



Electronic Signatures **Understanding the Differences**

Understanding the world of electronic signatures **and** Notarius's solutions

When Bill Clinton adopted the E-SIGN Act in 2000, he gave birth to a legal framework for electronic signatures in the United States.

Since then, most countries have in turn assigned the same legal value to electronic signatures as to handwritten signatures.

While all agree that they are effective and provide flexibility, not all electronic signatures have the same legal value. Notarius, specifically, offers three types of signatures:

- 1 **Basic electronic signatures**
- 2 **Trusted electronic signatures**
- 3 **Digital signatures**
(for individuals or organizations)

What makes them different...



Compliance requirements = Choice of signature

Each type of electronic signature has a different level of legal reliability.

As a result, their use will change depending on the context and compliance requirements.

So, it is not about finding THE best electronic signature, but rather the one that best suits your needs from a risk management perspective, as well as its ease of use.

To get a better understanding of their differences, we have put their use into context and assessed how each of them provides:

A way to identify signers

Identity

Proof that the signers are, in fact, the people who have signed the document

Authenticity

Mechanisms for detecting if someone has tampered with the document

Integrity

A way to verify signatures for years to come.

Longevity



Unless certain conditions apply¹ an electronically signed document has the same legal value as a document that has been signed by hand as long as the integrity of the document can be verified, the signers' identities can be established, and the signers' consent can be clearly demonstrated².

1. Unless there are rules that are specific to a particular field of law.

2. Based on the legal opinion of attorneys at Langlois Avocats S.E.N.C.R.L., available here: <https://www.notarius.com/hubfs/document/en/education/legal-framework-for-electronic-signatures.pdf>



1

Basic electronic signatures

For agreements between friends and family requiring only a very low degree of legal reliability

Let's say you rent your cottage to a friend. They email you a rental agreement in PDF format. You know this person well. You then scan your handwritten signature, affix the image of it to the PDF document, and send it back.

You have put **blind trust** in your friend, which means it can be considered as a basic electronic signature. But there are significant risks to it. In the event of a dispute, the rental agreement could be easily contested, as your friend can currently alter the document without leaving any trace. The basic electronic signature is the simplest, but also the least reliable, of the three types of signatures.

From behind a screen, everyone can claim to be the president of the United States. With a basic electronic signature, there is no way to verify who is behind the screen.

Identity

The basic signature, in the example above, is a handwritten signature image affixed to an electronic document, which means that anyone can take a photo of any handwritten signature and paste it on the contract at any time. As the signature is only an image, it does not protect the document from counterfeiting.

Authenticity

Integrity

1 Basic electronic signature

With respect to the rental agreement format, although PDF is a format recognized as stable and standardized, with a basic electronic signature, there is no assurance that it will be readable in 10 years. Longevity

In summary, the basic electronic signature is a possible solution **only** if one has blind trust in the other signer and if the document does not require a high degree of legal reliability.



As soon as a person has access to the image of your handwritten signature, they can copy it, affix it as a basic electronic signature, and steal your identity.



2

Trusted electronic signatures

For business agreements and contracts that require a good level of legal reliability

Need to sign a hiring contract or accept a bid of several tens of thousands of dollars? You will agree that you will need a solution with a good level of legal reliability to avoid any unpleasant surprises. First, you need to confirm the signers' identities and, second, you need to ensure that the contract you are about to sign will be recognized in the event of a dispute.

Trusted electronic signatures are therefore the most appropriate. Trusted electronic signature partners such as Notarius provide access to this type of signature.

The Notarius web platform, ConsignO Cloud, offers this type of solution.



Unlike a basic electronic signature, a trusted electronic signature links a signer's identity to at least one authentication factor.

On ConsignO Cloud, the signer's identity is verified via two authentication factors (for example, an email address and phone number), which exceeds industry standards.

Identity

Two-factor authentication enhances security and is often the solution adopted by large banking institutions.

2 Trusted electronic signature

To protect a signed document from being tampered with,, most platforms typically affix an organization's generic digital signature once all parties have signed. With ConsignO Cloud, we offer more. Our platform combines a generic digital signature that includes the signer's information at each step in the signing process to safeguard the integrity of the information throughout the process. When it comes to traceability, it is the best around.

To track signature activity processes, platforms create an audit trail for each signed document, which is often added to the signed document and is rarely protected. Our solution, on the other hand, also generates an audit trail, but it is completely independent and contains not only all signature-related activities (e.g., signature times, IP addresses, email addresses), but also a copy of the original and final documents. Most notably, ConsignO Cloud also digitally signs this audit trail to protect it.

Authenticity

Integrity

Moreover, in the event of subsequent changes to signatures, they can be detected free of charge via software such as Acrobat Reader or our site at Verifio.com.

Integrity



With **ConsignO Cloud**, the signing process is reduced from several days to a several hours, or even minutes.



