Digital Certificates User Guide

Information Classification – Public

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.

MPKI8 is being superseded with DigiCerts new digital trust platform DigiCert ONE which offers stronger security, simplified management, scalability, user-friendly workflows, and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)

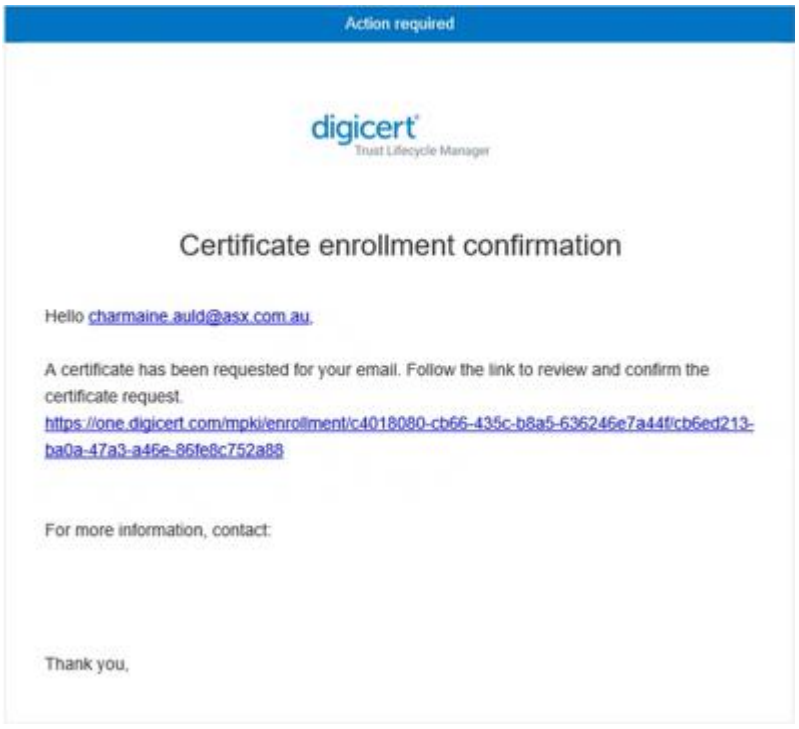
The basic security template uses a web browser to download the certificate and Windows certificate store to store and protect the private key.

Enrolling for a Certificate

Once the PKI Client has been installed the certificate can be enrolled. To enrol for a certificate:

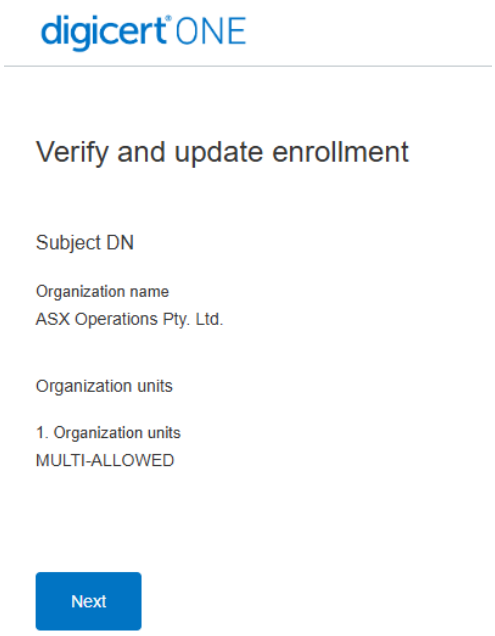
1. Click the link in the provided email.

