Certificates Guide

Q&A and technical requirements

2018

Contents

Certificate Questions and Answers

What type of certificate do I need to access the auction tool?

To access eCAT you need an electronic certificate that must be at least intended for the verification of the advanced electronic signatures within the meaning of Regulation (EU) No 910/2014 on the use of electronic signatures. The certificate must meet the following conditions:
a) it must be RFC 3280 compliant;
b) it must be version X.509 v3;
c) The public key of the certificate must be intended for the RSA algorithm;

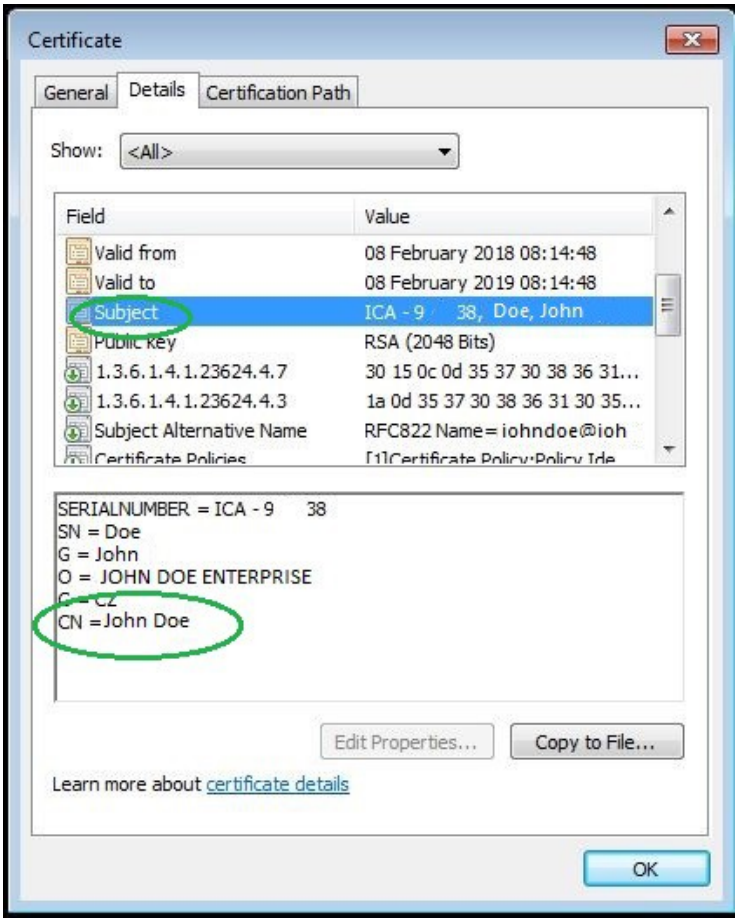
Extension	Content	OID	Criticality	Field Indication
Key Usage	Digital Signature	-	Critical	Mandatory
Extended Key usage	Client Authentication	1.3.6.1.5.5.7.3.2	Non-critical	Recommended

Where can I find the list of certificate issuers approved by JAO?

The list of trusted certificate authorities approved by JAO is available on our website: http://www.jao.eu/support/resourcecenter/overview (**"eCAT" -> "Approved Certificate Issuers**").

To whom must the certificate be issued?

The certificate must be issued to the name of the registered user. As a result, the "Subject" field must include the name of the user under the attribute "CN" (common name).



Can I use a pseudonym-type certificate?

This type of certificate is only accepted for communication via web services. If you want to use a pseudonym certificate you will also need to fill in and send us Appendix 3 of the Information System rules ("Specific conditions regarding the use of the PSEUDONYM-type electronic certificate").

How can I register my certificate?

In order to register your certificate, please send us a user account setup form, completed electronically and signed, together with the public part of the certificate (in a zipped file). You can send the documents using our Service Desk platform (http://servicedesk.jao.eu). Instructions on how to export the public part of the certificate can be found on our website: http://www.jao.eu/support/resourcecenter/overview **("Registration" -> "Registration Guide")**.

How long does the user account creation/modification process take?

We will confirm the creation/modification of the user account, at the latest five working days after receiving the form.

Can several users from the same company use the same certificate?

No, certificates used to access eCAT may not be shared.

How many certificates can I register for one user account?

You can only register one certificate per user account.