2 Trusted electronic signature

When it comes to archiving electronic documents, an additional best practice is to ensure the longevity of documents and signatures using the archive format PDF/A, ISO 19005 standard. In this respect, ConsignO Cloud offers free conversion of uploaded documents to PDF/A format and makes signatures compliant with the PAdES3 standard for the long-term validation of electronic signatures. As a result, the documents signed, and the audit trail can be read and verified for decades to come.

Longevity

This is how the ConsignO Cloud trusted electronic signature provides a good level of legal reliability. The solution is designed to simplify and speed up the signing process, regardless of whether the signers are internal or external to your organization, in addition to providing advanced security.

3. PAdES LTV (ETSI TS 102 778) is a standard that validates signatures long term and confirms that they were valid at the time they were affixed, regardless of the current status of the certificate (expired or revoked). ConsignO Cloud complies with level 4 (BLT-A) of the PAdES LTV specification. All proof and their compatibility over time are included in the document to validate signatures and time stamps.

3

Digital signature

(for individuals or organizations)

For documents requiring official seals or professional signatures

If you receive an engineering plan, a will, or an important document from an organization, you want to ensure that the person who signed it is in fact in good professional standing or that they are employed by the organization in question. This involves ensuring that the signer is actually associated with their professional association or organization.

This is where digital signatures come into play.

A digital signature uses cryptography to create a strong link between an identification file containing an individual's information and an electronic document.

Affixing a digital signature that has been issued by an accredited certification authority ensures the integrity of the information in an electronic document.



Nearly 50 professional associations in Canada currently use CertifiO digital signatures. In addition to being the standard for many industries, they can be used on [ConsignO Cloud](#) in complementarity with trusted electronic signatures.

More than just a digital identity, the CertifiO® signature can also incorporate an individual's professional designation.



certifiO
Professionnels



certifiO
Employés

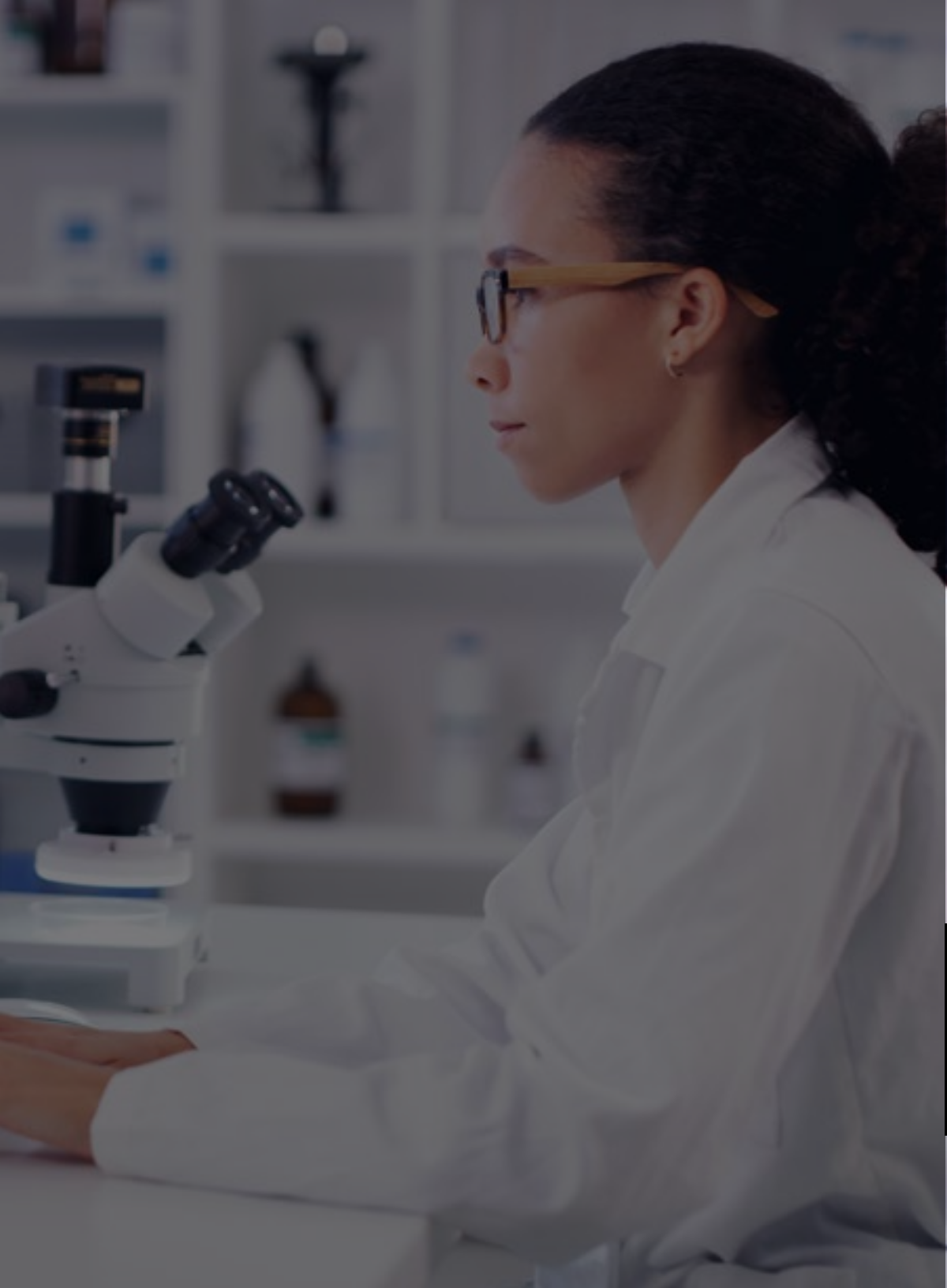
In addition, at Notarius, our rigorous face-to-face identity verification and security processes make our digital signatures even more reliable than most options on the market. Once they have proved their identity with Notarius and their association or organization has validated their designation or employment link, a user can obtain their CertifiO digital signature.

