User Certificate Guide

Last Update: April 2026

User Certificate Guide

1. Purpose & Scope

This document provides guidance for participants on how to obtain, configure, and manage digital certificates required to access the eCAT application, both via the trader interface and web services.

It outlines the applicable technical requirements, submission process, usage rules, and security obligations to ensure certificates are correctly set up and remain compliant with JAO standards.

This guide is intended for all external users requiring access to eCAT and should be followed when requesting, installing, renewing, or replacing certificates.

2. Who Is Required to Hold a Certificate

Each individual user accessing the auction tool must hold a certificate issued to them personally (CN = full name). If the same user is registered under more than one company, the same certificate may be used for login, provided all other requirements are met.

Pseudonym-type certificates are issued in the name of the company and will be accepted only for web services accounts, having to be accompanied by the Web Services Account Form. This type of certificate is not accepted for individual user accounts.

3. Usage Rules & Security Obligations

The certificate must be used only by the individual to whom it was issued.

The private key must remain securely stored on your system and must not be shared.

In case of private key compromise or suspected misuse, you should immediately notify JAO via Service Desk and provide a new certificate.

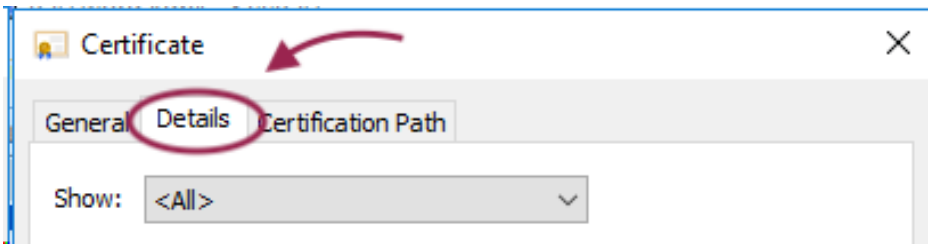
4. Certificate Technical Requirements

The certificate must comply with eIDAS requirements, meaning it must be issued by a Qualified Trust Service Provider recognized under the eIDAS Regulation. This ensures that the certificate meets EU standards for security, identity verification, and legal recognition across Member States.

In addition, the certificate must meet the technical requirements to be recognized by eCAT, as outlined below:

- The fields "CN, O and C are required for the Issuer field.
- The required signature algorithm is RSASSA-PSS.
  - ⇒ JAO will continue to accept the sha1RSA signature hash algorithm for backward compatibility. However, as of 2025, this algorithm is considered deprecated and vulnerable. Therefore, we strongly recommend using more secure alternatives such as sha256RSA or higher (e.g., SHA-384 or SHA-512).
  - ⇒ Please note that JAO may fully deprecate sha1RSA after a defined grace period. Consequently, we advise against acquiring certificates that rely on this algorithm.
- The requirement for the Public Key is to be minimum or higher than 2048 Bits;
- It is not mandatory, but advised to have the Basic Constraints field with the "Path Length Constraint = None" value
- It is mandatory to have the Key Usage field with Digital Signature value
- It is not mandatory but advised to have the Enhanced Key Usage field and, in case the certificate contains this field, it is mandatory to have the Client Authentication value.

The information specified in this section can be found under the ‘Details’ tab in the public part of the certificate, as shown on the screenshot below:



5. Reference Examples – Valid Certificates

ecdsa-with-SHA384

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4F:FF:12:AA:FF:02:9C
        Signature Algorithm: ecdsa-with-SHA384
        Issuer:
            C = LU
            O = TrustedCA Services S.A.
            CN = TrustedCA High-Security Issuing Authority 2026
        Validity:
            Not Before: Jan  1 00:00:00 2026 GMT
            Not After : Dec 31 00:00:00 2027 GMT
        Subject:
            C = DE
            O = Example Energy Trading GmbH
            CN = Example Energy Trading GmbH (Legal Name)
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (384 bit)
            pub:
                04:aa:bb:cc:dd: ...
            ASN1 OID: secp384r1
            NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
            X509v3 Subject Key Identifier:
                8A:3F:1B:9E:44:02:D7:5C:1F:2A:6B:9D:7E:11:CA:FE:33:88:90:AB
            X509v3 Authority Key Identifier:
keyid:12:34:56:78:9A:BC:DE:F0:12:34:56:78:9A:BC:DE:F0:12:34:56:78
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.2
                  CPS: https://trustedca.example/cps-2026
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.trustedca.example/2026/ca.crl
            X509v3 Authority Information Access:
                CA Issuers - URI:http://cert.trustedca.example/2026/ca.crt
                OCSP - URI:http://ocsp.trustedca.example
    Signature Algorithm: ecdsa-with-SHA384
    Signature:
        30:65:02:31:00: ...
```

Dilithium3

