

# **Digital Certificates User Guide**



Information Classification – Public

# Contents

ntroduction					
Security and ASX Recommendations	30				
Enrolling Via a Browser (Basic Security Template)	31				
Enrolling for a Certificate					
Renewing Certificates					
Revoking Certificates					
Export/Import certificates					
Frequently 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.

MPKI8 is being superseded with DigiCerts new digital trust platform DigiCert ONE which offers stronger security, simplified management, scalability, user-friendly workflows, and future-ready capabilities for evolving digital trust needs.

Austraclear Digital certificates will be issued from the new DigiCert ONE platform from March 2025.

DigitCert ONE 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.
- Austraclear issues DigiCert ONE Basic Security Certificates that can be enrolled via a web browser (basic security template). By default certificates are provided via the basic security template. The template provides certificates with 2056bit keys and SHA-256 signed.

# **Security and ASX Recommendations**

The digital certificates have an auto-renew feature which ensures that your certificates are automatically renewed before they expire to maintain uninterrupted service. Therefore, participants must promptly delete users in the Austraclear system who no longer require access to Austraclear or have left the company to prevent unauthorised access.

Austraclear Passwords must be a minimum length of 8 characters, with a maximum length of 14 characters, and contain a combination of at least three out of the four-character types: uppercase letters, lowercase letters, numbers and special characters. The maximum password age is 90 days meaning the system will prompt users to change their password starting 14 days before the 90 day expiration. Participants should ensure they set passwords of appropriate complexity to strengthen security.

**From 7 July, 2025**, the Austraclear systems password policy will be updated with the following changes. Users will still be able to log in with their current passwords until they expire. Once their password expires, users will be required to adhere to the new policy.

- The minimum password length will increase from 8 to 12 characters, with the maximum length of 32 characters.
- **Password complexity** must contain a combination of at least three out of the four-character types: uppercase, lowercase, numbers and special characters.
- The **maximum password age** will be extended from **90 to 365 days.** As a result, the system will prompt users to change their password starting 14 days before the 365 day expiration.

These changes are being implemented to enhance security and align with industry best practices.

## **Staff Cyber Training**

Participants' staff should be trained to recognise and report phishing emails and other social engineering tactics, such as impersonation, pretexting, and baiting, to prevent unauthorised access and security breaches.

## **Customer Email Protection Service**

To enhance security and protect against phishing attacks, customers should implement a robust email protection service that includes phishing detection, link and attachment scanning, and spoofing prevention. This can be achieved by deploying solutions such as Microsoft Defender for Office 365, Proofpoint, or Mimecast. Additionally, orgnaisations should enforce email authentication protocols like DMARC, SPF, and DKIM to prevent email spoofing and unauthorised use of their domain. Regular employee training on recognising phishing attempts, combined with real-time email alerts, will further strengthen defences against cyber threats.

## **Business Controls**

To ensure strong business controls, Participants should:

- Implement access controls restrict and regularly review user permissions
- Enable audit logging & monitoring track and detect suspicious activities in real time
- Use Multi-Level Approvals require dual authorisation for critical transactions and address discrepancies
- Enforce Segregation of Duties assign tasks to different individuals to prevent fraud
- Perform Compliance Audits periodically review security and regulatory compliance
- Establish Incident Response Protocols

These measures help business maintain security, prevent fraud, and ensure operational integrity.

# **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

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.

	Action required
	digicert Trust Lifecycle Manager
	Certificate enrollment confirmation
Hello charma	ine auld@asx.com.au.
A certificate h	as been requested for your email. Follow the link to review and confirm the
https://one.dk	sicert.com/mpki/enrollment/c4018080-cb66-435c-b8a5-636246e7a44t/cb6ed213-
ba0a-47a3-a4	5e-86fe8c752a88
For more info	rmation, contact:
Thank you,	

2. Once the link has been selected, the DigiCert ONE Verify and update enrolment opens.

Click Next and the below screen will appear

# digicert<sup>®</sup>ONE

## Verify and update enrollment

Subject DN

Organization name ASX Operations Pty. Ltd.

Organization units

1. Organization units MULTI-ALLOWED



3.

# Click Next and verify the certificate information

digicert <sup>*</sup> ONE		
Verify certificate information		
Seat ID charmaine auld@asx.com.au		Requestor email charmaine.auld@asx.com.au
Subject DN Common name ACLEAR DC1 DUMY6610	Organization units MULTI-ALLCWED, Participant ID - dumy66, Username - dumy6610, Project - Austraclear	
Organization name ASX Operations Pty. Ltd. Next		

4. Click on NEXT and you will come to the Copy Password page Click on Copy to Clipboard Icon next to Password and that will activate the Download Button:

Click on DOWNLOAD and Open Downloaded .P12 File and the Certificate Import Wizard will appear

# digicert<sup>®</sup>ONE

# Install your certificate



#### 2. Download and save the certificate to your computer.

Note: you will only be able to download the certificate once. Please ensure you save it after you click on the Download button.



