WHITEPAPER

Digital Signatures

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

CONNECTIVE

Introduction

Consumer purchases, business to business transactions, governmental administration are daily processes that require paper work which often needs to be signed. In this digital world many organisations aim to deal with these processes in both an efficient and secure way. Yet, **95% of all contracts** are still **on paper** with an analogue **'wet signature'**.

This has become an obsolete process as **digital signatures have become perfectly secure and time saving alternatives.**

In this whitepaper we will explain the difference between, electronic signatures and digital signatures, how they work and why they are inevitable for future proof businesses.

CONTENT

What is a digital 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.

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.

Technical and legal features of a digital 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.

The European legislation that oversees electronic identification and trust services for electronic transactions is called eIDAS (910/2014). This legislation recognizes different types of electronic signatures which will be explained later on in this document. The differences are mainly based on 2 key items:

1. the identity of the signer and
2. the integrity of the document.

Basically the question you have to ask, is "How sure are we about the identity of the signer?" and "How sure are we that the document could not be tampered with after signature?". Under eIDAS, all three signature types can be legally effective. The difference between them is the evidence that is needed to reassure a court that the signature is genuine and intentionally applied to a particular document.

Advantages of electronic signatures

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

1. 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 senior managers to return to the office, to obtain their signature;**
- ✓ **sign, print, scan and manually post a document;**
- ✓ **manually archive authorised 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. Digital 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;**

2. 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 digital 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.

3. Legal Compliance

In recent years, most countries worldwide have adopted legislation and regulations that recognise the legality of digital 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.

Digital 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.

4. 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 a digital signature. Thanks to the encryption of the document, you have the guarantee that the document remained unchanged after signing. With a digital signature you also always sign the whole lot of documents. There is no risk that some pages have been added or removed afterwards.

Digital 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.

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 digital signatures as your national ID can serve as a digital identity backing a digital signature, across borders.
Scalability	As manual actions diminish, more documents can be processed and more customers served.
Security	With digital 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.

Different types of electronic signatures & signing methods

On July 1 2016 the electronic IDentification, Authentication and trust Services 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.

First of all you need to know there are three types of electronic signatures:

1. Basic electronic signature (BES)
2. Advanced electronic signature or digital signature (AES)
3. Qualified advanced electronic signature or Qualified digital signature (QES)

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

1. Authenticity
Is the signature uniquely linked to the signer?

2. Identity
Are you capable to identify the signer?

3. Integrity
Is the signature linked to the data signed in such a way that any subsequent change in the data is detectable?

4. 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:

Signature type	Basic (BES)	Advanced (AES)	Qualified (QES)
Definition	All electronic types of signatures that prove acceptance or approval by the signer by using some sort of certificate. This can be a 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).	The Qualified or non-repudiation Digital 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 Qualified Trust Service Provider (QTSP) that is on the EU Trust List (EUTL) and thus certified by an EU member state.
Integrity Certain that content cannot be changed after signature?			
Identity of signer	Checking of the Identity of signer is not mandatory.	Identity of the signer is checked but not guaranteed.	100% Capable of identifying the signer. Initial face-to-face verification or another equivalent process is required.
Authenticity	Not mandatory that the signature is 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 signer.	Certain that the signature is created under the sole control of the signer. Multi-factor authentication is optional.	Certain that the signature is created under the sole control of the signer. Multi-factor authentication is required.
Hardware	No specific hardware mandatory.	Secure Signature Creation Device (SSCD) needed.	Qualified Signature Creation Device (QSCD) needed.
Legal validity	Burden of proof lies with the party that initiated the signature.	Burden of proof lies with the party that initiated the signature.	Non repudiative 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 requirements that are fulfilled mentioned above: Manual Biometric Banking card / iDIN SMS or mail a One Time Password (OTP)		The qualified electronic signature is currently widely available on smart cards, usb-tokens... However, new mobile initiatives are emerging (eg. Itsme®) .

How do digital signatures work?