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

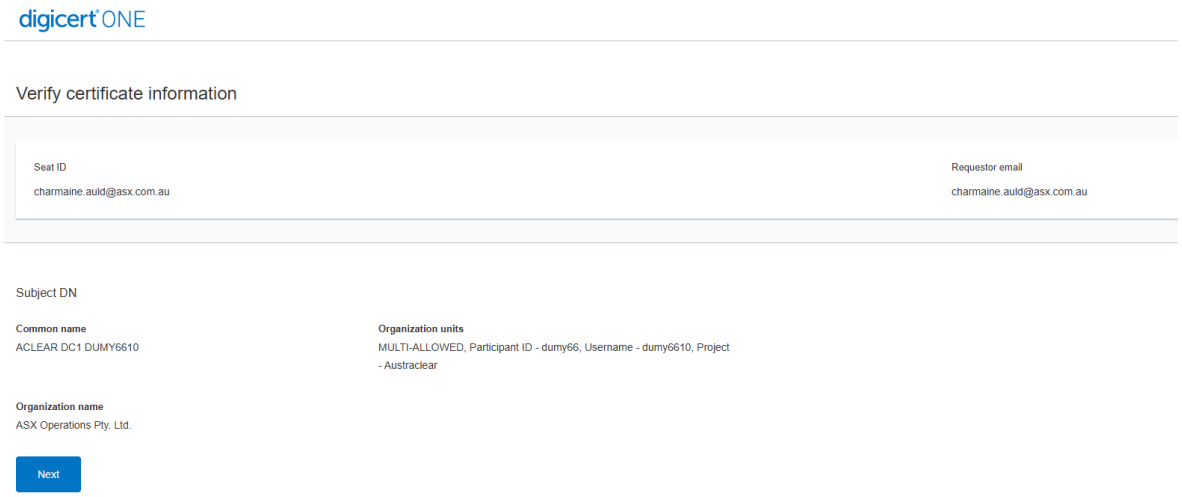


2. Once the link has been selected, the DigiCert ONE Verify and update enrolment opens.

Click Next and the below screen will appear



3. Click Next and verify the certificate information



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 ONE

Install your certificate

⚠ Do not close this window until you complete the installation process.

1. Copy your password.

You will not see this password again. It is required to install your certificate. Copy password to enable "Download" button.

B3I1tYuPb9TO

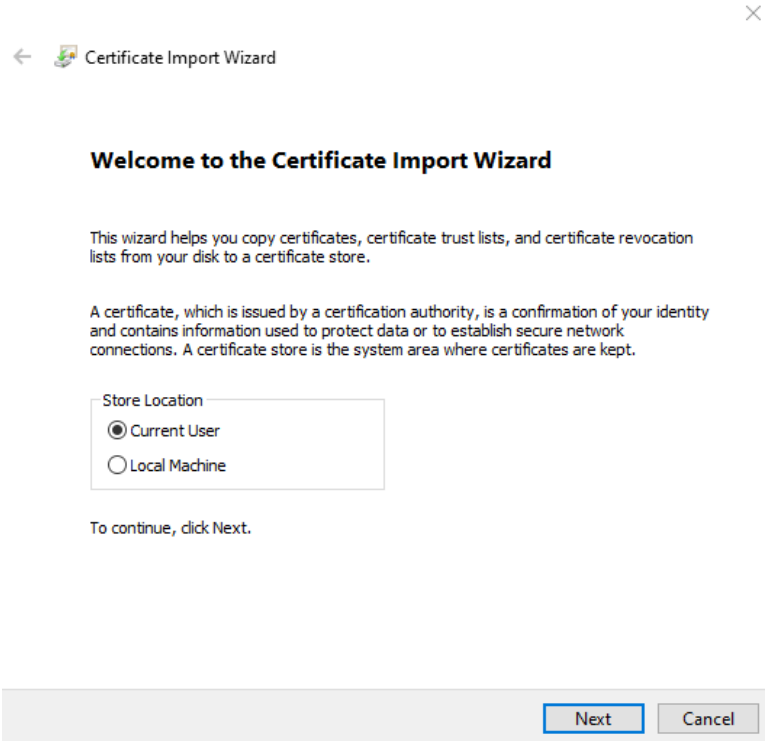
2. Download and save the certificate to your computer.

