CONNECTIVE

WHITEPAPER

Ultimate guide about electronic signatures

Update 2021

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

Table of contents

01

Introduction

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

That is why 2020 has become a real turning point. The spread of COVID-19, the continuation of social distancing and the continuously increasing number of **employees working from home**, have inevitably impacted the way people conduct their businesses, including operations as essential as signing agreements and contracts. The Covid-19 pandemic has forced companies, consumers, employees to **digitize fully** and quickly to be able to maintain business continuity.

> **Electronic signatures workflows are indispensable when it comes to keep business moving in a remote world.**

At a rapid pace they had to change their digital habits and adopt new ones. The legislation and regulations concerning electronic transactions/ signatures become key to respond to businesses' changing needs. If they had not already, businesses all over the world are **adding electronic signatures** to their toolkits or expanding the use of it. A quite logical evolution as electronic signatures workflows are indispensable when it comes to keep 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?

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

Technically, it is a 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 a(n) electronic document, contract or a 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 inter-changeably. 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** which provides an extra level of security and integrity of 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. 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 as they provide the highest levels of assurance about each signer's identity and the authenticity/integrity of the documents they sign.

In this whitepaper we will use the term 'electronic signature' instead of 'digital signature' for the sake of convenience and because it is the most commonly used term.

03

Are electronic signatures legally binding?

Yes.

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

Since 2016, eIDAS, the European legal framework on electronic signatures, has become directly applicable to all member states of the European Union. In the United States you have similar regulations called UETA and eSign Act which is applicable since 2002.

Other countries have enacted similar laws as well. Even less-developed countries are beginning to enact electronic signature laws, which have potentially been left unexploited in the past. Today they are becoming a key element to respond to businesses' changing needs.

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 (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

Qualified electronic signature (QES)

The differences between these types are mainly based on 4 key items:

- **Authenticity**
  Is the signature uniquely linked to the signer?
- **Identity**
  Are you capable 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 will explain how the three types differ in these aspects:

	SIMPLE OR BASIC (SES)	ADVANCED (AES)	QUALIFIED (QES)
Definition	All electronic forms of signatures that 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.	This 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 is 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, Electronic Signatures in Global and National Commerce Act (ESIGN) was enacted at the federal level while Uniform Electronic Transactions Act (UETA) is enacted at the state level.

It means that ESIGN is directly applicable to each of the U.S. states. While that each state of the U.S. may choose to enact UETA, in full or in part, or in modified form, as state law. Forty-seven (47) of the U.S. states 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 express, 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 for the period of time required by law and 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 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 just like eIDAS.

> It means that Qualified Electronic Signatures are fully court-admissible, while the other electronic Signatures require more evidence to be validated.

04

Advantages of electronic signatures

The use of electronic signatures brings along many advantages of which efficiency, user experience, legal compliance, security, positive impact on sustainability are the most important.

EFFICIENCY

Too often, finalizing a commercial or any other business process can turn into a time-consuming nightmare full of tedious paperwork. Time is spent conducting repetitive administrative tasks rather than achieving effective goals. That is why everybody is trying to optimize the process time by working digitally. 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)**