3. Install your certificate on any browser or platform. Once completed, you can close your browser

5.	Click Next
	×
÷	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
	O Local Machine
	To continue, click Next.
	Next Cancel
6.	Leave the Option as Current User and hit Next and the screen below will appear $ imes$
←	🛃 Certificate Import Wizard
	File to Import
	Specify the file you want to import.
	File name:
	C:\Users\auld_c\Downloads\Certificate_pkcs12 (1).p12 Browse
	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)

Next

Cancel

7.

# Select Next Paste the Copied Password into the Password Field

	×
←	
Private key protection To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	
B3l1tYuPb9TO	
Display Password	
Import options:	
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.	
Protect private key using virtualized-based security(Non-exportable)	
☑ Include all extended properties.	
Next C	ancel
8. The only Option to be ticked is the Imp	oort Option Include all extended properties
Hit Next and the screen below will appear	
	×
← 😺 Certificate Import Wizard	

#### Certificate Store

Certificate stores an	e system areas where	certificates are kept.
-----------------------	----------------------	------------------------

Windows can automatically select a certificate store, or you can specify a location for the certificate.

O Automatically select the certificate store based on the type of certificate

#### Place all certificates in the following store

Certificate store:

	DI	0	W	s	e	•	•	•
-				-	-			-

Next	Cancel

# 9. Select Option to Place all certificates in the following store and then click BROWSE And Select **PERSONAL** and hit OK



Click on FINISH and you should receive the below confirmation message



Once enrolled, the user will receive the following email from DigiCert

TEDNAL FRAME	
IEKNAL EMAIL	Do not click on links or open attachments unless you trust the sender and know the content is sate
	digicert' Trust Lifecycle Manager
	Hello <u>charmaine auld@asx.com.au</u> .
	For more information, contact:
	Thank you,

10. When enrolling the certificate, the root certificate authority is installed in the personal drive along with the Austraclear digital certificate. To finalise the process, the user must move the Root Certificate Authority from the personal drive to the Trusted Root Certification Authorities folder to enable the system to trust and validate certificates issued by that CA, ensuring secure communications.

Select the windows search bar and type manage user certificates



# Locate the ASX Operations Pty Ltd CA under the Personal -->Certificates folder click and drag this Root Certificate Authority and place it in the Trusted Root Certificate Authority folder.

藩 certmgr - [Certificates - Current l	- 🗆	×							
File Action View Help	File Action View Help								
Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statu			
<ul> <li>Certificates - Culterin Oser</li> <li>Certificates</li> <li>Trusted Root Certification Au</li> <li>Enterprise Trust</li> <li>Intermediate Certification Au</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Trusted People</li> <li>Client Authentication Issuers</li> <li>Other People</li> <li>AdobeCertStore</li> <li>Local NonRemovable Certific</li> <li>Local NonRemovable Certificate</li> <li>MSIEHistoryJournal</li> <li>Certificate Enrollment Reque:</li> <li>Smart Card Trusted Roots</li> </ul>	Issued Io	Issued By 4bfb346f-610a-4c2e-88b8-44d192 ASX Operations Pty. Ltd. CA ASX Operations Pty Ltd ICA ASX Operations Pty Ltd ICA ASX Operations Pty Ltd ICA ASX Operations Pty Ltd ICA ASX Operations Pty Ltd ICA Adobe Intermediate CA 10-3 Adobe Intermediate CA 10-15 Adobe Intermediate CA 10-15 Adobe Root CA 10-3 Adobe Root CA 10-3 ASX Operations Pty Ltd CA	Expiration Date 29/11/2024 14/12/2026 14/12/2026 8/01/2027 14/12/2026 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 13/01/2027 19/08/2025 6/08/2030 5/08/2068 5/08/2068 5/08/2068 5/08/2068 5/08/2068	Intended Purposes Client Authentication Client Authentication Client Authentication Client Authentication Client Authentication Client Authentication Client Authentication Client Authentication <all> <all> <all> <all> <all> <all> <all> <all> <all> <all> <all> <all> <all></all></all></all></all></all></all></all></all></all></all></all></all></all>	Friendly Name Private Key For PKC cert cert private_key_for_pkc cert private_key_for_pkc private_key_for_pkc vNone> <none> <none <none=""> <none> &lt;</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>	Stati			
	ASX Operations Pty Ltd CA ASX Operations Pty Ltd ICA ASX Operations Pty. Ltd. CA Renee Service Renee Service Renee Service Renee Service	ASX Operations Pty Ltd CA ASX Operations Pty. Ltd. CA ASX Operations Pty. Ltd. CA ASX Operations Pty. Ltd. CA ASX Enterprise Issuing CA G2 DigiCert PKI Platform Administrat DigiCert PKI Platform Administrat	8/10/2034 8/01/2035 8/01/2035 15/08/2025 24/04/2025 24/04/2025 24/04/2024 3/12/2023	<ali><ali><ali><ali><ali><ali><ali><ali></ali></ali></ali></ali></ali></ali></ali></ali>	<none> <none> <none> <none> Admin Certificate Admin Certificate <none></none></none></none></none></none>				
< >	<					>			

