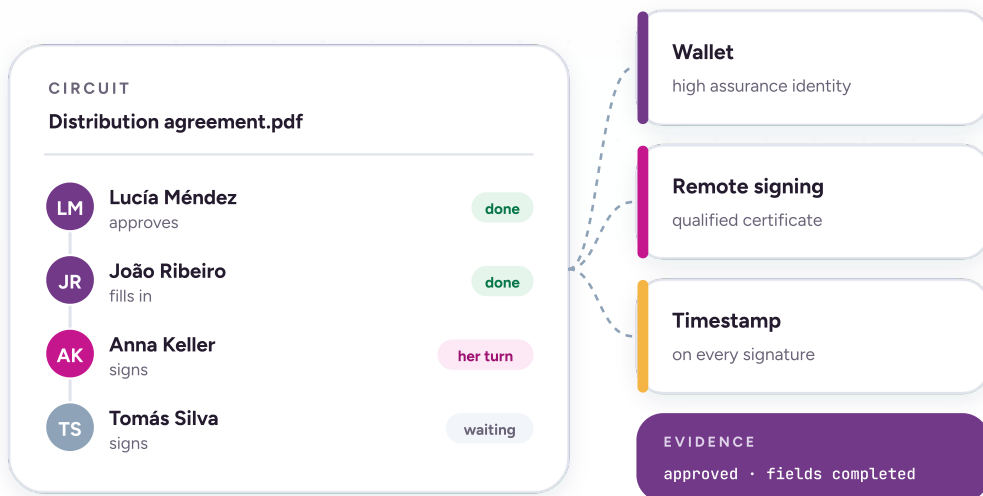


Orchestrating the Signature.

Processes, identity, integration and operation at scale: how a signature service is designed, connected and governed, and what digital wallets, artificial intelligence and post quantum cryptography change in it.



Rúbrica. Notebooks on signature, identity and digital trust

Volume 3. Orchestrating the 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 evidence available; before making a decision, consult a professional qualified in the relevant jurisdiction.

References to laws, standards, institutions and companies are made for historical and educational purposes. The trademarks mentioned belong to their owners. The epilogue describes a platform developed by the publisher and says so.

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

RÚBRICA · VOLUME 3

Orchestrating the Signature

How the services that coordinate signing among people, organizations and countries are designed, integrated and operated.

Contents

	Preface	5
01	Designing a signing process	7
02	The identity of the signer	13
03	Wallets and credentials	17
04	Providers and mechanisms	21
05	Integration	25
06	Operating at scale	29
07	Accessibility and languages	33
08	Artificial intelligence and signing	37
09	The post quantum transition	41
	Epilogue. Signing Flows	45
	Glossary	49
	Further reading	53

From signature to service

The first two volumes explained what a signature is and how its proof is preserved. This one deals with what it takes for thousands of signatures to happen every day, correctly, in many places at once.

A single signature is a solved problem. A signature service is something else. It has to coordinate people who do not know each other, in the right order, with the right level of identification for each of them. It has to talk to trust service providers in different countries, to the systems of the organizations that use it and to the devices of the people who sign. It has to keep each customer's data isolated, answer to auditors and keep working when an external service fails. And it has to do all of this in a way that a person with no technical background can understand at the moment of signing.

This volume works through those challenges. It begins with the design of processes and with the identity of the signer, which is where much of the value and much of the risk are concentrated today. It goes on to the choice of providers and mechanisms for each act, to integration with other systems and to operation at scale, including for those who offer the service to third parties. It devotes a chapter to accessibility and languages, which are often treated as details and are not. It ends with two forces that are reshaping the discipline: artificial intelligence and the transition to post quantum cryptography.

Like its predecessors, this volume names no products in its chapters. The one exception is the epilogue, where, for the first and only time in the series, we describe the platform developed by the publisher of these notebooks and the problems from this volume that it addresses. It is kept apart from the rest and labeled as such, so that readers can read it, or skip it, with that information in plain view.

Designing a signing process.

Before choosing technology, you have to understand the act: who takes part, what each person contributes, in what order, and what happens when something does not go as expected.

The temptation when digitizing a signing process is to copy the paper process. You print the document in your mind, recall who used to sign it and in what order, and reproduce that route on a platform. The result usually works, but it wastes almost everything the digital medium makes possible and carries over steps that only existed because of the limitations of paper.

Good design starts with a different question: what must be proven at the end? From there you can work out who needs to take part, what each person must contribute and what level of assurance each contribution requires.

The roles

Almost every process features the same parts, even if they go by different names.

ROLE	WHAT IT DOES	WHAT MUST BE PROVEN
Sender	Prepares the document, defines participants and rules, and sends it.	Which version was sent and with what instructions.
Filler	Supplies data within the document: an amount, a date, an account number.	What data was entered and when.
Approver	Authorizes the document to proceed, without signing it.	That this person, identified, approved that version.
Signer	Expresses their intent regarding the content.	Identity, authorization and integrity of what was signed.
Copy recipient	Receives the result for information or filing.	That they received the final document.

One person can hold more than one role: a customer fills in their details and then signs. What matters is that the system tells the acts apart, because each one has different consequences.

Routing patterns

The sequential and parallel routes introduced in the first volume combine into patterns that recur across every sector.



FIGURE 1 Five patterns that recur in every sector. They combine serial routes, parallel routes and individual copies.

- ✓ **Prior approval.** An internal approver reviews the document before it goes out to external signers. This keeps a mistake from reaching the customer.
- ✓ **Fill in before signing.** One or more participants supply data, and the document, now complete, moves on to signing. This is the pattern that eliminates the most manual work.
- ✓ **Any one of a group.** Any member of a group can act, for example any of a company's authorized representatives. The first to sign completes the step.
- ✓ **Individual copies.** The same document is sent to many people and each signs their own copy, with its own record. This is the pattern for internal policies and mass consents.
- ✓ **Final countersignature.** The organization signs or applies its organization seal last, once all the other parties have done so, so as not to commit itself earlier.

Exceptions are part of the design

A process that only covers the happy path fails at the first surprise. The questions worth answering before publishing a process are always the same.

- What happens if someone declines? Is everything cancelled, does it go back to the sender, can it be corrected and resent?
- Can a signer delegate to someone else? With what control and what record?
- What happens if nobody acts? How many reminders, how often, and when does the submission expire?
- Can a piece of data be corrected after someone has signed? The right answer is almost always no: the submission is voided and sent again.
- What happens if an external service, such as the signature provider, does not respond?

Rules belong to the person, not the document

One idea that greatly simplifies design is to attach rules to each participant rather than to the document as a whole. For each person you define how they sign, with what level of identification, whether they can download or print, and whether access requires a code. That way, within a single document, an internal employee can approve with their corporate account, a customer can sign with a code sent to their phone and an authorized representative can sign with their qualified certificate. And the platform can check before sending that every requirement can be met: a document that requires someone to use a type of certificate that is not available should not go out.

