White Paper

From Paper to the Cloud

Your guide to electronic and digital signatures

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

Your guide to electronic and digital signatures

This white paper walks through the basics of electronic and digital signatures (yes, there is a difference) as well as the latest related technologies and concepts – including remote signing.

CHAPTER 1

The what, why, and how of signatures

We'll use the first chapter as an introduction to electronic signatures, digital signatures, why they are needed, and how they work. Let's start with the basics: what signatures are used for. This is an important step in order to fully understand what's at stake with electronic and digital signatures.

What are signatures and why do we need them?

A signature can be defined as a unique and unchanging visual representation of a person – either physical person (a human) or legal person (an organization). Signatures are applied to documents for two purposes:

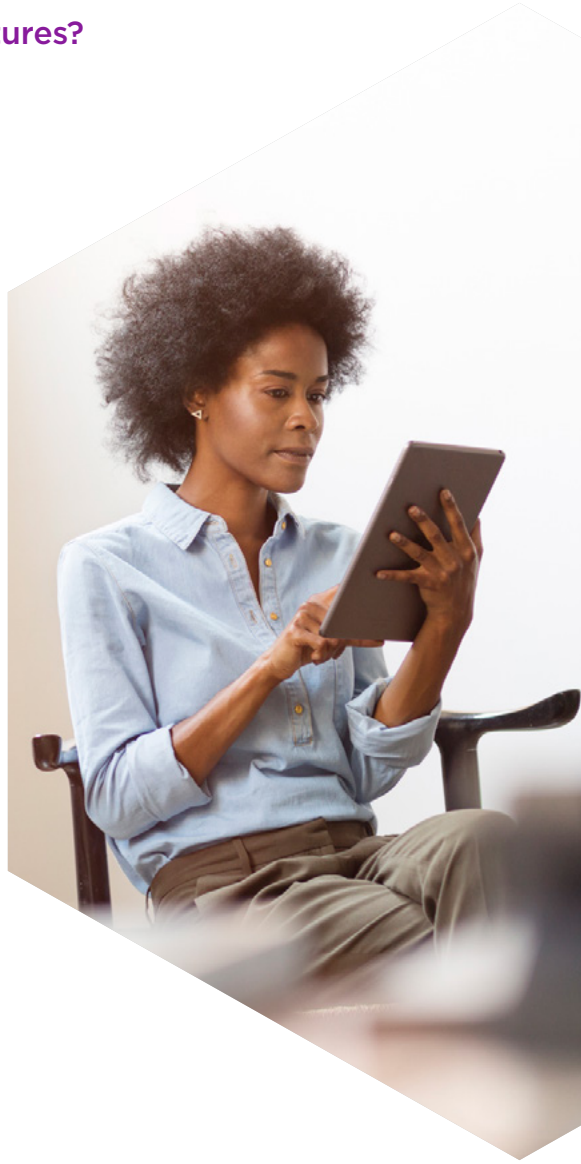
1. Certifying the **exactness** and **authenticity** of the document
2. **Engaging responsibility**, that is to say, approving or committing to honoring the terms written in the document

Signatures are legally binding, so disputes on a signature's authenticity are a logical consequence. To mitigate the risk of forgery and repudiation, signatures are traditionally made in the presence of witnesses.

However, in a world where technology is becoming ubiquitous and remote business has grown to become the new normal, in-person, paper-based signatures have become inconvenient and out of touch.

How do we safely replace in-person, paper-based signatures?

The word “safely” in the above title is crucial. Because simply replacing paper-based signatures for online transactions is nothing new. Electronic signatures have been around for decades. In fact, many countries introduced electronic signature regulations in the late ’90s, allowing for a successful transition from paper to online business.



But now that this online business model is skyrocketing, new scenarios and problems have emerged. The risks of forgery and repudiation have significantly increased. Many public and private organizations are still reluctant to accept electronic signatures, especially for documents carrying strong legal value, such as mortgage agreements, deeds, powers of attorney, certificates, contracts, etc.

What they wonder – and what you also might be wondering – is: How much of a risk are we taking if we accept an electronic version of a signature on this document? What happens if the signature is disputed?

