

Electronic Signatures in the Netherlands



Under Dutch law, agreements or contracts are free of form unless determined otherwise. Thus, the conclusion of a contract generally does not require any signature. However, in practice signatures are viewed as an established method of reliably confirming, controlling and proving (business) transactions. They are used for evidentiary reasons. If two parties choose to sign a contract for such reasons, they may use either a handwritten or electronic signature, depending on their evidentiary needs.

Documents signed with a wet signature have binding evidential value. If the electronic signing method used is sufficiently reliable, the electronically signed document will also have similar binding evidential value. However, when the electronic signing method is not sufficiently reliable, the electronically signed document only has free evidential value - ultimately left to the discretion of the judge.

Under the European eIDAS regulation, qualified electronic signatures (QES) are always considered to have the same legal effect as handwritten signatures. Pursuant to Dutch law, standard (SES) and advanced electronic signatures (AES) only have the same legal effect as a handwritten signature if the method of signing used is sufficiently reliable having regard to:

- The purpose for which the electronic signature is used
- All other circumstances of the case

Parties in business contractual relationships and e-commerce transactions often rely on standard electronic signatures. As opposed to scanned handwritten signature images that can readily be copied, a robust electronic signing platform, such as DocuSign eSignature, automatically creates a digital audit trail that provides evidence of the signature and transaction.

In relation to the “standard” electronic signature, Dutch courts have hinted that some uses may be better off with an advanced (AES) or qualified (QES) electronic signature, e.g. a medical statement might require either an advanced or qualified electronic signature, whereas for a document with a purpose of less significance a (standard) electronic signature (with appropriate safeguards) may suffice.

When determining whether an electronic signature is sufficiently reliable, a court also will take into account the circumstances, e.g. whether parties have met each other before and whether they have already executed the (or a previous) agreement. Nevertheless, it must be noted that the amount of court cases in which the validity of an electronic signature is challenged is relatively limited due to the wide-spread general acceptance of electronic signatures.

Support for electronic signatures in the Netherlands

The conclusion of an agreement requires an offer and acceptance, which need not be in writing or accompanied by a signature. In order to prove that a contract has been agreed to by the parties, the parties usually draft and sign a written instrument. The electronic signature on such a written instrument generally does not need to be technically sophisticated. An e-mail closing or scanned signature may often suffice. However, such basic electronic signing approaches suffer from a lower level of evidentiary value due to the lack of enhanced features, found in more mature electronic signing platforms, like DocuSign eSignature. Such electronic signature software platform, like DocuSign eSignature, provide further support in proving that the parties have expressed their agreement as to the obligations set out in the contract and as to the manner in which they are to be performed through such functionality as applying fraud evident seal(s) to the digital document and generating a digital audit trail, which DocuSign calls a Certificate of Completion.

Electronic transaction and signature court cases - examples from the Netherlands

District Court Rotterdam
17 September 2020,
ECLI:NL:RBROT:2020:8245

The District Court Rotterdam ruled that the electronic signature on a rental agreement was sufficiently reliable and thus equivalent to a wet signature.

A Signature Certificate may prove the conclusion of a rental agreement and contribute to the reliability of the electronic signature.

The defendant contested signing the rental agreement. The claimant, however, provided the Signature Certificate as proof, which contained data on the date and time the link was e-mailed, to which e-mail address, when the document was viewed and with which IP address. The defendant also did not contest that the personal information included in the certificate were his. In light of the foregoing the District Court found that the personal details included provided concrete safeguards and that the electronic signature in question was sufficiently reliable and thus equivalent to a wet signature.

District Court Noord
Nederland 24 April 2019,
ECLI:NL:RBNNE:2019:1715

The District Court found that the use of a signature that was 'copy-pasted' was insufficiently reliable for the purposes of a purchase agreement for a holiday home.

A signature that was copy-pasted is not sufficiently reliable for the purposes of a purchase agreement for a holiday home.

The dispute concerns the agreement to buy a holiday home. The agreement was sent digitally to the buyers (a husband and wife) and the signature of both buyers was digitally placed (copy-pasted) on the document. The couple attended the viewing together, but all later communications between buyer and seller took place solely with the husband. The wife later contested signing the buying agreement. In light of the manner of signing in question, the District Court considered the signing method unreliable.

Dutch Supreme Court,
ruling of 14 June 2019,
ECLI:NL:HR:2019:957

This case concerned whether or not an electronically signed medical statement from a doctor should have been admitted in court as such (ie. as a medical statement), as the law requires a signature. In this case, the Supreme Court ruled that the purpose for which a medical statement is used implies that an electronic signature under such a statement must be an advanced or qualified electronic signature.

A medical statement requires an electronic signature that is sufficiently reliable, such as an advanced or qualified electronic signature.

District Court Amsterdam
11 December 2019,
ECLI:NL:RBAMS:2019:8755

The District Court Amsterdam found that given the importance of the agreement at hand the electronic signing method used was insufficiently reliable.