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

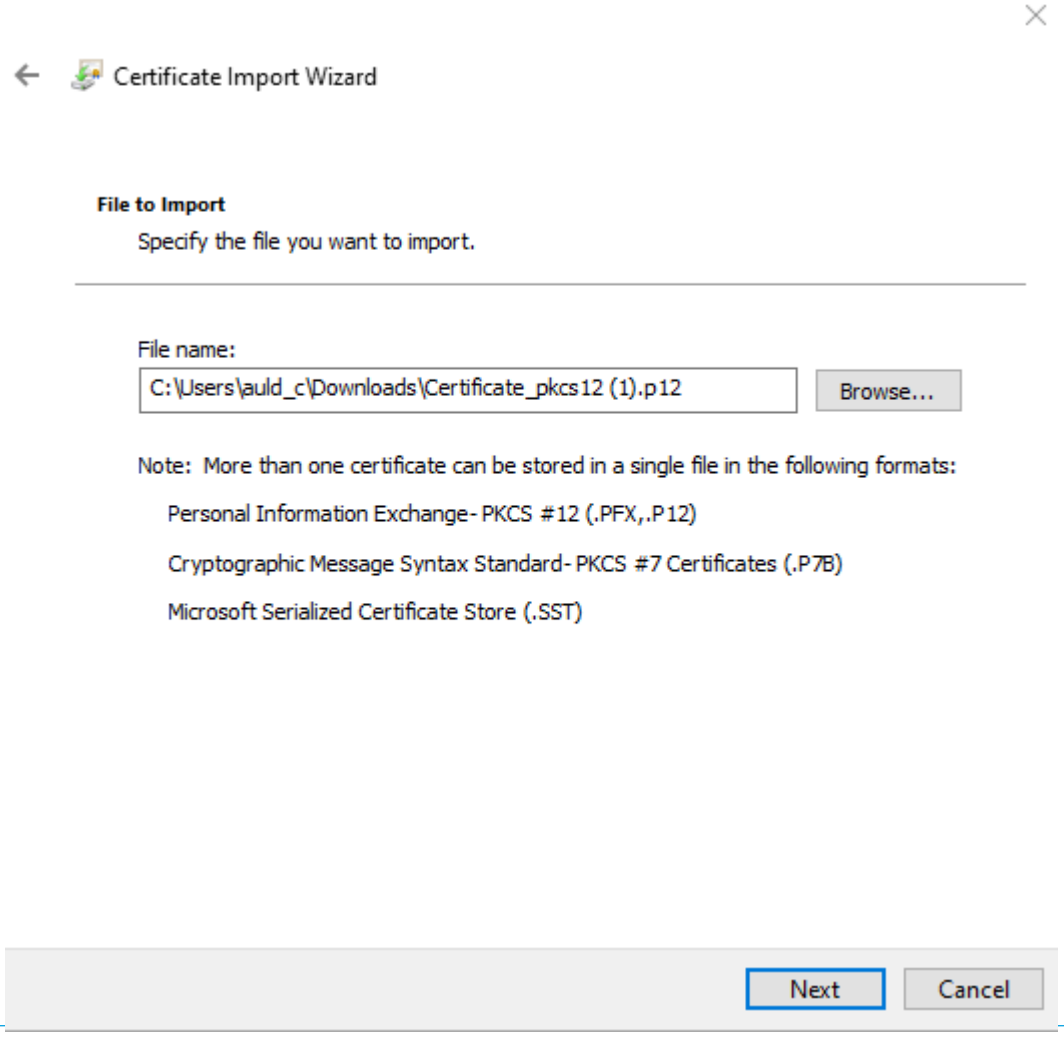
Download

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

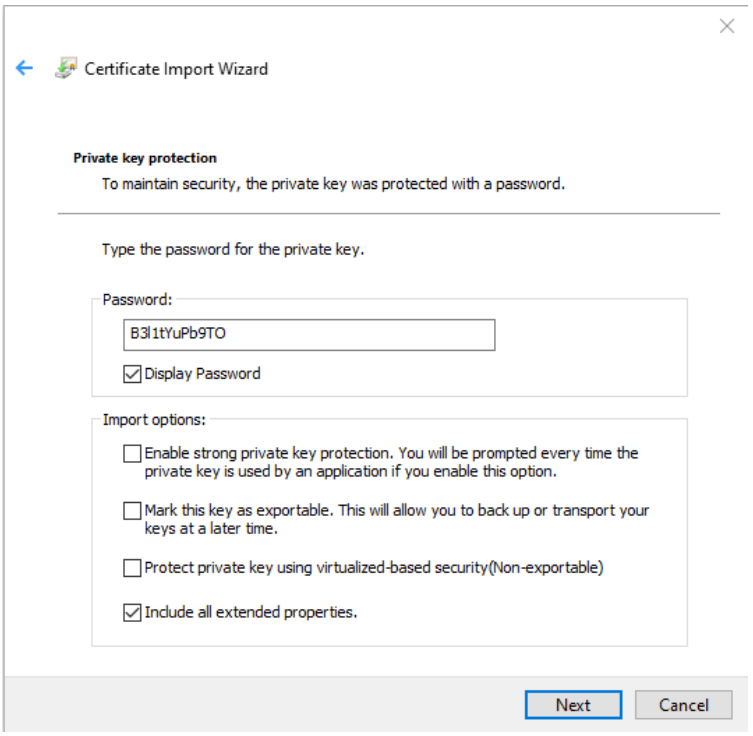
5. Click Next



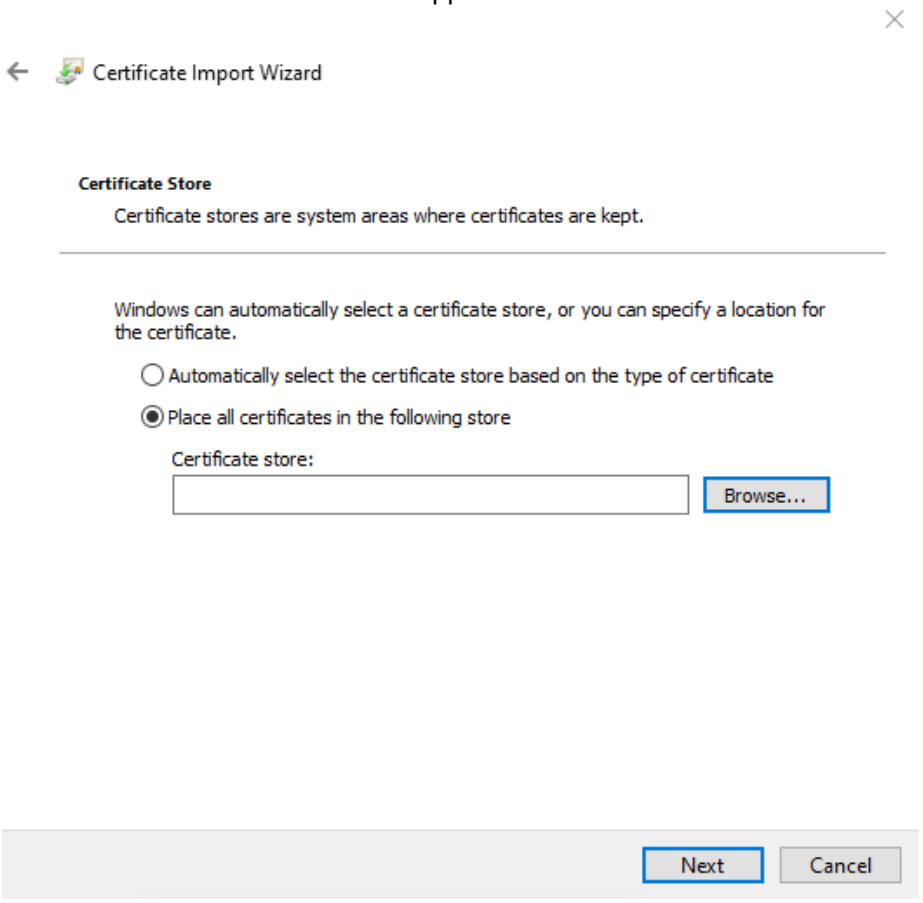
6. Leave the Option as Current User and hit Next and the screen below will appear



