

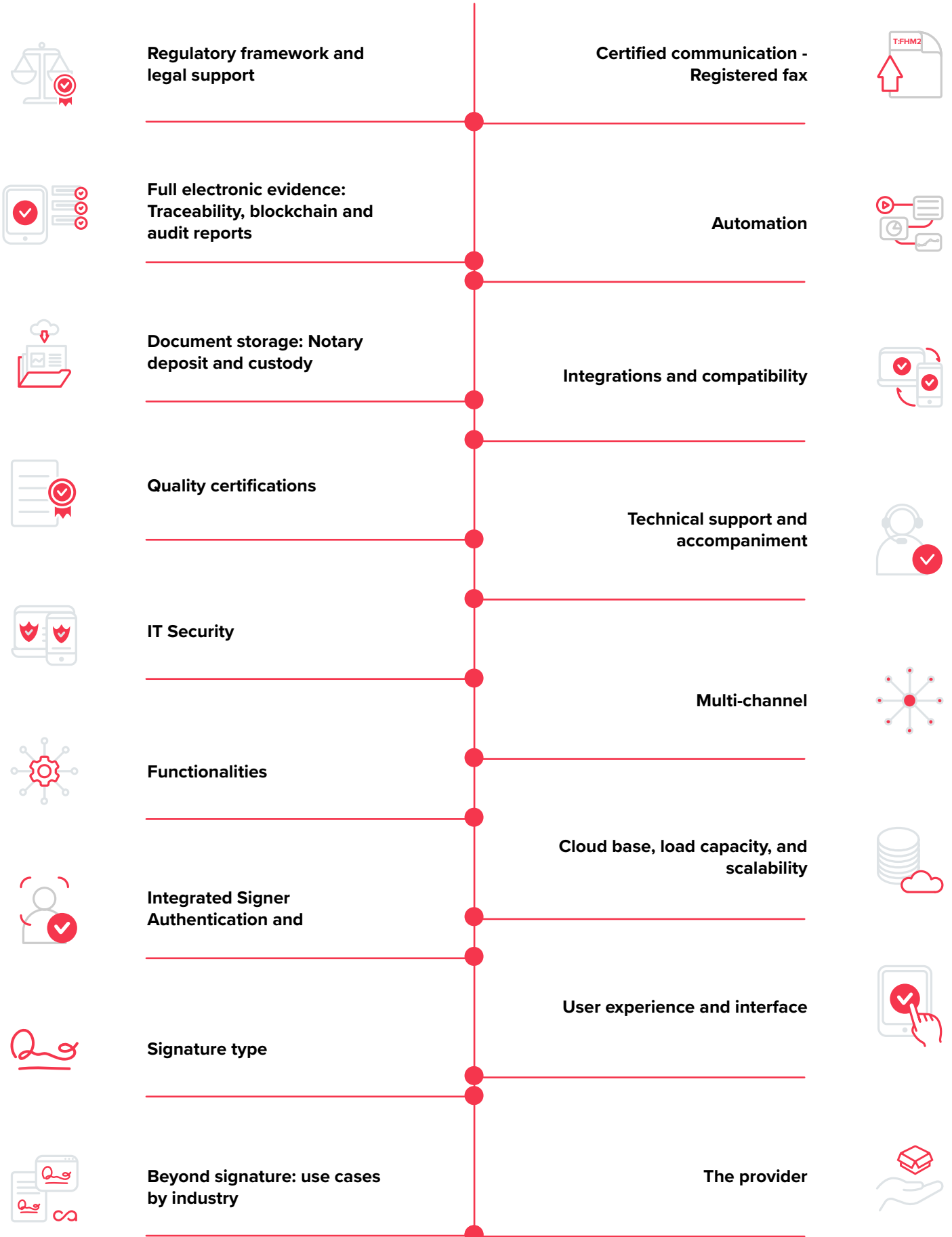
# Everything you need to know about how to choose the right electronic signature solution

---

**tecalis**

[tecalis.com](https://tecalis.com)





# How to choose an electronic signature solution

Considering the **wide variety of electronic signature solutions** on the market, it would be natural to conclude that they all offer more or less the same value and work similarly. However, this is far from being the case.