🚡 certmgr - [Certificates - Current	- 0	×				
File Action View Help						
🗢 🔿 🖄 🖬 🖌 🖬						
🗊 Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	s ^
V 📔 Personal	AAA Certificate Services	AAA Certificate Services	1/01/2029	Client Authenticati	Sectigo (AAA)	R
f Certificates	AddTrust External CA Root	AddTrust External CA Root	30/05/2020	Client Authenticati	Sectigo (AddTrust)	R
<ul> <li>Irusted Root Certification Au</li> </ul>	ASX Operations Pty Ltd CA	ASX Operations Pty Ltd CA	9/10/2034	<all></all>	<none></none>	
	ASX Operations Pty. Ltd. CA	ASX Operations Pty. Ltd. CA	8/01/2035	<all></all>	<none></none>	
> Enterprise trust	ASX Operations Root CA G2	ASX Operations Root CA G2	19/09/2034	<all></all>	<none></none>	R
Active Directory User Object	ASX Operations Root CA G2	ASX Operations Root CA G2	19/09/2034	<all></all>	<none></none>	R
Trusted Publishers	ASX Operations Root CA G3	ASX Operations Root CA G3	29/04/2040	<all></all>	<none></none>	R
Untrusted Certificates	🔄 ASX Operations Root CA G3	ASX Operations Root CA G3	29/04/2040	<all></all>	<none></none>	R
+ / <u> </u>			22/22/2025		••	-

## **Renewing Certificates**

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.

Please ensure you delete the old certificate via Manage User Certificates



Under Personal –Certificates, select the old certificate ACLEAR <username> and Delete

4	🚟 c	ertmgr - [Certificates - Current	User\Personal\Certificat	es]		-		×
re	File	Action View Help						
es	<b>(</b> = =	»   🚈 📩   🐇 🖻	] 📑 📘					
9	🤿 C	ertificates - Current User 🔥	Issued To		Issued By	Expirat	ion Date	^
	¥	Personal	nal 2 9a7a936e-7835-40a4-802b-79fa298899 4bfb348f-610a-4c2e-88b8-44d192				29/11/2024	
d	_	Certificates	ACLEAR ACH	<u>.</u>	ASX Operations Pty. Ltd. CA	17/03/2	2027	
on	>	Trusted Root Certification	CLEAR ACH	Open	ASX Operations Pty. Ltd. CA	14/12/2	2026	
sh		Enterprise Trust	CACLEAR ACLR	All Tasks >	ASX Operations Pty. Ltd. CA	14/12/2	2026	
rti		Intermediate Certification	CACLEAR ACSL		ASX Operations Pty. Ltd. CA	17/03/2	2027	
		Active Directory User Obje	ACLEAR DC1	Cut	ASX Operations Pty Ltd ICA	13/01/2	2027	
		Induced Publishers	CLEAR DC1 [	Сору	ASX Operations Pty Ltd ICA	26/02/2	2025	
	5	Third-Party Root Certifical	ACLEAR New	Delete	ASX Operations Pty Ltd ICA	13/01/2	2027	

# **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

Marking the digital certificate as not exportable prevents unauthorised access to the private key, enhancing security by keeping it confined to the original device. Austraclear strongly recommend users do not make the certificate exportable. If second certificates are required for BCP computers, Austraclear are able to issue multiple certificates for the one user to enrol on the individual PC.

# **Frequently Asked Questions**

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?

A: For DigiCert ONE, the operating system and browser platform support is as follows: Windows 10 (32-bit and 64-bit) Microsoft Edge or Google Chrome Windows 11 (64-bit) Microsoft Edge or Google Chrome

#### Q15: Are certificates exportable?

A: Marking the digital certificate as not exportable prevents unauthorised access to the private key, enhancing security by keeping it confined to the original device. Austraclear strongly recommend users do not mark the certificate as exportable.

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®