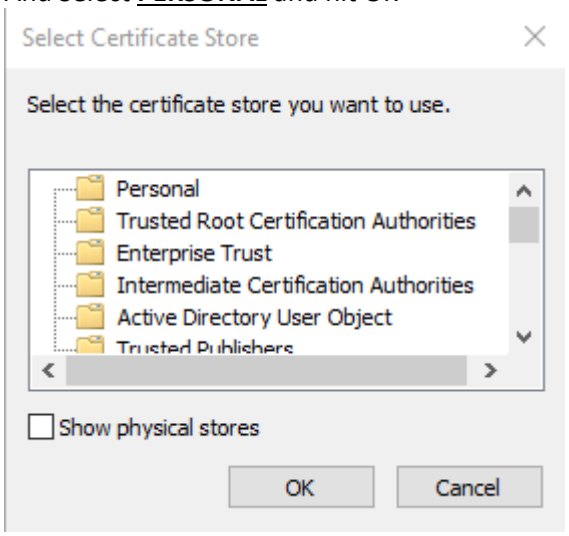
7. Select Next Paste the Copied Password into the Password Field



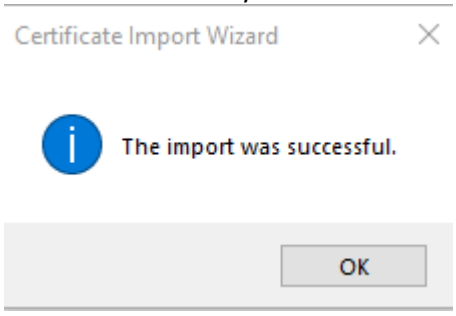
8. The only Option to be ticked is the Import Option Include all extended properties Hit Next and the screen below will appear



