

“e-Signing is an online tool to legally sign any electronic document, enabling recipients to verify your identity as signer and the integrity of your document.”



Certipost e-Signing in details

Description of Certipost e-Signing

The goal of Certipost e-Signing is to lower the barrier for electronic document signing dramatically by taking the legal and technical complexity away from the **Signer** who applies the signature and **Verifier** who trusts the signature. Certipost e-Signing is a service that will help users to create and verify Qualified Electronic Signatures with long term value. Qualified Electronic Signatures are electronic signatures that comply with the requirements from the European Directive (1) and Belgian law (2) concerning electronic signatures in such a way that from a legal point of view they are automatically accepted as equivalent to a handwritten signature. As the requirements from the European Directive and Belgian law are complex for the general public, Certipost has created this service to take this complexity away from the Signer and the Verifier can be assured of compliance of their signature and verification method to the European Directive and Belgian law. In addition, the Certipost e-Signing service offers a number of measures to make sure that supplementary conditions for long term non-repudiation (the characteristic that it can not be denied) of signatures are met.

Measures taken by Certipost e-Signing

During the creation of a signature, the Certipost e-Signing service will verify whether all required conditions are met to create a qualified electronic signature. Only when this is the case, an e-Signing signature archive will be created assuring the signer of the compliance of its signature with the legal requirements.

The following verifications are included with the Certipost e-Signing service:

- The use of a certificate with qualified level (Certipost e-Signing currently only accepts eID signing certificates and Certipost Qualified certificates)
- The correctness of signature itself on the original file
- Whether the qualified certificate was stored on a "Secure Signature Creation Device" (term applied by the European Directive, in practice this means a PKI [4] smartcard or a USB PKI token)
- Whether the certificate was not falsified (verification on the signature on the certificate by the Certificate Authority)
- Whether the certificate is still valid (not expired, revoked or suspended)

The signature archive is a ZIP file that contains three files:

1. The original file that was signed: it is of the utmost importance that the relation between the original file and the signature is maintained and that the original file is not altered in any way (even when only one character in the file is changed, the signature becomes invalid). By including the original file in the signature archive, optimal conditions are provided to live up to these requirements.



2. The signature itself in a XAdES-X-L-format: this is the signature itself. As a user you do not have to open this file. During the verification, the e-Signing service will interpret this file and all information it contains that allows to ensure that all elements of the signature are valid
3. A readme PDF file: this file is not required for the legal value of the signature, but gives some explanation about the signature archive, what its value is and how the Verifier can validate it.

The applied XAdES-X-L is an XML signature format according to the recognized XAdES standard (3) that implements measures to satisfy the legal requirements for advanced electronic signatures as defined in the European Directive (1) and for long term non-repudiation. Next to the electronic signature itself, the XAdES-X-L-file contains the certificate that was used during the signature, the information to proof whether the certificate was valid when signing, and a time stamp to proof that all information used for signing existed and not altered since.

The timestamp is applied to make sure that the signature keeps having value, even when the certificate that was used to sign is not valid anymore. This is required to be able to proof that the signature was valid at the moment it was created even if afterwards the certificate expired, was revoked or suspended. The validity of the signature can be proven as long as the timestamp is valid. This period can be extended by adding a new timestamp before the end of validity of the applied timestamp. The XAdES format allows adding as much timestamps as deemed necessary over time.

During verification, the same verifications are executed as during the creation, being complemented with a verification of the timestamp. This gives the assurance that at the time of signing all conditions were met for the signature to be a qualified electronic signature and thus have a legal value equivalent to a handwritten signature.

References

- (1) EC 1999/93: European Community (EC) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES
- (2) The 9th of July 2001 Belgian Law about electronic signatures
- (3) ETSI TS 101 903 standard
- (4) PKI: Public Key Infrastructure, is the infrastructure used by a trusted third party to issue digital certificates. Digital certificates binds the signature to the identity of the signer.