Templates and governance

Once a process works, it becomes a template: the document with its fields, roles and rules, ready to be reused by changing only the participants. In large organizations, templates become assets that need governance: who can create them, who approves changes to them, which version was used for each submission. That governance is itself part of the evidence: in a dispute, it may be necessary to show which rules a document was sent under five years earlier.

KEY POINTS

A good signing process is designed around the proof it must leave behind, distinguishes the acts of each participant, assigns rules to each person, anticipates exceptions before they happen and is governed as an asset of the organization.

Who is on the other side?

Cryptography guarantees that a key signed. Identity answers the question that really matters: who used that key. It is the layer where value, innovation and fraud are concentrated today.

In the first volume we warned that identity is the weak link in electronic signatures. This chapter explains how it is strengthened. It helps to start with a vocabulary that separates three moments that are often confused.

- ✓ **Identity verification** means checking, once, that a person is who they claim to be, for example by examining their identity document.
- ✓ **Authentication** means checking, each time the person returns, that they are the same person who was verified, for example with a password and a second factor.
- ✓ **Signature authorization** is the specific act by which the person activates their signature on a document, for example by entering a code or a PIN.

A sound signature needs all three, and the evidence must be able to show each one separately.

Levels of assurance

International standards classify the strength of identification into levels. The eIDAS Regulation defines three assurance levels for electronic identification means: low, substantial and high. The digital identity guidelines of the United States National Institute of Standards and Technology distinguish, separately, the strength of the initial verification and that of the authenticator, each on three levels. The names vary, but the logic is the same: the more serious the act, the stronger the proof must be that the person acting is who they say they are.

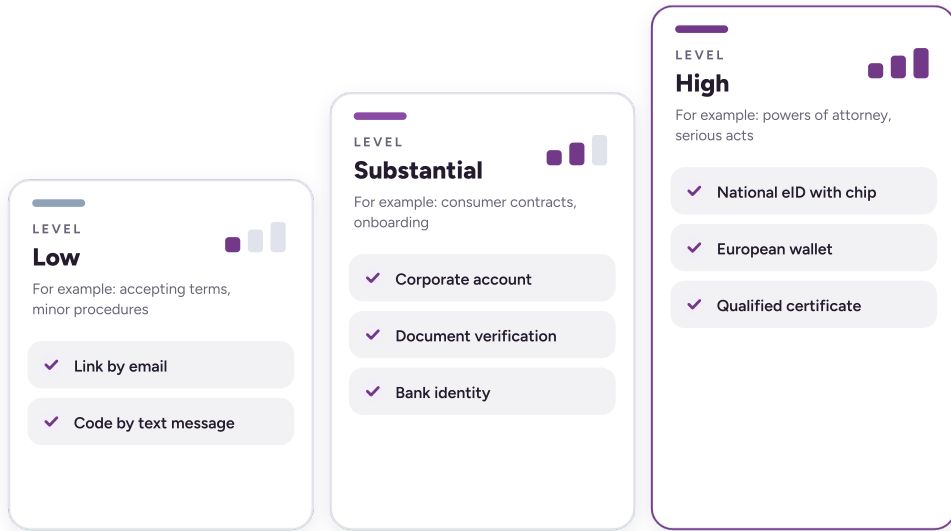


FIGURE 2 Levels of assurance for identification and the methods that usually reach them. The choice depends on the act, and more than one method per level should be offered.

The methods, from lightest to strongest

A link and a code

The most widespread method is to send the person a link by email and, optionally, a code by text message or through a messaging app. It proves that the person controls that inbox or that phone, not who they are. For many acts this is enough, especially when there is already a relationship with the person and their contact details were verified beforehand.

Corporate and social identities

Within an organization, the most natural identity is the corporate account, managed by the company's identity provider through standard protocols such as SAML or OpenID Connect. For consumer relationships, some processes accept identities from large scale providers. Their strength depends on how the account was originally verified.

National digital identities

Many countries offer their citizens an official digital identity, based on a chip identity card, on government apps or on bank credentials recognized by the state. They are generally a strong and inexpensive way to identify a person in their own country, and integrating them is becoming ever simpler thanks to standard protocols.

Document verification with liveness detection

When no digital identity is available, verification can be done remotely: the person photographs their identity document, the system checks its security features and reads the chip if there is one, and then compares the photo on the document with the face of the person in front of the camera, with checks that it is a live person and not an image. This is the method that made digital banking possible at scale. Its challenge is the race against impersonation techniques, which now include synthetic images and videos of ever increasing quality.

Certificates

Finally, the signing certificate itself, whether on a card, a token or in the cloud, identifies its holder, because issuing it required prior verification, often in person. When the signature is made with a qualified certificate, identification comes built into the signature.

Choosing without excluding

The most common mistake is to require the strongest method from everyone. A process that asks a foreign customer for a national digital identity, or a user signing from their phone for a card and reader, never gets completed. Good practice is to define, for each act, the minimum acceptable level, offer several methods that reach it and let each person use the one they have.

Consent must be proven too

Before signing electronically, many legal systems require the person to agree to doing so by that means, and data protection laws require informing them what data is collected and why. That consent is an act in its own right and must be recorded with

the exact text the person accepted, in their language, and with the version of that text in force at the time. A receipt of consent, given to the person, strengthens both transparency and proof.

A WARNING

Identity is also where fraud takes place. The most common attacks do not break the cryptography: they take over an email account, clone a SIM card, trick the person into handing over a code or present a synthetic face. No method is invulnerable. That is why it makes sense to combine methods according to risk, watch for signs of fraud and record everything needed to investigate later.

Identity in your pocket.

For decades, identifying yourself online meant asking someone else to confirm who you are. Digital identity wallets propose something different: that each person carries their own credentials and decides what to show.

All the methods in the previous chapter have one thing in common: the person depends on an intermediary that, in every transaction, confirms their identity to whoever asks for it. The corporate identity provider, the bank, the national identification system or the document verification service steps in every time. It works, but it has costs: each intermediary sees which services the person uses, every integration is different and the person has little control over what data is shared.

Digital identity wallets turn that model around. A trusted authority issues a signed credential, the person stores it in an app on their phone and presents it when needed. Whoever receives it verifies the issuer's signature without having to ask the issuer anything at that moment.

Three roles

The model is described in terms of three roles, which the technical literature often calls the trust triangle.