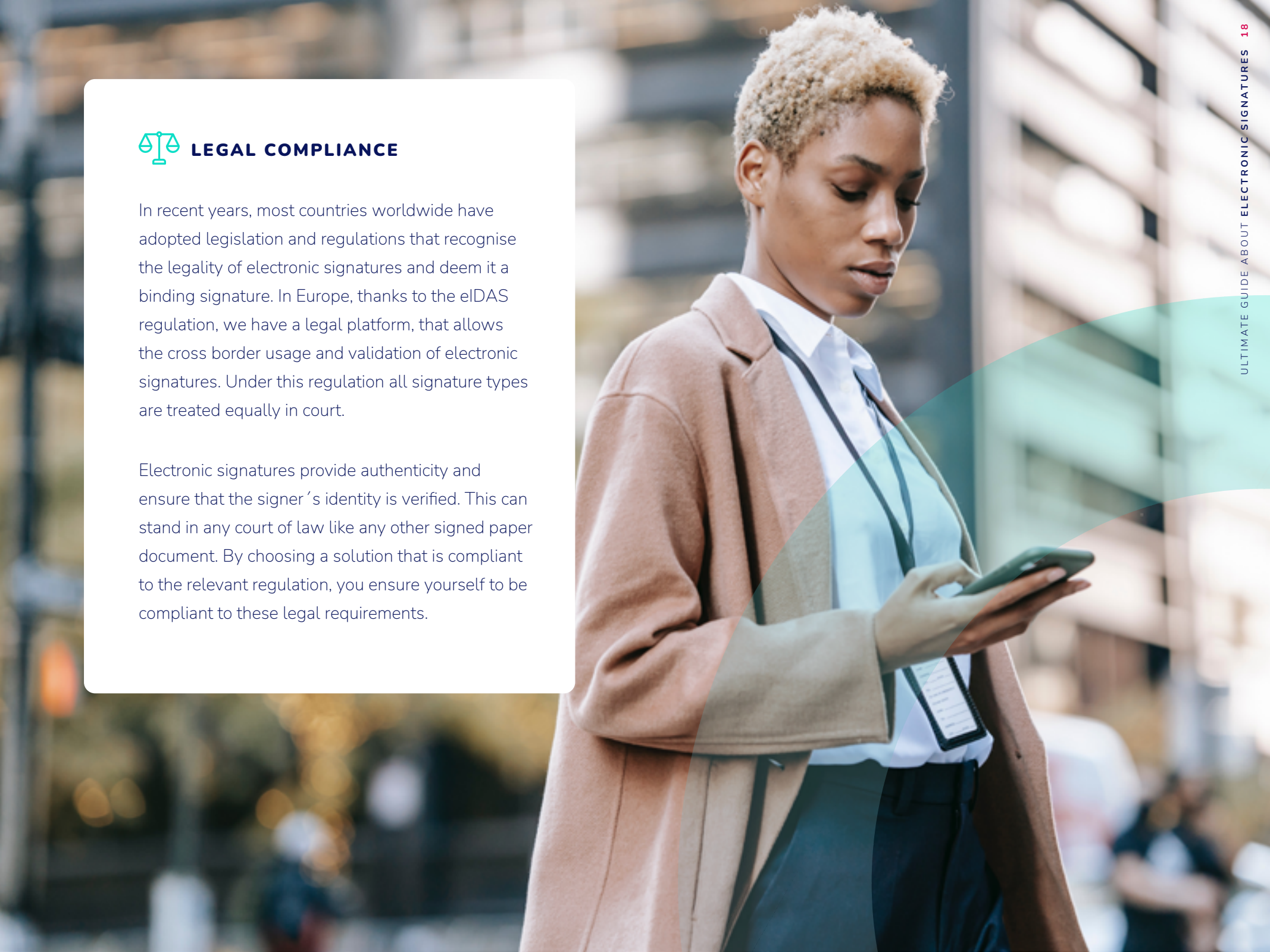
Towards your customers you can speed up your entire business lifecycle. Electronic signatures will:

- **Allow you to save time on contract creation**
- **Enable everyone inside and outside the organisation 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 organisation. 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: while they are on holiday, a loan can be made definitive; deals can be closed quickly. Think about a one-time-offer at a fair. Even at your doorstep you can easily confirm the delivery of an order.

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 get the deal closed within minutes.



LEGAL COMPLIANCE

In recent years, most countries worldwide have adopted legislation and regulations that recognise the legality of electronic signatures and deem it a binding signature. In Europe, thanks to the eIDAS regulation, we have 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 ensure yourself to be 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. Certainly in case of an electronic signature. Thanks to the encryption of the document, you have the guarantee that the document remained unchanged after signing. With an electronic signature you also always sign the whole lot of documents. There is no risk that some pages have been added or removed afterwards.

