Tendement whomadow Nextal certificate Install your certificate Men you begin certificate installation, you will see popugs that warn you about potential security issues. These warming are normal, and end of the certificate installation process. Review the sequence of these popugs, and then click histall certificate to begin the process. You must have ActiveX enabled before proceeding with this installation to certificate in the installatin to cerificate in the installatin to certificate in th				
	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 many har click Teels	- ° X
1.2	 Internet Options 	(<-)⊙) (((((((((((((((((() () () () () () () ()) () () ()) () <
		Symantec.
		View downloads Ctrl+J Manage add-ons
		© Ordering Code Signing Certificate Code Signing Certificate Go to pinned sites
		Please select a Code Signing Certificate Type: Internet options About Internet Explorer About Internet Explorer
		Language U Java* Language U Java* The situation is the two states in the states in the state is
		 Microsoft# Authentiscode# These certificates are used with the Microsoft IntESOK developer foots to sign ActiveX controls, CAB, EXE and DLL fles, and other potentially humit active content on Microsoft platforms.
		System Requerements. Memous Browner Requirement Internet Options 53 and higher Memous Browner Requirement Internet Revolution and revolution and revolution and the second present Memous Provide State (State State) and the second state of the second state of the second state of the second Explores 7/8 on Windows Visita? please configure Internet Explores as shown here before starting the enrolment.
		 Microard/B Office and VIDA These certificates are identical to Microsoft Authenticode certificates, and are used by developers to sign macros in Office and other VIDA environments.
		Memous Boovers' Requirement: basenet Dopters 50 and higher Mart une The same RC, profile and knownes error (kind), and renew Datio security restrictions when using Internet Explorer 7/8 on Windows Vista? please configure Internet Explorer as shown here before starting the excidence.
		○ Adobe® AR*
1.3	Click Security tab select > sites	Internet Options X General Security Provery Connections Programs Advanced Select a zone to view or change security settings. Image: Connection of Connections Programs Advanced
		Internet Local internet Internet Restricted spices Trusted sites
		This and cardiaria websites that you trut not to damage your computer or your files.
		Security levels for the zone: Allowed levels for the zone: All Heckium
		Prompts before downloading potentially unaffe content - Unsigned ActiveX controls will not be downloaded
		Enable Protected Mode (requires restarting Internet Explorer)
		Custom level
		OK Cancel Acciv
1.4	Click Add and type in URL	Trusted sites
	https:/products.verisign.com	You can add and remove websites from this zone. All websites in
		this zone will use the zone's security settings.
		Add this website to the zone:
		https://products.verisign.com Add
		Websites:
		Remove
		Require server vertification (https:) for all sites in this zone
		Close
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		ertificate for Favorites bar Favorites bar Status bar Status bar Lock the toolbars Show tabs on a separate row
		Code Signing Certificate Canadian Code Signing Certificate C	Pestore More Size More Size More Size More More Size More More Size More More Size More More Size More More Size More More Size More More

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

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



pki-client-std-admi n-guide.pdf guide.pdf

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

A: Symantec Managed PKI Service IP Address Range



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®