



WHITEPAPER

ULTIMATE GUIDE TO ELECTRONIC SIGNATURES

Everything you want to know about electronic signatures, including a straight-forward checklist that will help you choose the best solution for your company.

UPDATE 2022



TABLE OF CONTENTS

01	Introduction	04	05	How do electronic signatures work?	24
02	What is an electronic signature? Difference between an electronic and digital signature	06 07	06	Examples of electronic signature methods	26
03	Are electronic signatures legally binding? eIDAS UETA & eSIGN Act ZertES	08 10 12 14	07	Integration with systems and software	32
04	Advantages of electronic signatures Efficiency User Experience Legal Compliance Security Positive impact on sustainability Summary of advantages	15 16 17 18 19 20 22	08	The use cases are endless	34
			09	Checklist for choosing an electronic signature solution	36



01

INTRODUCTION

Since the digital age, many organizations aim to deal with daily processes in a digital, more **efficient and secure** way. Yet, oddly enough, when it comes to important and legally binding agreements or sharing trusted information, many companies are still reliant on paper.

A turning point emerged in 2020. The spread of Covid-19 forced social distancing and an ever-growing number of employees to **work from home**, which inevitably impacted the way business had to be conducted, including the signing of agreements and contracts. The Covid-19 pandemic forced companies, consumers, and employees to **digitize fully** and quickly to maintain business continuity.

Electronic signature workflows are indispensable when it comes to keeping business moving in a remote world.

Businesses had to change their paper-based processes at a rapid pace and adopt digital ones. Legislation and regulations concerning electronic transactions/signatures became key to respond to businesses' changing needs. If they had not already, businesses all over the world started **adding electronic signatures** to their toolkits or expanding the use of it. This is a logical evolution as electronic signature workflows quickly became indispensable to keeping business moving in a remote world.

In this whitepaper we guide you through everything you need to know about electronic signatures. We will help you evaluate, choose and deploy the best electronic signature solution for your business.





02

WHAT IS AN ELECTRONIC SIGNATURE?



An electronic signature is the digital counterpart of the handwritten version in the offline world.

Technically, it is mathematical code that ensures the document cannot be changed after signing.

This also goes for elements related to the identity of the person. Legally, it captures a person's intent to agree to the content of an electronic document, contract or set of data.

The difference between an electronic and digital signature

You may have noticed that the terms electronic signatures and digital signatures are used interchangeably. However, there is a difference. A digital signature is always an electronic signature, while an electronic signature is not always a digital signature.

The difference is that a digital signature relies on a **cryptography-based technology** that provides an extra level of security and integrity for the document. An electronic signature, on the other hand, can be merely the image of your signature pasted in a Word document. It can even be your mail signature.

Digital signatures are thus the most advanced and secure type of electronic signatures. They use the standards and procedures of Public Key Infrastructure (PKI) to sign electronic data with a cryptographic key. This ensures the contents of the message cannot be modified or tampered with, without breaking the validity of the digital signature.

You can use digital signatures to comply with the most demanding regulatory requirements. This is because they provide the highest levels of assurance of the identity of each signer and the authenticity and integrity of the document.

In this whitepaper, we will use 'electronic signature' throughout for the sake of convenience.

03

ARE ELECTRONIC SIGNATURES LEGALLY BINDING?


Yes.

An electronic signature is legally recognized and enforceable in almost every part of the world.

The Electronic IDentification, Authentication and trust services (eIDAS) regulation has been directly applicable to all member states of the European Union since 2016 to enable secure, seamless electronic interactions. In the United States, the Uniform Electronic Transactions Act (UETA) and E-SIGN Act were passed to help govern electronic transactions.

Many other regions and countries have or are in the process of enacting similar laws and regulations around electronic identification and trust services. They recognize the important role they play in enabling businesses and governments to securely conduct electronic transactions within and across borders.

To learn the details, we encourage you to download our [legal whitepaper](#) with an assessment conducted by DLA Piper. For now, in the following pages, you can read what you should know about:

- **eIDAS** 
- **UETA & eSIGN ACT (United States)** 
- **FAES (“ZertES” in German) (Switzerland)** 



eIDAS

On July 1, 2016, the electronic IDentification, Authentication and trust Services for electronic transactions regulation (eIDAS) established a new legal structure for electronic identification, signatures, seals and documents throughout the EU. This EU regulation classifies electronic signatures by the level of assurance they offer. We will explain what this means in the table below, but first, you need to know there are three types of electronic signatures:



Basic or Simple electronic signature (SES)



Advanced electronic signature (AES)






Qualified electronic signature (QES)

The differences between these types are mainly based on four key items:

- **Authenticity**
Is the signature uniquely linked to the signer?
- **Identity**
Are you able to identify the signer?
- **Integrity**
Is the signature linked to the data signed in such a way that any subsequent change in the data is detectable?
- **Authentication**
How confident are you that the signature is created under the sole control of the signer?