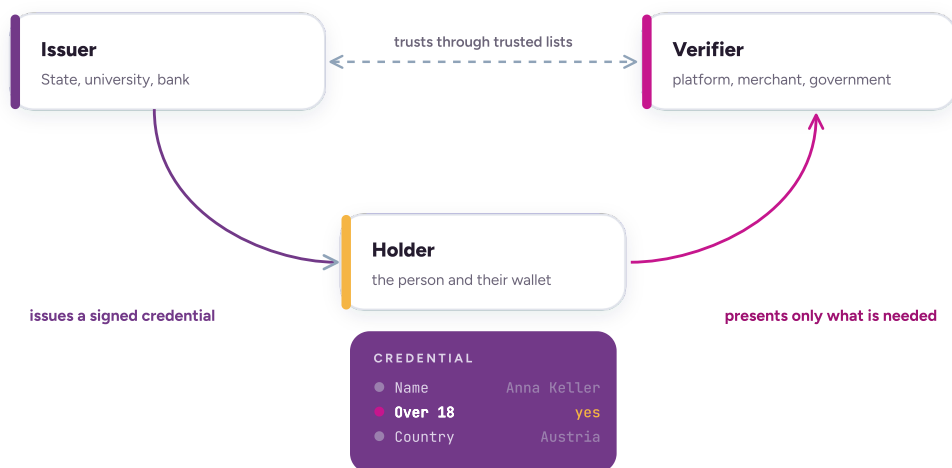


FIGURE 3 The triangle of trust. The issuer is not involved in each use; the verifier trusts it through trusted lists.

- ✓ **The issuer** is the party that vouches for an attribute: the state that issues an identity document, the university that awards a degree, the bank that confirms an account. It signs the credential with its key.
- ✓ **The holder** is the person who receives the credential and keeps it in their wallet. They decide when to present it and which attributes to reveal.
- ✓ **The verifier**, also called the relying party, is the one that receives the presentation: a retailer, a public authority, a signature platform. It checks the issuer's signature and that the credential has not been revoked.

The relationship between issuer and verifier is no longer direct. The issuer does not learn of each use of the credential, and that is a gain for privacy. In return, the verifier needs to know which issuers to trust, and that is where the trusted lists described in the second volume reappear.

Revealing only what is needed

One of the most valuable promises of digital credentials is selective disclosure. Someone who needs to know that a person is an adult does not need their date of birth, their address or their document number. Modern formats allow the wallet to present only the requested attributes, or even a derived statement such as "over

eighteen", with the same cryptographic guarantee as the full credential. For electronic signatures this means the evidence record can store exactly what the act requires, no more and no less, in line with the principle of data minimization.

The European wallet

The revision of the eIDAS Regulation adopted in 2024 turned this idea into public policy. Each member state must make at least one European Digital Identity Wallet available to its citizens and residents, on a timetable that the regulation and its implementing acts phase in from 2026. The wallet must allow people to identify themselves, store and present attribute credentials issued by third parties, and create qualified electronic signatures, free of charge for non professional use.

Three consequences matter for any signature service. First, the qualified signature stops being a product you have to buy and configure, and ends up in the pockets of hundreds of millions of people. Second, strong identification and signing can happen in a single gesture, from the same app. Third, verifiers must register and declare what data they request and why, so that the wallet can warn the person when more is being asked of them than is warranted.

BEYOND EUROPE

Wallets are not an exclusively European phenomenon. Several countries in Latin America and Asia have official identity apps, mobile driving licenses follow an ISO standard published in 2021, and the consortium that governs web standards approved the second version of its verifiable credentials data model in 2025. Names and formats vary, but the triangle architecture recurs.

Signing with a wallet

In a signing process, the wallet can play its part in two ways. In the first, it only identifies: the person presents their identity credential, the platform verifies it and records the result, and the signature is made by other means. In the second, the wallet also signs: the platform sends the wallet the document's hash, the person authorizes it

with their biometrics or PIN, and the wallet returns a qualified signature created with a key the person controls, whether on the phone itself or in an associated remote service.

In both cases the signature platform changes its role. It is no longer the one that identifies people or holds keys: it is the one that orchestrates. It requests what is needed, verifies what it receives, incorporates it into the document and records it. That change of role is one of the reasons the orchestration layer is gaining importance, and we will return to it at the end of this volume.

What is still missing

A technology that reaches mass scale brings new questions. What happens if the person loses their phone? How do you recover a wallet without opening the door to fraud? How do you verify a credential issued by a country whose trust framework is not recognized in the verifier's country? What about people who do not have a compatible phone? The rules give partial answers to each, and the experience of the first few years will fill in the rest. A prudent signature service prepares to accept wallets while continuing to offer alternatives.

KEY POINTS

Identity wallets shift trust from the intermediary to the signed credential. They make it possible to reveal only what is needed, bring qualified signatures within reach of millions of people and turn the signature platform into an orchestrator that requests, verifies and records.

Every act, its own signature.

No single signature is right for everything. What exists, for each act and in each country, is a sufficient mechanism and a provider able to deliver it. Choosing them well, and stating honestly which one was used, is the core craft of a signature service.

In the first volume we saw that the law recognizes several types of signature and that their evidentiary weight grows with their technical rigor. In the second, we saw that a signature depends on third parties to endure: certification authorities, time stamping authorities, validation services. A signature service lives where these two ideas meet. For every document, it must decide which type of signature applies and who provides it.

A decision in four steps

The decision can be laid out as a sequence of questions that move from the legal to the operational.

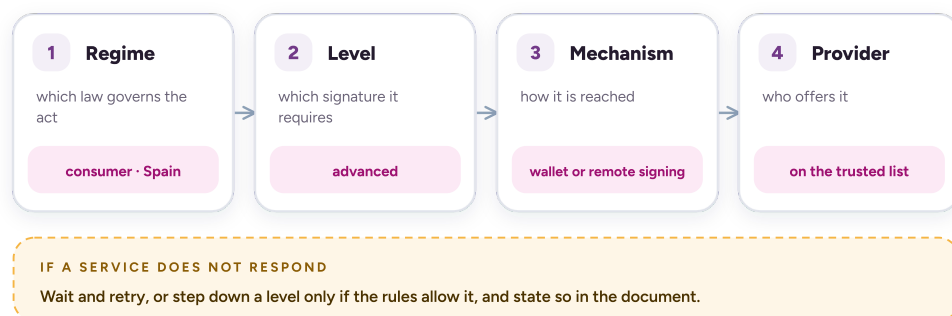


FIGURE 4 Choosing the signing mechanism, from the legal to the operational. The choice may differ for each participant in the same document.

- 1 **Which legal regime applies?** The country where the act takes effect, the countries of the parties and the nature of the document determine which law governs. A consumer contract in a European country, a deed in a Latin American country and a commercial agreement between companies on two continents are not governed by the same rules.
- 2 **What level does the act require?** Some acts accept any electronic signature; others require an advanced electronic signature; a few require a qualified electronic signature or its local equivalent, or even the presence of a notary or public officer. The level may differ for each participant in the same document.
- 3 **Which mechanism achieves it?** The same level can be reached by different routes: with a certificate on a smart card, with a remote certificate, with an identity wallet, or with the person's consent and an organization seal.
- 4 **Which provider offers it?** Finally, you must choose a trust service provider recognized in the relevant jurisdiction that offers that mechanism and is available.

