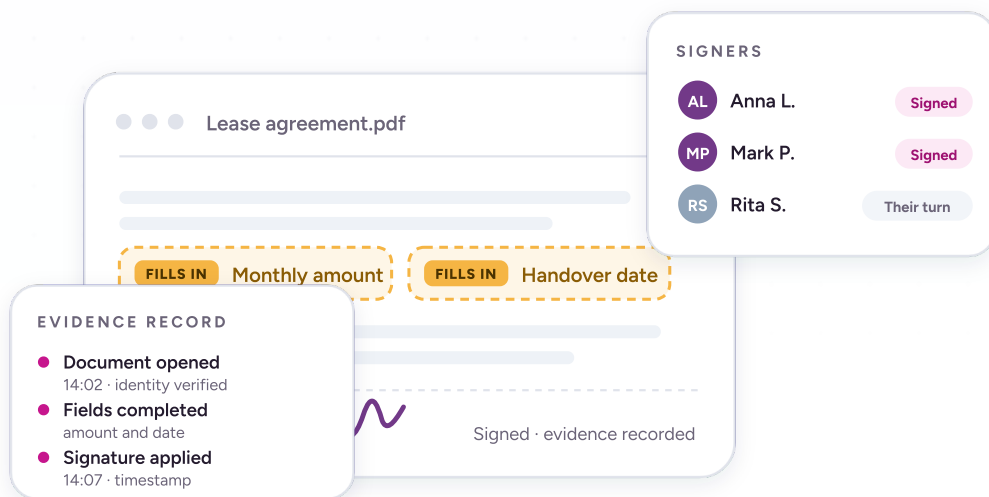


From rúbrica to digital signature.

The history, foundations, devices and legal doctrines of the electronic signature, and how the platforms emerged that now coordinate who signs, in what order and with what proof.



Rúbrica. Notebooks on signature, identity and digital trust

Volume 1. From Rúbrica to Digital Signature

First edition, October 2026.

Montevideo, Uruguay.

This book is a work of general information. It describes technical and legal principles of general scope and does not constitute legal advice. The validity of a signature in any specific case depends on the applicable law, the type of act and the available evidence; before making a decision, consult a qualified professional in the relevant jurisdiction.

References to laws, institutions and companies are made for historical and educational purposes. The trademarks mentioned belong to their respective owners.

Set in Figtree and JetBrains Mono, both under the SIL Open Font License.

RÚBRICA · VOLUME 1

From Rúbrica to Digital Signature

An introduction to the world of the electronic signature: where it comes from, how it works and where it is heading.

Contents

	Preface	5
01	What it means to sign	7
02	A brief history	11
03	The vocabulary	17
04	How it works inside	23
05	Signature devices	29
06	The doctrines	35
07	Uses and sectors	41
08	Advantages and limits	45
09	From document to process	49
10	Anatomy of a platform	55
11	What lies ahead	61
	Glossary	65
	Further reading	69

BEFORE WE BEGIN

Why this series

Signing is one of the oldest and most meaningful gestures we know. This book tells how that gesture became mathematics, law and infrastructure without losing its purpose.

Every day, millions of documents are signed without paper. A loan is approved from a phone, an employment contract is accepted during a lunch break, the minutes of a board meeting are closed with signatories spread across three countries. For the person signing, the experience usually comes down to a button. Behind that button, however, lie five decades of cryptography, three decades of legislation and an entire industry devoted to ensuring that a signature is worth as much today as it will be twenty years from now.

That industry has its own vocabulary, which confuses even those who work in it. People speak of electronic signatures and digital signatures as if they were the same thing, and they are not. They speak of advanced electronic signatures, qualified electronic signatures, timestamps, trust service providers and long term validation. Legal concepts are mixed with technical ones, and product concepts with both. As a result, many important decisions, such as what type of signature to require for a given act or how to preserve the proof that someone signed, are made without a clear map.

This series aims to provide that map. It is written for curious readers with no prior training in cryptography or law: process owners, lawyers who want to understand the technology, engineers who want to understand the law, students, and teams who must choose, deploy or operate a signature solution. When a concept demands precision, we explain it precisely; when an explanation would call for formulas, we prefer an image.

How the series is organized

The series consists of three volumes that can be read independently, although each supports the others.

- ✓ **Volume 1. From Rúbrica to Digital Signature.** The one you are holding. It traces the history of the signature, the basic vocabulary, how the digital signature works, the devices that store the keys, the legal doctrines that recognize it, its uses, its advantages and its limits, and the emergence of the platforms that coordinate signing processes.
- ✓ **Volume 2. The Proof That Endures.** It deals with what happens after signing: signature formats and levels, timestamps, validation, trusted lists, long term preservation and evidence records.
- ✓ **Volume 3. Orchestrating the Signature.** It covers the design of signing processes, the identity of the signer, integration with other systems and the operation of these platforms at scale, with a look at artificial intelligence and the cryptography of the future.

A caveat and a promise

The caveat: this is neither a law book nor a compliance manual. Laws change, and every jurisdiction has its nuances. We cite legislation to explain ideas, not to give advice on a specific case.

The promise: by the end of this volume, readers will be able to distinguish the types of signature, understand what happens when someone signs an electronic document, and know which questions to ask about a signature solution and why those questions matter. If they also find in the history of the signature some of the fascination that led us to write about it, so much the better.

ABOUT THE NAME

In Spanish, *rúbrica* is the word for the personal flourish that accompanies a handwritten signature and makes it hard to imitate. It comes from the Latin *rubrica*, the red earth used to write the titles of laws in red ink; over time the word came to name that distinctive stroke of the pen. It seemed a fitting name for a series about how that personal stroke found its equivalent in the digital world.

What it means to sign.

Before talking about keys and certificates, it is worth pausing on a simple question: what exactly does a signature do? The answer explains almost everything that follows.

A signature is not a drawing. It is an act. When someone writes their name at the foot of a contract, they are not decorating the paper: they are stating, before others and before themselves, that the text binds them. The ink is the medium; the commitment is what matters.

This distinction between the medium and the act is the key that allowed the law, at the end of the twentieth century, to accept signatures that use no ink. If a signature is valuable for what it does rather than for how it looks, any mechanism that does the same thing can, in principle, carry the same value. Legal scholars call this idea *functional equivalence*, and we will return to it in chapter six. To understand it, we must first pin down what those functions are.

The five functions of a signature

Legal scholarship and the international bodies that have studied the subject, in particular the United Nations Commission on International Trade Law (UNCITRAL), agree that a signature performs several functions at once. We group them into five.

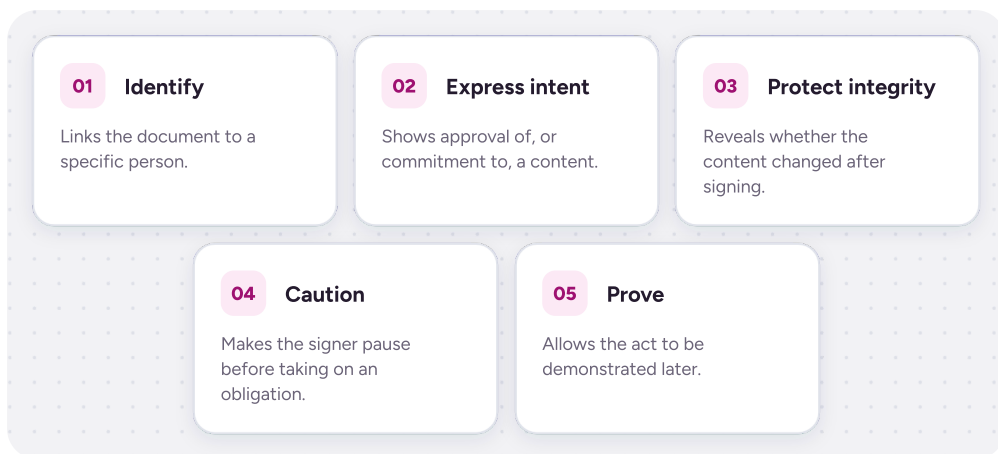


FIGURE 1 The five functions of a signature. Any mechanism, on paper or electronic, can be assessed by how well it fulfills each one.

Identifying the signer

A signature links the document to a specific person. On paper that link is indirect: a handwritten signature does not say who its author is; it only allows comparison with other known signatures of that person. In the electronic world, identification can be much stronger, because it can rely on a verified identity document, on a certificate issued by a trusted entity or on a combination of factors.

Expressing intent

To sign means to approve, accept, acknowledge or commit. A signature is the expression of intent regarding a specific content. That is why it matters so much that signers know what they are signing, that they have been able to read it and that the act of signing is deliberate rather than accidental. A button labeled “Accept” in small print does not express the same intent as a screen that displays the full document and asks for explicit confirmation.

Protecting the integrity of the content

A signature at the foot of the last page does not prevent someone from changing the second. On paper, that weakness is offset with initials on every sheet, wax seals, watermarked paper or the involvement of a notary. The digital signature, as we will see, solves this at the root: any change to the document, even a single comma, is detected.

Giving the act solemnity

The gesture of signing forces us to pause. That pause has legal and psychological value: it warns signers that they are about to take on an obligation. Some especially serious acts, such as a will or, in many jurisdictions, the sale of real estate, require additional formalities precisely to reinforce that warning.

Providing evidence

Finally, a signature serves to show afterwards that the act took place. This is perhaps the function that technology has changed the most. A handwritten signature proves little on its own: in a dispute, a handwriting expert is needed. A well constructed electronic signature can come with a detailed record of who accessed the document, when, from where, how they were identified and which exact version they signed.

KEY POINT

A signature **identifies, expresses intent, protects integrity, warns** and **proves**. Any signing mechanism, on paper or electronic, can be assessed by asking how well it performs each of these five functions.

Signing is not the same as authenticating

A common misconception is that logging in to a system is equivalent to signing. It is not. Authenticating means proving who I am in order to gain access; signing means committing myself to a content. I can authenticate to my bank a hundred times a month without signing anything, and I can sign a document sent to me without having an account in any system.

The difference matters because many processes combine the two. A system may ask the signer to authenticate with a code sent to their phone and then record their consent with a click. In that case, authentication provides identification, the click provides intent, and the system must take care of providing integrity and evidence. When any of these pieces is missing, the resulting signature is weaker, even if the screen looks the same.

