Table of Contents

Table 1 – Digital vs Electronic Signature Comparison

	Digital Signature	Electronic Signature
Definition	A digital signature, which should not be confused with a digital certificate, is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document	An electronic signature is an electronic indication of a person's intent to accept the content of a document or a collection of data linked to the signature
Issuance	Mostly issued by Governments via PKI (Public Key Infrastructure)	Issued by an individual or private/public institution
How to Sign	Signs with a digital certificate	With login and password, SMS, digital biometrics and several other data points
Types	On the basis of document processing platform, a digital signature is of two types - Microsoft and Adobe PDF	An electronic signature is of four types - basic electronic signature, click-to-sign signature, advanced electronic signature, and qualified signature
Regulation	A digital signature is regulated by the certification authority	Some national acts and regulations are applied to the electronic signature to validate it
Authorisation	Digital signatures are authorised by the government or non-government certification provider authority	Electronic signatures are authorised by the specific vendors, document creator or involved parties
Intention	The main intention of using a digital signature is to secure the document	The main intention of using an electronic signature is to verify the document
Security	A digital signature is comprised of more security features, so it is more secure	An electronic signature is comprised of less security features, so it is less secure
Verification	A digital signature can be verified to authenticate the original author	As the electronic signature is not certified, in some jurisdictions, it can be difficult to check and verify the owner of the document
Signatory Details	A digital signature can be used to get the details of signatory details as it is associated with the signature itself	The details of the signatory are not held with the electronic signature but can be held separately to the signature
Audit Logs	Digital signature generally holds the audit logs and helps track when the changes are made in the document	It is difficult to apply audit logs with the electronic signature. But some electronic signature solutions may provide this
Time-stamped	Digital signatures are always time-stamped, i.e. a date and time is permanently associated with the digital signature	Electronic signatures can be time-stamped, which is very good for legal binding. It will tie the signature with date and time in legal formalities
Reliability	Digital signatures are more reliable as these are more secured and least susceptible to tampering	Electronic signatures are less reliable as these are less secured and may be more susceptible to tampering
Quality of Standardization	A digital signature uses a highly advanced form of standardization known as Public Key Infrastructure (PKI)	The keying mechanism varies according to each jurisdiction
For which cases is it recommended?	For cases involving: - Greater legal security - Business risks - Significant value involved - Question about the impact that the proof of authorship can cause - Compliance - Sign contracts and documents between companies	For cases involving: - Lower business risk documents - Lower impact - Documents involving individuals as signatories - Internal documents that require a simple approval, acceptance or agreement to an adherence contract and others

Electronic Signatures

Definition

- The term "Electronic Signature" or “eSignature" is an electronic indication of a person's intent to accept the content of a document or a collection of data linked to the signature
- An electronic signature acts as an acceptance or approval of the contents within a document or form. All that is needed for an electronic signature is a mark, which can be captured through a check box, typed name, electronically signed name, or uploaded signature image. Other data that may be collected automatically are IP address and geolocation
- Just like its handwritten counterpart, an electronic signature is a legally recognised means of stating the signer's intent to adhere to the terms of the document they have signed
- Globally, an electronic signature is recognised as the data in electronic form which is attached to or logically associated with other data in electronic form and used by the signatory to sign

Benefits

- They make gathering signatures easier, faster, and more efficient when compared to using pen and paper. They also speed up approvals and agreements, eliminating any unnecessary delays
- They save you time and resources by avoiding the need to print, sign, scan, or post your documents and forms
- They streamline internal company processes that require signatures
- They include a digital date and time stamp
- They are portable, legally binding (in most jurisdictions) instantaneous and reduce environmental impact. They are sometimes supported by technology that verifies the authenticity of the signature

Business use cases

- Accident Reports
- Checklist Sign Offs
- Enrollment Forms
- Employee Reviews
- Internal Approvals
- Internal Evaluations
- Patient Registration
- Contract Agreements

Are they legally binding?