As is often the case, technology came to the rescue. The term “electronic signature” has become an umbrella for various technologies used to certify exactness and authenticity, and engage responsibility. Countries followed suit with adjusted regulations, creating a more robust – and consequently more complex – matrix of requirements for electronic signatures.

CHAPTER 2

Electronic signature types based on trust levels

An electronic signature serves as a computer-recorded proof of intent, proof of consent to sign electronically, and proof of identity. That is to say, a recorded proof that the intended person created the signature and consented to sign electronically. In case of dispute, a court can examine whether the records of intent, consent, and identity behind the signature can be contested.[1]

This is why electronic signatures are categorized by their level of assurance, or in other words, how much they can guarantee the intent, consent, and identity of the signatory. You may see different types of electronic signature categorization on the internet. They often depend on the angle chosen by the author(s): country-based, industry-based, regulation-based, etc.

DID YOU KNOW ...

There's a difference between electronic signatures and electronic seals.

- **Electronic signatures** bind a document to a physical person (an individual)
- **Electronic seals** bind the document to a legal person (an organization); it's also called a corporate/business signature

The model we're presenting in this white paper is based on both technology and regulation aspects, as we consider how it applies to the largest scenarios globally:

- **Low Assurance:** basic electronic signatures
- **High Assurance:** digital signatures
- **High Assurance and Standardized:** regulated digital signatures

And each of these levels correspond to specific requirements and technologies. Let's take a closer look ...

[1] *Definitions and requirements for electronic and digital signatures are typically more elaborate than how they are described in this document and vary across countries and states. Questions related to legal aspects of electronic and digital signatures should be discussed with an attorney.*

Low assurance level: basic electronic signatures

In its most basic form, an **electronic signature** does not carry a high level of assurance. A basic electronic signature could be a mouse-drawn, stylus-drawn, or finger-drawn signature on a device, a scanned signature pasted on an electronic document, a name typed into a digital document, or simply checking a box or clicking on an "I agree" button.

Much like a paper-based signature, it can be very easily disputed. This is why a basic electronic signature should be used only when:

- The risk of legal dispute is considered low enough to be acceptable (e.g. approving internal documents).
- It's used in combination with other technology that will add further proof of intent, consent, and identity. For example, the date and time might be recorded as body of evidence, and a one-time password might be sent to the signatory via email or phone before signing. This would at least tie the signature to an email address or a phone number.

The human and financial cost of implementing basic electronic signatures is generally low, but cost may vary depending on the number of extra proofs you want to receive with the signatures.

QUESTIONS TO ASK YOUR LEGAL ADVISERS

Are there use cases where it would be acceptable for my organization to use basic electronic signatures?

Which recorded proofs would we need to have in order to justify the legally binding aspect of the electronic signature in court in case of dispute?

High assurance level: digital signatures

Technology has provided a "stronger" version of the electronic signature, called a **digital signature**. A digital signature not only provides proof of intent and consent, but also proof of identity, which is why we call it "high assurance." In the European Union, this type of signature can be called an "advanced electronic signature."

More details about the European Union/eIDAS are on page 10.

The technology used to generate digital signatures is called public key infrastructure (PKI). PKI has an incredibly large number of use cases. It's a technology that can be used to secure website traffic, online transactions, documents, code/software, devices, emails, and much more.

More details about PKI technology and how it works on page 12.

The majority of document management platforms offer basic electronic signatures by default. Only some of them offer digital signing capabilities – a feature that they may outsource to organizations who have the right infrastructure in place to support digital signing, such as Entrust.

Due to the higher complexity of their implementation, digital signatures are usually more expensive. But for scenarios where a certain level of trust is required, digital signatures are worth the effort because:

- **They have a higher assurance level.** We always recommend that you get legal advice for the validity of electronic and digital signatures for your use cases, but it's safe to say that, when properly implemented, digital signatures are harder to dispute than basic electronic signatures.
- **They are more secure.** This is because a digital signature is generated using a digital certificate, which contains the verified identity information of its owner, similar to a passport or an ID. Digital signatures also "lock down" the content of the document once it is signed, making it tamper-evident.
- **They are more regulated.** A growing number of countries and regions are adopting laws and regulations favoring digital signatures. Plus, we're seeing more and more technological standards being developed to improve the digital signing experience for users, without compromising security.