Electronic signatures are also efficient in a way that they are less error prone. Manual checks are a higher risk than automated processes. Another advantage with regards to security, is that electronic signatures allow you to set up an administration of consents, which is mandatory under GDPR law.

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 last case you want to be sure about the identity of the mandated person.

The technical transfer of signatures differ in security level. 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. Signing can be done remotely, at any place in the world by simply using your computer or mobile phone. No business trips required which results in a positive impact on our environment, but also time- and cost savings and a much more pragmatic approach for doing business in general.

2 **Signing electronically, no need for paper documents**

Besides not having to travel for placing handwritten signatures, electronic signing also contributes to a paperless office. 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 our environment will be reduced as from day one you start using electronic signatures. It leads to less usage of paper, preserving our woods and your company's CO2 emission will be lowered as from the first electronic signature.

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

In many cases, documents to be signed can be uploaded within the electronic signatures tool for electronic signing and subsequently be stored within your companies 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.

Having not 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 archive 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 will even give the possibility to send signers a reminder email.

MOBILITY

Documents can be signed everywhere and on all devices. This comes in handy for travelling managers but is also convenient for signatures at the door step.

COMPLIANCE

When choosing an eIDAS compliant solution, the signatures are legally valid across European borders. Under eIDAS, there are three signature types. All three can be legally effective. The difference between them is the evidence needed to prove in court that the signature is genuine and intentionally applied to a particular document.

FUTURE PROOF

More and more countries work with a digital ID. This will increase in the future, as from September 29th 2018, all European citizens and companies must be able to log in to organisations 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

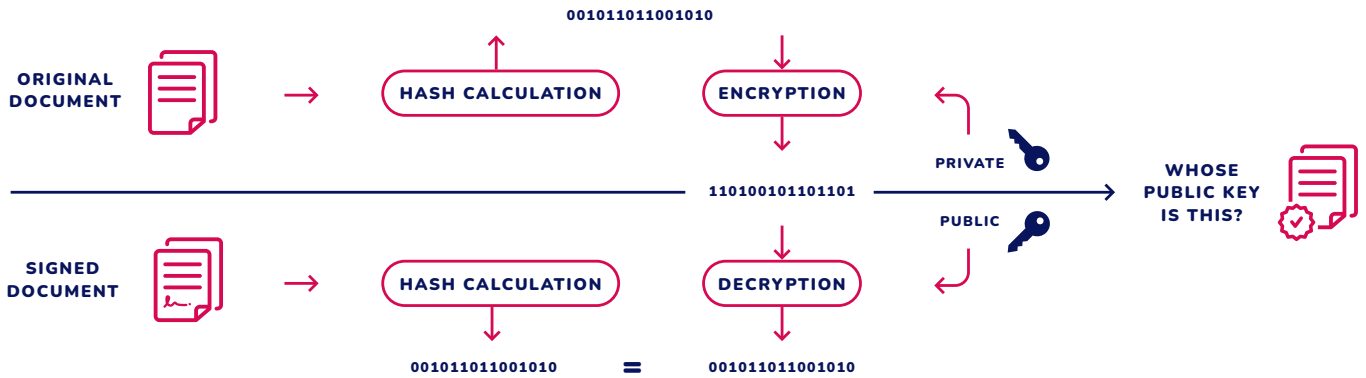
How do electronic signatures work?

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 he signs. 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 including the public key and other information, like 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 for example 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 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 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 in 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.