- This varies according to each jurisdiction. As an example, In the United States, Electronic signatures have carried the same legal weight as traditional, paper-based ones since the Electronic Signatures in Global and National Commerce Act (ESIGN) was passed in 2000. This legislation ensures that electronic signatures are legally binding in every state where federal law applies. Where federal law does not apply, most states have adopted the Uniform Electronic Transactions Act (UETA). Developed by the Uniform Law Commission, UETA provides a legal framework for the use of electronic signatures and helps ensure they are just as enforceable as their paper counterparts

Electronic signatures in Brazil

- Brazil has a tiered legal model, which means that most electronic signatures are considered legally valid unless explicitly stated otherwise. Head over to the Brazilian Standards section for more details

Conclusion

- Electronic signatures are just that: a pen and paper signature captured electronically. Because of this, there is not an authentication process that verifies the signee or document. What separates digital signatures from electronic signatures is the way digital signatures use a digital certificate to encrypt the final signed document. This includes evidence of the signer identification via unique link sent via email, SMS, shared password between the sender and a signer, or a similar method

Digital Signatures

The problem and its origins

Before we go into the details, it might be helpful to take a step back for a moment and look at the security concerns surrounding paper-based documents and workflows. The most common concerns individuals and organisations face when dealing with paper-based documents are:

- Is the person who signed the document who they claim to be? In other words, how can I verify if the signature is valid and hasn't been forged?
- How do I safeguard (or from the receiver's perspective, confirm) that the content within the document hasn't been tampered with?

The existence of notaries was invented to help address these very valid concerns and can be traced all the way back to the ancient Egyptian times. Notaries today play a key role in assuring the parties of a transaction that the document is authentic and can be trusted