In this table, we explain how the three electronic signature types differ in these aspects:

	 SIMPLE OR BASIC (SES)	 ADVANCED (AES)	 QUALIFIED (QES)
Definition	A simple or basic electronic signature must simply prove acceptance or approval by the signer. This can be a scanned image of a signature, a signature manually drawn on a desktop screen (& digitally saved), a click on an “I accept” button, etc.	An advanced signature must meet specific requirements providing a higher level of signer ID verification, security, and tamper-sealing (meaning the document cannot be changed once it is signed).	A qualified or non-repudiation signature is the only electronic signature type to have special legal status in EU. Unlike the other signatures, the burden of proof lies with the party that disputes the signature(s), not with the initiator. This makes it legally equivalent to a written signature. It is backed by a certificate issued by a trust service provider that is on the EU Trusted List (ETL) and certified by an EU member state.
Integrity	Content cannot be changed after signature.	Content cannot be changed after signature.	Content cannot be changed after signature.
Identity of signer	Identity of signer is not checked.	High probability of identifying the signer.	100% capable of identifying the signer. Initial face-to-face verification or another equivalent process is required.
Authenticity	Not certain that the signature is uniquely linked to the signer.	Certain that the signature is uniquely linked to the signer.	Certain that the signature is uniquely linked to the signer.
Authentication	Not certain that the signature is created under the sole control of the signatory.	Certain that the signature is created under the sole control of the signatory. Multi-factor authentication is optional.	Certain that the signature is created under the sole control of the signatory. Multi-factor authentication is required.
Hardware	Not needed.	Secure Signature Creation Device (SSCD) needed.	Qualified Signature Creation Device (QSCD) needed.
Legal validity	Legally irrefutable. Burden of proof lies with the party that initiated the signature.	Legally irrefutable. Burden of proof lies with the party that initiated the signature.	Legally irrefutable. Burden of proof lies with the party that disputes the signature.
Examples	Following signing methods can be either a basic or advanced electronic signature depending on the process: Manual, Biometric, Banking card / iDIN, SMS or mail a One Time Password (OTP)	Following signing methods can be either a basic or advanced electronic signature depending on the process: Manual, Biometric, Banking card / iDIN, SMS or mail a One Time Password (OTP)	The qualified electronic signature always comes with an e-identity and a card reader or token, or another specific certificate.

UETA & eSIGN ACT (United States)

The United States has a two-tier structure of laws —federal and state. Federal applies to the entire nation and to transactions involving parties of different states; while state laws apply only to the specific state and transactions conducted within that state. With respect to the U.S. eCommerce Laws, the Electronic Signatures in Global and National Commerce Act (ESIGN) was enacted at the federal level, while UETA was enacted at the state level.

This means that ESIGN directly applies to every state, while each state can choose to enact UETA in full, in part or in a modified form as a state law. To date, 47 of the 50 states in the U.S. have adopted UETA in some form.



Both ESIGN and UETA clearly define certain standards for compliance. There are four major requirements for an electronic signature to be recognized as valid under U.S. law. Those requirements are:

1 Intent to sign

Just like traditional wet ink signatures, electronic signatures are valid only if **each party demonstrates a clear intent to sign**.

2 Consent to do business electronically

Each party to the transaction **must agree to use electronic records** and electronic signatures in place of written documents and manual signatures.

This agreement may be expressed, or implied from the circumstances, except for consumer transactions, where the ESIGN Consumer Consent Process must be followed. Signers also have the option to opt-out.

(Source: DLA Piper)

3 Clear signature association

In order to qualify as an electronic signature under the ESIGN Act and UETA, the electronic signature **must be linked** or logically associated with the record and the signer.

4 Record retention

U.S. laws on eSignatures and electronic transactions require that each electronic record accurately **reflects the information in the document**. The electronic record should remain accessible to all persons entitled by law to access the document during the period of time required by law. The electronic record should be in a form capable of being accurately reproduced for later reference.