**The requirement for a partner** to provide a digital signature solution has now become mandatory for **virtually any business or organization**, regardless of its size and industry. There are many, and very different, digital signature service providers, so it is normal to feel somewhat overwhelmed and confused when choosing an electronic signature provider.

Looking **for an application to sign documents requires analysis and evaluation of the opportunity cost** because here the saying “cheap is expensive” can apply as much or more than in any other important decision for our business.

The following are not only the 3 or 4 considerations that other providers choose in a self-interested way, but all the **criteria and key points to take into account that no one details** in order to properly select the electronic signature solution that can meet the needs of a business or organization:



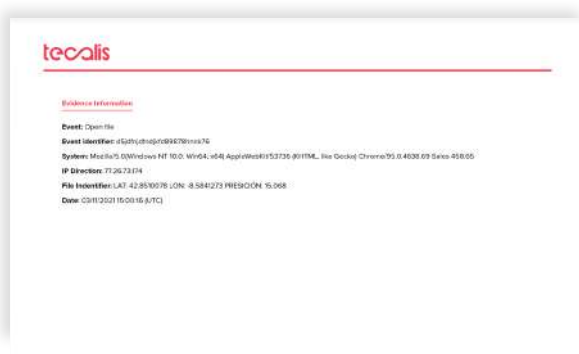
## Regulatory framework and legal support

The exercise of the electronic signature is completely **subject to the legal aspects that regulate how it should be produced**. Is the reference framework for electronic signatures not only at the European level but also the standard referenced by the regional norms of each state around the world.

The electronic signature solution provider must be a certified **Trust Services Provider** and must guarantee that the electronic signature complies with the technical standards set by eIDAS. The **GDPR** is also very important, as data processing is of particular relevance in electronic signature processes. Likewise, **the solution must be certified by an external auditor**.

The regulatory support does not end here and is due to the fact that after the exercise of the signature according to the most demanding standards, **all the activity must be recorded to have support** in case it is needed. This is commonly known as electronic evidence.

Contact an expert in regulatory compliance and analyze the regulatory needs of your industry regarding the use of electronic signatures.



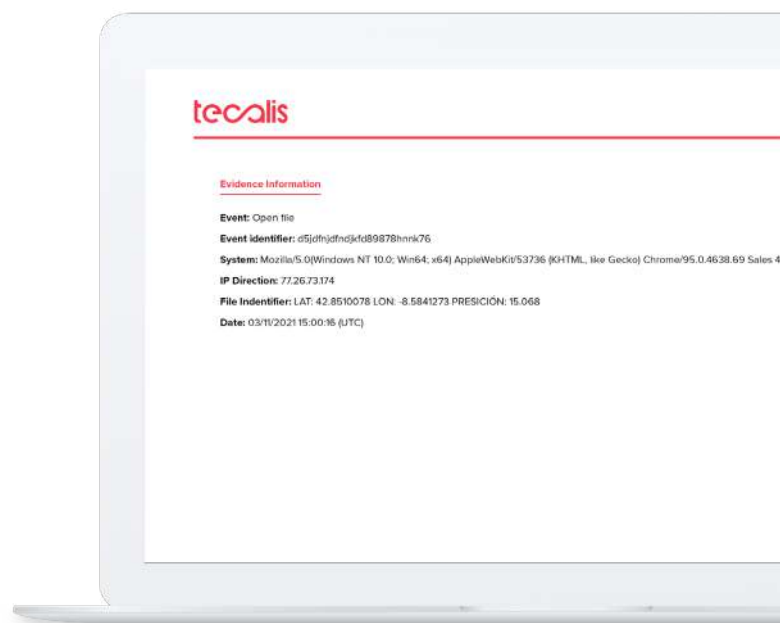
## Full electronic evidence: Traceability, blockchain and audit reports

We continue answering the question of how to choose the best electronic signature solution or application: **electronic evidence** in the signing process is a crucial point.