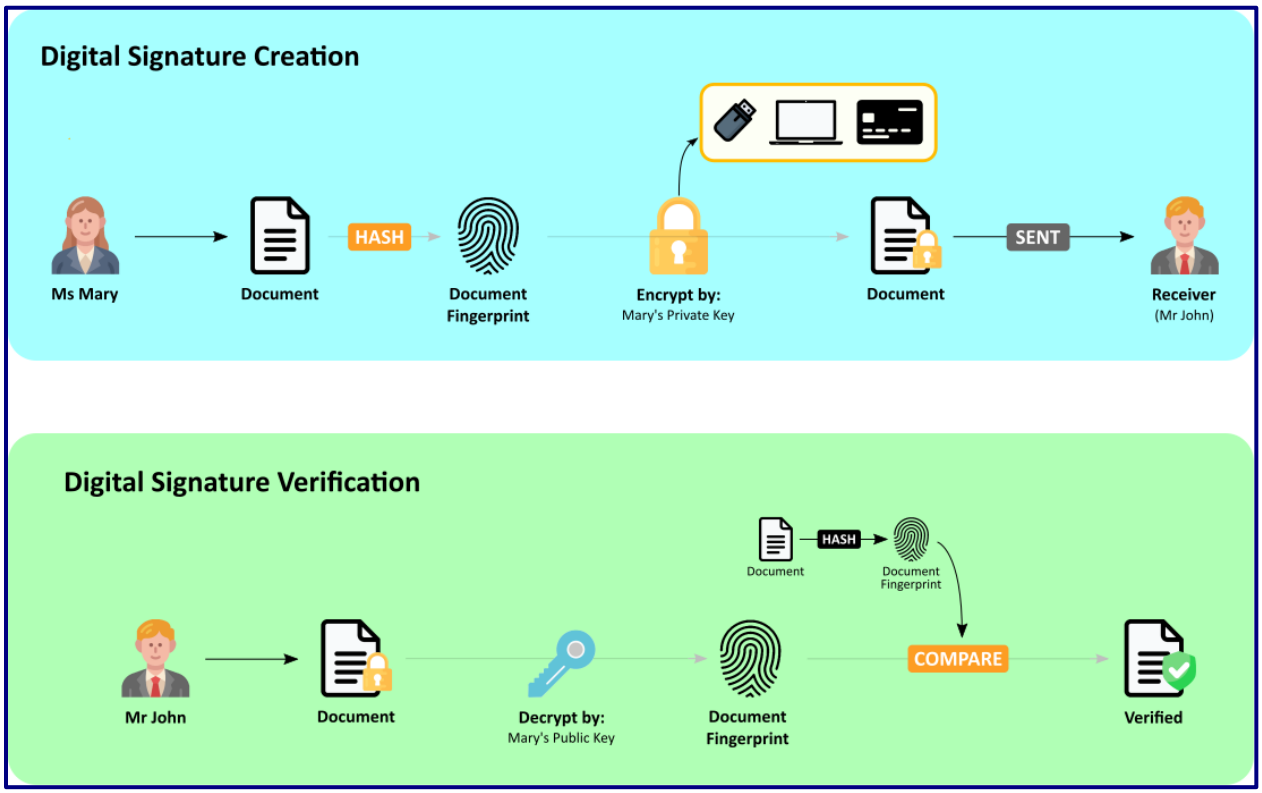
Definition

- A digital signature differs from an electronic signature as it uses an encrypted digital certificate to make the document tamper-evident which can be verified with its public key, created upon signing. The process creates an audit trail, which provides details on each step taken to sign the document. Digital signatures are based on Public Key Infrastructure (PKI) or cryptographic operations and are used to validate the authenticity and integrity of a message, software, or a digital document
- A digital signature is either issued by a Government body or a Govt. recognised institution
- A digital signature, as opposed to a traditional signature, is not a name but two "keys" or sequences of separated characters. It applies cryptographic measures to the content of a message or document to show the following to the message's recipient:
    - That the sender of the message is real (authentication)
    - That the sender cannot deny that they sent the message (non-repudiation)
    - That the message has not been altered since it was sent (integrity)
- A digital signature is legally recognised but does not possess legal status. Its purpose is not to certify the signer's intentions like an electronic signature, but just to encrypt the data of a document to give it greater security
- In some jurisdictions, a digital signature can be used for a wider range of file types, such as videos, sound, etc., making it more versatile than the traditional paper signature

What makes a digital signature different from an electronic signature?

- A digital signature is an electronic signature captured through an eSignature software using special encryption. This cryptographic operation creates a digital "fingerprint" for each document sent for signing (refer to Figure 1 – Digital Signature Creation for more details). This provides better security by ensuring the document cannot be altered. It also verifies the signees of a document by comparing the aforementioned digital "fingerprints" (refer to Figure 1 – Digital Signature Verification for more details), protecting individuals and organisations from fraud

Figure 1 – Digital Signature Creation and Verification Process



Benefits

- They provide a more secure process for gathering signatures thanks to top-level encryption
- Digital signatures can authenticate the document and signees, providing a layer of protection above a more general electronic signature
- Recipients of the document can verify the identity of the sender, detect message tampering and spoofing
- They are particularly useful in highly regulated industries, such as insurance, real estate, government, and financial services

Business use cases

- Rental Applications
- Employee Contracts
- Loan Agreements
- Non-Disclosure Agreements
- Vendor Contracts
- Government Documents

Conclusion

- Digital signatures are used to verify the authenticity of digital messages and documents to ensure their integrity. They provide enhanced security as a Government background check is performed prior to digital certificate issuance

European Standards

Three types of electronic signature

- The European eIDAS Regulation defines three types of electronic signature: "simple" electronic signature, "advanced" electronic signature, and "qualified" electronic signature
- The requirements for each type are based on the requirements for the preceding type. As such, a qualified electronic signature meets more requirements whilst a "simple" electronic signature meets less

Simple electronic signatures

- An electronic signature is defined (as per eIDAS Article 3), as "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"
- Therefore, something as simple as signing a document and sending a scanned copy using an email account, username and password, or accepting the terms and conditions of a website can constitute a simple signature
- There is a logical association between the sending account (the email address) and the signature. However, it doesn't prove who the signer really is
- That's why this electronic signature, often referred to as "simple", offers the lowest level of security

Advanced electronic signatures

An advanced electronic signature is an electronic signature which meets the following requirements:

1. Uniquely links to the signer
2. Enables identification of the signer
3. Is created in such a way as to allow the signer to retain control
4. Is linked to the signed data in such a way that any subsequent change to this data is detectable

An advanced electronic signature has a higher level of security than simple signatures.

Qualified electronic signatures

A qualified electronic signature is an advanced electronic signature which additionally:

- Is created by a qualified signature creation device
- Is based on a qualified certificate for electronic signatures

The electronic signature generated using electronic National Identity Documents and electronic signature certificates stored on encrypted cards are examples of this type of electronic signature.
Qualified certificates for electronic signatures are provided by providers (public and private) which have been granted qualified status by a national competent authority as stated in the national "trusted lists" of the EU member state.
Many providers of qualified certificates will deliver the corresponding private key on a qualified signature creation device.

Digital Signature Services

- DSS (Digital Signature Services) is an open-source software library for electronic signature creation and validation. DSS supports the creation and verification of interoperable and secure electronic signatures in line with European legislation. In particular, DSS aims to follow the eIDAS Regulation and related standards closely
- DSS can be reused in an IT solution for electronic signatures to ensure that signatures are created and verified in line with European legislation and standards. DSS allows reuse in a variety of different ways: in an applet, in a stand-alone application or in a server application. DSS can also be used as a reference implementation for IT solutions which do not directly reuse it. DSS was developed by Nowina Solutions and is maintained up to date via new releases

Brazilian Standards

Overview

In Brazil, the use of electronic and certificate-based digital signatures is evolving and their acceptance in the business community and by public entities is increasing. Recently, this process has accelerated, and more laws and provisional measures have been issued regarding the use of electronic or digital signatures, and more businesses, governmental bodies and entities have started using and accepting electronically or digitally signed documents. However, it should be emphasized that no one can be obliged to contract electronically in Brazil, and the option for a handwritten signature should always be available.