WITHOUT AUTHENTICATION

Manual scribble

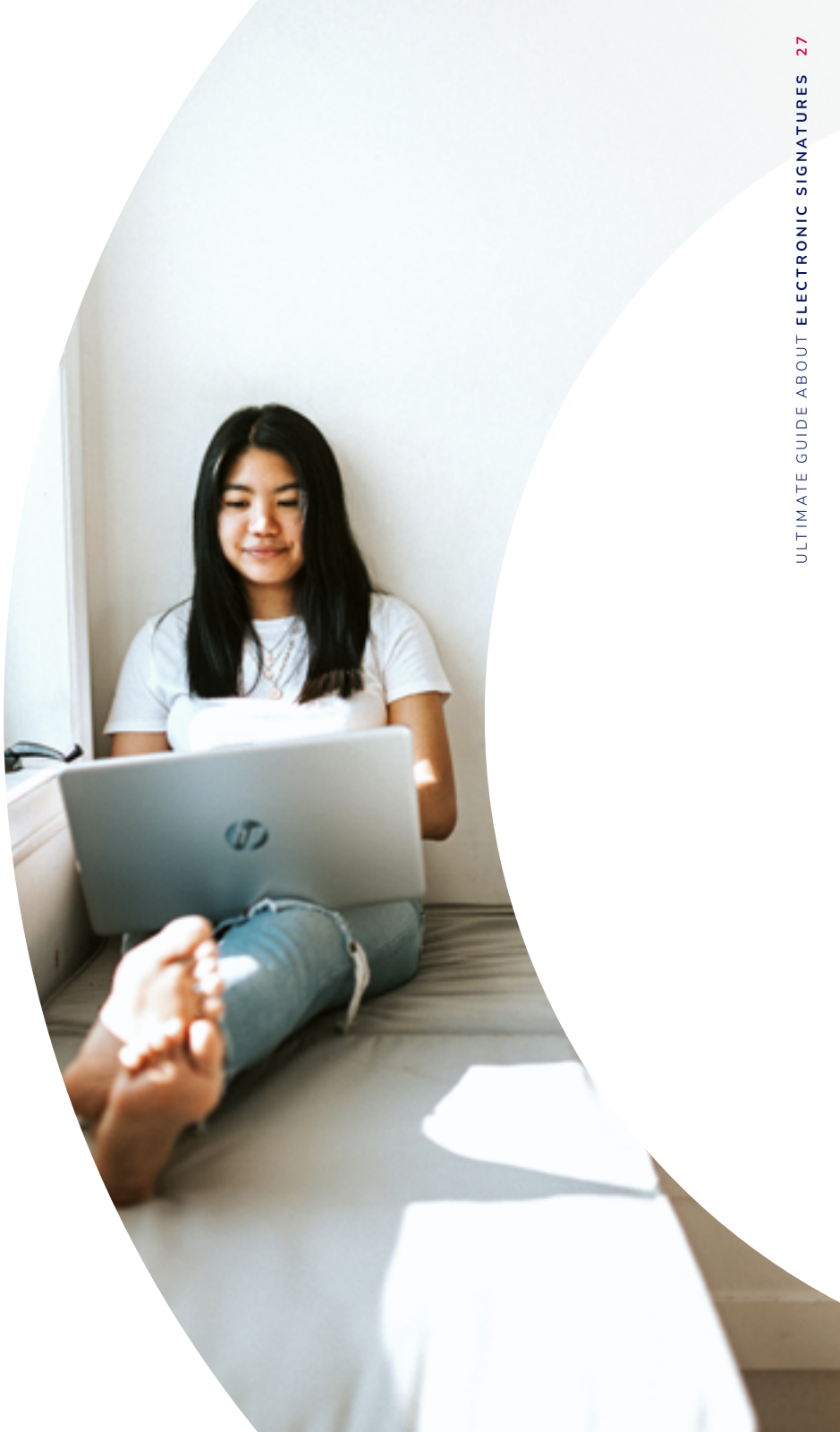
A basic, manual signature can be drawn on-screen by simply using your mouse or touchpad or using your fingers or a stylus on a touchscreen. This is also considered as an electronic signature.