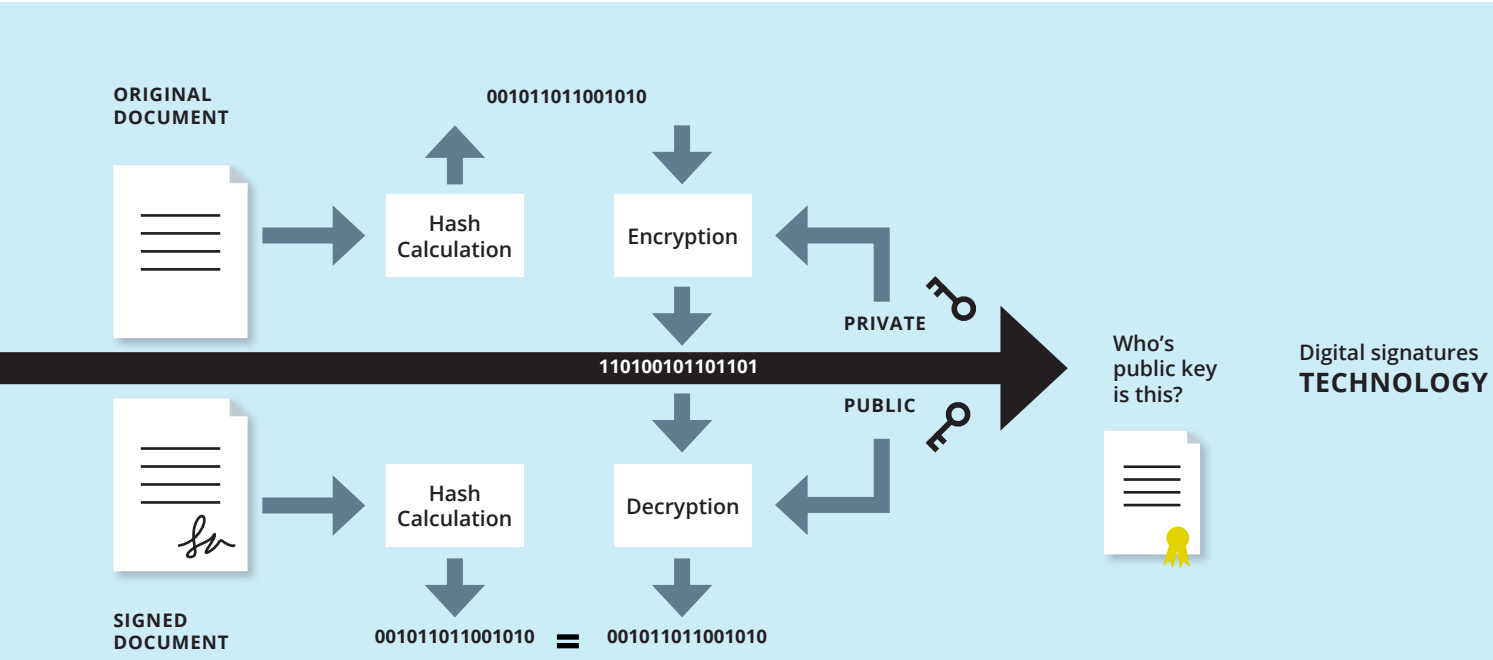
Digital signatures are based on a specific protocol, called Public Key Infrastructure (PKI). This protocol uses cryptographic algorithms to create two long numbers. These are called keys. One of the keys is public, the other one is private.

As digital 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 digital 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 digital 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 digital signature.



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 nowadays are cloud-based and work out-of-the-box with latest operation systems and browsers. Important as well is that your solution can be easily integrated in existing business processes through a flexible Application Programming Interface (API). Some solutions support the usage of smartcards and other external hardware devices for which often Java Applets are being used to communicate in browsers. Be aware, browsers such as Google Chrome don't longer support Java Applets, so always inform your supplier diligently on how the Customer Journey will look like. 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 digital 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.

Checklist for choosing an electronic signature solution

To help you choose the right electronic signature solution, we have created 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, US Sign act, 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.

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.

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 a digital 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?
- [ ] Is it device independent?
- [ ] 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 MS Dynamics, Salesforce?

Want to know more?

This document is a good start to learn the basics of digital signatures. If you want to know more about digital signatures and how it can be efficient for your organisation, please do not hesitate to contact us on **www.connective.eu/contact**

CONNECTIVE