Source: <https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/so-you-want-to-go-digital/>

FAES (“Zertes” in German) (Switzerland)

On December 19, 2003 electronic signatures were legalized in Switzerland when the Federal Law on Electronic Signatures (further referred to as ZertES) came into effect.

The Swiss Federal Act on Electronic Signatures (the FAES) regulates the conditions under which service providers may use certification services with electronic signatures. Additionally, the FAES provides a framework outlining the provider's obligations and rights applicable to the provision of certification services. The law promotes the use of secure services for electronic certification to facilitate the use of qualified electronic signatures. Under FAES, the electronic signature is equal to a handwritten signature.

The FAES' tiered structure and standards of legal value are similar to those of the European Union's eIDAS Regulation. In the FAES regulations, next to the general notion and concept of "electronic signatures", there are three additional variants, namely simple, advanced and qualified electronic signatures, which is just like eIDAS.

It means that qualified electronic signatures are fully court-admissible, while the other electronic signatures require more evidence to be validated.



The page features a dark blue background with several decorative orange lines. One line starts at the top right and curves downwards towards the center. Another line starts at the bottom left and curves upwards towards the center. A third line starts at the bottom left and curves downwards towards the bottom right.

04

ADVANTAGES OF ELECTRONIC SIGNATURES



The use of electronic signatures delivers many advantages, including greater efficiency, an improved user experience, legal compliance, security and a positive impact on sustainability.



Efficiency

Too often, finalizing a commercial or any other business process can turn into a time-consuming nightmare full of tedious paperwork. Often, time is spent conducting repetitive administrative tasks rather than achieving effective goals. That is why everyone is looking to digitize their processes to optimize and eliminate time-consuming steps. Introducing electronic signatures can be another step to accelerate your business.

Within the office you no longer need to:

- **Wait for the signatory to be available for a wet signature.**
- **Sign, print, scan and manually post a document.**
- **Manually archive documents.**
- **Manually verify if the documents have been signed by the right (mandated) person.**

For your customers, you can speed up your entire business lifecycle. Electronic signatures will:

- **Allow you to save time on contract creation.**
- **Enable everyone inside and outside the organization to sign any time from any device.**
- **Streamline the whole approval and signature process and make it error-proof.**
- **Enable the same level of security and trust as with conventional documents.**
- **Help you close deals faster.**

User Experience

User experience is a customer's perception of their interaction with your organization. It is shaped by the contact moments they have with your company. By leveraging electronic signatures you can improve these interactions. These signatures provide the convenience that documents can be signed everywhere. For instance, your customers or employees can quickly and easily complete documents while traveling on holiday; or accept a one-time offer at an event; or confirm the delivery of an order from their doorstep.

Moreover, all kind of devices can be used, which makes electronic signing extremely user friendly. No more piles of paper to initial or paper work to archive. Just send the contract by e-mail (automatically or manually) and complete the transaction or close the deal within minutes.





Legal Compliance

In recent years, most countries worldwide have adopted legislation and regulations that recognize the legality of electronic signatures and deem it a binding signature. For example, in Europe, thanks to the eIDAS regulation, there is a legal platform that allows the cross-border usage and validation of electronic signatures. Under this regulation all signature types are treated equally in court.

Electronic signatures provide authenticity and ensure that the signer's identity is verified. This can stand in any court of law like any other signed paper document. By choosing a solution that is compliant to the relevant regulation, you can ensure the transaction you complete are compliant to these legal requirements.





Security

When it comes to signatures, authenticity and security are priorities. Each type of electronic signature is already more secure than a manual signature on paper. Thanks to the encryption of the document, you have the guarantee that the document remained unchanged after signing. With an electronic signature, you are also always signing the document in its entirety. There is no risk that some pages have been added or removed afterwards.

Electronic signatures are also more secure and efficient because they are less prone to errors. Having to rely on manual checks puts you at higher risk than when you can automate processes. Another advantage with regards to security is that electronic signatures allow you to set up an administration of consents, which is mandatory under the EU's General Data Protection Regulation (GDPR).

Depending on the type of security required, you can adjust the level. Do you need somebody to sign in for a newsletter or for a \$100,000 contract? In the latter example, you probably want to be sure about the identity of the mandated person.

You need to also consider the technical transfer of signatures, which can provide varying levels of security. When high security is needed, you can include encryption. By applying the right level, you can find the right balance between user friendliness and security.