I have two user accounts as I work for two companies registered with JAO, can I use the same certificate?

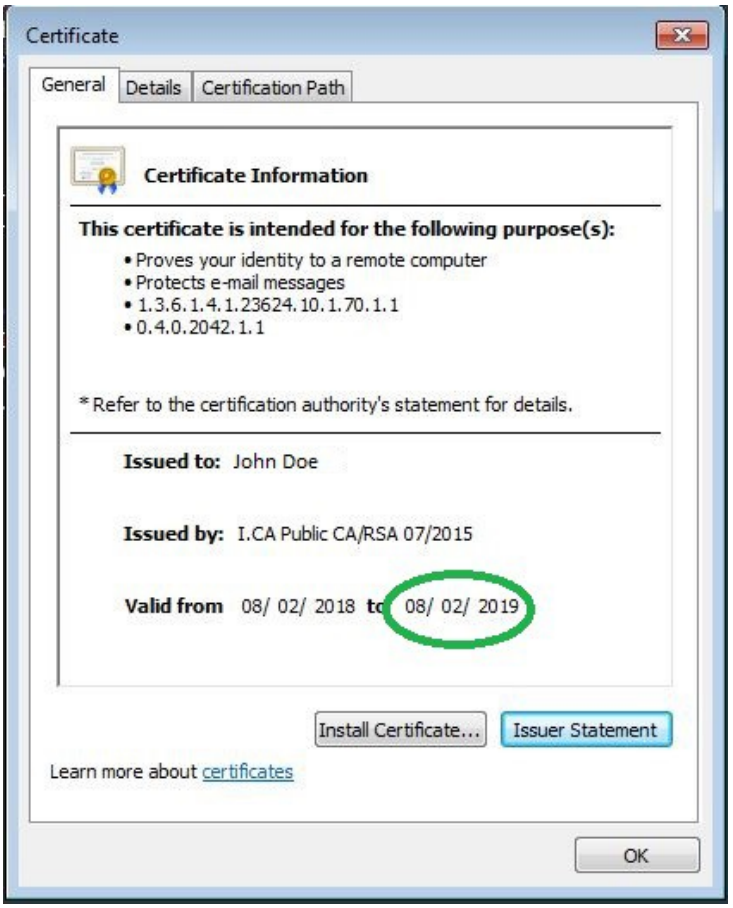
Yes, as long as the certificate meets our other criteria.

How do I update my certificate?

When you renew your certificate, you must provide us with a new user account form and the public part of the certificate in a zipped file (via our Service Desk platform: http://servicedesk.jao.eu).

Will I receive a reminder about the expiry date of my certificate?

No, JAO accepts no responsibility for sending reminders for expiring or expired certificates. We strongly advise the user to set a reminder a few months before the expiry date of their certificate to allow sufficient time to obtain a new certificate and send it to us. We recommend that the user send the user account form at least ten working days prior to the expiry date.

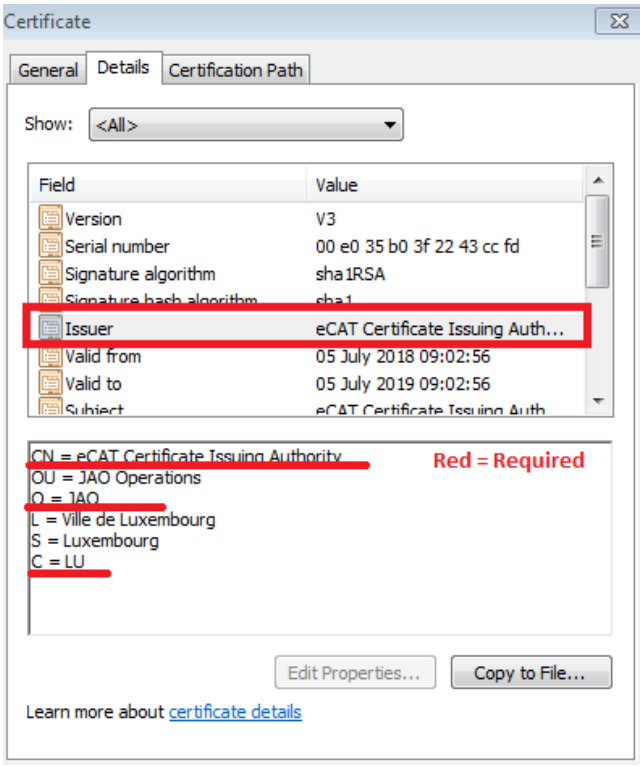


I want a read-only user account. Does my user account form still need to be signed?