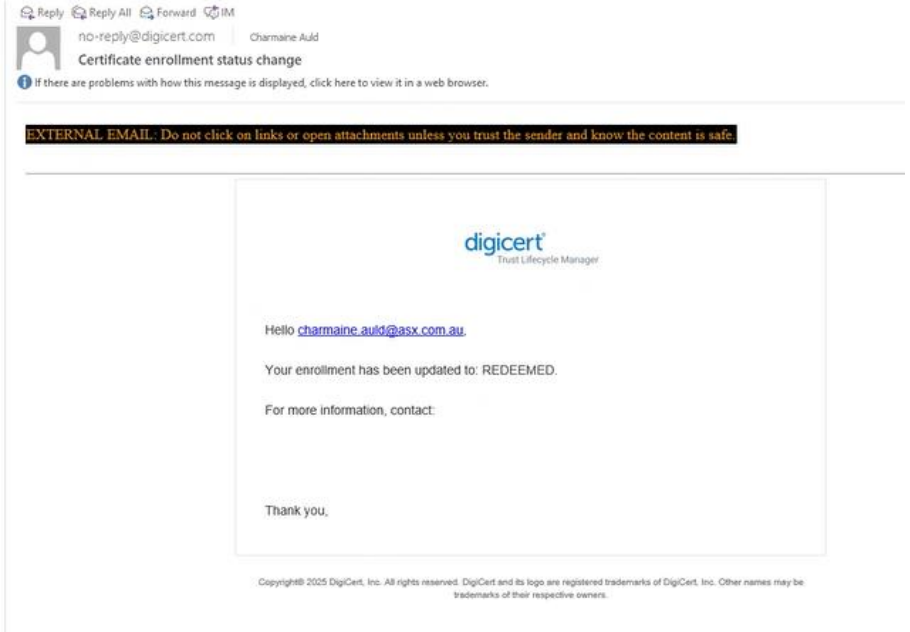
9. Select Option to Place all certificates in the following store and then click BROWSE And Select **PERSONAL** and hit OK