High assurance and standardized level: regulated digital signatures

Regulated digital signatures is a term we use for signatures that are regulated under a local regulatory regime. For example “qualified signatures” in the European Union, “secure electronic signatures” in Singapore, or “certified digital signatures” in South Korea.

Using a regulated digital signature provides the assurance that the digital certificate, the identity verification process, and the digital signature generation process are compliant with the local regulatory standards.

In countries and jurisdictions with a regulation in place for electronic and digital signatures, the task of maintaining digital certificates and a signing infrastructure is usually handled by government-owned or government-approved service providers who have met regulatory requirements. Such service providers may also be required to pass external audits to verify their compliance and apply to the national government authority to be recognized as the trusted service providers for electronic and digital signatures.

In the European Union, such service providers are called trust service providers (TSPs) or qualified trust service providers (QTSPs) where they have been awarded the “qualified” (higher level) status.

eIDAS: electronic signatures in the European Union (EU)

Let's look at a concrete example of a multi-tiered approach to electronic signatures with a distinction between low assurance, high assurance, and regulated high assurance signatures under eIDAS. eIDAS means "electronic identification and trust services." It's an EU regulation released in 2016 that provides a legal framework for the recognition of, among other things, electronic signatures across all countries of the European Union.

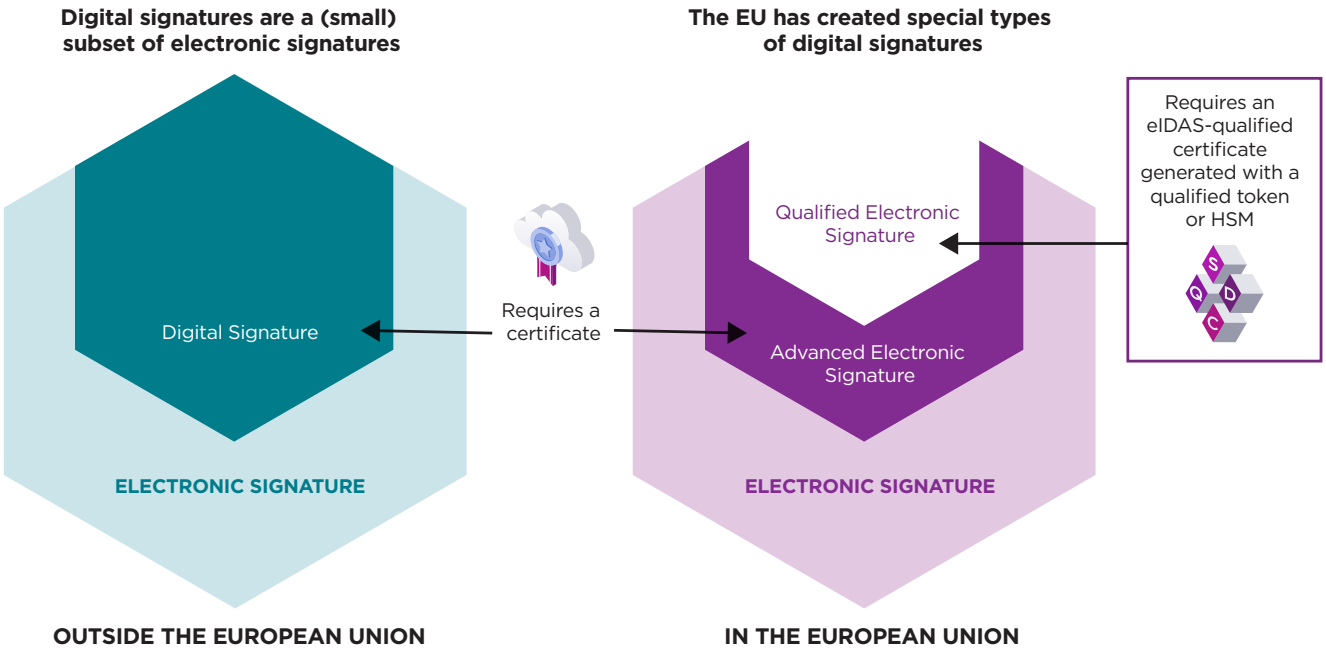
The objective of this regulation is to harmonize electronic signature standards across the EU member countries to help the organizations carry out cross-border transactions seamlessly and in an expedited manner.

eIDAS allows companies to choose which level of legal recognition they want to use, without enforcing digital signatures for all use cases.