Aa Handwritten signature

With this signing method you type in your name using your keyboard. You will then be able to choose from different preconfigured handwritten fonts to represent your signature.

OK Approval Button

A simple click with your mouse on an approval button. This results in an approval signature.



WITH AUTHENTICATION

Biometric Signature

To sign with a biometric signature a biometric signature pad or biometric pen is required. The signature pad and biometric pen allow to capture the 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. These biometric data are added to the signature, creating a unique biometric signature profile, which would allow the signature pad manufacturer to verify the authenticity of the signature when required.

Signing with a smartcard or token (USB)

The most commonly known kind of smartcard that can be used for electronic signing is the (national) electronic identity card of a country like for example LuxID, Estonian ID, .beID,... Other specific examples of smartcards are the Belgian Lawyer ID, the Common Access Card (CAC) or the Personal Identity Verification Card (PIV) in the USA, and many more.

This smart card contains a personal certificate with a private key which is issued by a qualified provider. In order to sign documents, the signer has to put the smartcard in the card reader or insert the token in the USB port and enter his or her personal PIN code to authenticate him or herself.

Login and password (including SSO)

- In some onboarding processes a user identifies himself by **choosing his username** (often email address) **and password** and sometimes by filling in some extra information. These credentials can be used to authenticate himself when signing documents electronically.

- If you want to go for a more secure login and password solution for signing, solutions like **Swisscom** enforce a one-time identification via **Face2Face** or **video** to ensure the signers identity. Afterwards the signer can choose to either create a login and password combination to reuse for authentication purposes or on the signer can choose to authenticate himself via a mobile application. 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.

- Also, the **SSO (Single-Sign-On)** principle is an example of signing with the **login and password** signing method. A person can use their credentials that are used to login to a company's platform to sign documents. This is often combined with a multifactor authentication.

With a one-time password (OTP) via sms or email

When signing with an SMT 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 case of an Email OTP, the email address of the signer is needed. 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.

A most common use case is that a user first creates his/ her mobile identity via an onboarding process. This can for example be by identification via an electronic id card or via the bank login methods. Afterwards the user creates a password that will be linked to his/her mobile ID. Once the Mobile identity is created it can be used for authentication in for example an electronic signature process. An example of a mobile identity is itsme® in Belgium. Because of the fact that the onboarding is related to the ID card or the banks KYC this becomes a very powerful signing method resulting in advanced or qualified signatures.

Public/ government/ initiatives

To access secure online government applications, some governments created authentication services. These authentication means can in some cases 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 in combination with MNO´s = mobile Network operators)

In some countries there are also bank initiatives that create your personal electronic ID for secure identification. The bank identity can either be mobile where your identity is stored on your mobile SIM card or otherwise via a hardware authenticator like bank card readers or one-button authenticators, ...

Bank identities are also a perfect method to sign documents in an electronical 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 are for example voice, facial characteristics, and fingerprints. After you are sure about the identity of the person 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 make sure that the chosen electronic signature solution fits with your customers' systems.

Most solutions are built to integrate with the latest operation systems and browsers, but do check if it runs smoothly on the latest versions before you choose and whether it has a flexible interface (API). For instance, Google Chrome no longer runs Java applets and other browsers may follow suit. Some electronic signatures use Java. Therefore check how the solution is performing in all commonly used browsers. You want to make it easier for your customer, not harder!

There are also standalone solutions offered in the market. They 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 an 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 mobiles 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 above, electronic signatures are valid and enforceable and have the same legal effects as their written equivalents. Of course, this is so long as the requirements, described by regulations and laws, are met. Depending on country to country and law to law, it still happens that certain documents require a handwritten signature to be legally valid. Therefore, we always recommend to contact 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 in- and outside the company.

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 cross-border? Does it comply with the latest eIDAS regulation for Europe?
- [ ] 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 organisation 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@connective.eu

www.connective.eu

CONNECTIVE