Click on FINISH and you should receive the below confirmation message

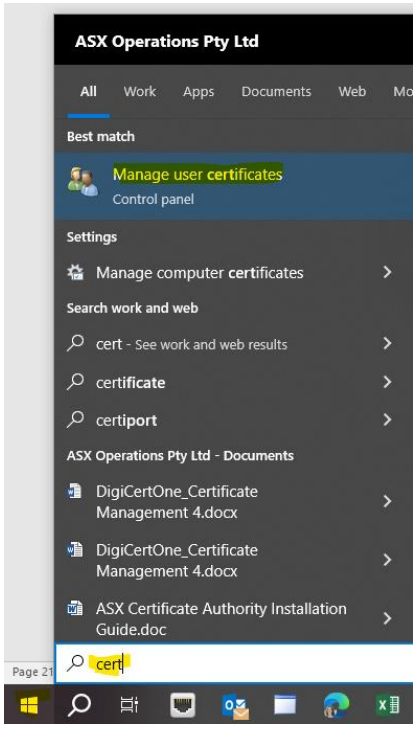


Once enrolled, the user will receive the following email from DigiCert

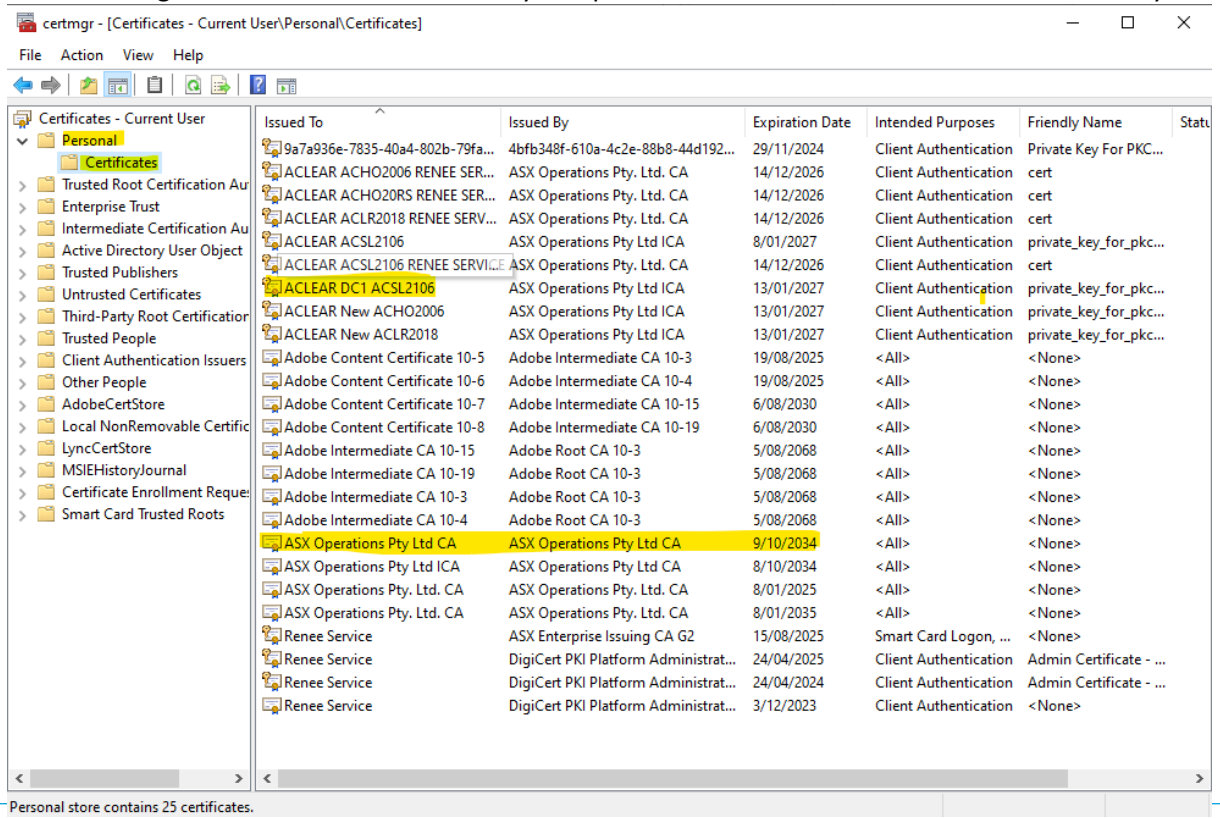


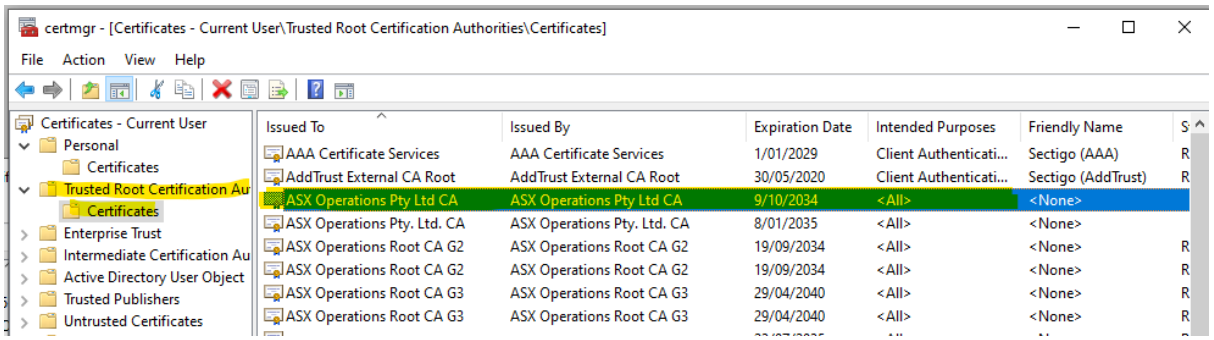
10. When enrolling the certificate, the root certificate authority is installed in the personal drive along with the Austraclear digital certificate. To finalise the process, the user must move the Root Certificate Authority from the personal drive to the Trusted Root Certification Authorities folder 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.



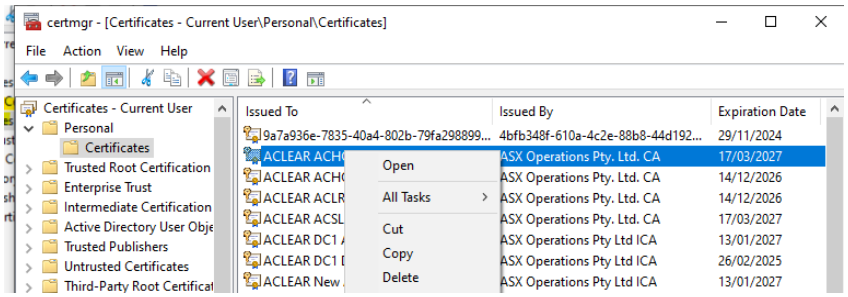


Renewing Certificates

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



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.