Under eIDAS, there are three types of signatures:

- Basic electronic signatures (low assurance)
- Advanced electronic signatures (high assurance)
- Qualified electronic signatures (regulated, high assurance)

Comparing electronic and digital signature types

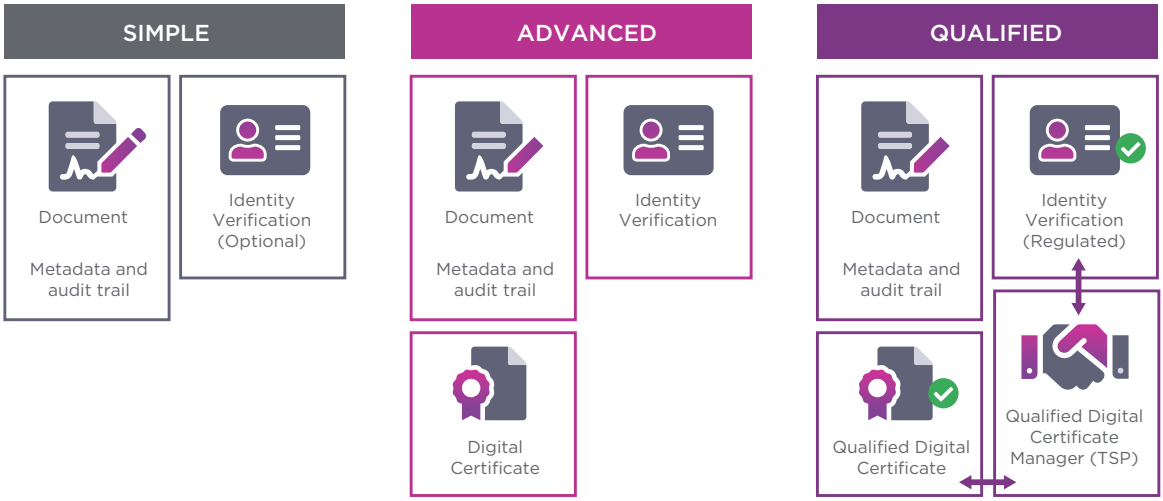


Qualified electronic signatures provide the strongest assurance level, which is why eIDAS sets stringent requirements for them. In short, they must be:

- Generated using specific protocols
- Generated using certified hardware
- Generated using a qualified certificate from a QTSP

But eIDAS doesn't decide which type of signature must be used under which scenarios. It's up to local governments to enforce certain types, or up to businesses to decide the level of assurance they want to use. Only qualified electronic signatures offer the highest level of trust. The expression "eIDAS-compliant signature" by itself therefore is not conclusive of the level of trust offered. The actual level of trust will depend on the type of electronic signature that is used.

Types of electronic signatures under eIDAS:



An electronic signature is defined under eIDAS as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign."

Thus, something as simple as writing your name under an e-mail might constitute an electronic signature.[2]

- An **advanced electronic signature** under eIDAS is in fact a digital signature, using a digital certificate from any TSP
- A **qualified electronic signature** under eIDAS is in fact a digital signature, using a qualified digital certificate and a qualified signature creation device, issued by a qualified TSP

Outside of the European Union, there are many other countries – such as Mexico, Singapore, and Japan – using a tiered approach. These countries often have one or more official, government-approved (typically government-owned) TSP(s). Not all signatures must be generated using these TSPs, but some official government documents might require it.

This is why it's important to obtain appropriate legal advice about the applicable local regulations. There could be some cases where the signatures you need must leverage a digital certificate from a specific TSP that's approved or managed by the local government.

[2] *Learn more about electronic signatures here at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Introduction+to+e-signature*

CHAPTER 3

The technology behind digital signatures

How PKI works

Digital signatures are a type of electronic signature based on public key infrastructure (PKI). PKI is a well-established technology used everywhere around the world for identity and security purposes.

You can think of PKI as a digital credential system for various *things*, including humans and machines – similar to how a passport works. These digital "passports," called digital certificates, are unique to their person/machine, and delivered upon verification of the person's/machine's identity. For a machine, it could be its MAC or IP address.[3] For a human, it could be their name and email address. For an organization it could be its legal name and address.