Positive impact on sustainability

Electronic signatures also come with a great positive impact on our environment and sustainability in general.

1 Signing remotely, no need to travel

Being able to sign documents electronically eliminates the need to travel. Instead, you can sign documents remotely, from any place in the world by simply using your computer or mobile phone. When business trips can be minimized, there is a positive impact on our environment, as well as a time and cost savings, which can be generally beneficial to your business.

2 Signing electronically, no need for paper documents

Besides not having to travel to place handwritten signatures on documents, signatures, electronic signing also contributes to a paperless office. There is no need for printing, copying, scanning or physically archiving your signed contracts anymore as the entire process will be digitized. Your company's footprint on the environment will be reduced from day one, as you start using electronic signatures. You will use less paper, which preserves our forests, and you will lower your company's CO2 emissions.

3 **Signing electronically, no need for physical archiving**

In many cases, documents to be signed can be uploaded within the electronic signatures tool and subsequently stored within your company's document management system. The entire process is automated, meaning the risk of human error throughout the signing process is less.

Some signing tools even offer the possibility to store and archive those documents in a secure and safe way by incorporating an archiving component within their signing solutions.

Not having to print these documents (often in multiple copies), drastically reduces the amount of paper used in your offices. Additionally, documents are available online at any time and accessible from anywhere.



Summary of advantages

EFFICIENCY

Electronic signatures simplify processes and strongly reduce document management time. The signing process can be automated, leaving out all manual tasks such as obtaining a signature, printing, scanning, posting, archiving and verifying.

ENHANCE CUSTOMER RELATIONSHIPS

Your customers expect businesses to provide online services nowadays. Introducing electronic signatures will provide you with the necessary tools to delight and satisfy your customers, avoiding customer churn.

COST REDUCTION

Electronic signatures can be incorporated in any business process. It increases employee productivity and reduces many hours of man power, so employees can perform other types of tasks that provide better value. At the same time it drastically reduces administrative costs. You'll have a lower consumption of paper, no need for stamps, and ink, nor physical archiving or scanning facilities.

TRACK YOUR PROGRESS

No more losing time chasing signatures ever again. It can be frustrating and time consuming to wonder: "Has he signed yet?" or "Where is my document at?". Electronic signature software makes it easy to track your documents in an online dashboard, while some software solutions even provide you the ability to send signers a reminder email.

MOBILITY

Documents can be signed everywhere and on all devices. This means work can be done and transactions completed when your customers and employees are on the go.

COMPLIANCE

With an electronic signature solution that complies with all your relevant laws and regulations, you can confidently conduct business across borders.

FUTURE PROOF

More and more countries work with digital IDs. For example, as of September 29th 2018, all European citizens and companies must be able to log in to organizations in the public sector in other member states with their national ID. This will enhance the use of electronic signatures as your national ID can serve as a digital identity backing an electronic signature across borders.

SCALABILITY

As manual actions diminish, more documents can be processed and more customers served.

SECURITY

With electronic signatures, you can safeguard your documents with a high level of security and evidence. Each signature is protected with a tamper-proof seal, which alerts you if any part of the document is changed after signing. Depending on the confidentiality, security can be adjusted. For the highest level of confidentiality, stronger types of authentication can be used. Signed documents thus come with a highly detailed evidence of the signer's identity, which gives you a strong guarantee on document integrity and the signer's identity.

05

HOW DO ELECTRONIC SIGNATURES WORK?