All data, signed documentation, technical attachments on the signature, and other relevant information must be sealed and encrypted with a timestamp endorsed by a **Certification Authority**. The digital signature solution must be robust and capable enough to collect as much information and quality electronic evidence as possible. **The more record, the more support**.

Not all digital signature applications are capable of performing a **complete trace of actions**, and even less than **this occurs under an end-to-end application encrypted by blockchain**.

After this, it should be possible to **issue an electronic evidence document** as a **full report** of the signing process in order to **formalize its technical and legal support**. In this way, when audits must be carried out,



either because the company wishes to do so or because an organization or institution **requests** it, the reports can be presented for the performance of these audits.

## Document storage: Notary deposit and custody

After the electronic signature execution, it must be **securely stored** and made **available** to both the parties and the requesting company. The electronic signature provider chosen should guarantee **at least 5 years of custody on the documentation and the signature process**.

This **document service** must be **reliable** and available at any time, including signed documentation, attachments, electronic evidence report, and audit reports.

In addition to this service, a protocol can be included for the system to provide legal validity to the process through a notarial endorsement. This allows the generation of a notarial act that accredits both electronic signature and certified communication in case of dispute or claim.

## Quality certifications

In addition to the electronic signature solution complying with eIDAS and GDPR regulatory standards, it must be **able to be customized by the provider to comply with any of the regulations of a sector or region**.

Beyond legality, solutions must be **tested and endorsed by independent institutions**. Certifications such as **ISO 9001, ISO 27701, and IQnet certification** should be tracked.

## IT Security

**SMS, eMail, token, PIN, biometrics...** Different authentication methods can be combined to **establish MFA security**. Securing the signature process is a must.

Complying with the standards of the aforementioned certifications will guarantee extended security, with the maximum guarantees of the privacy and security policies required for processes of this type.

Likewise, the supplier must confirm that its systems are secure and unhackable, auditing the solution to demonstrate that its technological capacity regarding security is of the highest level

## Functionalities

The functionalities of the chosen electronic signature platform will be those **that determine what we can and cannot do with the tool**. A digital signature solution will not be useful if it does not have the features required by our business, even if it complies with the highest regulatory standards.

Therefore, it is important that it is **versatile**, constantly updated, and evolving, and that it allows performing any action that may eventually be needed:

### Templates and layouts

Most of the time, the documentation to sign is not dynamic. It is very important to have the possibility of **embedding templates on different documents by distributing fields on a static document**. Otherwise, the document could not be signed with this electronic signature solution.

Equally, for dynamic documents, it is often necessary to **add layouts to load additional fields** that were not originally included in the

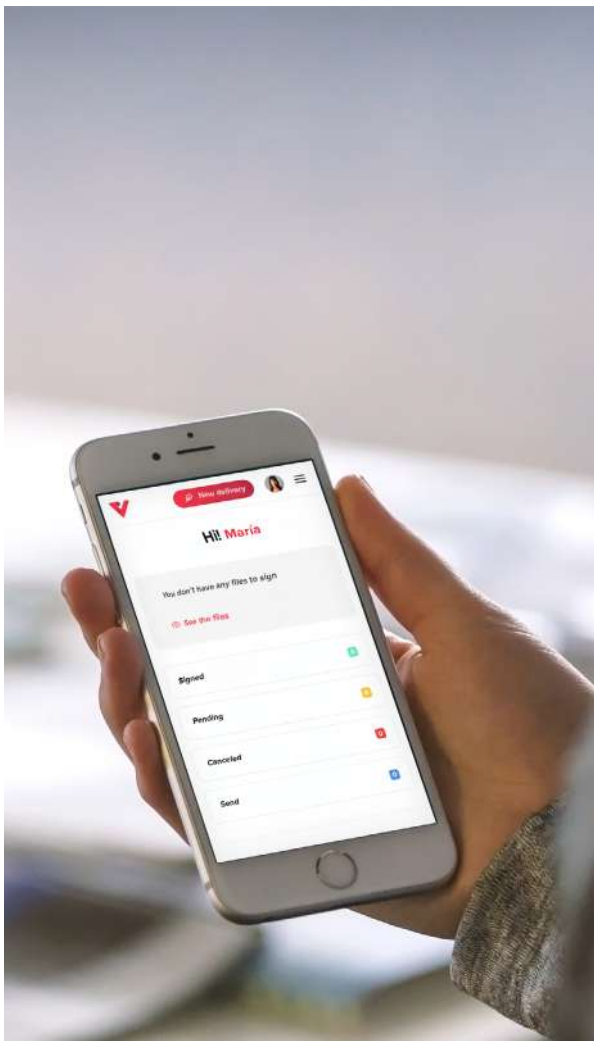
document. Optional, mandatory, or auto-filled fields; we must be able to do whatever we want with the document to sign to avoid headaches and wasted time later on.