Agreements in relation to large sums of money and imposing obligations in combination with other relevant risk factors may warrant advanced or qualified electronic signatures.

A factoring agreement was concluded by e-mail and digitally signed by the two directors. The parties had never been in contact with each other in person. Here, the District Court considered that, in view of the purpose for which the electronic signatures were used in this case, i.e. entering into an agreement on the basis of which large sums of money could be - and actually were - transferred under the threat of a hefty fine regime and a bail on the basis of which the directors became jointly and severally liable for the performance of this far-reaching agreement, the method of signature cannot be regarded as sufficiently reliable. According to the District Court, identity fraud should have been a foreseeable, and not negligible, risk in fully digital trading relationships. To guarantee identification with an electronic signature, a qualified or advanced electronic signature should have been used.



Comparison: Informal electronic signature versus an electronic signing platform

Although an informal electronic signature/consent is in principle capable of constituting a signature, it does carry higher risks.

It may be necessary to produce evidence, perhaps long after the event, of the processes that were followed for any given signed document and what the contents of the document were. This evidence might be needed in court, or perhaps in other situations such as due diligence or inspection by auditors.

Using a genuine electronic signature (standard, advanced or qualified) through a software platform, such as DocuSign eSignature (as opposed to a scanned copy of a handwritten signature), renders contracting more secure in that the validity of contracts will be more difficult to challenge. DocuSign eSignature provides a structured auditable environment, including fraud evident document protections and a digital audit trail, called a Certificate of Completion, and a step by step process for electronically signing documents.

Document integrity

An informal electronic signature leaves open the possibility of dispute about what the signed document consists of, and whether it might have been altered subsequently. Secure handling (e.g., tamper evident protections) of the signed document and associated secure electronic signatures reduces this risk.

Identity of signatory

What if the signatory subsequently denies that they signed the document? Can you prove that it was them? Many businesses wish to have the flexibility to choose a level of identity assurance that reflects the nature of the document and the value and importance of the transaction. DocuSign eSignature provides various different identification options to provide the signers with the ability to confirm their identity when using standard (SES), advance (AES) or qualified electronic signatures (QES).

Overall, it is normally open to a business to choose the kind of electronic signature that it considers suitable for the transaction. Enhanced electronic signatures, called digital signatures (i.e. AES and QES), offer the highest assurance levels of document integrity and identity of a signatory, typically used in specific highly regulated industries and certain government documents. However, experience suggests that businesses take a pragmatic view, balancing efficiency against heightened identity needs, and primarily use for most transactions standard electronic signatures (SES).

Formalities requirements

Aside from evidentiary requirements that parties may have in some cases, Dutch law also may impose formalities in other very specific instances. For example, in the situation where the law explicitly prescribes that a document should be in writing. In order to fulfil the requirement of being 'in writing' electronically, the law requires that the agreement is created electronically and that the:

- 1/ Agreement is consultable by parties
- 2/ Authenticity of the provisions is sufficiently guaranteed
- 3/ Moment of creation of the agreement can be determined with sufficient certainty
- 4/ Identity of the parties can be established with sufficient certainty

Furthermore, if the law includes a written requirement and the involvement of a judge, government organ or a professional exercising a public task (e.g. a notary) an electronic signature may not be used as a substitute of a wet signature. In addition, there are exceptional cases in which the law prescribes the type of electronic signature that may be used, for example in relation to the (electronic) statement of elements of the employment contract.

Many Dutch law formality requirement may be satisfied using an electronic signing platform, such as DocuSign eSignature. Care is still necessary to ensure that the chosen kind of signature (e.g., SES, AES or QES) and signing process does comply with the formality requirement, and that the processes have been used appropriately.

The increasing need for remote working also has sparked a greater need to adapt formalities to modern-day needs of society, where interactions are increasingly virtual. This is particularly so with regard to the conclusion of contracts between people not physically in the same place. Therefore, there are clear trends throughout the world where the remaining formalistic and cumbersome physical (or wet) signing requirements and procedures are being eliminated to further encourage users to even more broadly use electronic documents and signing technologies.

DISCLAIMER: The information in this White Paper is for general information purposes only and is not intended to serve as legal advice. It is limited to the laws of the Netherlands. Laws governing electronic signature may change quickly, so DocuSign cannot guarantee that all the information in this White Paper is current or correct. Should you have specific legal questions about any of the information in this White Paper, you should consult a suitably qualified legal practitioner.

February 1, 2022

About DocuSign

DocuSign helps organizations connect and automate how they prepare, sign, act on and manage agreements. As part of the DocuSign Agreement Cloud, DocuSign offers eSignature, the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time. Today, over a million customers and more than a billion users in over 180 countries use the DocuSign Agreement Cloud to accelerate the process of doing business and simplify people's lives.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

[docusign.com](https://www.docusign.com)

For more information
sales@docusign.com
+1-877-720-2040

DocuSign®