Are Notarius' Signatures Legally Reliable and Recognized by Courts?

notarius

At Notarius, we're often asked if our digital and electronic signatures are legally reliable and recognized by courts. While seemingly simple, the answer to this question requires an understanding of a few different concepts. Let's first clarify a few terms, definitions, and concepts concerning signatures in electronic format.

Terms, Definitions and Concepts

We consider the expression **"electronic signature"** as encompassing all signatures in electronic format. Electronic signatures therefore include images of handwritten signatures, voice recordings agreeing to a transaction, documents signed using an electronic signature platform, as well as documents signed by holders of a digital signature certificate.

SELF-ASSERTED ELECTRONIC SIGNATURE

The expression **"self-asserted electronic signature"** means that the signer's identity is self-declared and not otherwise verified or trusted by a third party. For example, Adobe's self-signed digital certificate or the signature block in a Gmail account fall under this definition.

TRUSTED ELECTRONIC SIGNATURE

The expression **"trusted electronic signature"** implies that the signer's identity has, at a minimum, been verified or validated by a third party. For example, a document that is signed using ConsignO Cloud requires the signer to use *two factor authentication* (by providing an email address and cell phone number, for example) so that the signer is authenticated before the document is signed. If the authentication information is embedded into the signature, it is referred to as a "trusted electronic signature" since the authentication credentials come from a third party and are disclosed to the concerned parties in a transparent manner.

DIGITAL SIGNATURE

At Notarius, a **"digital signature"** refers to a signature with a higher level of reliability than an electronic signature because it:

contains information that is cryptographically protected

is issued by a trusted certification authority through a robust public key infrastructure

2 pieces of identification

\+

Face-to-face identity verification with an agent

requires the signer to hold a digital signing certificate

requires strong authentication methods

Based on this terminology, Notarius' different CertifiO signatures are *digital signatures* and the ConsignO Cloud solution allows two types of signatures to be processed in its platform: *trusted electronic signatures* (for signers who do not possess a digital signing certificate) and *digital signatures* (for signers holding a digital signing certificate issued by Notarius).

Reliability of the Signature

To determine whether a signature is valid in law and recognized by courts, we must examine the signature's reliability. At Notarius, a signature's reliability is based on four fundamental attributes:

Identity: To what extent can the parties concerned be assured that the signer is the person he or she claims to be?

Authenticity: Is all of the information that attests to the signers' identities and the document's integrity embedded into the document?

Integrity: To what extent can the parties concerned be assured that the document has not been modified?

Longevity: To what extent can the parties concerned be assured that the document can be opened, read, and authenticated for decades to come?

Using current technologies, the best way to ensure a high level of legal reliability when it comes to a signer's *identity* and a document's *integrity* and *authenticity* is to use a digital signature backed by a digital signing certificate which is issued to the signer by a trusted certification authority through a robust public key infrastructure. As mentioned above, *trusted electronic signatures* also provide a high level of reliability.

Currently, the best way to guarantee a document's longevity is to ensure that it complies with the PDF/A standard (ISO 19005) and to use a digital signature that complies with the PAdES standard, which ensures the long-term validity of signatures.

Notarius is one of the few certification authorities in the world, if not the only, that combines extensive expertise in public key infrastructure operations and PDF and PDF/A standards. For example, Notarius is the only certification authority that is a member of the PDF Association. Thanks to this combined expertise, Notarius' clients can create, verify, and preserve highly reliable electronic documents for decades to come.

Validity in Law

The following components must be assessed to determine whether an electronic signature is valid in law (unfortunately, there are **NO** shortcuts):

What type of document will the signature be used on? What process will be used? And what are the terms and conditions? For example, the terms and conditions could include a *forum conveniens* clause according to which the parties agree to the jurisdiction governing their contract. (A "jurisdiction" could be a state, province, country, or even Europe as a whole.)

Depending on the type of document used and the applicable jurisdiction, **what laws govern electronic signatures?**

Depending on the applicable jurisdiction, **are there any specific statutory or regulatory rules** mandating a certain type of signature or document that could directly impact whether an electronic signature is valid under the law? (For example, in the province of Quebec, there are only three legally valid forms of wills, and none of them is an electronic document signed only by the testator.)