## Collaborative documents: comments and edits

For the finalization and closing of many agreements, the signatory must be able to **comment on certain clauses, collaborate in the drafting of the document, and resolve doubts** in the process.

## Sendings

Choosing a powerful electronic form tool means choosing a tool that offers a wide variety of options concerning deliveries.



Being able to send the document **without a previous signatory, send it in bulk or sequentially, program time and date**, or set an **expiration date** for the signature are basic elements, but not all electronic signature solutions offer them. Automatic forwarding of reminders and requests must be present.

After the signature process, a not widespread important feature is that **a copy is automatically sent as an email attachment**. Instead of having to download the document through a link, it is more agile to have it attached to the confirmation email.

## Observer and validator

Additional figures to those of signatory and applicant are necessary in many cases. For example, the company's **legal department** should be an observer at the signing, keeping a record, and registering the agreement.

Similarly, there may be a **validator**, who must **unblock the signing process once the document has been approved** (lawyers, notaries, legal departments...).

## Payments

The signatory can be asked to make a **payment before or after the signing process**. This is very useful and speeds up many steps in contracting processes. A **unique functionality that makes the difference**.

## Delegation and interlocution

The person receiving the signature request **may delegate the signature to another person**. On the other hand, the **interlocutor** can forward the signature request to the person who is responsible for signing, for example, an inter-company agreement.

Discover here in detail all the features of the most functional electronic signature solution on the market.

## Integrated Signer Authentication and Identification (KYC)

This “star feature” is the icing on the cake when choosing an electronic signature solution. **Identity verification** is the process by which we certify that **a person is really who they say they are**.

Known in many industries, especially the financial and related sectors, as **Know Your Customer**, the **integration of this process prior to signing** adds further support. This becomes necessary in sensitive operations and industries where, by regulation, it is necessary to perform this process according to the highest technical and security standards.

Not only will we be ensuring that the person who signs is the one who should do so, **avoiding identity fraud**, but also that he/she will be able to **perform operations of any nature remotely** and sign agreements that carry a **high-level risk**.

## Signature type

**Simple, advanced, qualified, advanced with biometrics, signature with KYC...** We can count by thousands the messages that bombard us with these terms.

The best recommendation that can be made in this regard is that an **expert in electronic signature and knowledgeable in the field of electronic signatures** should be able to **provide you with the best possible solution for your needs**.

The answer is clear: **you should not use a signature type that falls below the support you need**, but it is neither productive nor necessary to spend resources on a **complex and expensive type of signature that your activity and business do not require at all**. If the supplier can offer the points we have discussed regarding regulatory support, storage, and electronic evidence in practically all cases, it is unnecessary to use a qualified signature.

Contact Tecalis and an expert in electronic signature solutions will evaluate your needs and propose a tailored plan for your business and activity.

## Beyond signature: use cases by industry

Is your provider **specialized in your sector of activity**? When we are wondering which e-signature solution to choose, we have to take into account that the provider must know your industry. Many solutions are based on a basic format that does not meet the specific needs of the user’s industry.