```
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number: 4F:FF:12:AA:FF:02:9C
        Signature Algorithm: dilithium3
        Issuer:
            C = LU
            O = TrustedCA Services S.A.
            CN = TrustedCA Post-Quantum Issuing Authority 2026
        Validity:
            Not Before: Jan  1 00:00:00 2026 GMT
            Not After : Dec 31 00:00:00 2027 GMT
        Subject:
            C = DE
            O = Example Energy Trading GmbH
            CN = Example Energy Trading GmbH (Legal Name)
        Subject Public Key Info:
            Public Key Algorithm: dilithium3
            Dilithium3 Public-Key: (level-3 security, ~256-bit classical /
~128-bit quantum)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
            X509v3 Subject Key Identifier:
                8A:3F:1B:9E:44:02:D7:5C:1F:2A:6B:9D:7E:11:CA:FE:33:88:90:AB
            X509v3 Authority Key Identifier:
```

RSASSA-PSS with SHA-256

```
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number: 4F:89:12:AA:56:02:9C
        Signature Algorithm: RSASSA-PSS
            Hash: SHA-256
            Salt Length: 32 bytes
            MGF: MGF1 with SHA-256
        Issuer:
            C = LU
            O = TrustedCA Services S.A.
            CN = TrustedCA Qualified Issuing Authority
        Validity:
            Not Before: Jan  1 00:00:00 2025 GMT
            Not After : Jan  1 00:00:00 2027 GMT
        Subject:
            C = DE
            O = Example Energy Trading GmbH
            CN = Example Energy Trading GmbH (Legal Name)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
    Signature Algorithm: RSASSA-PSS with SHA-256
```

6. Steps to Configure Your Certificate

1. Obtain a certificate from a trusted provider
2. Export the public part of the certificate (please see point 3 for directions)
3. Complete the User Account Form
4. Submit a ticket to JAO Support with your request, attaching the completed User Account Form and the public part of the certificate. We advise to Zip the certificate file to ensure the attachment is processed
5. JAO validates the information and creates or updates the user
6. Install the private part of the certificate in your preferred browser or API tool

7. Exporting the Public Part of the Certificate

Exporting the certificate provides only the public part, which is safe to share.

The steps differ slightly depending on the operating system:
Windows uses the Windows Certificate Manager.
macOS uses Keychain Access.

7.1 Exporting a Certificate Using Google Chrome

Windows

- Open Google Chrome.
- Select Menu (⋮) → Settings.
- Select Privacy and Security → Security.
- Scroll down and select Manage certificates.
- The Windows Certificate Manager will open.
- Select the tab where the certificate is located (usually Personal).
- Highlight the certificate and select Export….
- Choose DER encoded binary (.cer)
- Save the file to your computer.

macOS

- Open Google Chrome.
- Select Menu (⋮) → Settings.
- Select Privacy and Security → Security.
- Select Manage certificates.
- Keychain Access will open automatically.
- Select the keychain where the certificate is stored (typically login or System).
- Select Certificates in the left panel.
- Right-click the certificate and select Export
- Save the file as .cer

7.2 Exporting a Certificate Using Microsoft Edge

Windows

- Open Microsoft Edge.
- Select Menu (⋯) → Settings.
- Select Privacy, search and services.

- Scroll to the Security section and select Manage certificates.
- The Windows Certificate Manager will open.
- Select the appropriate tab and locate the certificate.
- Select the certificate and choose Export
- Choose DER encoded binary (.cer)
- Save the file to your computer.

macOS

- Open Microsoft Edge.
- Select Menu (···) → Settings.
- Select Privacy, search and services.
- In the Security section, select Manage certificates.
- Keychain Access will open.
- Select login or System keychain.
- Select Certificates.
- Right-click the certificate and select Export
- Save the file as .cer

8. Installing the Certificate in Your Browser

Windows

Chrome and Edge both use the Windows Certificate Store, so the installation steps are the same for both browsers.

- Locate your certificate file (usually .p12 or .pfx).
- Double-click the file.
- The Certificate Import Wizard will open automatically.
- Select Current User, then click Next.
- Confirm the certificate file shown and click Next.
- Enter the certificate password (if provided to you). Click Next.
- When asked where to store the certificate, select Automatically select the certificate store. Click Next.
- Click Finish to complete the installation. A message will appear confirming that the import was successful.

After installation, the certificate is ready to use in both Google Chrome and Microsoft Edge.

macOS

Chrome and Edge both use Keychain Access to manage certificates.

- Find your certificate file (usually .p12 or .pfx).
- Double-click the file.
- Keychain Access will open automatically.
- When prompted, choose the login keychain.
- Enter the certificate password (if provided to you).
- The certificate will now appear in Keychain Access under the Certificates category.
- Ensure the certificate shows as valid (a green icon).

Once installed, the certificate is available for use in both Google Chrome and Microsoft Edge.

8.1 After Installation

When you access a website that requires the certificate, the browser will automatically detect it. You may be asked to select the certificate if more than one is installed. No additional browser configuration is required.

Do not share your .p12/.pfx file with anyone. It contains your private key.

9. Renewal & Replacement

JAO does not send renewal reminders. You are responsible for monitoring your certificate's validity period.

A renewal request must be submitted well in advance of the certificate expiry date to allow sufficient time for processing and replacement, ensuring uninterrupted access. We advise to send the request at least 2 weeks in advance.

Once your certificate is expired you will lose access to the auction tool.