The provider catalog

A service that operates in several countries needs a provider catalog: which certification authorities, time stamping authorities and remote signing providers it can use, in which jurisdictions they are recognized, which mechanisms they offer, with what levels of identity verification and at what cost. That catalog changes over time, because providers join and leave the trusted lists, change their terms or cease operating. Keeping it up to date is part of the job.

Remote signing has made this task much easier. Thanks to standardized interfaces, in particular the Cloud Signature Consortium specification and the European standards for server signing, a platform can integrate once with a protocol and work with every provider that implements it. The document never travels: the platform sends the hash, the provider identifies the person, receives their authorization and returns the signature.

Your own certificate or signature by consent

Among the available mechanisms there is one distinction worth understanding well, because it is a frequent source of confusion.

- ✓ **Signature with one's own certificate.** The person signs with a certificate issued in their name, whether on a smart card, a token, in the cloud or in their wallet. The signature identifies them directly, and its strength depends on the type of certificate.
- ✓ **Signature by consent.** The person expresses their intent on the platform after identifying themselves with the required method, and the platform applies an organization seal to the document with a certificate belonging to the organization, recording who consented and how they were identified. The proof rests on the evidence record and the organization seal, not on a personal certificate.

Both are legitimate and both have their place. Signature by consent is very common and is enough for many acts. Signature with one's own certificate is necessary when the law or the contract requires it. What is not legitimate is presenting one as if it were the other.

Declared degradation

External services fail. A time stamping authority does not respond, a revocation server is down, a remote signing provider suffers an outage. The signature service must decide what to do in those cases, and the decision is not merely technical.

There are two acceptable responses. The first is to wait and retry until the service comes back, without publishing an incomplete result. The second is to proceed at a lower level, if the act allows it, and say so: the document states what level it reached and why it fell short of the intended one. The unacceptable response is to carry on

silently, delivering a lower level signature without anyone noticing. We call the practice of stepping down a level only when the rules allow it, and recording the fact, declared degradation.

AN EXAMPLE

A document was meant to reach the archival level, with a timestamp and validation material. At closing, the provider's revocation server did not respond. The process rules allowed completion at a level with a timestamp but without revocation material. The document was closed, the certificate of completion stated the level achieved and the reason, and the platform scheduled another attempt to complete the material once the service was back.

Check before sending

It pays to avoid these problems by detecting them early. When the rules are attached to each participant, as we saw in the first chapter, the platform can verify before sending that every one of them is achievable: that a provider is available for the required mechanism, that the signer's country is covered, that the requested level of identity verification can be met. A document that cannot be completed should not go out, and the sender should know exactly what is missing and for whom.

KEY POINTS

Choosing a signature mechanism runs from regime to level, from level to mechanism and from mechanism to provider. A mature service keeps a provider catalog by country, distinguishes signature with one's own certificate from signature by consent, checks before sending and, when something fails, steps down a level only when the rules allow it, and says so.

The signature no one sees.

The most efficient signatures are the ones that happen inside other systems: the bank opening an account, the human resources system onboarding an employee, the portal selling an insurance policy. For that to work, the signature service has to know how to talk to other systems.

A signature platform used only through its own screens is useful, but limited. Someone has to export the document from another system, upload it, set up the participants, wait, download the result and load it back where it belongs. Every manual step is an opportunity for error and a cost. Integration removes those steps: the source system requests the signature, the platform manages it and the result comes back on its own.

The building blocks of an integration

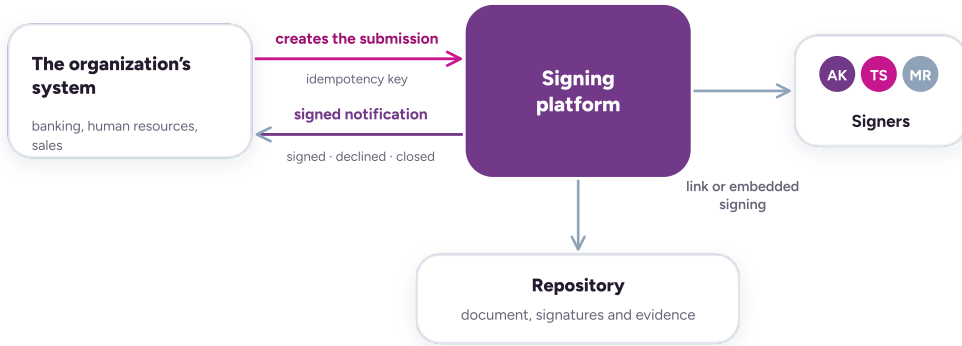


FIGURE 5 The pieces of an integration. The source system requests the signature, receives signed notifications and obtains the complete result for its archive.

The programming interface

The foundation is an application programming interface, almost always in the REST style over HTTPS, that lets systems create submissions, check their status, download documents and evidence, and manage templates and users. A good interface is documented with a machine readable specification, such as OpenAPI, which makes it possible to generate clients in different languages and to test calls before writing any code.

Event notifications

Asking over and over whether a document has been signed yet is inefficient. The alternative is for the platform to send notice: when a relevant event occurs, such as a signature, a rejection or the completion of the process, it sends a message to an address the source system has specified. These notifications, known in the trade as webhooks, must be signed by the platform so the receiver can verify that they are authentic, and they must be retried if the receiver does not respond.

Embedded signing

Sometimes the signer should not have to leave the source system. Instead of receiving an email with a link, they sign inside the bank's portal or the merchant's app, in a window provided by the signature platform. The experience is seamless, and the

evidence is still the signature platform's, which knows who acted and how they were identified.

Three properties that set a serious integration apart

- ✓ **Idempotency.** On real networks, messages get lost and get repeated. If a system sends the same request to create a submission twice because it never received the first response, the platform must recognize it and not create two. The usual technique is for each request to carry a unique key chosen by the sender.
- ✓ **Ordering and retries.** Event notifications may arrive out of order or more than once. The receiver must be able to recognize them by their identifier and rebuild the correct state, and the platform must keep retrying, with increasing intervals, until the receiver confirms.
- ✓ **Versioning.** An interface that changes without warning breaks everyone who depends on it. Mature interfaces declare their version, keep the previous one running for an announced period and document every change.

Credentials and permissions

Every system that connects needs a credential, and that credential should carry only the permissions it needs: an application that only sends documents should not be able to delete users. Credentials must be rotatable without interrupting service and revocable immediately if a leak is suspected. And every action taken with them must be logged under the name of the system that acted, just as actions by people are.

