eIDAS Trust Framework and digital signatures

At the top of the Trust Framework we have the *EU Trusted Lists*. Member States have the obligation to establish, maintain and publish trusted lists with each qualified trust service provider under their control and the services provided by them.

In order to allow access to the trusted lists of all Member States, the Commission makes available to the public the trusted lists as notified by Member States.

Certificates for signatures and for seals are provided by QTSPs under the eIDAS legal framework. There are some 240 QTSPs, providing different Trust Services.

We focus here only on two types of certificates provided by QTSPs to organisations and legal representatives of organisations:

qualified certificate for electronic seal
: An electronic seal is data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity, where **the creator of a seal is a legal person (unlike the electronic signature that is issued by a natural person)**. In this document we will informally refer to a legal person as an `organisation`, when we do not require the more precise terminology.

  In this purpose, electronic seals might serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity. Nevertheless, across the European Union, when a transaction requires a qualified electronic seal from a legal person, **a qualified electronic signature from the authorised representative of the legal person is equally acceptable**.

qualified certificate for electronic signature
: An electronic signature is data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign, **where the signatory is a natural person**.

  Like its handwritten counterpart in the offline world, an electronic signature can be used, for instance, to electronically indicate that the signatory has written the document, agreed with the content of the document, or that the signatory was present as a witness.

  We are interested here in a qualified certificate for electronic signature issued to a natural person who is an authorised representative of the legal person, informally called a **certificate of representation**, because it is typically **used by the legal representative to sign documents on behalf of the organisation that the natural person represents**.

  In case you want to seal a document as a legal person (e.g. as a business or organisation), you might be instead interested in an electronic seal.

The qualified certificate for electronic seal is typically installed in a server (using a hardware security module, or HSM) and used to automatically seal documents like eInvoices (typically in XML format), by automated backend processes.

The qualified certificate for electronic signature is used by the natural person who is an authorised representative of the legal person. It is used under the control of the natural person to sign documents typically in PDF format, like contracts, where the natural person acts on behalf of the organisation.

These concepts are described in the following diagram:

Figure 1 Signatures of PDF and XML

In DOME we use eIDAS certificates to sign/seal Verifiable Credentials, which are JSON documents. Verifiable Credentials represent several types of documents in structured format and be machine readable and machine verifiable. Advanced/qualified signatures provide the same legal validity as “traditional” PDF or XML documents.

This is represented in the following diagram, complementing the one above:

Figure 2 Signatures of JSON documents

Revision #1
Created 10 November 2025 19:54:24 by Roger Miret
Updated 10 November 2025 19:54:43 by Roger Miret