

Unified Patent Court provides more clarifications about the requirements of the certificates accepted by the CMS.

Following our previous announcements regarding the access to the CMS and the authentication process, which will be based on a strong authentication scheme, the UPC IT team provides, here, more technical details about the needed certificates in order to be able to access to the CMS system.

To use the CMS, you need two certificates (provided by one of the Qualified Trust Service Providers – QTSP under the eIDAS regulation):

- One certificate used for the authentication (required for the login):



- One certificate to electronically sign the documents you want to upload in the CMS:



Important to know:

- ONLY the authentication certificate must be stored on a physical device.
- The signature certificate could also be stored on this device, but it is not mandatory.

These certificates can be acquired, by EU Citizens as well as non-EU citizens from a QTSP. You can find such providers via the link here after.

This is an official website where you can check the trusted providers but it is not managed by UPC.



[List of providers from EU](#)

About the UPC authentication certificate

UPC requires a physical device (smart card or USB stick) containing the **authentication certificate** for the user authentication (login).

The **suitable provider needs to provide a secure physical device** (smart card or a USB stick) containing this authentication certificate.

About the UPC electronic signature certificate

Regarding the electronic signature, the required certificate must be **QCert for Esig (Qualified certificate for electronic signature)** meaning that the user can sign with a valid qualified electronic signature according to eIDAS (the QTSP should offer a Qualified Signature Creation device).

In practice, two cases can occur for the authentication certificate:

CASE 1: User has already one authentication certificate, stored on a physical device, and he would like to check if this certificate is valid and can be accepted by the CMS.

CASE 2: User has no such authentication certificate, and needs to acquire this new certificate (see directly page 4 to proceed).

➡ **CASE 1: I have already an authentication certificate. How can I check if this certificate is valid?**

1. Export your certificate (in a file);
2. Go on the DSS validation tool using this link:
<https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/certificate-validation>
3. Upload your exported certificate file;
4. Click on "Submit" button.

You will get two reports (simple and detailed).

Your certificate is valid if (1) the two panels are displayed in "**Green**", and (2) details regarding the key usages and trust anchor must be present and match the specific values (see details here under).

Validation results

Simple Report
Detailed Report
Diagnostic tree

Certificate
Certificate file name
Print

Qualification	Issuance Time (2022-09-08 08:46:09) : Cert for unknown type Validation Time (2022-11-05 00:00:00) : Cert for unknown type
Common name	
Given name	
Surname	
Email	
Country	
Key usages	digitalSignature keyEncipherment
Validity	2022-09-08 08:46:09 - 2025-09-08 08:46:09
Revocation	✓
OCSP	
CRL	
AIA	
CPS	

Certificate
Certificate file name

Common name	Qualified CA 3
Organization name	
Country	
Key usages	keyCertSign crlSign
Validity	2015-03-06 14:12:15 - 2035-03-05 13:21:57
OCSP	http://ltgroot.ocsp.
CRL	http://crl./LTGRCA2.crl
AIA	http://ca./LTGRCA2.crt
CPS	https://repository
Trust Anchor	<div> <div> ABC Qualified Time Stamping </div> <div> ABC Global Qualified Certification Authority 3 </div> </div>

Figure 1 - Result of the DSS Validation

The **first panel** displays:

- The Key Usage field must be “**digitalSignature**” OR;
- Extended Key usage field must be “**clientAuth**”.

The **second panel** gives information about the **trust anchor** linked to the certificate. The Trust anchor field must be present and contains the name of a provider (ABC in the figure here above, as sample) / certificate (Global Qualified Certification Authority 3, in the figure here above, as sample) part of the Trusted Providers List.

If your certificate matches these criteria, it is considered as valid and can be tested in the CMS (see here after the process to test the certificate with the CMS).

➡ CASE 2: I have no certificate. How can I acquire these certificates?

The required certificates are:

- The authentication certificate for the access / login on the CMS;
- The qualified electronic signature certificate to sign the documents to upload in the CMS.

These certificates can be delivered by a provider listed on the EU Trusted Providers list ([list of providers from EU](#)).

On this Trusted Providers list, you must select a provider having the type “QCert for Esig”.

1 Select a country (yours or another one)

2 Select a provider (in the selected country)

Currently active trust service providers

Service provider 1 QeRDS Service provider 2 QCert for Esig QCert for ESeal QRAC QTimestamp

3 Check the available services (in the selected provider)

Once you have selected a provider, you need to contact it and ask for:

- An **authentication certificate** where:
 1. Key usage attribute must be “**digitalSignature**” OR extended key usage attribute must be “**clientAuth**”;
 2. Delivered on a **physical device** (smartcard or usb stick);
 3. **Certificate chain** needs to be built until a **Trust Anchor** (this last one must be a provider part of the EU Trusted List).
- An **electronic signature certificate**: where the intended purpose is “**Non-Repudiation**” and this one is not necessary to be on a physical device.

Case Management System

New authentication and electronic signature

How to authenticate to the CMS system?

UPDATE - 11 November 2022

Technical Details

We provide you, here after, with some additional technical details describing the Strong Authentication mechanism used by the CMS (for which the authentication certificate is needed).

The Strong Authentication is ensured via **mutual authentication** between the client (*browser*) and the server (CMS web application): the client supplies a client authentication certificate that authenticates the visiting user's identity.

What happens on the client side?

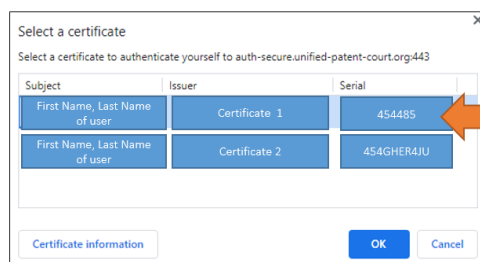
The browser consults the Operating System's trust store (Keychain on Mac OS X, certmgr.msc on Windows) to find any candidate certificates, i.e.:

- **Unexpired certificates** with the Client Authentication purpose set, i.e.: "digitalSignature" in the Key usages field or "clientAuth" in the "Extended key usages" field, for example:

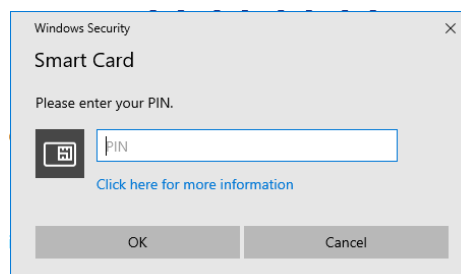
Key usages	digitalSignature nonRepudiation	Extended key usages	clientAuth emailProtection
-------------------	---	----------------------------	--------------------------------------

- **A private key** available for the certificate (on a secure device, such as a smart card or a USB stick).

Certificates that meet the above requirements are shown in a prompt when trying to login to the CMS:



Once the certificate is selected, the PIN is asked in another window:



What happens on server side?

The client authentication certificate must be issued by a certification authority listed in the EU Trusted list of the European Commission.

To ensure this, in addition to the certificate validity, the CMS checks that the certificate chain is built until a **Trust Anchor**, as defined by RFC 5280.

For more information, please refer to the following documentation where we have summarized the most asked questions in our FAQ section on our UPC web site.



[Frequently Asked Questions page](#)

We hope that this will answer to your questions and do not hesitate to contact us for any further information.

<https://www.unified-patent-court.org/contact>