Integration without programming

Not every organization has developers available. No code automation platforms, which connect applications through visual building blocks, let a business user assemble workflows such as "when a proposal is approved in the sales system, send it for signature and, once it is completed, save it to the contract repository". For that to work, the signature service must offer connectors for those platforms, with the same guarantees as its programming interface.

Where the signed document goes

The process does not end with the signature. The document and its evidence have to reach the place where the organization keeps them: a document management system, a contract repository, an archive. Integration with those repositories, and delivery of a complete package containing the document, the signatures, the certificate of completion and the evidence record in a verifiable format, is what makes the long term preservation described in the second volume possible.

KEY POINTS

Integration means making the signature happen inside the organization's own processes. It requires a documented interface, signed and retried event notifications, idempotency, stable versions, credentials with minimal permissions, connectors for people who do not write code and complete delivery of the result to the place where it is kept.

Many customers, one platform.

A signature service rarely serves a single organization. It serves many, sometimes through resellers who in turn have their own customers. Operating this way demands isolation, customization, metering and accountability.

When a platform serves many organizations from a single deployment, each of them must feel that the platform is its own: with its own users, templates, brand and data, invisible to everyone else. This model, which the software industry calls multitenant, is economical and lets the service improve for everyone at once. But it shifts the risk: an isolation failure no longer affects one customer, but all of them.

The organization as a tree

The most general way to represent customers is as a tree. At the root is whoever operates the platform. Below it may sit resellers or partners, who in turn have customers, who in turn may have subsidiaries or departments. Each level sees and manages what belongs to it and what hangs below it, and nothing else.

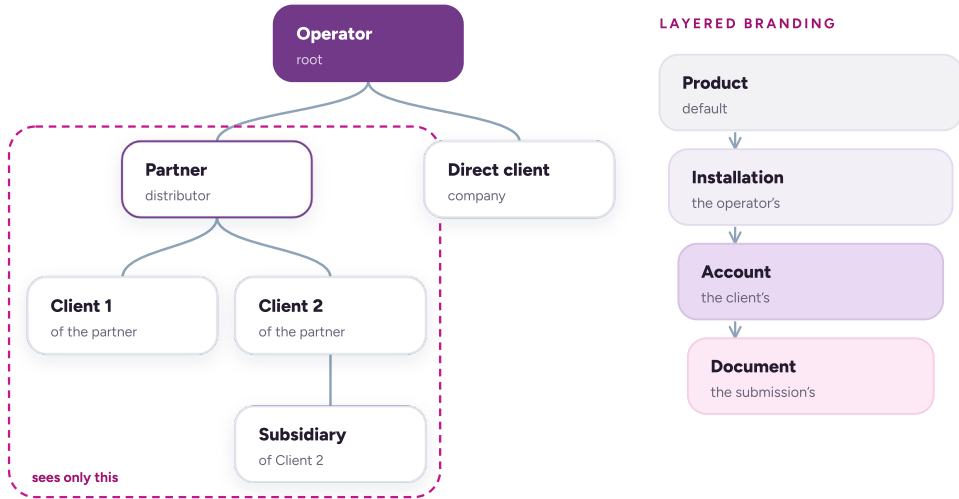


FIGURE 6 The organization as a tree. Each level sees its own and what hangs from it; branding is inherited from the top down and each layer can override it.

The tree handles very different situations with a single model: a company with one account, a group with subsidiaries in several countries, a trust service provider offering signatures to its customers under its own brand, an integrator reselling the service inside its own software.

Isolation, in layers

Keeping one organization from seeing another's data cannot depend on every developer remembering to filter every query. Serious platforms enforce isolation in several layers at once: in the application; in the database itself, through row level security rules that the database enforces even when the application gets it wrong; and in encryption, sometimes with separate keys for each customer. When the database guarantees isolation, a bug in the code produces an empty result, not a data leak.

Branding, also in layers

The signer should see the brand of whoever sent them the document, not the platform's. That calls for layered customization: at the level of the product, the deployment, each account and sometimes each document, so that each level inherits

whatever it does not define. Emails, signing pages, the certificate of completion and notifications must all respect that hierarchy, and the domains used to send email must be configured so that messages are delivered and do not look fraudulent.

Metering usage

Every document sent, every signature, every timestamp, every identity check has a cost, often paid to third parties. The platform must meter every use, attribute it to the right account in the tree and make it visible at every level. That metering is used for billing, but also for spotting anomalies: a sudden surge in submissions from one account may be a commercial success or a stolen credential.

Operating and monitoring

Whoever operates the platform needs a dedicated console, separate from the customers' own, to see the status of external services, stalled submissions, errors and consumption. Operators' actions are logged too, with the same rigor as users' actions. And security events must be exportable to each customer's monitoring systems, so their teams can see them alongside the rest of their activity.

Where the data lives

Many data protection laws, and many policies of public sector and financial customers, require knowing in which country documents are stored and who can access them. Some restrict it. A service that operates in several countries needs to be able to place each customer's data in the appropriate region and, in certain cases, to offer deployment on the customer's own infrastructure. Shared cloud, dedicated cloud and on premises deployment are three answers to the same question, each with a different balance of cost, control and responsibility.

Accountability

The customers of a signature service cannot audit it themselves. They rely on independent certifications. The most common are the international standard ISO/IEC 27001 for information security management, the control reports known as SOC 2 in the

US market and, for trust service providers in Europe, the ETSI EN 319 401 standard and those derived from it, which form the basis of supervision under eIDAS. Every certification has a scope: it is important to read what it covers and what it does not.

A USEFUL DISTINCTION

A signature platform can use the services of a qualified trust service provider without being a qualified provider itself. In that case, trust in the certificates, their issuance and their revocation is the provider's responsibility, while the platform answers for orchestration, evidence and custody of the documents. Blurring these two roles in marketing is a common and misleading mistake.

KEY POINTS

Operating at scale means serving many as if each were the only one: a tree of organizations, isolation guaranteed by the database, layered branding, metering of every use, a monitored operator console, control over where the data lives and independent certifications whose scope is understood.

Signing is an act **for everyone.**

A signature expresses intent only if the signer was able to read and understand what they were signing. Accessibility and language are not design details: they are conditions for valid consent.

Imagine a blind person who receives a contract to sign. If the signing page does not work with their screen reader, they have two options: ask someone else for help, who will see the content and may end up acting on their behalf, or give up. Either way, the promise of electronic signature, that every person expresses their own intent for themselves, is broken. The same happens to someone who does not read the language of the document or the instructions well, to someone with motor impairments who struggles to fill in a small field, or to someone who needs more time than a single use code allows.

The reference standard

The Web Content Accessibility Guidelines, known as WCAG and published by the consortium that governs web standards, are the global reference. Version 2.2, released in 2023, organizes its requirements under four principles: content must be perceivable, operable, understandable and robust. Each requirement has a conformance level, and the middle level, called AA, is the one laws usually require.