The main laws and regulations governing the use of electronic and digital signatures in Brazil include:

1. **The Brazilian Civil Code: Article 104, III of the Brazilian Civil Code**: establishes the freedom of contract forms, meaning that a legal agreement is valid if it is in a form either prescribed by law or not explicitly prohibited by law
2. **The Provisional Executive Act 2.200-2 (MP 2200)**: The Provisional Executive Act of 24th August 2001, provides for the validity of general electronic agreements signed with a digital signature

Per the Brazilian Civil Code, an electronically signed agreement must have a:

1. Capable agent
2. Licit, possible, and determined or determinable object
3. Form that is prescribed or not prohibited by law

Brazil maintains its own public key infrastructure (PKI) for digital certificates called "Infraestrutura de Chaves Públicas Brasileira" (ICP-Brasil). The authorized PKI-Brazil certifying authorities can be found here: https://estrutura.iti.gov.br/. **MP 2200 guarantees the legal validity of digitally signed documents in the following situations:**

1. Documents produced within ICP-Brasil
2. Documents produced outside ICP-Brasil if minimum parameters for evidencing the authorship and integrity are met

For documents produced outside ICP-Brasil, the validity parameters of authorship and integrity are met when: (1) proof of the signer identification is provided; and (2) proof of the integrity of the signed document is provided, subject to the acceptance of the authentication method by all parties that are signing the document.

Electronic signatures that comply with the Brazilian Civil Code and MP 2200 are considered to have the same legal effect as a handwritten signature. Additionally, digital signatures backed by ICP-Brasil are granted a legal presumption that the signature belongs to the person who signed and that the content of the electronic document remains unchanged. In contrast, electronic signatures created outside of ICP-Brasil do not carry this legal presumption and the authorship and integrity of the document might be proven.

Special considerations

Transacting with public sector entities

There are no special requirements or restrictions for using digital or electronic signatures with government entities in Brazil other than the general rules established by the Brazilian Civil Code and MP 2200. However, government entities are not obliged to accept the use of electronic or digital signatures. Additionally, each government entity may establish its own procedure for electronic or digital signature (e.g., mandatory use of an ICP-Brasil digital certificate and/or use of a specific platform to sign documents electronically). It is therefore necessary to check with each applicable government entity to determine if digital and/or electronic signatures are accepted and, if so, what procedures must be followed.

Use cases that require a traditional signature

In Brazil, certain agreements and transactions have particular formats prescribed by law. For example, "solemn contracts" or "special contracts" must be in writing and must be registered within the Registry of Deeds or other specific Registries. Some examples of solemn contracts are collaterals and real estate sales, disinheritance (which can only be made by will), as well as marriage and prenuptial agreements. Additionally, documents requiring notarization cannot be replicated electronically.

Notwithstanding the above, several formalities have been eased due to the Covid-19 pandemic. Provided that some formalities are met (which may vary and must be assessed on a case-by case basis), some types of agreements are now allowed to be signed electronically. For example:

1. Due to the recent creation of Electronic Notarial Acts System ("e-notariado"), some instruments that must be registered with the Real Estate Registry Office and/or executed through a public deed are now allowed to be signed electronically. To be considered valid, electronic notarial acts must fulfill the following requirements (i) notarial video conference to obtain the consent of the parties on the terms of the legal act; (ii) explicit agreement by the parties to the terms of the electronic notarial act; (iii) digital signature by the parties, exclusively through the "e-notariado"; (iv) signature of the Notary Public using the KPI-Brazil digital certificate; and (v) use of long-term documents formats with digital signature
2. Certain corporate-related documents may now be signed electronically. The formalities may change depending on each Brazilian state, since each Commercial Board may decide whether or not to receive and accept a document electronically or digitally signed by a third-party system or subscription portals
3. Agreements for the license (or transfer) of patents, industrial designs, trademarks, supply of technology, technical assistance and franchising are required to be registered with the INPI ("Instituto Nacional da Propriedade Industrial" which translates as "National Institute of Industrial Property"). In this case, it is important to note that the Contract Department of the INPI recently started accepting, for recording purposes, agreements executed electronically. If the agreement is signed by Brazilian parties, both parties must use a valid digital certificate issued by the Certification Authorities accredited by the KPI-Brazil. For foreign parties, however, the INPI accepts e-signatures without a digital certificate, when electronically notarized and apostilled