Signing is not the same as sealing

On paper, organizations use seals: the seal of a government office, a company stamp, the date stamp of a reception desk. A seal does not express the intent of a person; rather, it attests that a document comes from an organization or that it was received at a certain moment.

The electronic world preserves that distinction. There is the *electronic signature*, which belongs to a natural person, and there is the *organization seal* (the “electronic seal” of the European regulation), which belongs to a legal person and guarantees the origin and integrity of a document it issues. There is also the *timestamp*, which identifies no one and only proves that a document existed at a given moment. All three use similar techniques and serve different functions. We will encounter them throughout the series.

Why the signature had to be reinvented

For centuries, the combination of paper, ink and witnesses was enough. Documents traveled physically, the parties usually knew each other and disputes were settled with experts and testimony. Three changes upset that balance.

- 1 **Distance.** Remote commerce, first by mail, then by telegraph and fax, and finally over networks, separated the parties. Signing on paper and sending the original became slow and expensive.
- 2 **Volume.** Banks, insurers, public administrations and employers came to handle millions of documents. Every paper signature means printing, sending, receiving, scanning and filing.
- 3 **Dematerialization.** When documents are created, used and archived in electronic form, printing them just to sign them makes no sense. And a scanned signature pasted into a PDF performs almost none of the five functions: it can be copied with two clicks.

The electronic signature was born to solve those three problems without giving up the five functions. How it did so, and how hard it was for technology and law to reach agreement, is the subject of the chapters that follow.

From clay to algorithm.

A brief history of the signature: five thousand years of seals, pen strokes and witnesses, and fifty years in which mathematics found a way to replace them.

Seals before names

Long before most people could write, there was already a need to mark an object or an agreement as one's own. In Mesopotamia in the fourth millennium BCE, people used carved stone cylinder seals that, when rolled over damp clay, left a unique image. These seals closed containers, authenticated tablets bearing contracts and accompanied their owners to the grave. The essential idea was already there: a mark that was hard to reproduce, associated with a person and applied to the medium of the agreement.

The Egyptians, Greeks and Romans inherited and refined the practice. In Rome the signet ring became widespread, used to impress a personal emblem into wax to close letters and documents. A broken seal was visible proof that someone had opened the message. Integrity and authorship, two of the five functions, were achieved with an object that fit on a finger.

The handwritten signature and the *rúbrica*

Signing with one's own written name became common much later, as literacy spread. In medieval Europe several forms coexisted: the wax seal of nobles and bishops; the cross drawn by those who could not write, often accompanied by witnesses; and the notarial sign, an elaborate personal design that each scribe registered upon taking office and had to reproduce on every document he authorized.

From that tradition comes the *rúbrica* of the Spanish speaking world: a personal flourish, sometimes more important than the name itself, that makes a signature hard to imitate. The word preserves the memory of its origin. The titles of laws and the chapter headings of legal books were written in red ink, *rubrica* in Latin, and the term came to mean first the heading and later the distinctive mark added to a signature.

With the printing press and the growth of trade, the handwritten signature became the dominant mechanism. Some laws made it mandatory for certain acts. The English Statute of Frauds of 1677, for example, required certain contracts to be in writing and signed in order to be enforceable in court. Many later legal systems followed a similar path and reinforced the pairing of written document and handwritten signature as the evidence par excellence.

The telegraph tests the law

The first major challenge came in the nineteenth century with the telegraph. If a merchant accepted an offer by telegram, had he signed? The message arrived written by an unknown operator, hundreds of miles from its author. Courts in several countries had to answer the question. One of the most frequently cited lines of reasoning is that of a New Hampshire court in 1869, which held, in substance, that it made no difference whether the operator wrote the acceptance with a steel pen an inch long or with a copper wire a thousand miles long. What mattered was the author's intent, not the instrument.

That argument contains the seed of the functional equivalence that the law would adopt more than a century later. The same happened with telex and with fax: each new technology forced judges to ask whether the mechanism performed the functions of a signature, and each time the answer depended more on the available evidence than on the form.

The public key revolution

The underlying problem remained unsolved. A telegram or a fax could be forged with relative ease, and nothing in it allowed an alteration to be detected. What was needed was a mechanism that would verifiably link a content to its author. The answer came from cryptography.

In 1976, the researchers Whitfield Diffie and Martin Hellman published a paper titled *New Directions in Cryptography* that transformed the discipline. They proposed the idea of public key cryptography: a system in which each person has two related keys, a private one kept secret and a public one that can be shared with anyone. Among the applications they envisioned was precisely the one that concerns us: a signature that only the holder of the private key could produce and that anyone could verify with the public key.

The following year, Ron Rivest, Adi Shamir and Leonard Adleman, of the Massachusetts Institute of Technology, presented the RSA algorithm, which made that idea practical. Years later it emerged that researchers at the British intelligence agency had reached similar conclusions in the early 1970s, but their work remained secret until 1997. The digital signature as we know it was born in those years.

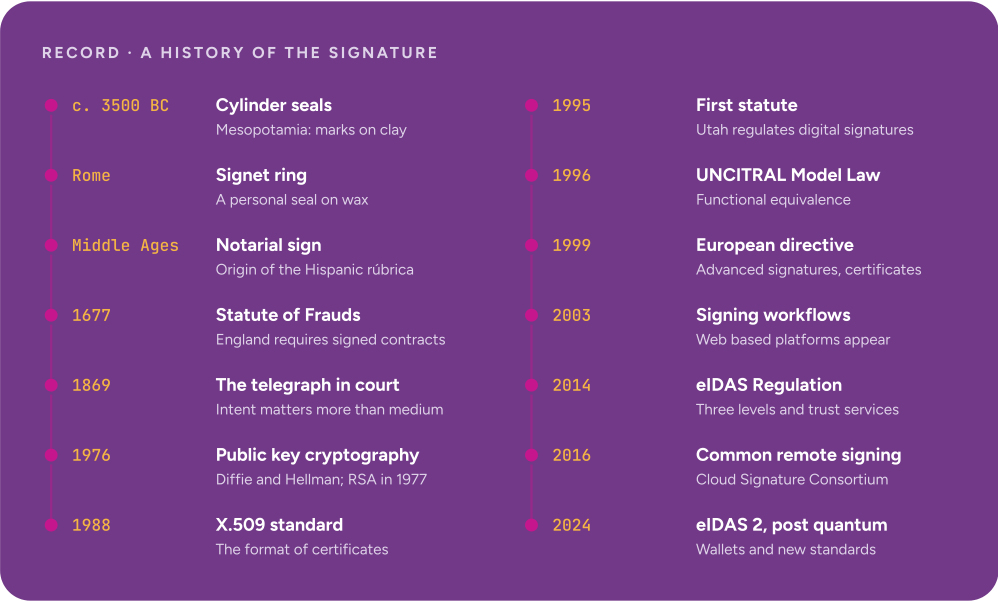


FIGURE 2 Some milestones in the history of the signature, presented in the style of an evidence record.

From idea to infrastructure

A digital signature solves the link between a content and a key. But how can we know to whom a public key belongs? If an impostor generates a key pair and presents it as belonging to someone else, the mathematics will not detect it. A reliable way to associate keys with identities was needed.

The solution was the *digital certificate*: an electronic document, signed by a trusted entity called a certification authority, which states that a certain public key belongs to a certain person. In 1988 the International Telecommunication Union published the X.509 standard, which defines the format of these certificates and, through successive revisions, remains the foundation of the global public key infrastructure. Every time a browser shows a padlock next to a web address, it is using X.509 certificates.

During the 1990s the missing pieces fell into place: standardized signature algorithms, increasingly robust cryptographic hash functions, protocols for checking whether a certificate had been revoked and, toward the end of the decade, timestamps issued by trusted third parties. The first formats for signing office documents also appeared. Around the year 2000, the PDF format incorporated digital signatures embedded in the file itself, which made it possible to view, print and verify a signed document with an ordinary reader.

The laws arrive

The technology was ready before the law. The first specific digital signature law was enacted by the state of Utah, in the United States, in 1995. It was a highly detailed law that regulated the certification infrastructure almost like a technical regulation. Laws followed in Germany and Italy in 1997, also with a markedly technological approach.

In 1996 UNCITRAL adopted its Model Law on Electronic Commerce, and in 2001 a specific Model Law on Electronic Signatures. Their contribution was conceptual: rather than prescribing a technology, they set out general principles, such as functional equivalence and technology neutrality, that any country could adopt. These model laws inspired much of the legislation in Latin America.

In 1999 the European Union adopted a directive on electronic signatures that introduced the distinction between the electronic signature and the advanced electronic signature, as well as the notion of qualified certificates. In the United States, the federal law known as E-SIGN, enacted in 2000, took a minimal approach: it declared that a signature or a contract may not be denied validity solely because it is electronic, without requiring any particular technology.

In Latin America the movement was swift. Colombia legislated in 1999, Argentina and Brazil in 2001, Chile in 2002. Uruguay passed its law on electronic documents and electronic signatures in 2009, which also created the public body responsible for

accrediting certification service providers. Paraguay did so in 2010 and modernized its regime in 2021. Each country chose its own combination of approaches, and that diversity is one of the challenges we will examine in chapter six.

From directive to regulation, and from regulation to wallet

The European experience showed that a directive, which each country transposes in its own way, led to fragmentation: a signature valid in one Member State could struggle to be recognized in another. In 2014 the European Union adopted Regulation 910/2014, known as eIDAS, which has applied uniformly in all Member States since 2016. eIDAS consolidated three levels of signature, created the organization seal for legal persons (the “electronic seal” in its text), regulated trust services and established official trusted lists of qualified providers.

Its reform, Regulation 2024/1183, often called eIDAS 2, was adopted in 2024. Its main innovation is the European Digital Identity Wallet: an application that every citizen will be able to carry on their phone to identify themselves, present credentials and sign at the qualified level. Member States must offer at least one such wallet by the end of 2026. It is a fundamental change in the way we sign.

From document to process

While legislators debated, the market discovered another need. Signing a document was possible; coordinating several people who had to sign it, in a certain order, with reminders and with a record of everything that happened, was another matter. In the early 2000s, companies emerged that were devoted to exactly that: sending a document to one or more signers by email, guiding them to sign in the right place and returning the signed document to the sender together with a certificate of what had taken place. That is how signing workflow platforms were born, the subject of chapter nine.

Every communication technology forced us to ask again what a signature is. The answer was always the same: what matters is intent and evidence, not the instrument.

Electronic, digital, advanced.

