

ZEFORT

The Ultimate Guide to eSignatures

Learn how to maximize the benefits of electronic signatures while minimizing your risks.



Table of Contents

1. An introduction to eSignatures
2. How eSignatures can boost your business
3. What makes eSignatures safe and legally binding
4. Process makes perfect



Author

Ilkka Ventus, Chief Business Officer at Zefort

Ilkka is an experienced commercial tech evangelist. He has broad international experience in many areas e.g. Sales, HR and Financial administration in complex environments in Banking & Insurance, Information technology, and Retail industries.

1. An introduction to eSignatures

Taking care of business remotely is here to stay. During the pandemic, working from home and organizing remote meetings became business as usual for many industries. Now, even though the pandemic is phasing out, many of the best practices for remote work will remain.

One of these best practices is digital signing. Today, scheduling face-to-face meetings just to put ink on a dotted line seems redundant as you can easily do the task online, regardless of time or place. Originally driven by the B2C industries, digital signing has become widespread in the B2B business, too.

What are eSignatures?

Electronic signature, eSignature, digital signature – all these essentially mean the same thing, a personal confirmation on a digital document that the signee approves and agrees with the terms of a document.

Electronic signatures come in many forms: you can use a special pen to jot down your name on a touchscreen-enabled device or simply reply to an email stating your consent. However, for the purpose of conducting efficient business,

eSigning means sending a signing request from a dedicated eSigning service to everyone who must sign the document.

What do I need to do?

Here's the good news: getting started with eSignatures is easy and does not require technical know-how. There are many excellent eSigning services available that let you upload your document and send off signing requests in a matter of minutes.

There are a few questions you should consider before you start, however. Are eSignatures legally binding in your target market? What happens to your documents after they have been signed? And, most importantly, how can you get the most benefits for your business from electronic signing?

This guide is meant to tackle these questions. If you need additional help to get started, reach out to us at Zefort!



2. How electronic signatures can boost your business

No matter the size or domain of your business, electronic signatures are likely to make your life a lot easier and more productive. Here are some examples on how you can utilize digital signing in various business cases.

Save time (which equals money)

In today's business, saving time and effort results in saved money. Compared to traditional ink on paper, using electronic signatures means that you don't have to worry about sending out paper copies of a contract or booking face-to-face meetings. Simply send off a signing request from your contract management tool and you're on your way!

Electronic signatures can also significantly speed up entire business processes. When you can get an important signature in a matter of minutes

(instead of days), you can close deals and make agreements faster.

Automate processes

Electronic signatures are an important enabler for automated processes. Instead of manually sending documents via email or traditional mail, you can use software to automatically send signing requests and archive signed documents. You can also automate things like reminder messages or the distribution of the signed document.

Automation is particularly useful for high-volume B2C business. If your daily number of new customers jumps from 100 customers to 500 customers on a peak day, an automated process can handle the volume increase and eliminate delays for both you and your customers, resulting in better customer experience.

Enable international operations

Today, many companies do business internationally or hire international talent to work for them remotely. Using electronic signatures is not only an enabler for international operations but it can also add an extra level of security.

By using a nationally available strong digital identification method together with the electronic signature, you can verify the identity of your employee or business partner at the beginning of your relationship with certainty.

Speed up administrative work

Large organizations come with lots of internal administrative work. From board meeting minutes and annual financial statements to employment

contracts and performance reviews, there are plenty of documents that require validation through signing.

A digital signing process provides an easy, convenient way to reach out to internal stakeholders and get their sign-offs faster.

Manage risks and meet requirements

Depending on your industry, various regulations or legal requirements may affect your business. For example, you might be required to verify the identity of your customer. Digital signatures that utilize strong digital identification help you fulfill compliance requirements and manage your risks.

Add visibility to signing processes

If it is your responsibility to ensure that documents actually get signed, electronic signatures have a lot to offer. When you send out signing requests from a digital system, you can typically track the status of each signee: have they opened the signing request or reviewed the document yet and, eventually, get an instant notification once the signature has been completed.

This way, you will always know who to contact when a multi-party signing process stalls. Or, better yet, you can leave it up to your contract management system to send out reminders and gentle nudges to the person keeping the process on hold.

3. What makes eSignatures safe and legally binding?

Can you count on electronic signatures to hold up in a court of law? What makes them even more secure than traditional signatures? In an ideal world, business always goes perfect and there are no disputes between contracting parties. Unfortunately, this is not always the case, however – and that’s why you should understand a couple of aspects when it comes to electronic signatures.

eIDAS makes eSignatures legal in the EU

The European Union and its eIDAS regulation make the situation very clear for EU countries: digital signatures are as legally binding as traditional ink on paper.

Since its launch in 2014, the eIDAS regulation has made several types of electronic signatures legally binding and enforceable. In addition to clearing the legal status of digital signatures,

eIDAS provides a framework and standards for electronic identification (eID), electronic signatures and digital documents in its member countries. So, by using an eID service, you can verify the signer’s identity when making the signature.