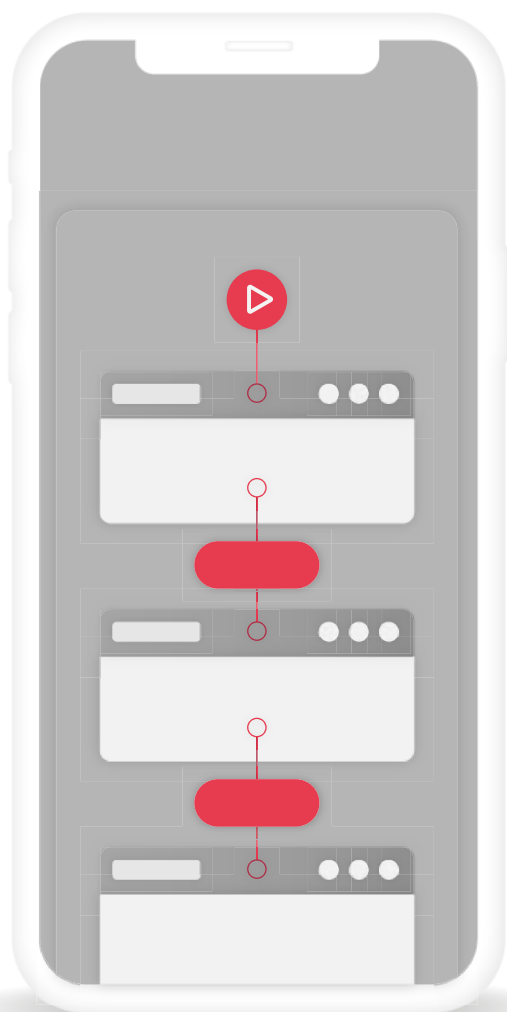
Employee onboarding, customer onboarding, hiring, acceptance of conditions, medical acceptance, consents, notifications on rate changes... This is a minuscule sample of the use cases that can occur, **having an electronic signature provider that is a specialist is crucial for the solution to adapt to your operations**.

## Certified communication - Registered fax

Not all electronic signature solutions have - **as standard and integrated** - a **certified communication service**.

Only the most powerful ones are able to reach a higher validity than the registered fax. Having **a guarantee of non-repudiation, traceability, instant reception, sending and validation, as well as sealing and proof certificate in sending, delivery and reading** are key points in certified communication services.

[Click here and learn more about certified communication services.](#)



## Automation

Simple and convenient automation could be considered an additional functionality, since **not all solutions have the possibility of automating flows and actions related to the signature and its additional steps**, and, of those that do, the vast majority require IT experts to do so. **Full automation capability** must be available, **linked to the client's own applications, systems, and operations**.

The ideal is to have an e-signature provider that facilitates both perspectives: a complete and customizable **API integration** or the use of the solution through its **own native platform developed by the provider**. In either case, automation must be present.

## Integrations and compatibility

As we have been saying, the way of integrating the solution is an important decision that must be adapted to our organization and users. API or native platform, which should we choose? Both.

Signature requests must be able to be launched automatically from the company's business applications without human intervention.

In this sense, a good **integration capability** is necessary. Not all eligible e-signature solutions can be **integrated in a matter of minutes into the organization that needs to use them**, without the need to initiate a complete project to get the tool up and running.

The e-signature solution offered by the vendor must be able to **connect with the customer's systems and applications, including their CRM or CRP**. Likewise, it must be available for ad-hoc integrations if necessary.



SAP, SalesForce, Oracle, Navision, Office 365, Google Suite... **compatible with any environment, tool, and operating system.** We must take this into account for the actuality and how ready is the signature solution in case we would like to start working with a new system.