The words of the signature are used loosely and rarely mean the same thing to a lawyer, an engineer and a salesperson. This chapter establishes a common vocabulary.

Few fields of knowledge have so many similar terms with different meanings. Electronic signature, digital signature, advanced electronic signature, qualified electronic signature, recognized signature, recognized certificate, qualified certificate. Some differences are substantive; others are merely a matter of translation or country. Telling them apart is the first step toward avoiding wrong decisions.

Electronic signature: the broad legal concept

Electronic signature is the most general term. In most legislation it refers to any data in electronic form that is attached to or associated with other electronic data and that a person uses to sign. The definition is deliberately broad. It covers a name typed at the end of an email, an image of a handwritten signature pasted into a document, a ticked box that reads "I agree", a stroke drawn with a finger on a screen, a code received by text message and, of course, a cryptographic signature backed by a certificate.

That all of these forms are electronic signatures does not mean they all carry the same weight. It means that none of them can be dismissed solely because it is electronic. Its weight as evidence will depend on how well it performs the five functions described in chapter one, and that is something a judge will assess if a dispute arises.

Digital signature: the technical concept

Digital signature, strictly speaking, refers to a technique: the signature based on public key cryptography that we will describe in chapter four. It is a mathematical mechanism that links a content to a private key and makes it possible to detect any alteration.

The confusion arises because some countries use “digital signature” as a legal category. Under Argentine law, for example, a digital signature is one that meets certain technical requirements and relies on a certificate issued by a licensed certifier, and it enjoys presumptions that an ordinary electronic signature does not. In other countries the expression does not appear in the law and is used only in technical language. It is therefore advisable always to ask in which sense the term is being used.

A NOTE ON TRANSLATION

The Spanish version of the European regulation uses the term **cualificada**; much of Latin America says **calificada** or **reconocida**; English says **qualified**. They are the same idea in different dress. What is not the same is “digital” as a technique and “digital” as a legal category.

The three levels

The model that has spread most widely around the world, consolidated by the European eIDAS regulation, distinguishes three levels of electronic signature, each including the previous one and adding requirements. Brazil adopted the same three levels; Uruguay, Paraguay and other countries adopted variants with two, an ordinary signature and a higher level one based on a certificate from an accredited provider.

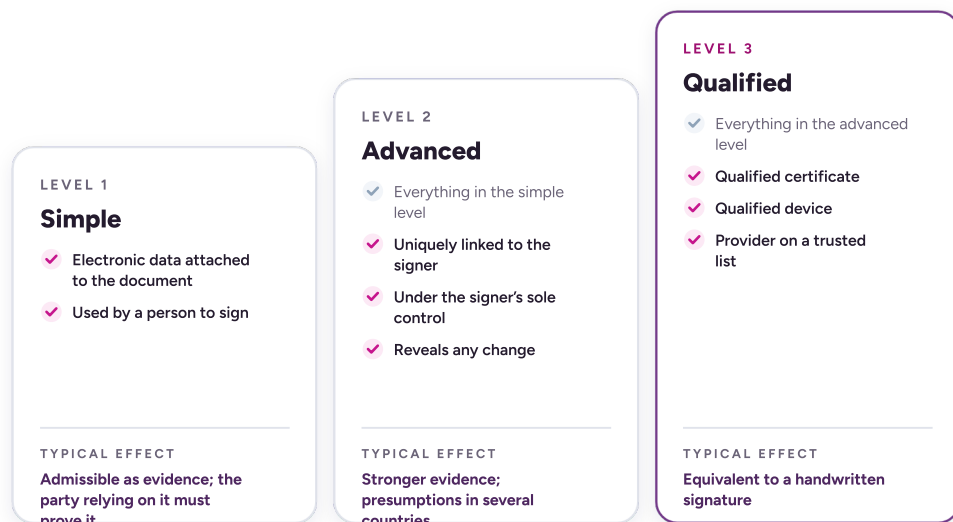


FIGURE 3 The three levels of electronic signature in the European model, adopted with variations elsewhere. Each level includes the requirements of the one before; what it adds is shown in color.

Simple electronic signature

This is the basic category. It imposes no particular technical requirements. Its advantage is ease of use: anyone can sign without devices or certificates. Its weakness lies in evidence: if the signature is challenged, the party relying on it must show that it was indeed made by the named person and that the document has not changed. For many everyday acts, such as accepting a quote, approving a purchase order or confirming a booking, this level is sufficient, especially when accompanied by a good evidence record.

Advanced electronic signature

Article 26 of the eIDAS regulation sets four conditions for it, which deserve careful reading because they recur, in similar words, in many laws:

- 1 it is uniquely linked to the signatory;
- 2 it is capable of identifying the signatory;
- 3 it is created using signature creation data that the signatory can, with a high level of confidence, use under their sole control;

- 4 it is linked to the signed data in such a way that any subsequent change is detectable.

In practice, only cryptography meets the fourth condition. The third is the most debated: what does “sole control” mean when the key is not in an object the signer holds in their hand but on a remote server? We will return to this in chapter five.

Qualified electronic signature

This is an advanced electronic signature that is, in addition, created with a qualified signature creation device and based on a qualified certificate issued by a trust service provider that has been assessed and appears on an official list. Its legal effect is the strongest: in the European Union, Article 25 of eIDAS gives it an effect equivalent to that of a handwritten signature, and a qualified electronic signature issued in one Member State must be recognized in all the others.

In several Latin American countries the top category goes by other names, such as digital signature, advanced electronic signature with a recognized certificate or qualified signature, and the requirements vary in their details. The logic is the same: a certificate issued by a provider accredited by a public authority, a key protected by an assessed device and an enhanced legal effect, often expressed as a presumption of authorship and integrity.

The other pieces of the vocabulary

TERM	WHAT IT IS
Digital certificate	An electronic document, signed by a certification authority, that links a public key to the identity of its holder for a period of validity.
Certification authority	An entity that verifies identities and issues certificates. When it is accredited or supervised by a public body, it is usually called a certification service provider or trust service provider.
Trust service provider	A term from the European regulation, now adopted in other regions, for an entity that provides services such as issuing certificates, timestamps, validation or preservation of signatures. If it meets enhanced requirements and appears on the official list, it is <i>qualified</i> .
“Electronic seal” (organization seal)	The equivalent of a signature for a legal person. It guarantees the origin and integrity of a document issued by an organization, without expressing the intent of a natural person.
Timestamp	Proof, issued by a trusted third party, that a piece of data existed at a given moment. It identifies no one; it establishes a verifiable date and time.
Validation	The process of checking that a signature is authentic, that the document has not changed and that the certificate was valid at the time of signing.
Trusted list	An official list, published and signed by an authority, of the supervised trust service providers and the services they provide.

A rule of thumb

For any process that requires a signature, it is worth asking three questions, in this order. First, what does the law require for this act? Some acts accept any electronic signature, others require the highest level and still others require paper or the involvement of a notary. Second, what is the risk of a dispute? A high value contract, or

one with a party who might deny having signed, justifies a higher level than an internal authorization. Third, what experience can the signer tolerate? Requiring a physical device from an occasional customer may mean the process is never completed.

The answer is almost never “always the highest level”. It is the right level for each act, combined with the best possible evidence. Modern platforms, as we will see, make it possible to combine levels within a single process: an internal approver with a simple electronic signature, a customer with an advanced electronic signature and an authorized representative with a qualified electronic signature, all on the same document.

How it works inside.

The digital signature rests on three ideas: a hash that changes with any alteration, a pair of keys that only work together, and a certificate that states who they belong to. No formulas are needed to understand them.

First idea: the document's fingerprint

A *cryptographic hash function* takes content of any size, whether a single sentence or a two hundred page contract, and produces a short string of fixed length. That string works as a fingerprint of the content. The functions used in signatures today, such as SHA256, have three properties that make them useful.

- ✓ **They are deterministic.** The same content always produces the same hash.
- ✓ **They are sensitive to the smallest change.** Altering a single character produces a completely different hash, bearing no resemblance to the previous one.
- ✓ **They are one way.** The content cannot be reconstructed from the hash, and it is practically impossible to find two different contents with the same hash.

The following example shows the second property. The two sentences differ by a single zero.

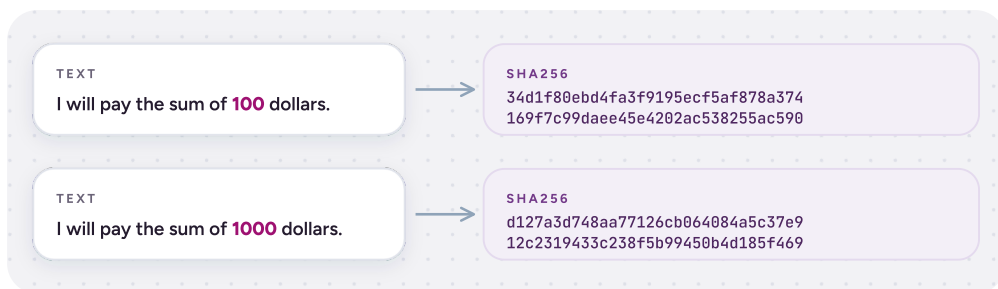


FIGURE 4 A single character of difference produces hashes with no resemblance at all. The values are real and can be recomputed with any SHA256 tool.

The consequence is powerful: to know whether a document has changed, there is no need to compare it word by word with the original. It is enough to compare their hashes.

Second idea: two keys that complement each other

Public key cryptography uses pairs of mathematically related keys. What one key does, only the other can verify. The private key remains in the sole possession of its holder and is never shared. The public key can be published without risk, because the private key cannot be derived from it in any reasonable amount of time.

Signing a document consists, in simplified terms, of two steps. First, the hash of the document is calculated. Then an operation that only the holder of the private key can perform is applied to that hash. The result is the signature: a block of data attached to the document.

Verifying the signature also involves two steps. The recipient of the document independently calculates the hash of the content in front of them. They then use the signer's public key to check that the signature corresponds exactly to that hash. If the document has changed, even by a single comma, the hashes do not match and verification fails. If the signature was made with a different private key, it fails as well.

