

Instructions for qualified electronic signatures (QES)

Electronic signature:

To move steadily towards a **paperless administration**, your legal representative should use the **qualified electronic signature (QES)** when signing the document. This digital format, particularly following the pdf standard, replaces the exchange paper documents blue ink signed. Please note that only the QES within the meaning of Regulation (EU) No 910/2014 (eIDAS Regulation) will be accepted.

Documents signed with a **QES** benefit from the highest level of security and legal certainty under the eIDAS Regulation. A qualified electronic signature has the same legal value and effect as a handwritten “blue ink” signature across Europe.

N.B. The **advanced** electronic signature is not considered equivalent to a “blue ink” signature.

Please find more background information here:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+the+legislation+-+signature>

1) SEARCH FOR A TRUST SERVICE PROVIDER FOR OBTAINING QUALIFIED TRUST SERVICES

The Qualified Trust Service Providers (QTSPs), commercial service providers, who are qualified members of the European Union's Trust Scheme, are listed in the Trusted List Browser (<https://esignature.ec.europa.eu/efda/tl-> browser). This tool and its content are established and maintained through a collaboration between the Member States and the European Commission. Anybody living inside or outside the European Union is able to acquire these qualified Trust Services with a guarantee that these services are going to be recognised by all the Member States.

The private market of the QTSPs offers several qualified Trust Services. We strongly advise you to perform a thorough market research in order to acquire the services by the QTSP that best fit your business needs.

*N.B.: Only take provider having “**QCert for ESig**”. The provider must not necessarily be established in the same country as the contractor.

2) PROVE YOUR IDENTITY

To sign a document with a qualified electronic signature, you will need to acquire a specific digital **certificate**, which is a strong personal digital entitlement (e.g. as your passport).

Such a certificate can be enabled by your national eIDcard, or is issued by a **QTSP** who is authorised to collect, verify and store your data. Some of your personal data (e.g. your names) are present in the certificate. For more details about the data collection and usage of the personal data, you can contact the qualified service provider you are collaborating with.

3) SIGN A DOCUMENT WITH A QES

EUIBAs accept QES in which the following criteria are met:

- The signatory's identity is clearly mentioned in the qualified digital certificate used for producing the QES.
- The QES was produced inside the QSCD.

4) CHECK IF YOUR DOCUMENT IS SIGNED WITH QES BEFORE DISPATCH

It is important to test that your document is correctly signed with a qualified electronic signature and **not with an advanced electronic signature**. Please check this before the dispatch by uploading your document through the DSS Demonstration validation tool available at:

<https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation> where you can check the validity of a certificate by indicating the number and type of valid signatures in a document. “Qualification: **QESig**” means that it is a valid document.

The screenshot displays the validation results for a signature. At the top, a blue header shows the signature ID: "Signature SIGNATURE_EMMANUEL-GHISLAIN-LELOUX_20210827-0949". Below this, a table lists the following details:

Qualification:	QESig Qualified Electronic Signature
Signature format:	PAdES-BASELINE-T
Indication:	TOTAL_PASSED ✓
Certificate Chain:	EMMANUEL GHISLAIN LELOUX DigitalSign Qualified CA - G3 BT Class 2 CA - G3
On claimed time:	2021-08-27 07:49:00 (UTC)
Best signature time:	2021-08-27 07:49:38 (UTC)
Signature position:	1 out of 2
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 6167, 44057, 8580]

At the bottom of the validation area, there is a blue button labeled "Timestamps 1".

Key attention points:

- The signatory's data should be clearly indicated in the electronic signature properties. Your name and surname will allow your identification as the signatory.
- A qualified electronic signature can be verified only in electronic form, not on a printed version of the document.
- Please bear in mind that modifications after signing the document will break the integrity of the existing electronic signatures. It is therefore important that the document is no longer changed after signing.
- Please avoid applying your visible signature on top of the visible signatures that already present in the document
- The electronically signed documents provided to the EUIBAs should not be locked or password-protected.

Should you have questions regarding the installation and sending please contact :

eu-sign-service@ec.europa.eu