In Europe, the European Accessibility Act has applied since June 2025 to a list of products and services that includes online banking and online retail, two of the areas where people sign the most. Many other countries have equivalent rules for the public sector, and the trend is to extend them.

What it means for a signature

- The entire journey, from opening the link to confirming the signature, can be completed using only a keyboard and with a screen reader.
- Document fields have names that are announced, and errors are explained in text, not by color alone.
- Color contrast is sufficient for people with low vision, and the page adapts when text is enlarged.
- Codes and sessions allow enough time, or let users extend it, and do not require solving visual puzzles.
- Authentication does not depend on remembering or transcribing information, a requirement that version 2.2 of the guidelines made explicit.
- The PDF document itself, when it is generated, is accessible: it has structure, a reading order and alternative text for images.

The language of consent

Language is a form of accessibility. A service that operates in several countries must offer its interface, its emails, its legal notices and its certificate of completion in each participant's language, and the evidence record must store the language in which each participant saw the texts they accepted. A single document may have participants who speak different languages: there is one contract, but each person's experience should be their own.

Translation is not just a matter of swapping words. Dates, numbers, currencies and name formats vary from country to country. Legal texts must be reviewed by professionals in each jurisdiction. And machine translation, however useful, is not good enough for the texts a person accepts as part of their consent.

Plain language

A text can be in the right language and still be incomprehensible. The plain language movement, promoted by several governments and by an ISO standard published in 2023, advocates writing so that readers can find, understand and use information the

first time. In a signing process, that means short instructions, buttons that say what they do and notices that explain the consequence of each action. Signing should not require knowing what an advanced electronic signature is.

KEY POINTS

Consent is valid only if the person was able to perceive, understand and act for themselves. The WCAG guidelines at level AA, each participant's language recorded in the evidence, and plain language are part of what makes a signature valid, not an extra.

When a machine signs.

Artificial intelligence already drafts documents, reviews clauses and fills in forms. Soon it will act on behalf of people and companies. The question is not whether it will take part in signing, but how to prove what it did and who answers for it.

The signature was born to attribute an act to a person. For centuries, the question was whether that person was who they claimed to be. Artificial intelligence systems add a new question: whether it was the person who acted or a system on their behalf, and under what authorization. This chapter surveys the uses that already exist, the ones being built, and the principles that make it possible to adopt them without losing the proof.

Helping the sender

The most immediate use is on the sender's side. An assistant can read a document and suggest where the signature and data fields go, who should sign and in what order, and what level of signature the type of act requires in the relevant country. It can spot a missing page, two amounts that do not match, or a clause that contradicts an approved template. In every one of these cases the machine proposes and a person decides, and the record should distinguish what was suggested from what was accepted.

Helping the signer

On the other side, an assistant can explain to signers, in their own language and in plain words, what they are signing: their obligations, deadlines and costs. It is a powerful promise for understanding and accessibility, and also a risk: if the explanation is wrong, the person may consent to something other than what they believed. That is why the explanation must be presented as what it is, an aid, and the record must keep what the person was shown, just as it keeps the legal texts they accepted.

Agents

One step further are agents: systems that do not merely answer questions but carry out actions in other systems. Open protocols published since late 2024 let an agent use a platform's functions in the same way a traditional integration would: create a send, check its status, download the evidence. In that scenario, the person says "send this agreement to the three partners for signature" and the agent does it.

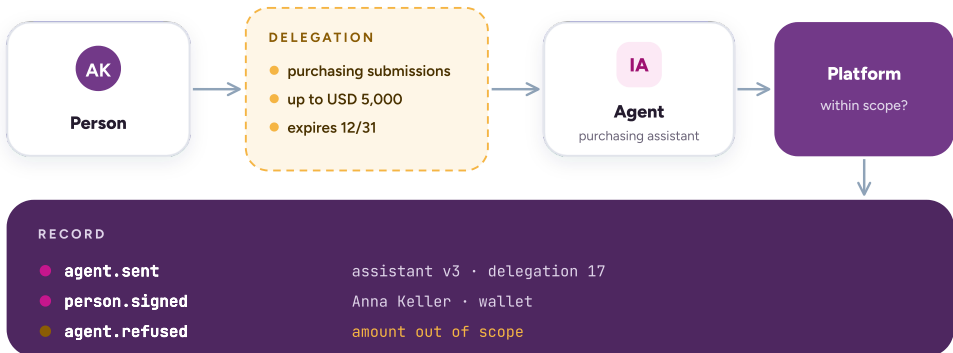


FIGURE 7 An agent acting for a person. The delegation sets the scope, the platform checks it on every act and the record tells the machine apart from the person.

An agent that prepares and sends documents raises few new problems if it is treated like any other integrated system: with its own credential, minimal permissions and a record of every action. An agent that signs on behalf of a person is another matter. It requires answering three questions.

- 1 **Who authorized it?** There must be an explicit delegation, from an identified person, with a defined scope: what kind of documents, up to what amount, for how long.
- 2 **Did it act within that authorization?** The platform must check the scope on every act and reject whatever exceeds it, rather than simply trusting the agent.
- 3 **How is it distinguished in the proof?** The signature and the record must make clear that an agent acted, which agent, under what delegation and on what instruction. A signature made by a machine that appears to have been made by a person is a forgery, even if the person authorized it.

The regulatory framework

The European Union's Artificial Intelligence Act, adopted in 2024, sets out obligations that scale with the risk of each use, including transparency obligations when a person interacts with an artificial intelligence system. Other countries are moving ahead with their own laws and guidance. At the same time, the organization seal (the “electronic seal” of eIDAS), which we saw in the first volume as the signature of an organization, offers an existing tool for attributing automated acts to the entity responsible for them. Practice will probably combine both: organization seals for the acts of an organization's systems, and explicit, recorded and limited delegations for the acts of agents that represent people.

Principles for adopting artificial intelligence

- ✓ **The machine proposes, the person decides**, unless there is an explicit, limited and recorded delegation.
- ✓ **Every act by a machine is recorded** as an act by a machine, with its identity, its version and the instruction it received.
- ✓ **What is shown is kept**: summaries, explanations and suggestions are part of the evidence.
- ✓ **Document data is protected** from the models as well: what is sent, to which provider, in which region, and whether it is used for training.
- ✓ **Responsibility has a name**: behind every agent there is a person or an organization that answers for it.

KEY POINTS

Artificial intelligence can prepare, explain and execute, and that improves signing processes. But a signature is still the attribution of intent. Every act by a machine must be recorded as such, every delegation must be explicit and limited, and there must always be someone who answers for it.

Before the machine arrives.

Quantum computers capable of breaking today's cryptography do not exist yet. But the signatures we make today must remain verifiable thirty years from now. That is why the transition has already begun.