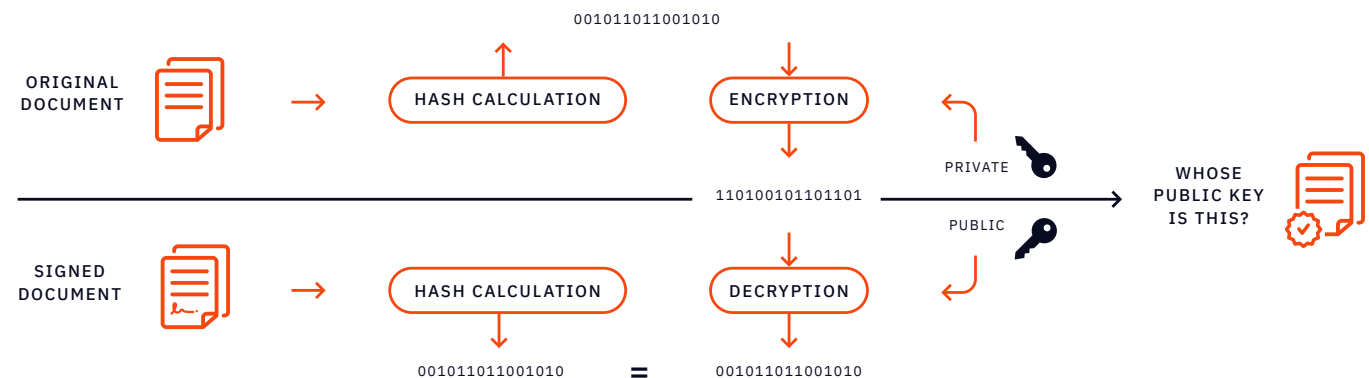


Electronic signatures are based on a specific protocol, called Public Key Infrastructure (PKI). This protocol uses cryptographic algorithms to create two long numbers. These are called keys. One of the keys is public, the other one is private.

As electronic signatures are unique to a signer, each time a signer signs the document, the signature is created using the signer's private key. This private key is always securely kept by the signer and is included in the signature when signed. Basically, the electronic signature securely associates a signer with a document in the form of a coded message. Next to this key, the signature also contains the certificate of the signer, which includes the public key and other information, like the date and time at which the document was signed.

Before signing, a cryptographic function is used to create a message digest (comparable with some data), called a hash. Afterwards this hash is encrypted (signed) with the private key of the signer and included in the electronic signature.

When the document arrives at the receiver, another hash will be created. By decrypting the hash that was included in the signature you will be able to compare it with the hash that was created for the document. If they don't match, the receiver of the document will see that the document is tampered with, resulting in an invalid electronic signature.



06

EXAMPLES OF ELECTRONIC SIGNATURE METHODS

Many different signing methods exist. It varies from simple methods, like an approval button or a handwritten signature, to more advanced or even qualified, and therefore very secure, signing methods, like signing with a national electronic ID card.

What you need to know is that, depending on the signing method, a signing process is often preceded by **user authentication**. This is the process of verifying someone's credentials prior to giving them access to a system – in this case, signing electronically.

Authentication contributes to the enforceability of signed documents, as it validates with whom a company, organization or institution is transacting with. Whether or not a company decides to ask for an authentication during the signing process will depend on the value of the transaction and the trade-off with the user experience.

Although authentication doesn't necessarily mean a more cumbersome user experience it is still more complex and demands more from the user than a simple scribble with the finger on a smartphone or desktop.

In this section, we want to give you more insights into which signing methods exist today.

DISCLAIMER: The information in this section is for general informational purposes only and is not intended to constitute legal advice. Connective does not guarantee the information contained herein is up-to-date or accurate nor we make any statements on the legal validity of signing methods. Please note legislation governing electronic signatures is changing quickly and can differ in each jurisdiction. If you have questions about the content or statements made in this section, or about whether Connective's solutions fit the needs of your organization, please reach out to a legal professional in your region.



There are several signature options organizations can use when they don't need to authenticate the user.



Manual scribble

Using a mouse, touchpad, stylus or even a finger, the signer can draw their signature on a touchscreen. This is also considered an electronic signature.