**Download here detailed information about systems and integration models for electronic signature and identity verification services.**

## Technical support and accompaniment

In this sense, it is important that the supplier does not leave us to our own devices after choosing the electronic signature solution. Knowing that we can count on their **support, backing and accompaniment** is crucial, **guiding us through the integration process, helping us with the implementation in the channels, and resolving both usage and technical doubts.**

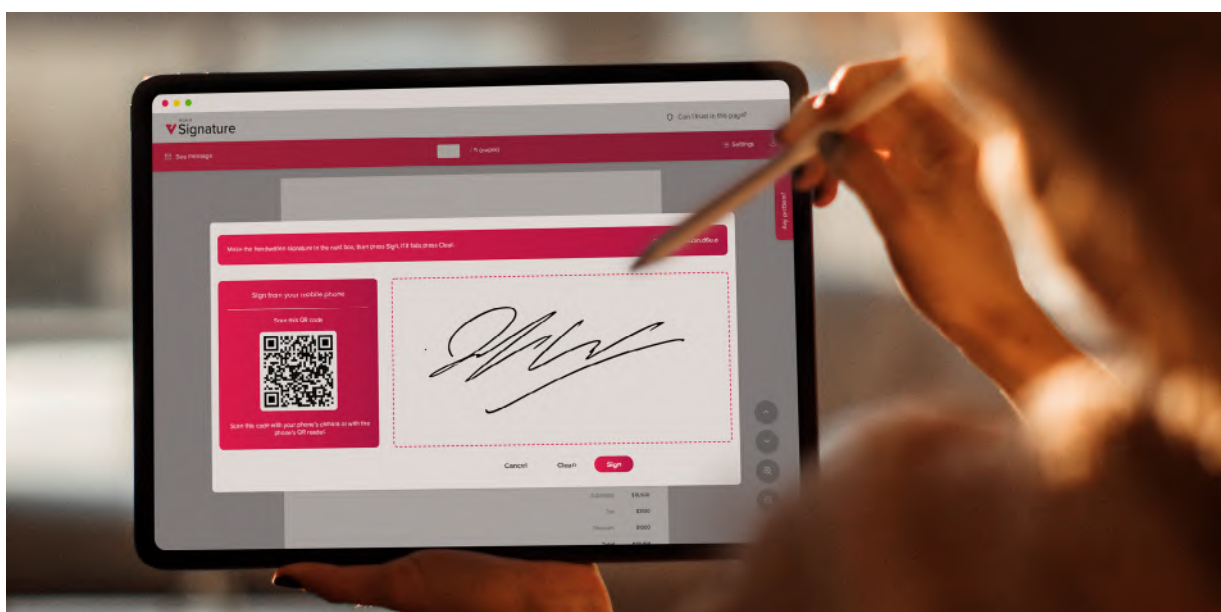
## Multi-channel

The electronic signature tool must be prepared to **work in any imaginable channel and device:** desktop computers, tablets, mobile ... and within these both through the client's apps and the internet browser.

We do not know what **device, operating system, or web browser** uses the person to whom we send the signature request, so it is essential that it can be done on any device without problems and with agility.

Something much less common is its integration in the systems applied in points of sale or commercial offices. Only the best electronic signature solutions can be easily integrated into supports such as **Wacom, tablets, POS, Kiosks or smart pads, ATMs, among others.** From the client's platform or systems, it must be possible to send the signature request to a device in the client's commercial network, so that the signature can also be made in person.

In the same way, multiple ways of sending the signature request with total guarantee and maximum security must be ensured, **not only by email** but also by **SMS, WhatsApp, Slack, and similar services.**



## Cloud base, load capacity, and scalability

It might seem obvious, but not all signature solutions work in the cloud. This ensures that the solution is operational under any circumstances and reduces the risk of crashes or hangs.

Cloud-native technologies are characterized by the use of containers, microservices, serverless functions, development pipelines, infrastructure expressed as code and event-driven applications. Advanced, future-proof development is, without any doubt, cloud development.

The solution must be **scalable**, ensuring that it grows and evolves with our business, **supporting the load of users** that make use of it at the same time with agility and without any problem.