In the first volume we saw that digital signatures rest on mathematical problems that today's computers cannot solve in a reasonable time: factoring enormous numbers, in the case of RSA, or computing discrete logarithms over elliptic curves. In 1994, the mathematician Peter Shor described an algorithm that, run on a sufficiently large quantum computer, would solve both problems efficiently. No one has built that machine yet, and experts disagree on when it might exist. But its mere possibility is enough to change planning.

Why it matters for signatures

For encryption, the threat is immediate: an adversary can store encrypted communications today and decrypt them tomorrow. For signatures, the threat is different. A quantum computer would make it possible to forge new signatures with current keys, but it would not alter signatures already made. The risk, then, is that in the future no one will be able to tell an authentic signature from 2026 apart from a forgery made in 2040 with the same key.

We already know the answer from the second volume: archive timestamps. If, before current algorithms become insecure, a timestamp using a resistant algorithm is applied over the signature, that timestamp proves the signature existed when it could not yet be forged. Timestamp renewal, designed for the gradual obsolescence of algorithms, is also the defense against a sudden leap.

The new standards

In 2016, the United States National Institute of Standards and Technology launched an international competition to select algorithms resistant to quantum computers. After several rounds of public analysis, in August 2024 it published the first final standards. Two of them are for signatures: FIPS 204, based on problems over lattices, and FIPS 205, based solely on hash functions. A third signature algorithm, also based on lattices and with more compact signatures, is going through standardization.

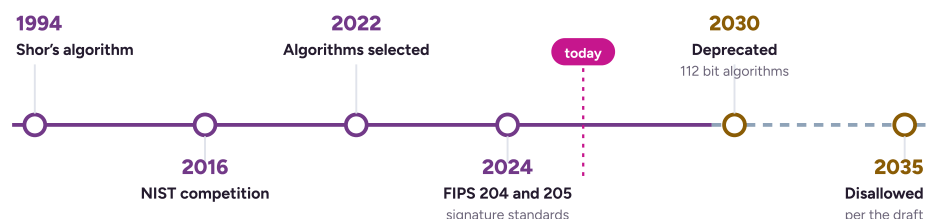


FIGURE 8 Milestones of the post quantum transition. The 2030 and 2035 dates come from a draft and may change.

That same year, the institute published a draft transition timeline that proposes deprecating current signature algorithms offering 112 bit security from 2030 and disallowing them from 2035. European cybersecurity agencies have published roadmaps with similar horizons. The dates may change, but the direction is clear.

What changes in practice

Larger keys and signatures

Post quantum algorithms have keys and signatures considerably larger than today's: from a few hundred bytes they grow to several thousand, and in some cases to tens of thousands. For a PDF with several signatures, certificate chains and timestamps, that means heavier files. For devices with little memory, such as some smart cards, it can be a real limit.

The whole chain must migrate

A post quantum signature is only as strong as its certificate chain, its timestamp and its revocation material. The transition involves certification, timestamping and validation authorities, device manufacturers, PDF readers and trusted lists. None of them can do it alone, and for years both worlds will coexist.

Hybrid certificates

For that coexistence, hybrid certificates and signatures are being studied, combining a current algorithm with a post quantum one so that the signature remains verifiable by older software while being protected for the future. Standards bodies are working on their formats, and the first implementations in document signing are likely to adopt one of these forms.

Crypto agility

The most important lesson of the transition is not an algorithm but a property: crypto agility. A system is agile when it can change algorithms without being redesigned, because it never took any particular algorithm for granted. In a signing service, that means knowing which algorithms each provider uses, being able to choose among several, recording in the evidence which algorithm was used at each step, and keeping an inventory that makes it possible to find every document protected by an algorithm that is weakening.

READINESS CHECKLIST

- Inventory where each algorithm is used: signatures, timestamps, chains, records.
- Make sure long lived documents reach the archive level and carry renewable timestamps.
- Require providers to have a transition plan with dates.
- Test formats with large signatures before you need them.
- Record the algorithm in every event in the evidence.

KEY POINTS

Quantum computing threatens our ability to tell authentic signatures apart from future forgeries. The defense combines archive timestamps renewed in time, new algorithms that are already standardized and, above all, agile systems that can change algorithms without being rebuilt.

What we built with these ideas.

Throughout three volumes we have avoided naming products. In these pages we make an exception, the only one in the series: we describe the platform developed by the publisher of these notebooks and the problems from this volume that it addresses.

A NOTE BEFORE READING

This epilogue is not neutral, and it does not pretend to be. It is written by those who build the product it describes. We have tried to hold it to the same standard as the rest of the series: to state only what can be verified and to say what the product does not do as well.

What Signing Flows is

Signing Flows is an electronic signature service for PDF documents. The sender uploads a document, chooses who must act and in what order, places the fields and sends it. Each participant receives a link, does their part in the browser, and the service closes the document with the evidence that accompanies it.

Its unit of work is the circuit: a document, its people, the way it travels and the rules that govern it. A circuit can run in sequence, in parallel or as individual copies, the patterns we described in the first chapter. Each person has a role: signs, approves without signing, reviews without signing, or only receives a copy.

Three ideas from this volume lie at its foundation. Rules belong to the person, not to the document: for each participant the service defines how they sign, with their own certificate or by consent with a platform seal, what level of identity is required of them and what they can do with the document; and a document that asks someone for something the account cannot provide is not sent, and it states for whom and what is

missing. The organization is a tree, with isolation enforced in the database itself and layered branding, so that signers see the brand of whoever is writing to them. And nothing is claimed that the evidence does not support.

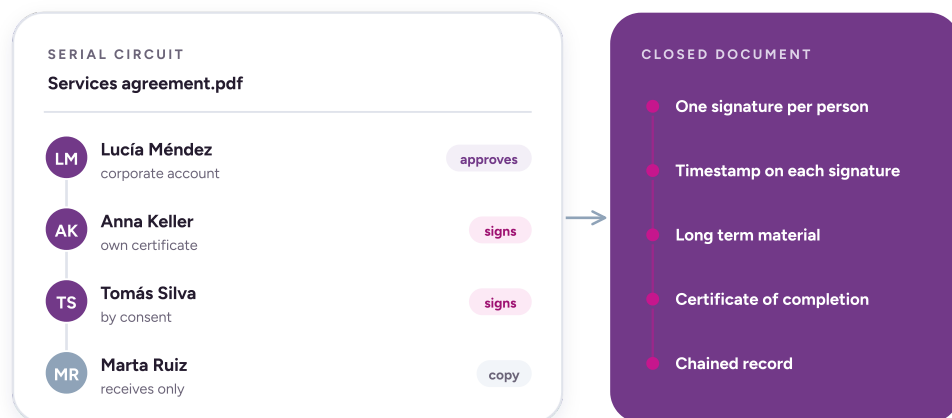


FIGURE 9 A Signing Flows circuit and what the document carries when it closes.