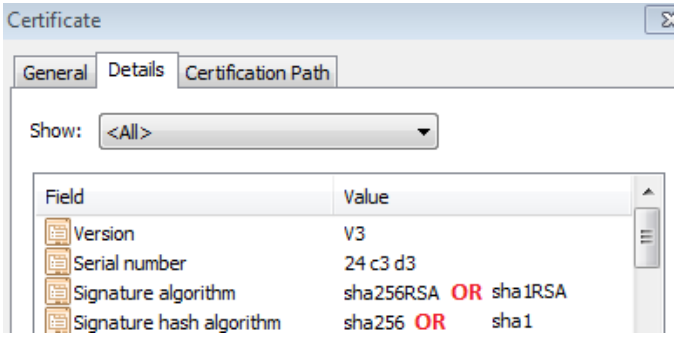
Yes, regardless of the type of user account (full-access or read-only), the user account form must be signed by an authorized person within your company, based on your extract from the commercial register or a power of attorney.

Certificate Technical Requirements

Requirements for **Issuer** field (highlighted in red):

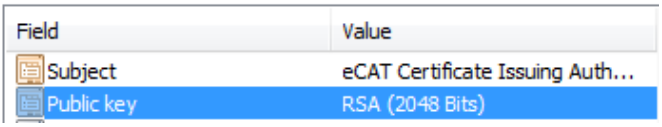


Signature algorithm and **Signature hash algorithm** requirements:

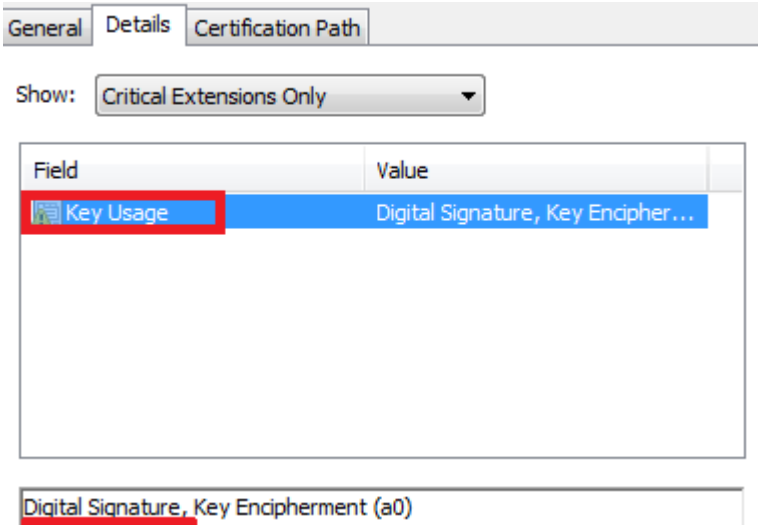


It is recommended that you use sha256RSA as it is a newer and more secure algorithm, although sha1RSA will still work. Some Certificate Issuing Authorities will be retiring their sha1RSA certificates soon.

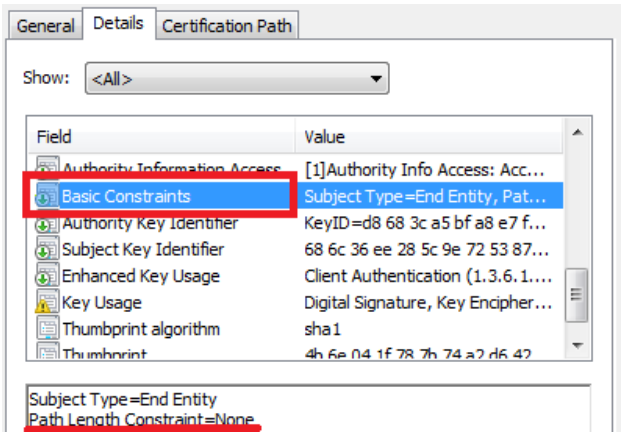
Public key requirements:



Key Usage field requirements (mandatory in red):



It is advised that in **Basic Constraints**, the Path Length Constraint = None



Enhanced Key Usage field requirements (mandatory in red):