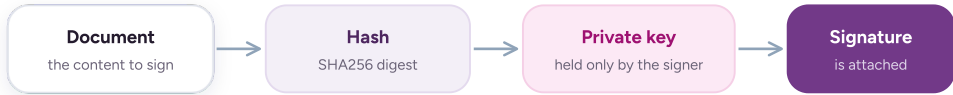
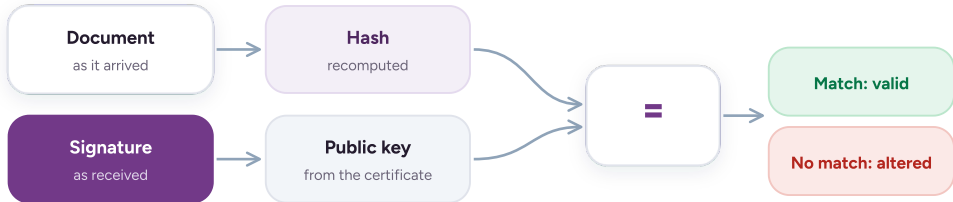
SIGN**VERIFY**

FIGURE 5 Signing and verifying. The signer applies the private key to the hash; the verifier recomputes the hash and checks it using the public key.

A TECHNICAL NUANCE

The signature is often explained as “encrypting the hash with the private key.” The image is useful and fits the RSA algorithm reasonably well, but it does not accurately describe other widely used algorithms, such as those based on elliptic curves, which produce the signature by a different route. What they all share is the outcome: only the private key produces the signature, and anyone with the public key can verify it.

Third idea: the certificate

Mathematics guarantees that a signature was produced by a certain private key. It does not say whose key that is. That is the purpose of the digital certificate, which is essentially a statement signed by a certification authority: “this public key belongs to this person, and this statement is valid between such and such dates.”

Among other data, a certificate contains the holder’s name and often an identifier such as their identity document number, the public key, the name of the issuing authority, the validity dates, the permitted uses of the key, and the addresses where one can

check whether it has been revoked. All of this is signed by the authority, so that no one can alter the certificate without it being noticed.

The chain of trust

And why trust the authority? Because its own certificate was signed by a higher level authority, and so on up to a *root*: a certificate that signs itself and is trusted by explicit decision. That decision is made by an operating system, a browser, a PDF reader or, in the case of signatures with legal effect, a public body that publishes the list of recognized authorities.

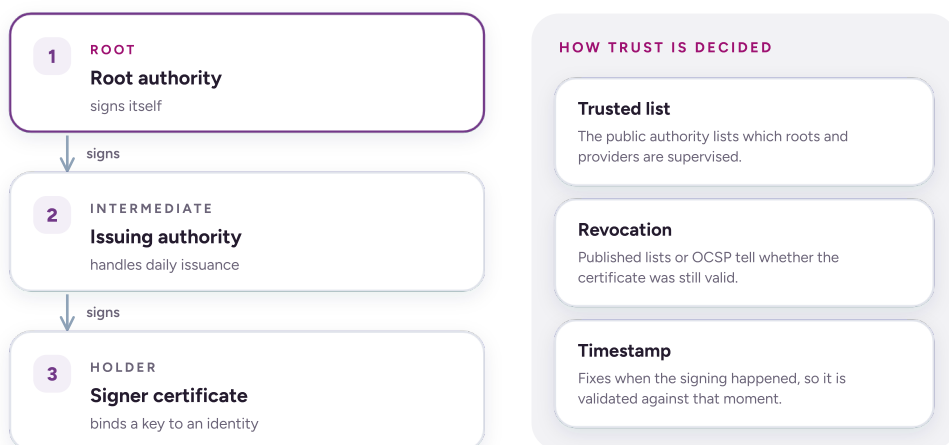


FIGURE 6 The chain of trust. Each certificate is signed by the one above it; the root is accepted by explicit decision, often because it appears on a trusted list.

When a certificate ceases to be valid

A certificate can lose its validity before its expiration date. The holder may have lost their card, the key may have been compromised, or the holder's data may have changed. In such cases the authority revokes the certificate and announces it through two main channels: certificate revocation lists published periodically, and an online query service, the OCSP protocol, which answers in real time whether a specific certificate is valid.

For anyone validating a signature, the relevant question is not whether the certificate is valid today, but whether it was valid at the moment of signing. Answering that question years later requires having kept the revocation information from that time and knowing

with certainty when the signature was made. Hence the importance of the fourth piece.

Fourth piece: time

The time shown on the signer's computer clock proves nothing: anyone can change it. To fix the moment of a signature in a verifiable way, one turns to a *time stamping authority*, a trusted third party that receives the hash of a document or a signature, adds the date and time from a reliable clock, and signs the whole. The most widespread protocol for this was defined in 2001 in RFC 3161, a document of the body that standardizes internet protocols.

A timestamp makes it possible to assert that the signature existed before a certain instant. Combined with the revocation information from that instant, it makes it possible to show years later that the certificate was valid when the signature was made, even if it subsequently expired or was revoked. The long term signature formats we will study in volume two are built on this combination.

Algorithms age

The security of the digital signature depends on certain mathematical problems being very hard to solve with the available computing power. That power grows, and researchers find shortcuts. That is why algorithms have a useful life.

History offers clear examples. The MD5 hash function, widely used in the 1990s, was discredited when it was shown that collisions could be manufactured, and in 2008 a group of researchers exploited it to create a forged authority certificate that browsers would have accepted. SHA1, its successor, fell in 2017, when the first practical collision was published. RSA keys of 1024 bits, common twenty years ago, are now considered insufficient, and keys of 2048 bits or more are used instead.

This aging has a practical consequence that is often overlooked: a signature made today with secure algorithms may become doubtful fifteen years from now. Documents that must retain their value for decades need mechanisms to renew their protection periodically. The most visible horizon of this problem is quantum computing, which threatens current public key algorithms and has already prompted the publication of new standards. We address it in chapter eleven and in greater detail in volume three.

KEY POINTS

The **hash** detects any change. The **key pair** links the signature to whoever holds the private key. The **certificate** links the key to an identity. The **timestamp** fixes when it happened. Together, the four pieces fulfill the functions of identification, integrity and proof that the handwritten signature only partly achieved.

Where the key lives.

All the security of the digital signature depends on a secret: the private key. Where that secret is kept, and who can use it, is the question that gave rise to an entire family of devices.

If someone copies a private key, they can sign on behalf of its holder without leaving a trace. That is why the most important question in any signature scheme is not which algorithm it uses, but where the key is generated, where it is stored, and what is needed to use it. Over thirty years the industry has given very different answers to that question, and each one strikes a different balance between security, cost and convenience.

The key in a file

The simplest solution is to store the private key in a password protected file, usually in a standard format called PKCS #12, with extensions such as .p12 or .pfx. It is easy to distribute and install, and many organizations used it for years.

Its weakness is obvious: a file can be copied. If someone obtains the file and guesses or steals the password, they have the key. Moreover, the holder cannot know whether their key has been copied. For this reason most legal frameworks do not accept file based keys for the higher signature levels, and good practice reserves them for low risk uses or for platform seals protected by other means.

The smart card

The classic answer to the copying problem is a chip. A smart card contains a small processor capable of generating the private key internally and performing the signing operation without the key ever leaving the chip. The computer sends it the hash of the document, the card asks for a PIN and returns the signature. The key cannot be exported: if the card is lost, the key is lost, and the certificate is revoked.

Smart cards were born in the 1970s and spread first in telephony and banking. Their use for signatures grew with electronic national identity documents. Estonia, starting in 2002, was one of the first countries to provide its entire population with an identity card carrying authentication and signature certificates, and it is today the reference case. Belgium, Spain, Portugal, Germany and many others followed the same path. In Latin America, Uruguay added a chip with certificates to its national identity card in 2015, and other countries are moving in the same direction.

The price of that security is friction. Signing requires a reader, a driver installed on the computer and, often, an intermediate component that connects the browser to the reader. Every operating system or browser update can break that chain. For a user who signs once a year, the learning cost usually outweighs the benefit.

The USB token

The USB cryptographic token is essentially a smart card and its reader in a single object. It became popular among professionals who sign frequently, such as accountants, notaries, customs brokers and public officials. It offers the same protection as the card with fewer parts, although it shares the card's dependence on drivers and intermediate components.

The hardware security module

At the other end of the scale is the HSM, or hardware security module. It is a dedicated device, the size of a server or of a card inserted into one, designed to generate, store and use cryptographic keys with very demanding physical and logical protections. An HSM detects attempts to open it and can erase its keys if someone tries to tamper with it. It is certified under standards such as FIPS 140, from the United States government, or under protection profiles of the international Common Criteria scheme.

HSMs protect the keys of certification authorities, those of timestamping services and those of organization seals. And for the past decade they have also protected the keys of individuals, in what is known as remote signing.

Remote or cloud signing

Remote signing inverts the model. Instead of each person having a device, the trust service provider keeps the keys of many people in its own HSM, and each holder activates their key remotely, authenticating with a second factor such as a code on their phone or an app. The key never leaves the HSM and is used only when its holder authorizes it.

The 2014 eIDAS Regulation expressly recognized that a qualified electronic signature can be created in this way, provided the provider manages the device on behalf of the signatory with equivalent guarantees. European technical standards then defined the requirements for the components that activate remote signing and for the modules that execute it, and distinguished levels according to how much control the signatory retains.

To connect applications with remote signing services from different providers, the Cloud Signature Consortium was formed in 2016 and published a common application programming interface. Thanks to it, an application can ask any compatible provider to sign a hash on behalf of a user, following a single protocol, without custom integrations for each one. This interoperability is one of the factors that contributed most to freeing higher level signatures from dependence on a physical object.

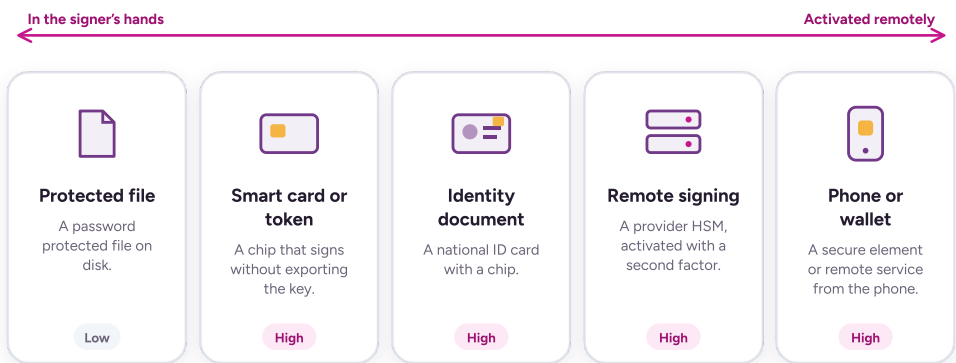


FIGURE 7 Where the private key lives. From left to right, the key moves from the signer's hands to a service the signer activates remotely.