What a closed document carries

- ✓ **One signature per person**, each over the state of the document at the moment that person signed.
- ✓ **A timestamp on each signature**, requested from the configured timestamping authority.
- ✓ **Long term preservation material**: the certificate chain and revocation information for each signature, and a timestamp over the finished file. With a timestamping authority and reachable revocation sources, the document reaches the PAdES archive level (LTA), as measured by the European Commission's validator; without them, it remains at a lower level and says so.
- ✓ **A certificate of completion**, issued only once, carrying the platform seal, in Spanish and English.
- ✓ **A chained evidence record**, in which each event is linked to the previous one by its hash.

What it does not claim

We think a list of what a product does not promise is more useful than a list of its virtues. These are some statements Signing Flows does not make about itself, and why.

THE STATEMENT	WHY NOT
"Once signed, it cannot be modified"	Later permitted changes coexist with earlier valid signatures. Each signature covers the document as it was when signed.
"We are a trust service provider"	It uses the services of one. Trust in the certificate, its accreditation and its revocation are the provider's responsibility.
"We never hold private keys"	With remote signing providers, the key stays with the provider. With the local engine, the platform keeps a key in a file.
"The validator says valid, so nobody altered it"	A validator's default policy can approve a file in which a locked field was rewritten.

In its console, capabilities that an installation does not have enabled appear grayed out, with the reason shown and no dates.

Why now

The chapters of this volume describe a fundamental shift. For twenty years, the industry's question was how to sign. Today signatures are available in many forms and from many providers, and they will be even more so when the European Digital Identity Wallets put qualified signatures in every citizen's pocket. The question becomes how to orchestrate: which signature to request from each person, from which provider, with which identity, and how to prove it afterward. Five forces push in that direction.

- **Identity has become portable.** Wallets, national identities and verifiable credentials multiply the ways of identifying a person, and someone has to choose and record the right one for each act.

- **Legal regimes are national; processes are not.** A single contract crosses countries with different laws and providers, and the rule has to live with each participant.
- **Trust service providers are looking for distribution.** They need platforms that bring their services to organizations of every size, under their own brand and with their own tree of customers.
- **Artificial intelligence is entering the process.** A layer that records every act and distinguishes people from machines makes it possible to incorporate it without losing the proof.
- **Cryptography is going to change.** The post quantum transition rewards those who record in the evidence which algorithm they used at each step and can renew their archive timestamps in time.

Signing Flows was designed from the start to orchestrate those pieces, rather than to sign with a single mechanism.

Where it comes from

Signing Flows is the result of a long shared evolution. Members of Interfase, the Uruguayan company that publishes these notebooks, have worked with digital certificates and public key infrastructure since 2000. A pioneer of public key infrastructure, whose origins go back to the first commercial products in the field in the mid 1990s, has worked alongside Interfase through much of the history these volumes recount, and Signing Flows is now part of its citizen identity orchestration offering.

It seemed fair to close the series this way: with the record that the ideas described in these pages are not only theory, and with an invitation to verify them.

Glossary

The main terms in this volume, in the sense in which they are used here. The basic concepts are in the glossaries of volumes 1 and 2.

Agent

An artificial intelligence system that carries out actions in other systems on behalf of a person or organization.

Crypto agility

The ability of a system to change cryptographic algorithms without being redesigned.

Declared degradation

The practice of completing a process with a lower level of signature than planned only when the rules allow it, recording the level achieved and the reason.

Delegation

An explicit, limited and recorded authorization for another person or a system to act on someone's behalf.

Digital identity wallet

An application in which a person stores credentials issued by third parties, and from which they can present them and, in some cases, sign.

Embedded signing

Signing that takes place inside another organization's application, in a window provided by the signing platform.

Hybrid certificate

A certificate that combines a current algorithm with a post quantum one, so that it works with older software and resists quantum computers.

Idempotency

The property of an operation that produces the same result even when it is repeated several times.

Levels of assurance

Scales that rate the strength of a person's identification, such as the low, substantial and high levels of eIDAS.

Multitenant

A model in which a single software installation serves many organizations, with their data isolated from one another.

Orchestration

The coordination of people, providers, mechanisms and systems so that a signing process is completed and its proof secured.

Provider catalog

An inventory of the trust service providers a service can use, with their jurisdictions, mechanisms, levels and conditions.

Row level isolation

A security rule that the database applies to each row, so that each organization can see and modify only its own data.

Selective disclosure

The ability to present only some attributes of a credential, or a claim derived from them, without revealing the rest.

Signature by consent

A mechanism in which a person expresses their intent after identifying themselves and the platform applies an organization seal to the document, recording who consented and how.

Verifiable credential

A set of claims about a person, signed by its issuer, that the holder keeps and presents to whoever needs it.

Webhook

A notification that a platform sends to another system when an event occurs, signed to prove its origin and retried if it is not acknowledged.

REFERENCE

Further reading

The regulations, standards and documents cited in this volume, grouped by topic.

Identity and wallets

European Union. Regulation (EU) 2024/1183, amending Regulation (EU) No 910/2014 and establishing the European Digital Identity Framework.

NIST. Special Publication 800 63, Digital Identity Guidelines, revision 4.

W3C. Verifiable Credentials Data Model, version 2.0, 2025.

ISO/IEC 18013 5, mobile driver's licenses, 2021.

Remote signing and providers

Cloud Signature Consortium. API specification for remote signing, version 2.

ETSI. TS 119 431 and TS 119 432, server signing. CEN. EN 419 241, trustworthy systems supporting server signing.

Integration

OpenAPI Initiative. OpenAPI Specification, version 3.

Operations and security

ISO/IEC 27001, information security management systems, 2022.

AICPA. Trust Services Criteria for SOC 2 reports.

ETSI. EN 319 401, general policy requirements for trust service providers.

Accessibility and language

W3C. Web Content Accessibility Guidelines (WCAG) 2.2, 2023.

European Union. Directive (EU) 2019/882, the European Accessibility Act.

ISO 24495 1, plain language, 2023.

Artificial intelligence

European Union. Regulation (EU) 2024/1689, the Artificial Intelligence Act.

Post quantum cryptography

Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

NIST. FIPS 204 and FIPS 205, post quantum digital signature standards, August 2024.

NIST. IR 8547, draft on the transition to post quantum cryptography, 2024.

Rúbrica.

NOTEBOOKS ON SIGNATURE, IDENTITY AND DIGITAL TRUST

A signature is an instant. A signing service is everything that makes it possible.

This third volume explains how a signing service is designed, integrated and operated: the processes, the identity of the signer, digital wallets, the choice of providers, integration with other systems, operation at scale, accessibility, and what artificial intelligence and post quantum cryptography change.

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.