Similar to real-world passports, one must trust that the information contained in the digital certificate is correct. When you give your passport to a border control agent, they'll verify it's a genuine passport and they'll check which government issued it and whether they trust this government. The same goes for digital certificates. They include the name of the issuer, and computers can decide whether they want to trust this issuer or not.

What's the link between this and our document signatures, then? Well, these digital certificates are what signatures need to have strong proof of identity to avoid repudiation of the signature, and the issuers of digital certificates are the TSPs we discussed earlier.

TSPs are the entities tasked with delivering digital certificates. They verify people's and organizations' identities, and issue digital certificates for them. The identity verification process typically includes official database checks, ID verification, and even live video sessions depending on local requirements.

Once issued, these digital certificates can be used as part of a digital signing process where, for every digital signature created on a document, a copy of the digital certificate is included in the signature. This allows anyone to see the identity information associated with the signature and see the issuer (TSP) of the certificate.

SPECIFIC CERTIFICATES FOR SPECIFIC USE CASES

Contrary to real-world passports, digital certificates can be limited to specific use cases. For example, TLS/SSL certificates are digital certificates used exclusively as proof of identity for websites. Code signing certificates are used exclusively as proof of identity for software, etc.

[3] *We mention machine identity for illustration purposes only. This use case is out of the scope of document signatures.*

The digital signing process

A digital signature is more than just a visual mark on a document. It's actually a cryptographic operation, based on strong algorithms that will:

- Tie the signature to the exact content of the document
- Tie the signature to the digital certificate used for the signature

Hopefully this helps you understand why digital signatures are considered "stronger" than basic electronic signatures. The way they are generated makes them more authentic, provided that you trust that the identity information in the digital certificate was verified and is accurate.

1

Identity verification

The TSP verifies the identity of the employee and/or their organization.

2

Certificate issuance

The TSP issues them a digital certificate that contains this verified information as well as the name of the TSP.

3

Digital Signature

The employee generates a digital signature. The application used for the signature will ask for the digital certificate and embed a copy of it in the signature.

4

Signed documents

The digitally signed document will contain the organization's and/or employee's verified identities, the local signing time/date, and it will be tamper-evident.

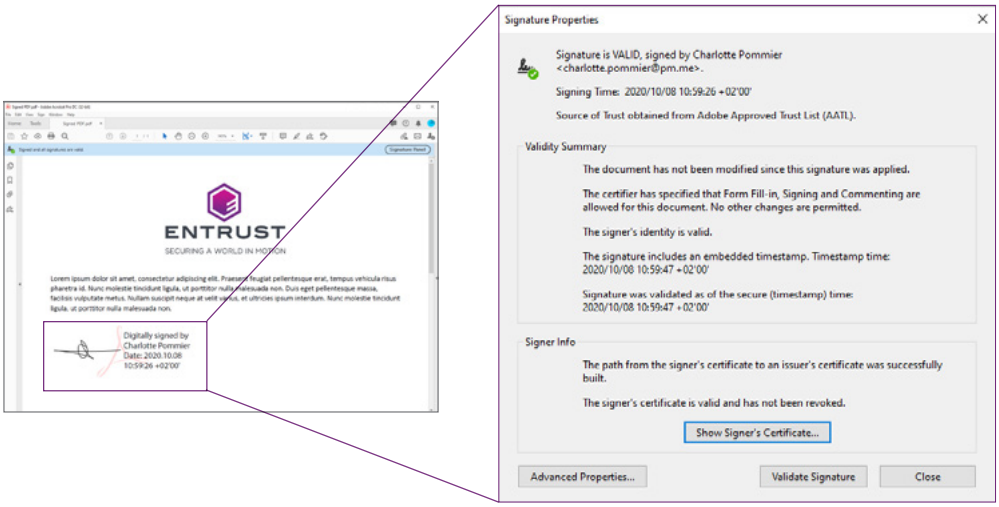
The digital signing process involves cryptographic algorithms based on public and private keys, which are a foundational element of PKI. However, this white paper will not cover the technical details behind these algorithms and the public/private key concepts.