The phone as a signature device

Modern phones include protected hardware zones, such as secure enclaves or dedicated security chips, capable of storing keys that cannot be extracted. Some countries and carriers have also used the SIM card to host certificates. Estonia launched a SIM based mobile identity scheme in 2007 and, years later, an app based one, and both are used on a massive scale for identification and signing.

The European Digital Identity Wallet provided for in the 2024 regulation follows this line: a phone app that, supported by a secure element or a remote service, will allow any citizen to sign at the qualified level free of charge for non professional purposes. If that goal is met, higher level signatures will cease to be a specialists' procedure and will become as common as paying with a phone.

What “sole control” means

All these options attempt to meet the same legal requirement we saw in chapter three: that the key be under the sole control of the signatory. With a card in hand, the answer seems obvious. With a key on someone else's server, control is exercised differently: through authentication of the holder each time they wish to sign, and through technical guarantees and audits ensuring that not even the provider itself can use the key without that authorization.

The debate over which model offers more real control remains open. A card can be lent together with its PIN; a well designed remote service can require strong authentication that is hard to delegate. What experience shows is that security depends not only on where the key is located, but on the entire process surrounding its use.

DEVICE	WHERE THE KEY IS	STRENGTH	FRICTION
Protected file	On the user's disk	Low: it can be copied	Very low
Card or token	On a chip held by the user	High: it cannot be exported	High: reader and drivers
Identity document with chip	On the national identity card or document	High, and already in the citizen's hands	Medium or high, depending on the country
Remote signing	In the provider's HSM	High if activation is strong	Low: a phone is enough
Phone or wallet	In the phone's secure element or in a remote service	High	Very low once set up

For anyone designing a signing process, the conclusion is clear: it is rarely advisable to tie oneself to a single device. The signatories of the same document may have different tools, and a good platform should be able to accept each of them with their own.

How the law learned to trust.

The technology was ready before the law. This chapter surveys the principles by which legislators recognized the electronic signature and the models that emerged from combining them.

When the digital signature became available, the law faced a dilemma. If it required a specific technology, it risked becoming obsolete within a few years and excluding valid alternatives. If it required nothing, it left judges and citizens without criteria for knowing which signatures were reliable. The answers given to that dilemma rest on a handful of principles that are now common ground.

Functional equivalence

This is the founding principle. Clearly formulated by UNCITRAL in its model laws, it holds that an electronic mechanism satisfies a legal signature requirement if it performs the same functions that the handwritten signature performs in that context: identifying the person and indicating their approval of the content, using a method as reliable as is appropriate for the purpose of the document.

Functional equivalence does not say that every electronic signature is equivalent to a handwritten one. It says that the right question is not “is there ink?” but “are the functions fulfilled?” It is the same question that the New Hampshire court asked itself when faced with the telegraph, turned into a rule.

Technology neutrality

The law should neither favor nor exclude any particular technology. It should describe requirements and outcomes, not algorithms or devices. This principle protects legislation from technical obsolescence and prevents a rule from becoming a market barrier in favor of a single supplier.

Neutrality has practical limits. When the law requires that any subsequent modification be detectable, it is in effect requiring cryptography. And the higher signature levels rely on detailed technical standards that, without naming products, do define very precise requirements. Neutrality is maintained in the text of the law and made concrete in the accompanying technical standards, which can be updated more readily.

Non discrimination

A signature may not be denied legal effect or admissibility as evidence solely because it is electronic or because it does not meet the requirements of the higher level. The eIDAS Regulation states this expressly in Article 25, and the 2000 United States federal law was built almost entirely on this idea.

The principle does not require accepting every signature as conclusive proof. It requires that the signature be assessed rather than dismissed in advance. A simple signature can be perfectly valid; what changes is who must prove what if it is challenged.

Party autonomy

In private relationships, the parties may agree on which signature methods they will accept between themselves. A bank and its customer may agree that certain transactions are confirmed with a code and a fingerprint; two companies may agree that their purchase orders are signed with a particular mechanism. Such a prior agreement strengthens the value of signatures made under its terms.

Autonomy has limits when the law requires a specific form for certain acts or when one of the parties is in a weaker position, as is the case with consumers. In those cases protective rules generally prevail over what was agreed.

The burden of proof and presumptions

Here lies, to a large extent, the practical difference between signature levels. When a simple electronic signature is challenged, the party relying on it must prove that it is authentic: that it was made by the person who claims to have made it and that the document has not changed. With a higher level signature, many legal systems reverse that burden through presumptions: the signature is presumed to belong to the certificate holder and the document is presumed unaltered, and it is the party denying this who must prove otherwise.

This reversal explains why organizations with a high risk of dispute, such as banks for certain loans or employers for certain agreements, prefer higher level signatures even though they cost more. It is not that a simple signature “is worthless”; it is that, if someone denies it, defending it may require expert analysis, technical records and time.

NON REPUDIATION, WITH NUANCES

In information security, *non repudiation* is the property that prevents someone from denying having performed an action. The digital signature is often presented as a guarantee of non repudiation. In legal terms it is wiser to be more cautious: it is always possible to claim that the key was used by someone else, that there was coercion, or that the signer did not understand what they were signing. What a good signature provides is not the impossibility of denial, but evidence so strong that denial becomes very difficult.

Three legislative models

Broadly speaking, three models emerged from the combination of these principles. No country fits exactly into one, but the classification helps explain why the same signature can have different effects depending on where it is used.

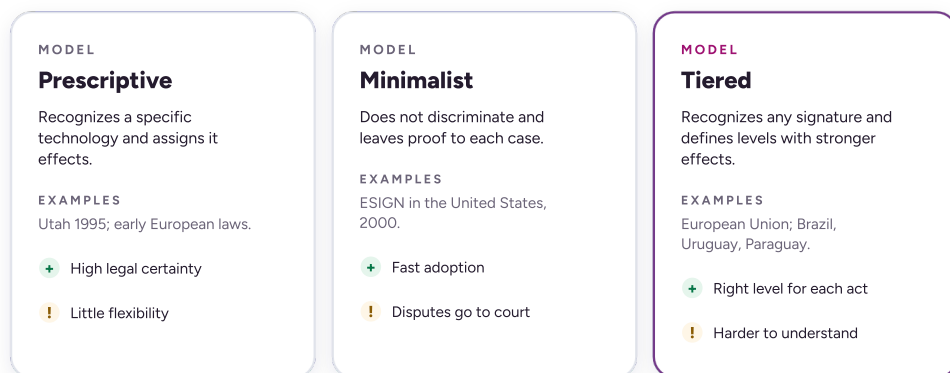


FIGURE 8 Three legislative models. No country fits one perfectly, but the classification explains why the same signature can have different effects in different jurisdictions.

The prescriptive model

This was the model of the first laws, such as Utah's in 1995 and the European laws of the late 1990s. It defines a specific technology, the digital signature with a certificate issued by a licensed authority, and grants it legal effect. Anything outside that technology receives no specific treatment. It offers a high degree of legal certainty to those who use the prescribed technology and little flexibility for everything else.

The minimalist model

This is the model of the 2000 United States federal law and of several laws inspired by UNCITRAL's first model law. It merely affirms that an electronic signature cannot be rejected for being electronic, and leaves it to the evidence in each case to decide. It favors innovation and rapid adoption, at the cost of shifting the debate over reliability to the courts.

The tiered model

This combines the two previous models. It recognizes any electronic signature under the principle of nondiscrimination and, at the same time, defines one or more higher levels with technical requirements and enhanced effects. It has been the European Union's model since 1999, consolidated by eIDAS, and the one adopted, with variations, by many Latin American countries. Its strength is that it allows the appropriate level to be chosen for each act. Its challenge is complexity: the levels must be understood in order to make good use of them.

Recognition between countries

A signature valid in one country is not automatically valid in another. Within the European Union, eIDAS solved the problem for qualified electronic signatures: they must be recognized in all Member States, and each country's trusted list makes it possible to verify the providers of the others. Outside that area, recognition depends on bilateral or regional agreements, on the equivalence of the regimes and, in many cases, on the will of the parties.

In Latin America there are mutual recognition initiatives, such as the agreements among Mercosur countries and the work of Red GEALC, the Latin American and Caribbean Network for Electronic Government, on cross border recognition of digital signatures. Progress is gradual. For an organization operating in several countries, this means that a single signature platform must be able to work with different providers and rules depending on the jurisdiction of each act.

Acts that still require something more

Almost all legal systems maintain exceptions. Wills, certain family law acts, transfers of real estate and acts requiring notarial intervention are usually excluded from the general electronic signature regime or subject to additional requirements. The exceptions are shrinking over time, as mechanisms such as the electronic notarial deed or remote notarial appearance emerge, but they still exist and should be checked before designing any process.

The law does not ask a signature what it is made of. It asks what it does, and how much trust it deserves for the act it supports.

What we sign for.

The electronic signature has moved from technical curiosity to infrastructure for banks, governments, hospitals and businesses. A survey of its uses shows that each sector asks different things of it.

There is no single use case for the electronic signature, but rather an enormous variety of acts that share the need to record an expression of will. What is interesting is that each sector emphasizes different functions: in some, identification matters most; in others, speed; in others, preservation over decades. Understanding these differences helps explain why signature platforms have become so configurable.

Banking and finance

This was one of the first sectors to adopt the electronic signature on a large scale. Account openings, loan agreements, promissory notes, direct debit authorizations, data updates and regulatory consents are now signed, in many countries, without setting foot in a branch. The priority is twofold: to identify the customer with certainty, in order to comply with anti money laundering rules, and to obtain strong evidence in case of disputes. That is why banking combines identity verification, often with biometrics, with advanced or higher level signatures and very detailed evidence records.

Public sector

Governments sign and receive signatures in enormous volumes: resolutions, case files, certificates, sworn statements, public tenders. Many countries have built their digital government strategies on higher level signatures, often supported by the national

identity document. The priority is full legal validity and long term preservation, because an administrative act may need to be produced decades later. Interoperability also matters: a case file may pass through several agencies, and each must be able to verify the signatures of the others.