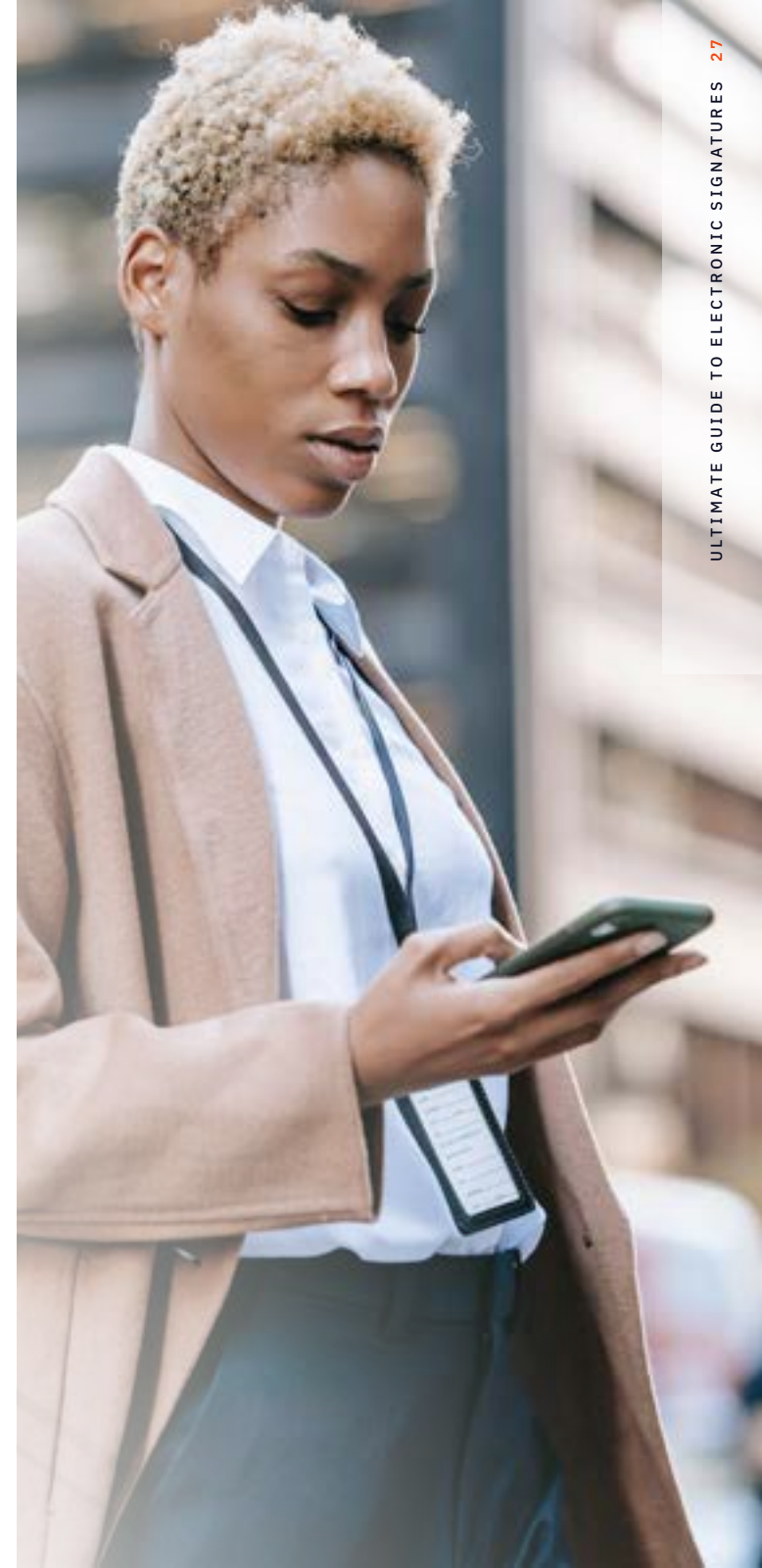
Handwritten signature

Using a keyboard, the signer can type your name and then choose from pre-configured handwritten fonts the style they want to represent their signature.



Approval Button

Using a mouse, the signer simply clicks on an approval button, which results in an approval signature.



When organizations need to validate the user is who they say they are, there are a number of ways to authenticate them.



Biometric Signature

The signer uses a biometric signature pad or biometric pen to sign with a biometric signature. Biometrical characteristics of a signature, like where the pen is located, when the pen tip is pressed down, and how hard it is pressed down, can be captured with a signature pad or a biometric pen. This biometric data is added to the signature, creating a unique biometric signature profile, which allows the signature pad manufacturer to verify the authenticity of the signature when required.



Smartcard or Token (USB)

In order to sign documents, the signer has to put their smartcard in a card reader or a token in a USB port and enter their personal PIN code to authenticate themselves. A smartcard contains a personal certificate with a private key, which is issued by a qualified provider.

Some of the most commonly known smartcards are those issued by a country, such as LuxID, Estonian ID and .beID. Other smartcard examples are the Belgian Lawyer ID, the Common Access Card (CAC) or the Personal Identity Verification Card (PIV) in the USA.



*** Login and password (including SSO)

- In some onboarding processes a user identifies themselves by **choosing his username** (often email address) **and password**. Sometimes, they may be asked to fill in some extra information. These credentials can be used to authenticate the user when signing documents electronically.
- More secure login and password solutions, like **Swisscom**, can enforce a one-time identification via **Face2Face** or video to ensure the signer's identity. Afterwards, the signer can choose to either create a login and password combination or use a mobile application for authentication purposes going forward. Thanks to the previous identification, a personal certificate will be linked to the identity, which makes it much more secure, resulting in advanced and qualified electronic signatures.
- Using the **single-sign-on (SSO)** principle, signers can use the credentials they've established to sign into a company's platform to also sign documents. This is often combined with multi-factor authentication.