In that jurisdiction and with the exception of any specific statutory or regulatory rules governing forms of signatures for the type of document under consideration, **what is the default legal framework** that applies to electronic signatures?

It is up to every organization that is considering using electronic signatures to conduct the four-step analysis described above for each type of document it wishes to use. As a starting point for this analysis, here are a few general points concerning the validity in law of electronic signatures.

In Canada, the United States, and Europe, the general legislative framework governing the validity of electronic signatures is based on the work of the United Nations Commission on International Trade Law (UNCITRAL) at the end of the 1990s. Based on this work, model laws were proposed and eventually adopted everywhere in Canada, the United States, and Europe. The same general principle applies in all jurisdictions:

The legal effects of an electronic document cannot be denied solely on the basis that it is an electronic document.

In addition, a careful reading of laws on electronic signatures reveals that there are two types of electronic signatures as defined under law:

- ***Authentic* legal signatures,** which courts accept as evidence that ***does not require*** corroborating evidence. It is normally the responsibility of the party claiming that the electronic signature is not valid to prove that such is the case;
- ***Inauthentic* legal signatures,** which courts accept as prima facie evidence ***requiring*** corroborating evidence. It is normally the responsibility of the party claiming that the electronic signature is valid to prove that such is the case.

It is also possible to extract the following main guidelines concerning the validity of electronic signatures in Canada, the United States, and Europe:

In Canada, the validity of most electronic signatures is governed by provincial laws. To varying degrees, all of the provinces adopted the same model legislation on e-commerce from the Uniform Law Conference of Canada (ULCC) at the beginning of the 2000s. Notarius' trusted digital signatures and electronic signatures surpass the provincial and Canadian federal requirements concerning their legal validity in e-commerce.

In the U.S., the use of electronic signatures has become an accepted practice since Congress adopted the *Electronic Signatures in Global and National Commerce Act (ESIGN Act)* in 2000. This law is based on a previous law, *the Uniform Electronic Transactions Act (UETA)*. Forty-seven states have ratified UETA, while the states of New York, Washington, and Illinois have adopted similar laws. Notarius' digital and trusted electronic signatures are fully compliant with U.S. legal requirements and guarantee a signer's identity as well as the integrity, authenticity, and longevity of all electronically signed documents.

The European Union's regulation on electronic identification authentication and trust services (eIDAS) is the law regulating electronic signatures in Europe. This law shares similarities with North American legislation. Notarius meets the requirements set out in Europe's eIDAS regulation with regard to the issuing of certified electronic signatures as it conforms to standards ETSI EN 319 401, ETSI EN 319 411-1, and ETSI EN 319 411-2. Notarius' eIDAS certificate (no. C EIDAS-122017-0CU00210) covers all of Notarius' activities, both technical and administrative, for the development, operation, and support of digital signature products in its role as a trusted third party.

In short, Notarius' *digital signatures* and *trusted electronic signatures* provide high-level legal reliability, and documents signed using these signatures are considered valid in law, subject to rare and specific legislative and regulatory exceptions that bar the use of all electronic or digital signatures.

Validity in Courts

With regard to the four-step analysis described above, it is impossible to state with certainty that any form of signature will be universally accepted in all jurisdictions and for all types of documents. Notarius nevertheless maintains that all of its signatures would be deemed valid in all courts in Canada, the United States, and Europe *if used in a context where no specific legislative or regulatory exception bars their use or prescribes a highly specific type of electronic signature.*

To date, after more than 20 years in business and millions of documents across the world signed using its products, there has been no single court case in which a Notarius signature has been deemed invalid by a court, which the leading provider of electronic signatures cannot claim.

Certifications

- First certification authority in North America to be certified **ISO 27001**;
- Only Canadian firm that issues trusted signatures recognized by **Adobe** (Adobe Approved Trust List – AATL) and **eIDAS** (electronic IDentification Authentication and trust Services);
- Notarius also holds **ISO 9001** certification in quality management.

Approved Trust List MEMBER

PDF association MEMBER

ISO 27001 CERTI TRUST

ISO 9001 CERTI TRUST

eIDAS CERTI TRUST

For More Information

notarius.com | 1-888-588-0011 | info@notarius.com

notarius

Digital transformation.
Legally reliable documents.