Human resources

Employment contracts, pay slips, internal policies, confidentiality agreements and leave requests. Volumes are high and signatories often lack special devices. The priority is ease of use and traceability: knowing who received what and when they accepted it. In some countries certain employment documents require an advanced or higher level signature, and the platform must be able to raise the level for those documents only.

Health care

Informed consents, prescriptions, medical records, test reports. The signature attests to the professional's authorship and the patient's will. The priority is the integrity of sensitive documents and the protection of personal data. The electronic prescription, in particular, has become one of the highest volume uses of higher level signatures in several countries.

Real estate and insurance

Lease agreements involving landlord, tenant and guarantors; policies, endorsements and claim statements. These are processes with several parties who often do not know one another, and in which each must fill in their own information before signing. The priority is coordination: ensuring that each person sees what concerns them, completes their fields and signs in the correct order.

International trade

Sales contracts, letters of credit, certificates of origin, transport documents. The parties are in different countries and governed by different laws. The priority is cross border recognition and the ability to verify signatures issued under other regimes. In 2017 UNCITRAL adopted a model law on electronic transferable records, designed for instruments such as the bill of lading, which extends the logic of the electronic signature to documents that represent goods.

Professions and notaries

Notaries, accountants, customs brokers, lawyers and architects sign documents that others must be able to verify with certainty. In many countries they were the first users of tokens and cards. Today notaries are exploring the electronic notarial deed and remote appearance, which require combining signature, video identification and preservation with special guarantees.

SECTOR	WHAT IT EMPHASIZES	USUAL LEVEL
Banking	Customer identification and evidence for disputes	Advanced or higher, with biometrics
Public sector	Full validity, preservation, interoperability	Higher, often with the identity document
Human resources	Ease of use, volume, traceability	Simple or advanced depending on the document
Health care	Professional authorship, integrity, privacy	Higher for professionals; simple or advanced for patients
Real estate and insurance	Coordination of several parties and their own data	Simple or advanced
Foreign trade	Recognition between countries	Advanced or higher

The organization seal

Alongside signatures by individuals, the use of organization seals, the “electronic seals” of eIDAS, is growing. Electronic invoices, automatically issued certificates, attestations, bank statements and university diplomas receive an organization seal without human intervention, to guarantee that they come from whom they claim and have not been altered. In an organization that issues documents in bulk, organization seals applied automatically can easily exceed signatures by individuals in volume, even though they are far less visible.

Documents with many hands

One common feature runs through almost all these uses: important documents are rarely signed by just one person. A loan involves the customer, their guarantors and the bank; a lease, the landlord, the tenant, the guarantors and the real estate agency; the minutes of a meeting, every member of a governing body. Moreover, before signing, someone must review, someone must approve and someone must fill in data. That reality, more than the signature itself, is what gave rise to signature workflow managers.

Advantages, limits and misconceptions.

The electronic signature has obvious benefits and others that only emerge over time. It also has limits that are worth knowing before promising what it cannot deliver.

The obvious advantages

- ✓ **Time.** A contract that on paper required days of mailing and successive signatures can be completed in hours or minutes. For commercial processes, that difference translates directly into closed sales and customers who do not walk away.
- ✓ **Cost.** Printing, shipping of originals, scanning and much of the physical archive disappear. The saving per document may seem small, but it is multiplied by volume.
- ✓ **Distance.** The parties can sign from anywhere, at any time. This extends the reach of an organization without opening offices.
- ✓ **Environment.** Less paper, less ink, less travel. The effect is real, although it should not be overstated: digital infrastructure also consumes resources.

The advantages discovered later

- ✓ **Verifiable integrity.** A digital signature reveals any subsequent alteration. On paper, detecting a replaced page may require a forensic examination; in a digitally signed document, a validator is enough.
- ✓ **Evidence of the process.** A good platform records every step: sending, opening, identification, reading, signing. That trail is usually richer than any proof available in the paper world.

- ✓ **Visibility.** Whoever sends a document knows at all times who has signed, who has opened it and who has not yet done so. Bottlenecks become visible and measurable.
- ✓ **Integration.** A signed document can automatically feed other systems: document management, accounting, human resources. The signature stops being the end of a manual process and becomes an event within an automated one.
- ✓ **Accessibility.** When well designed, the electronic signature allows people with visual or motor disabilities, who on paper depended on others, to sign by themselves using screen readers and the settings of their own device.

The limits

The digital divide

Not everyone has a modern phone, a stable connection or the familiarity needed to follow a digital process. A service that accepts only electronic signatures may exclude those who most need that service. Good practice recommends keeping alternatives available and designing processes for the least experienced user, not for the average one.

Identity remains the weak link

Cryptography guarantees that a signature was made with a certain key. It does not guarantee that the person who activated that key is who they claim to be. If identity verification when the certificate was issued was weak, or if the factor that activates the signature can be stolen, a technically flawless signature can end up in the wrong hands. Much of the fraud associated with electronic signatures does not attack the mathematics: it attacks identification.

Preservation is not automatic

A document signed today may be impossible to validate ten years from now if the certificates, the revocation information and the timestamps were not preserved, or if the algorithms used have since weakened. Preserving the validity of a signature requires deliberate decisions, which we discuss in Volume 2.

Interoperability has seams

A perfectly valid signature may appear as “not verified” in a reader that does not trust the authority that issued the certificate. A signature format may be accepted in one country and unknown in another. These frictions do not invalidate the signature, but they create distrust among users who do not understand why the same document looks different in two programs.

Common misconceptions

WHAT PEOPLE SAY	WHAT IS WORTH KNOWING
“A scanned signature is an electronic signature.”	It is in the broadest sense, but it is the weakest of all: it is easily copied and does not protect the integrity of the document.
“An electronic signature has no legal validity.”	In the vast majority of countries it does, with different effects depending on the level. What it may lack is the reinforced effect of a higher level signature.
“If the PDF reader shows a warning, the signature is invalid.”	Often the warning only indicates that the reader has not been configured with the authority that issued the certificate. The signature must be validated against the correct trusted list.
“A digital signature cannot be forged.”	The mathematics is very robust, but the key can be used by someone else if its protection fails. Security belongs to the process as a whole.
“A signed document is valid forever.”	Only if it is preserved with the necessary proof and its protection is renewed as algorithms age.
“The highest level is always best.”	Not necessarily. A level that is excessive for the risk of the act adds friction and may keep the process from being completed.

KEY POINT

The electronic signature does not eliminate risk; it moves it elsewhere. From paper that is lost or altered to identity that is impersonated or proof that was not preserved. A good solution is recognized by how it manages those new risks, not by the number of features it offers.

From the signed document to the signed process.

Signing a document was already possible. The hard part was coordinating everyone who needed to take part in it. Signing workflow platforms were born from that need.

In the late 1990s, digitally signing a document was technically possible and, in several countries, legally valid. Yet almost no one did it. The reason was not a lack of confidence in cryptography but the lack of a practical path. Anyone who wanted three people to sign a contract had to send them the file, explain how to sign with their tools, wait for each of them to return it, check that all of them had signed the same version and archive the result. It was easier to print.

Two roots

Signing workflow platforms have two roots that came together at the beginning of this century.

The first lies in the workflow and document management systems that large organizations had used since the 1980s and 1990s. Those systems already knew how to route a document through a series of approvals, record who had seen it and archive it. Public administrations, in particular, developed electronic case files with internal signing circuits. But these were closed systems, designed for users within a single organization.

The second root is email and the web as a universal channel. By the early 2000s, anyone with an email address and a browser could receive a link and open a document. It was enough to combine that channel with workflow logic and some signing

mechanism for a document to travel, in minutes, the path that on paper took weeks.

The pioneers

One of the first companies in the field was founded in the United States in 2003 and popularized the idea of the electronic “envelope”: a package with one or more documents, a list of recipients and instructions on what each of them had to do. Another was born in 2005; a document software company acquired it in 2011 and later turned it into the basis of its signing service. Around 2010 a third appeared, which a cloud storage company acquired in 2019. Dozens of providers in Europe, Latin America and Asia joined them, many of them originating from certification service providers that saw the workflow as a way to bring their certificates to a wider audience.

The first services relied mainly on the simple electronic signature: the signer received a link by email, reviewed the document, clicked or drew a signature, and the platform applied a platform seal to the result and produced a certificate recording what had happened. That record, more than the signature itself, was the piece that provided evidentiary value. Over time, platforms added the option of using advanced and qualified electronic signatures, identity verification and providers from different countries.

Adoption grew steadily throughout the 2010s and accelerated sharply in 2020, when the pandemic forced millions of organizations to sign remotely almost overnight. What until then had been an efficiency improvement became, for months, the only way to keep operating.

The vocabulary of the workflow

Over the years a vocabulary took shape that almost all platforms now share, although each gives it its own names.

CONCEPT	WHAT IT IS
Envelope	The unit of work: one or more documents, the participants and the rules for its route.
Participant	Each person involved. A participant may have different <i>roles</i> : signer, approver, reviewer, someone who fills in data or someone who only receives a copy.
Routing	The order in which participants act: sequential, one after another; parallel, all at once; or mixed, with groups acting in parallel within a sequence.
Fields	The places in the document where each participant signs, enters a date, fills in an amount or selects an option, each assigned to the right person.
Access authentication	What the participant is asked for in order to open the document: a code, a message to their phone, a digital identity or a certificate.
Reminders and expiration	Automatic notices to those who have not yet acted, and a date after which the envelope is no longer available.
Declining and delegation	The option to refuse to sign while giving a reason, or to reassign the task to another person when the rules allow it.
Template	A document with its fields, roles and routing already defined, which can be reused by changing only the participants.
Certificate of completion	The report that accompanies the signed document and summarizes who did what, when, and how they were identified.