One-time password (OTP) via SMS or email

When signing with an SMS OTP the mobile phone number of the signers must be known. In the signing process they will need to enter the last four digits of their phone number. In return, they'll receive a one-time password, via SMS, which is needed to authenticate themselves.

In the case of an email OTP, the email address of the signer must be known. The signer needs to complete the email address. In return, a password will be sent to that address, which is needed for the authentication.





Mobile Identities

A mobile identity refers to a person's digital identity and the technology used to manage it, meaning an application on a smartphone, tablet or other wearable technology.

The most common use case is when a user creates their mobile identity via an onboarding process. Initially, the process may require the use of a smartcard or other login method to validate the user's identity. Once completed, the user can create a password that will be linked to their mobile ID and can be used for authentication going forward. An example of a mobile identity is itsme® in Belgium. Because the onboarding is related to an ID card or a bank's Know Your Customer (KYC) process, this becomes a very powerful signing method that results in advanced or qualified signatures.



Public / Government Initiatives

To access secure online government applications, some governments created authentication services. This authentication, in some cases, can also be used in a signing process to electronically sign documents in a secure way.

E.g. FranceConnect, ... FAS Belgium, MitID (Former NemID), ...



Bank Authentication - sometimes used in combination with mobile network operators (MNOs)

In some countries there are also bank initiatives that create a personal electronic ID for secure identification. The bank identity can either be mobile, where the identity is stored on a mobile SIM card, or contained on another hardware authenticator, like a bank card reader or one-button authenticator. Bank identities are also a perfect method to sign documents in an electronic way. Some examples are iDIN, Bank ID Norway, Bank ID Sweden, Finish Trust Network and many more.



Biometric Authentication

Before signing, a secure authentication process can be done that relies on the unique biological characteristics of individuals to check they are who they say they are. These biological characteristics can include voice, facial characteristics and fingerprints. After the identity of the person is validated, the document can be signed electronically. The biometric authentication will be captured in document audit trails, which counts as proof of a safe, secure, legally-binding Electronic signature.

Eg. SmileID of Electronic ID, FaceID of Apple, ...

07

INTEGRATION WITH SYSTEMS AND SOFTWARE

When deciding to go through with electronic signatures, you can make your life easier by **integrating the solution into your existing business applications**. Also, it is good to make sure the electronic signature solution fits with your customers' systems. You also want to see if it includes easy to use application programming interfaces (API) that help you customize the solution for your specific needs.

Most solutions are built to integrate with the latest operating systems and browsers, but do check if it runs smoothly on the latest versions before you make your choice. For instance, some electronic signatures use Java, but Google Chrome no longer runs Java applets and it's likely other browsers may follow suit. Therefore, check how the solution works in all commonly used browsers because you want to make it easier, not harder, for your customers and employees to complete contracts and transactions.

There are also standalone solutions offered in the market that allow you to login to a central electronic signature portal. You might want to check the interface here as well. That way you can seamlessly integrate electronic signature functionality into your own web applications.

Do not forget about **responsive design** either. Smartphones and tablets are about to surpass PC's in internet use. Meet your customer's expectations in this field and check how the solution looks on smartphones and tablets. Of course, it should support both iOS and Android.



08

THE USE CASES ARE ENDLESS

Technically, any document that requires a signature can be signed electronically. And as mentioned earlier, electronic signatures are valid and enforceable and have the same legal effects as their written equivalents. Of course, this is as long as the requirements, described by regulations and laws, are met.

Therefore, we always recommend contacting your legal department if you have any doubts about the legal validity of electronic signatures.

Still, the use cases are endless. Here are just a few interesting examples of documents that can be signed electronically.