## User experience and interface: a crucial factor in agile contracting processes

Many deals fail to close due to friction in

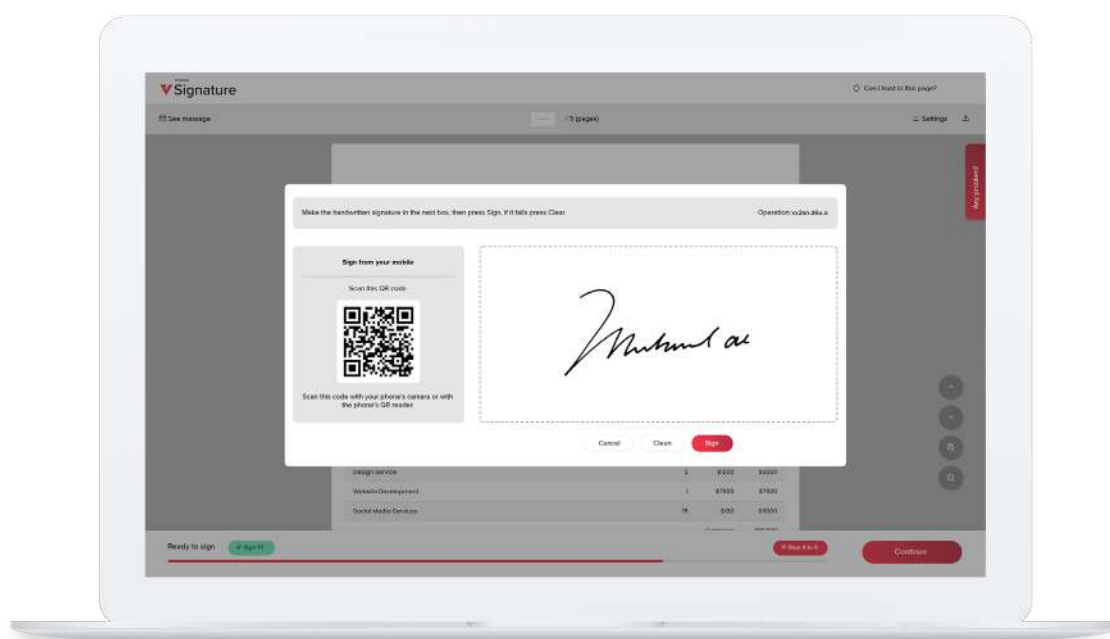
**the signing process.** It is crucial the chosen e-signing solution provides signers a top-notch UX/UI experience that is agile and conveys the desired image, guiding the user through a fast, smooth process that urges them to sign.

The messages we send are crucial in certain phases of signature-related processes. It must be versatile and be able to adapt to the **branding, design, and communication of operations according to the company or institution**, without generating an exaggerated gap between the web interface, application or client system, and the electronic signature provider.

## The provider

As we already mentioned in the “use cases by sector” point, it is important that the **provider is a specialist**, not a mere “solution seller”. This will ensure that your electronic signature is able to adapt and include all the functionalities that your business or organization needs, regardless of the nature of your activity.

Beyond that, the **seriousness** and positioning of the provider are important aspects when



choosing an electronic signature. The **ability to offer** all of the above points, support, and that they provide **follow-up and monitoring**, such as a final **evaluation of the integration**, **are points to take into account**.

Consulting their website, **assessing the treatment offered by their experts** and **specialized advice**, consulting their **activity in the different social channels** can give us an idea of the type of company we are dealing with.