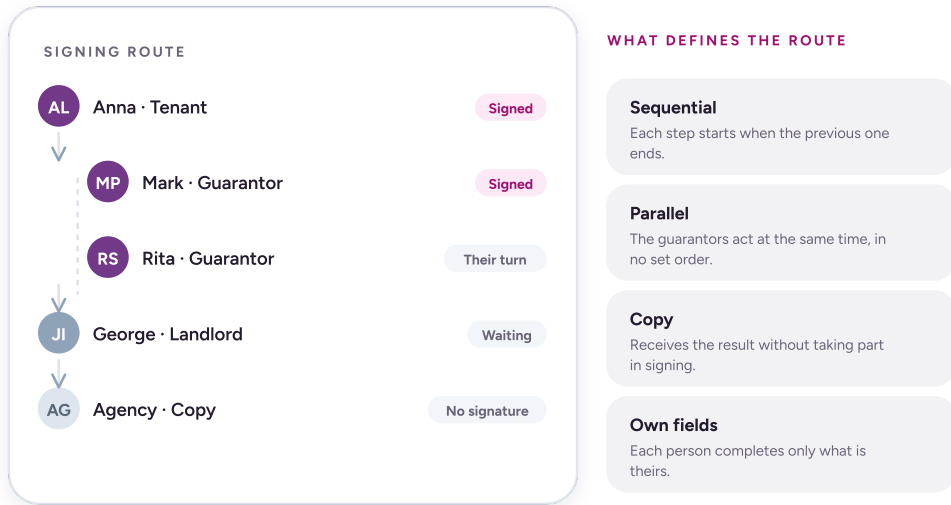


FIGURE 9 A mixed signing route: a signer, two guarantors acting in parallel, a landlord who signs last and an agency that only receives a copy.

From standalone tool to organizational fabric

As they matured, signing workflow platforms ceased to be isolated tools and became integrated into each organization's systems. Application programming interfaces allowed a customer management, human resources or procurement system to create envelopes automatically and be notified when a document had been signed.

Embedded signing allowed signers to stay within the application they were already using. Integrations with document repositories meant that the signed document was archived automatically, in the right place.

At the same time, the market became segmented. On one side were general purpose platforms operating at large scale, focused on ease of use and a broad ecosystem of integrations. On the other were more specialized solutions, focused on higher level signatures, on compliance with national regimes or on operation by trust service providers. Industry analysts began to evaluate not the signature itself, which they regard as a basic capability, but the complete workflow and the identity of the signer.

What changed in the idea of a signature

The deepest contribution of signing workflow platforms was not technical but conceptual. They changed the unit of analysis. Before, the question was whether a signature was valid. Now the question is whether a signing process was correct: whether each person saw the version they were meant to see, completed their part, was identified at the appropriate level, signed in the intended order, and whether all of that was recorded in a way that can be demonstrated later.

That shift in the unit of analysis, from document to process, is the starting point of the next chapter, where we describe what to expect today from a platform that coordinates signing processes.

Anatomy of a platform.

What a system that coordinates signing processes does on the inside. Seven layers, what is expected of each today, and what distinguishes a mature solution from one that only appears to be.

Seen from the outside, a signing workflow platform looks simple: you upload a document, choose the signers and wait. Seen from the inside, it is a system with very different responsibilities that must work together. To analyze it, it helps to break it down into layers. The breakdown we propose does not correspond to any particular product; it is a way of organizing the questions that any organization should ask.

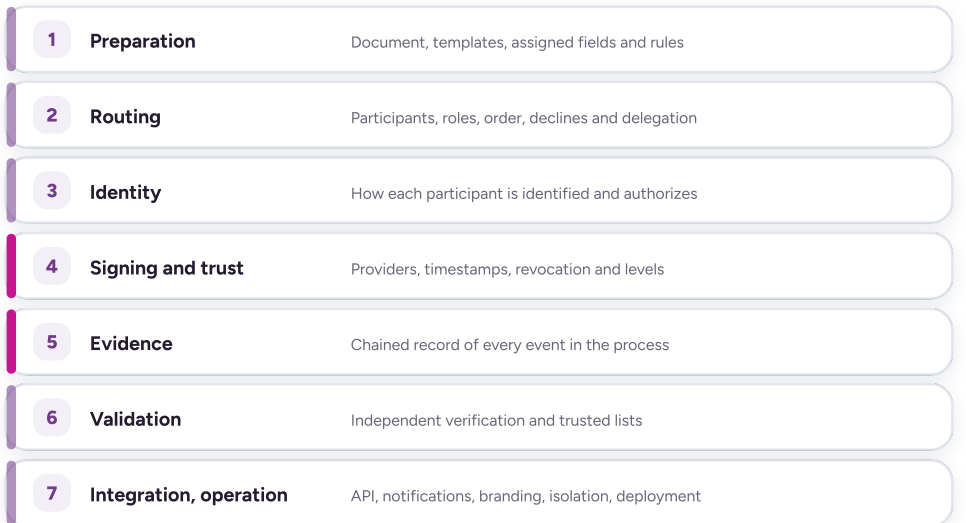


FIGURE 10 Seven layers of a signing workflow platform. In magenta, the two layers that sustain the proof.

1. Document preparation

Everything begins with a document, almost always a PDF, although it may originate from a template or from another system. This layer decides what needs to be filled in and who fills it in. One observation the market was slow to absorb is that most documents are not signed first: they are completed first. A promissory note needs the amount; a lease, the handover date; a consent form, the patient's identity document number. If those data are filled in by hand before sending, much of the benefit is lost.

A mature platform makes it possible to assign fields to each participant, with rules for mandatory entries and validation, and guarantees that what has been completed becomes part of the version being signed. When necessary, it also converts the document to a format suitable for archival preservation, such as PDF/A, before the first signature, because converting it afterward would invalidate the signatures.

2. Routing and participants

This is the layer of the workflow proper: who takes part, in what role and in what order. Sequential, parallel and mixed routing are basic features today, as are the roles of signer, approver and copy recipient. What distinguishes a mature solution is how it handles the difficult cases: a group in which a signature from any one member is enough, a participant who is only defined once the previous one acts, a signer who delegates to an authorized representative, a document that must go back because someone declined it.

The recipient's experience also matters. Each participant should see only what concerns them, in their own language, from any device, with timely reminders and without having to create an account.

3. Identity

Before signing, it is necessary to know who is signing. The options range from a code sent by email or to a phone to verification of an identity document with a liveness check, and include national digital identities, corporate identity providers and certificates on a card or in the cloud. Industry analysts agree that much of the value of these platforms has shifted to this layer.

The key question is not how many methods a platform offers, but whether it allows the right method to be chosen for each participant and each act, and whether it records separately in the evidence how each person was identified and how they authorized their signature. Identifying oneself and authorizing a signature are distinct acts, and solid proof must be able to show both.

4. Signing and trust services

This layer produces the cryptographic signature. A platform may sign with its own keys, applying a platform seal over each participant's simple signature, or delegate signing to external providers, for example through the common remote signing interface discussed in chapter five. It may also request timestamps and revocation responses from third parties and embed them in the document.

Three features separate the mature from the merely apparent here. The first is the ability to work with several providers and to choose, for each act, the appropriate one according to the country and the required level. The second is resilience: what happens if an external service does not respond. Good practice is to define an order of preference and fallback options and, if something still fails, to have the document remain at the level it actually reached and state as much, rather than failing silently or appearing to have a level it lacks. The third is control over what may change after each signature: the PDF format allows a signed document to declare whether, for example, others may fill in fields or add signatures, and a careful platform uses those rules so that each signer knows exactly what their signature protects.

5. Evidence

Throughout the process, the platform records events: sending, each opening, each identification, each completed field, each consent, each signature, each refusal. That record is the backbone of the proof. But a record is only worth something if it can be shown that no one altered it, including the organization that operates the platform itself.

The most careful solutions chain events together through their hashes, so that each event includes the hash of the previous one. Altering or deleting an event breaks the chain and is detected. An additional step, typical of the most demanding designs, is to periodically anchor the hash of the record in an external location that the operator does

not control, such as a timestamping service or immutable storage held by a third party. That way, not even the system administrator can rewrite history without leaving a trace.

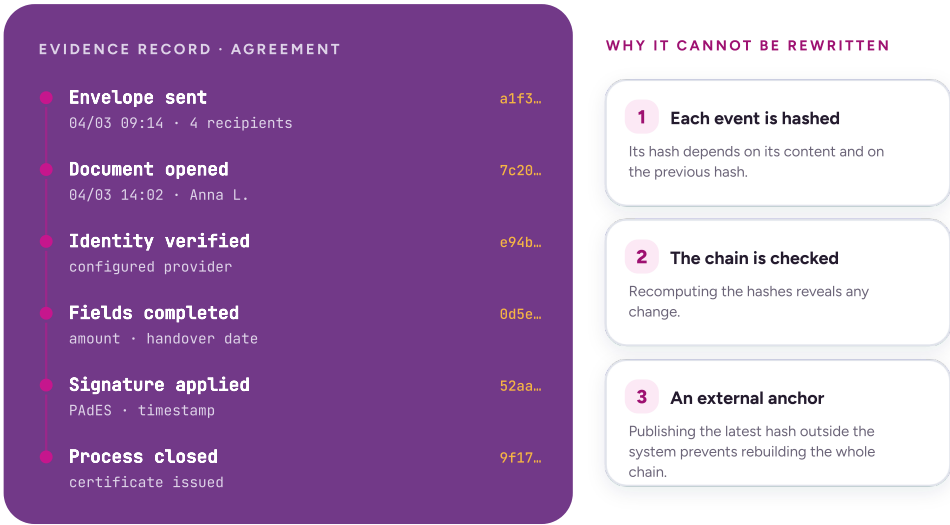


FIGURE 11 A chained evidence record. Each event includes the hash of the previous one; changing or deleting any event breaks the chain from that point on.

6. Validation

Signing is half the job. The other half is enabling anyone, at any time, to check that the signature is valid. A mature platform delivers documents that can be validated with independent tools, not only its own, and where possible offers an open validator that explains what it checked and what it did not. Transparency is part of trust: a validator that only says “valid” or “invalid” teaches less than one that shows the certificate chain, the timestamp, the revocation information and the document's modification rules.

Validation depends on the trust placed in the authorities. That is why the most complete solutions read each country's official trusted lists, rather than relying solely on the list built into a reader or an operating system.

7. Integration and operation

The last layer connects the platform with the rest of the world and makes it possible to operate it. It includes application programming interfaces, automatic notifications to other systems when something happens, integrations with repositories and automation tools, brand customization and user administration. It also includes aspects the user does not see but a demanding buyer does ask about: isolation between the data of different organizations, data residency, activity logs for auditing, connection with the customer's security monitoring systems, and the option of deployment in the cloud or on the customer's own premises.

A relevant trend is that these platforms are ceasing to be merely a service that a company subscribes to and are becoming infrastructure that others operate. A trust service provider, a government or a large corporate group may want to offer the service under its own brand to its own customers, with a hierarchy of accounts, usage metering and its own pricing. Designing for that scenario requires conceiving the platform from the outset as a system with several levels of administration.