SALES

- ✓ Price offerings
- ✓ Order confirmations
- ✓ Partner contracts
- ✓ NDA 's
- ✓ Quotes
- ✓ Proposals
- ✓ Terms & Conditions

HUMAN RESOURCES

- ✓ Company policies
- ✓ Temporary and permanent contracts
- ✓ Internal rules
- ✓ Health insurance documents
- ✓ Annual performance evaluation
- ✓ Internal mobility

PROCUREMENT

- ✓ Statements of work
- ✓ Master service agreements
- ✓ NDA's - Vendor contracts & agreements
- ✓ Purchase orders
- ✓ Contract terms
- ✓ Credit requests
- ✓ Financing agreements

FINANCE

- ✓ Online mortgages
- ✓ Account openings
- ✓ Customer onboarding
- ✓ Credit conventions
- ✓ Debit/credit card request

OPERATIONS

- ✓ Price offerings
- ✓ Order confirmations
- ✓ Partner contracts
- ✓ NDA 's
- ✓ Terms & Conditions
- ✓ Change requests
- ✓ Requirements sign-off

LEGAL

- ✓ Terms and Conditions
- ✓ Order confirmations
- ✓ Agreements
- ✓ NDA 's
- ✓ Sales contracts
- ✓ Powers of attorney
- ✓ Policy Management
- ✓ Compliance documents

09

CHECKLIST FOR CHOOSING AN ELECTRONIC SIGNATURE SOLUTION

To help you choose the right electronic signature solution, we have set up a checklist for you. By checking all these points you will be sure to buy a user-friendly solution that will satisfy all parties involved, both inside and outside your organization.

Efficiency

- ☐ Does it enable you to sign the file types you typically use? (e.g.PDF, DOC, DOCX, TXT, XML,...)
- ☐ Does it work with your existing applications?
- ☐ Does it enable document tracking via an intuitive dashboard?
- ☐ Does the solution provide you with inbuilt automated signature flows?
- ☐ Does it integrate with your existing applications or those you might use in the future, e.g. contract management, HR services?
- ☐ Does the vendor know and understand your business?
- ☐ Does it allow for company branding?

Legal

- ☐ Does it comply with the regulations relevant to your organisation? (eIDAS, GDPR, etc....)
- ☐ Can you use it across borders? Does it comply with relevant regulations in the countries you are operating in - e.g., across Europe, the U.S. or Australia?
- ☐ Does it encompass the e-identities or relevant other identity methods in the countries you want to serve? (.beID, itsme, iDIN, SwissID,...)
- ☐ Does it support Advanced and Qualified Electronic Signature (AES and QES) for documents with multiple signers?
- ☐ Does it enable anyone to validate the signature, even without access to the system? In other words: are the documents self-contained? If not, you might need the signing provider later in case a dispute arises.
- ☐ Does the solution offer WYSIWYS: What You See Is What You Sign? If you want to make sure the whole document is read before signing, this feature is a must in the solution you choose. It ensures that the document can only be signed, when it is fully read.

User experience

- ☐ Is it easy to prepare documents for signature?
- ☐ Is the solution self-explanatory and intuitive? Make sure your users do not need to follow training or read a manual to use it.
- ☐ Can you set the order of the signers?
- ☐ Does it offer a wide range of built-in signature methods (SMS code, mail code, challenge-response, eID, other digital certificates, etc. ?)
- ☐ Can you offer a choice of signing methods to your signers (allowing to use the device they have at hands)?
- ☐ Can you sign packages of documents?
- ☐ Does it provide the ability to sign on any device?
- ☐ Does it enable anyone inside or outside the organization to validate the signature even without accessing to the system?
- ☐ Does it fit in with the consumer flow? Test the complete end-to-end-flow to make sure it is a smooth user experience.
- ☐ Does it support multiple languages both for initiators and signers?

Technical requirements

- ☐ Do you want to use a cloud solution or self-host the solution? Is the solution available in the way you prefer? Does the software offer the required level of security?
- ☐ Does it create an electronic signature and hash for each signer in the transaction? In other words: does it tamper-seal the document between signers following the eIDAS requirements?
- ☐ Is it compatible with the latest versions of all common operating systems (both PC and mobile)?
- ☐ Does it offer a completely responsive design? Can users also sign on their smartphone or tablet?
- ☐ Does it have a flexible Application Programming Interface (API)?
- ☐ Is the solution easy to implement?
- ☐ Are there out of the box connectors available for programs, such as Microsoft Power Automate, Salesforce?

Cost

- ☐ What is the cost model of the solution? Do you pay per signature or for the complete solution? Do you need to buy or is SAAS (hiring) also an option? Estimate your future expenses.

WANT TO KNOW MORE ABOUT ELECTRONIC SIGNATURES?

info@gonitro.com

www.gonitro.com