Identity



If a professional or an employee is no longer permitted to practise, their association or organization will revoke their **CertifiO** digital signature.





3 Digital signature (for individuals or organizations)

Notarius is the only company in Canada that issues digital signatures recognized by both Adobe® and Microsoft®.

In fact, when a professional signs with their CertifiO digital signature, they provide a unique link between the document's digital fingerprint and their identity. At the same time, Notarius's certified infrastructure provides the necessary proof to demonstrate that, at the time of signing, the signer's identity and its attributes (affiliation, employment relationship, membership number) were valid.

Identity

Authenticity

Notarius's signature solutions incorporate this validation proof into the document (PAdES standard), which follow it throughout its lifetime. This ensures the signature's longevity and, consequently, its link to the electronic document.

Longevity



Notarius adheres to the PAdES LTV (ETSI TS 102 778) and PDF/A standards, it is an excellent way to ensure unparalleled legal reliability in those formats.

When you use a CertifiO digital signature in our ConsignO Desktop software, you can authenticate any file format (DWG, BIM, XLS) by adding them as attachments to a PDF/A-3. As



3 Digital signature (for individuals or organizations)

As with ConsignO Cloud, documents signed with a CertifiO signature cannot be altered without leaving a trace.

Integrity

It is the most reliable signature in the industry and meets the highest standards of compliance. When a digital signature is affixed to a document, it guarantees the document's integrity and provides a higher level of security, even more than a hand-signed document.

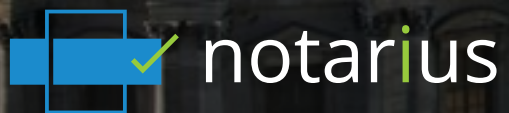


It is possible to create a digital signature via a platform that does not verify the signer's identity. This involves identity checks conducted by a third party such as **Notarius** that can ensure that the digital signature is compliant.

Today, we can realize projects that we never would have dreamt possible because our society has built itself around rigorous ethics and exceptional accountability.

But, while the digital world is dictating the pace, the same values that inspire confidence must be preserved. To do so, ensuring the reliability of identities, documents, and information must be a priority. This is what Notarius has been working toward since 1996.

With our solutions, professionals and organizations meet the highest compliance requirements while leveraging the latest technology. At Notarius, we believe professionals should be able to maintain high standards in their practice, except faster, smarter, and more efficiently.



The world is going digital.
Be digitally reliable.



notarius.com



info@notarius.com





1 888 588-0011



Follow us

Differentiate between the 3 types of electronic signatures according to Notarius.

Now that you have a better understanding of electronic signatures, all that is left to do is decide which Notarius solution offers the degree of legal reliability required for your documents.

	Basic electronic signature (not offered by Notarius)	ConsignO Cloud trusted electronic signature 	CertifiO digital signature 
Identity	Not verified.	Confirmed via two-factor authentication.	Face-to-face verification with two proofs of identity.
Integrity	None.	Tampering detection guaranteed with a digital certificate.	Detection of alterations is guaranteed through the digital certificate linked to the individual or organization.
Authenticity	There is no way to verify the authenticity of a document containing a basic signature.	High level of comfort with respect to authenticity thanks to an identity that is backed by two-factor authentication and an audit trail.	Very high level of comfort with respect to authenticity based on the signer's digital certificate issued following a rigorous and standardized identity verification process.
Longevity	Usually none.	PDF/A are stand-alone files regulated by ISO + PAdES standards.	PDF/A are stand-alone files regulated by ISO + PAdES standards (with ConsignO Cloud and ConsignO Desktop).
Identity Assurance Level (IAL)	PCTF Level 1	PCTF Level 2	PCTF Level 2
Use Cases	Documents requiring only a very low level of legal reliability.	Documents requiring good legal reliability.	Professional documents requiring advanced legal reliability.