Questions for evaluating a solution

By way of summary, these are some questions that any organization can ask a provider, or ask itself if it builds its own solution.

- 1 Can participants fill in data within the document before signing, subject to rules, and does what they complete become part of what is signed?
- 2 What routing options does it support, and how does it handle declines, delegations and groups?
- 3 What identification methods does it offer, can a different one be chosen for each participant, and does the evidence distinguish identification from authorization?
- 4 Which signature, timestamp and revocation providers can it work with, and what happens if one does not respond?
- 5 What signature format and level does it produce, and is that sufficient for preservation over the years?
- 6 How is the evidence record protected against alteration, including alteration by the operator itself?

- 7 Can the documents be validated with independent tools? What does its validator say about what it checks and what it does not?
- 8 How are each organization's data isolated, where do they reside and who can access them?
- 9 Which features are not available today, and does the platform say so clearly or conceal it?

The last question seems minor, but it is not. In a field where trust is the product, a platform that honestly shows what it does not yet do, and why, deserves more trust than one that promises everything.

What lies ahead.

The electronic signature is entering a new stage. Five forces are driving it, and each raises questions that the following volumes of this series take up in greater detail.

Identity in your pocket

The European Digital Identity Wallet is a highly visible change. When hundreds of millions of people can identify themselves and sign at the qualified level from their phones, free of charge for personal use, higher level signatures will no longer be the exception. Similar initiatives are advancing in other regions, based on chip enabled identity documents, official applications or verifiable credentials issued by governments and banks.

For signing platforms, this means accepting signers who arrive with their own identity and their own means of signing, instead of imposing one on them. The platform ceases to be the party that identifies and becomes the party that orchestrates identities issued by others.

Remote identity verification

The combination of document reading, facial recognition and liveness checks makes it possible to verify a person who has never appeared at an office. It is the gateway to many signing processes, especially in banking and consumer services. At the same time, impersonation techniques based on synthetic images are growing more sophisticated, and identity verification has become a race between defenders and attackers. European technical standards already set requirements for remote identification, and other regions are likely to adopt or adapt them.

Artificial intelligence

Artificial intelligence is entering signing platforms along two paths. The first is assistance: automatically extracting the parties, dates and amounts from a contract, suggesting where each person should sign, summarizing a long document for the sender, flagging unusual clauses. The second is agents: programs that act on behalf of a person or an organization, prepare envelopes, follow up and, eventually, might sign within delegated limits.

This second path raises fundamental questions. If an agent signs, who is expressing intent? How are the limits of what it may sign defined, and how is it proven afterward that it acted within those limits? The answers will probably build on familiar instruments, such as the organization seal and powers of attorney, but they are still taking shape. What already seems clear is that the evidence record, which today documents what people did, will also have to document what machines did on their behalf.

Post quantum cryptography

A large scale quantum computer could break the public key algorithms on which almost all digital signatures rely today. Such a computer does not yet exist, and estimates of when it might vary widely. But the risk is significant enough that the United States National Institute of Standards and Technology published its first post quantum cryptography standards in August 2024, including two signature algorithms, and that European authorities recommend planning the transition.

For electronic signatures, the transition has a particular feature: signed documents must remain verifiable for decades. This requires thinking now about how to protect existing signatures, for example by renewing their archive timestamps with new algorithms, and about how classical and post quantum signatures will coexist for years within the same systems.

Trust as shared infrastructure

Finally, the underlying trend is that digital trust is becoming infrastructure, like energy or telecommunications. Public trusted lists, supervised providers, common remote signing interfaces, identity wallets, qualified preservation services. Signing platforms

no longer set themselves apart by their cryptography, which is largely standard, but by knowing how to combine those pieces to solve real processes, in different countries, under different rules, in a way that people can understand.

IN THE COMING VOLUMES

Volume 2, *The Proof That Endures*, examines in detail signature formats and levels, timestamps, validation, trusted lists and preservation over time. **Volume 3, *Orchestrating the Signature***, addresses process design, identity, integration, operation at scale, artificial intelligence and the post quantum transition.

For five thousand years, signing meant leaving a mark. In the years ahead it will increasingly mean demonstrating a process.

Glossary

The main terms in this volume, in the sense in which they are used here.

Advanced electronic signature

A signature uniquely linked to the signer, capable of identifying them, created using means under their exclusive control and revealing any subsequent modification.

Certification authority

An entity that verifies the identity of persons or organizations and issues digital certificates linking that identity to a public key.

Chain of trust

A sequence of certificates in which each is signed by the next, up to a root that is trusted by explicit decision.

Digital certificate

An electronic document signed by a certification authority stating that a public key belongs to a holder for a given period.

Digital identity wallet

An application, usually on a phone, that stores identity credentials and allows them to be presented and used for signing.

Digital signature

A signing technique based on public key cryptography. In some countries, also a higher level legal category.

“Electronic seal” (organization seal)

The equivalent of a signature for a legal person: it guarantees the origin and integrity of a document issued by an organization.

Electronic signature

Any electronic data that a person associates with other electronic data with the intention of signing them.

Evidence record

An ordered set of events from a signing process, protected against alteration, that makes it possible to demonstrate afterward what took place.

Exclusive control

A legal requirement under which only the signer can activate their signing key, either because it is held on their own device or because its remote use requires their authentication.

Functional equivalence

The principle that an electronic mechanism satisfies a legal signature requirement if it fulfills the functions that a handwritten signature fulfills in that context.

Hash function

A function that transforms content of any size into a hash of fixed length, so that any change in the content produces a different hash.

HSM

Hardware security module: a device dedicated to generating, storing and using cryptographic keys, with certified physical and logical protections.

OCSP

An online query protocol that reports whether a specific certificate is valid or has been revoked.

Private key and public key

A pair of mathematically related keys. The private key, kept secret, produces the signature; the public key, which can be shared, allows it to be verified.

Qualified or recognized certificate

A certificate issued by a supervised provider that meets reinforced requirements for identity verification and operation.

Qualified electronic signature

An advanced electronic signature created with a qualified device and based on a qualified certificate. In the European Union, it is equivalent to a handwritten signature.

Remote signing

Signing in which the signer's key is kept in a secure module operated by a provider and is activated remotely through the holder's authentication.

Revocation

The cancellation of a certificate before its expiration, communicated through published lists or through an online query.

Signing workflow platform

A system that coordinates the route of one or more documents among several participants, with roles, order, fields, identification and an evidence record.

Smart card

A card with a chip capable of generating and storing a private key and of signing without the key ever leaving the chip.

Technology neutrality

The principle that the law describes requirements and effects without favoring or excluding any particular technology.

Timestamp

Proof, signed by a trusted third party, that a piece of data existed at a given moment.

Timestamping authority

A trusted third party that issues timestamps: signed proof that a piece of data existed at a given moment.

Trust service provider

An entity that provides services such as certificate issuance, timestamps, validation or preservation. It is qualified if it meets reinforced requirements and appears on an official list.

Trusted list

An official list, signed by a public authority, of supervised trust service providers and their services.

Validation

The process of checking the authenticity of a signature, the integrity of the document and the validity of the certificate at the time of signing.

REFERENCE

Further reading

The laws, papers and standards cited in this volume, grouped by topic. All are publicly available or can be consulted in specialized libraries.

History and foundations

Diffie, W. and Hellman, M. "New Directions in Cryptography". *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1976.

Rivest, R., Shamir, A. and Adleman, L. Paper introducing the RSA algorithm. *Communications of the ACM*, vol. 21, no. 2, 1978.

Howley v. Whipple, 48 N.H. 487. Supreme Court of New Hampshire, 1869.

Statute of Frauds, England, 1677.

Stevens, M. et al. "Short Chosen Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate". *CRYPTO 2009*.

Stevens, M. et al. Paper on the first full collision of SHA1. *CRYPTO 2017*.

International frameworks

UNCITRAL. Model Law on Electronic Commerce, 1996. Model Law on Electronic Signatures, 2001. Model Law on Electronic Transferable Records, 2017.

European Union. Directive 1999/93/EC on a Community framework for electronic signatures.

European Union. Regulation (EU) 910/2014 on electronic identification and trust services (eIDAS).

European Union. Regulation (EU) 2024/1183, amending Regulation 910/2014 as regards establishing the European Digital Identity Framework.

United States. Electronic Signatures in Global and National Commerce Act (ESIGN), 2000. Uniform Electronic Transactions Act (UETA), 1999. Utah Digital Signature Act, 1995.

Latin American legislation cited

Argentina, Ley 25.506 de Firma Digital, 2001. Brazil, Medida Provisoria 2.200 of 2001, which established ICP Brasil, and Ley 14.063 of 2020. Chile, Ley 19.799, 2002. Colombia, Ley 527, 1999. Paraguay, Ley 4.017, 2010, and Ley 6.822 de los servicios de confianza, 2021. Uruguay, Ley 18.600 de Documento Electrónico y Firma Electrónica, 2009.

Technical standards

ITU. Recommendation X.509, public key certificate framework, 1988 and subsequent revisions.

IETF. RFC 3161, Time Stamp Protocol, 2001. RFC 5280, certificate and revocation list profile, 2008. RFC 6960, OCSP protocol, 2013.

ISO. ISO 32000, Portable Document Format (PDF), 2008 and 2017.

ETSI. EN 319 142, PDF advanced electronic signatures (PAdES). EN 319 102, procedures for signature creation and validation. EN 319 401, general requirements for trust service providers.

CEN. EN 419 241, trustworthy systems supporting server signing. EN 419 221, protection profiles for cryptographic modules.

Cloud Signature Consortium. Remote signing interface specification, version 2.

NIST. FIPS 140, security requirements for cryptographic modules. FIPS 204 and FIPS 205, post quantum signature standards, 2024.

Rúbrica.

NOTEBOOKS ON SIGNATURE, IDENTITY AND DIGITAL TRUST

Five thousand years of signing, explained for those who must now decide how to do it.

From the cylinder seal to the identity wallet on a phone, this first volume traces the history, technical foundations, devices and legal doctrines of the electronic signature, and explains how the platforms emerged that now coordinate signing processes among people, organizations and countries.

Volume 1 · From Rúbrica to Digital Signature

History, foundations, devices, doctrines, uses and platforms.

Volume 2 · The Proof That Endures

Formats, levels, timestamps, validation and preservation.

Volume 3 · Orchestrating the Signature

Processes, identity, integration, operation at scale and the future.