It’s useful to know that not all EU member states necessarily offer a national solution for digitally verifying the signees identity, however. This does not mean that you can’t use electronic signatures in these countries: you can still utilize a basic-level signature through email, for example.

If you have the option, always prefer electronic signature methods with strong identity verification. Strong authentication results in a digital fingerprint, a logged signing event stored in a digital seal in the original signed PDF document. Therefore, it’s much easier to verify these signatures later if needed.

eSignatures come with built-in security

Compared to their traditional counterparts – a stack of paper signed with a pen on its last page – digital signatures have a lot to offer in terms of safety and security.

3 levels of electronic signatures

The European Union eIDAS digital identification regulation defines three levels of electronic signatures: basic, advanced, and qualified electronic signatures.

At the basic level, a name written in an email constitutes a binding electronic signature, for example. The advanced electronic signature (AES) adds a level of security, as the signature is uniquely linked to the signee through an electronic identification (eID) service.

The qualified signature level defined by eIDAS requires that the signee uses a dedicated qualified signature creation device (QSCD) when signing the document.

eSignatures outside the EU

Outside the EU, the legal validity of eSignatures varies country by country. For example, throughout the United States, electronic signatures have the same legal status as handwritten signatures, due to the E-Sign Act (2000) and the Uniform Electronic Transactions Act (UETA). Remember to check the legal status of eSignatures before you enter a new market.

Metadata ensures authenticity

When a document is signed in accordance with eIDAS, it includes metadata on the signing certificate, the signing service that was used and other technical details, such as information on the digital seal used to protect the document. It is important to save the original version of the signed digital document: edited digital versions or printed copies lose all the metadata.

First, using digital signatures implies that you are utilizing digital documents as part of your process. That's great – a digital process is likely to be faster and more efficient. In addition, it's much easier to archive and backup a digital document, keeping it safe for future use.

When a document is sealed with a digital signature, it becomes nearly impossible to forge or counterfeit. If you open a document with an altered signature in Adobe Reader, for example, the reader instantly informs you that the signature has been tampered with. Also, a digital signature adds a timestamp for the signature – the document always indicates exactly the exact date and time of signing.

Further, with digital signatures, you do not have to send duplicates of your documents via email. You can simply share a signing link to the document stored in your signing service. This way, you get to control who has access to the document while not having to worry about different document versions.



When a document is sealed with a digital signature, it becomes nearly impossible to forge or counterfeit.

4. Process makes perfect

When you think of electronic signatures, it's easy to focus on just the actual signing event – getting a digital signature to seal the deal. It's important to also consider the bigger picture, however, such as what happens *before* and *after* the document is signed and how digital signatures work as part of your process as a whole.

What happens to your signed document?

Far too often, a signed document is simply forgotten after the deal is closed. This should not be the case: a signed contract, for example, is a living document that defines your responsibilities, schedules and deliverables. Several people may need to access this information on a regular basis.

Many eSignature services are designed to provide an excellent signing experience. At the same time, they might be lacking critical features when it comes to post-sign activities. It may be difficult to quickly find specific documents, share them with your team and generally manage a large volume of documents.



Contract Lifecycle Stages

How can you ensure your signed documents are always readily available, then? Before diving into this, let's take a quick look at the entire process.

Digital contract management process

To simplify, the lifecycle of a contract (or any other document that needs to be signed) can be split into three phases: pre-signing, signing and post-signing. Pre-sign activities focus on creating and finalizing the contract, signing makes the deal official and post-sign ensures that the contract obligations are met.

When you move to and from the signing phase, try to cut down the amount of manual work to the minimum. This is not only because manual work takes extra time and effort, but also because human work is always prone to mistakes and delays.

A practical example: if your team member is required to manually upload a document to a eSigning service and then later download it (and save it in a specific folder on a network drive), the chances are they simply won't do it, the task gets forever delayed or a wrong document version is archived.

So, look for automation: does your eSign service have API integration to your document management system to allow automatic content transfer? Or, better yet, can you complete the signing step directly from your contract management system?

Utilize a contract archive

Today, misplacing signed contracts is simply not an option. You want to keep your contracts safe to keep the business running, manage your risks and ensure compliance with any legal and compliance requirements.

Instead of using a delicate folder structure on a network drive, or a generic document management system, you are likely to get the most benefit out of a dedicated contract archive. A good contract archive adapts to your needs: it can be either a daily tool for contract management or an automated “set up and forget” archive for signed digital documents.

What to look in a contract archive

If you are looking for a dedicated contract archive, here are some questions that help you select a suitable tool for you.

1. Can I store any number of documents indefinitely?
2. Can I find any required documents easily with the help of rich metadata?
3. Does the solution allow multiple users with different roles and document sharing?
4. Does the archive come with a built-in signing feature?
5. Can I set up automation with my other tools through integrations and APIs?



Zero-Effort Contract Management

Zefort is a smart contract archive that lets you sign, store and share all types of documents easily and securely in the cloud. With Zefort, you can automate your existing processes to save time, money and manual effort. Perfect for companies of all sizes, our customers love us for great user experience, rich feature set and exceptional customer support.

Let's talk