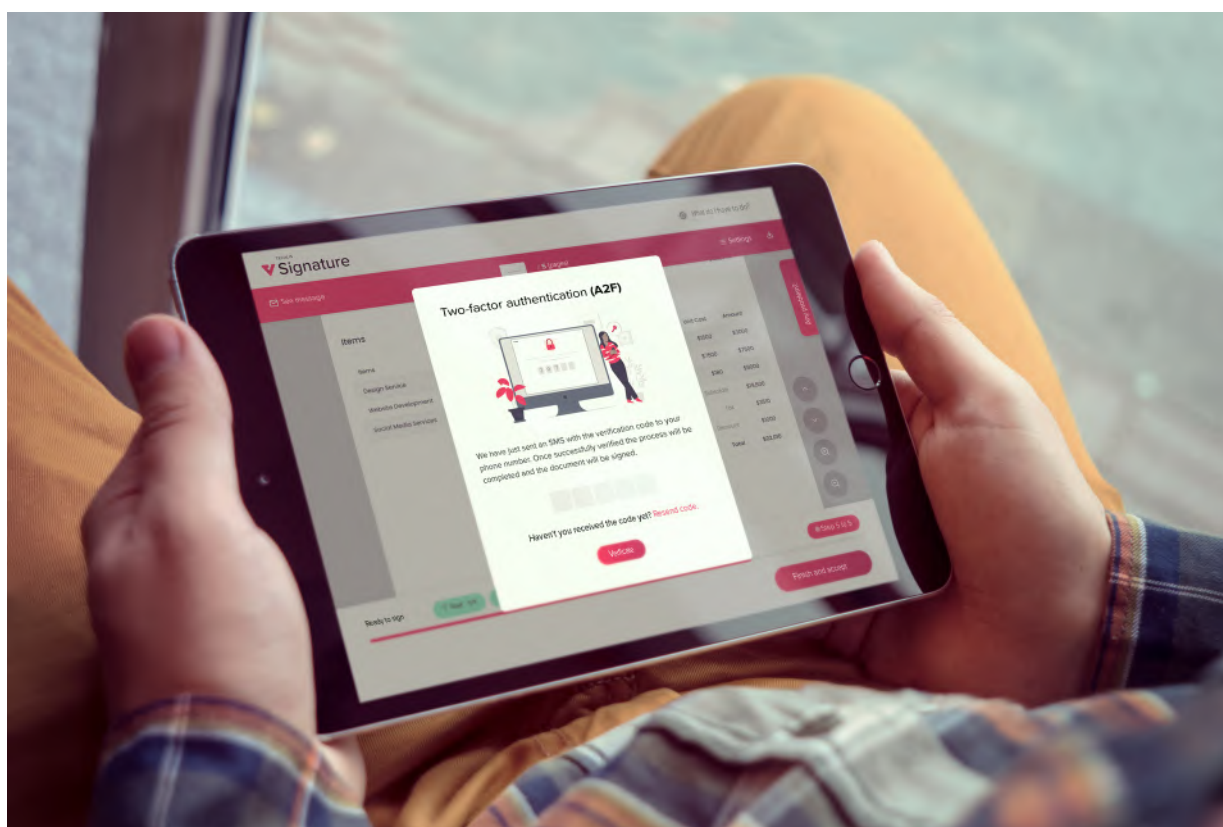
## Conclusion

Choosing an electronic signature provider is neither simple nor something that should be done without thinking about technical and operational aspects. Like any digital product, digital signature solutions are more or less capable, have more or fewer functionalities, and are buggy or not.

Therefore, taking time to **analyze and evaluate** the solutions and providers you have found is necessary given the **importance of the decision to be made**. The adoption of digital signatures by companies is boosting their business not only in terms of growth but also in terms of productivity and efficiency, but for this to happen, the solution that makes this possible must be effective, error-free, agile, and have the support it needs.

Consider each one of **the points outlined in this guide and cross-check this information with the needs of your company and the reality of your industry**. You will then be able to choose an electronic signature provider with confidence, security, and good results.

**Contact Tecalis and an expert in electronic signature solutions will evaluate your needs and propose a tailored plan for your business and activity.**



# tecalis

tecalis.com



**Lendha Espinoza Barroso**

[lendha.espinoza@tecalis.com](mailto:lendha.espinoza@tecalis.com)

(+34) 692 276 159



**Rafael Calvo García**

[rafael.calvo@tecalis.com](mailto:rafael.calvo@tecalis.com)

(+34) 600 967 559

©2021 Tecalis. All rights reserved.