For more information about PKI technology, go to our PKI solutions page

Note that a digital certificate can be used multiple times. You don't need to receive a new digital certificate every time you want to digitally sign a document. And just like real-world passports, digital certificates have an expiration date, set by the TSP. They are typically valid for up to three years but it depends on the TSP and the regulation they comply with.

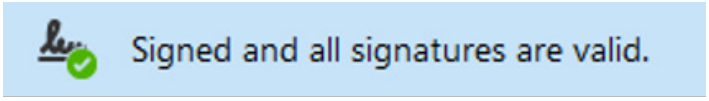
Many applications integrate support for digital signature generation and verification. PDF readers like Adobe Acrobat even provide visual indicators for the user to quickly find the name of the employee and the organization, and to see if any changes have been made to the document.

An example of digital signature displayed in Adobe Acrobat Pro

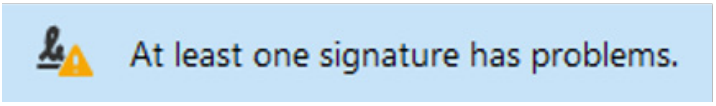


With Adobe Acrobat, signatures will be labeled one of three ways:

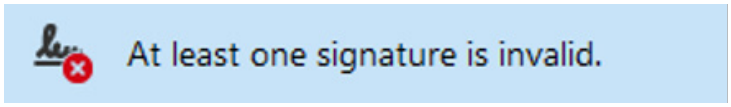
Valid and trusted. The document hasn't been changed since the digital signature was applied, the digital certificate is valid, and it was issued by a TSP that Adobe knows and trusts.



Valid but not trusted. The document hasn't been changed since the signature was applied, the digital certificate is valid, but it was issued by a TSP that Adobe doesn't know or doesn't trust.



Invalid. The document has been changed since the signature was applied.



As you can see, the concept of trust is quite important with digital signatures. Legal value set aside, a digital signature can be trusted or not by applications based on who issued the digital certificate. This is why it's always recommended to get your digital certificates from a TSP that is known and trusted by major PDF applications. In the case of Adobe, they have their Adobe Approved Trust List (AATL) program for approved TSPs, and they also recently created an additional list called EUTL (European Union Trust List), which contains all currently qualified TSPs in the European Union. These TSPs are therefore trusted by Adobe as well.

CHAPTER 4

Local and remote signing

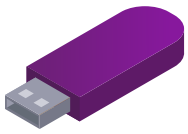
Now that you've reached this chapter, you should feel more comfortable with the concepts of electronic signatures, digital signatures, TSPs, and PKI.

We previously explained that digital signatures are more expensive than basic electronic signatures because of the complexity of their implementation. You need a digital certificate from a TSP (and sometimes you need a specific TSP that complies with local regulations) and you need an application that can generate digital signatures.

But what we haven't talked about yet is digital certificate storage.

Just like you wouldn't share your passport with anyone, you don't want to share a digital certificate that contains your identity details, because anyone who grabs it can digitally sign documents under your name. But a digital certificate isn't something physical like a passport, it's a computer file. You need a safe place to store it, and a computer, unfortunately, is not a safe place.

This is why TSPs must issue and store digital certificates for document signatures in secure hardware. If you ask a TSP for a digital certificate, they will verify your identity, then most of them will provide that digital certificate in one of two ways:



- **USB Token:** The TSP will ship a secure USB token to you (unless you already have a compatible USB token with you). These are not your typical USB tokens. They are specifically designed to host digital certificates, which cannot be extracted from the token.

- **Hardware Security Module (HSM):** The TSP will let you generate the digital certificate in your own HSM (if you don't have one already you'll need to buy one). This is a big device similar to a server, but dedicated to hosting sensitive material. It is much more powerful than a USB token, and can be connected to a network. This option is great when the digital certificate needs to be accessed from your local corporate network, or when you need to automate the signing process. But an HSM is much more expensive than a USB token.

Both these options are used in a "local signing" model. This means that the digital certificate is used by the local machine where the signature is performed; the USB token is plugged directly into the employee's computer, or the HSM is connected directly to the company's local network.[4]

[4] *Note that we've simplified the presentation of storage options. Digital certificates themselves aren't sensitive material; it's specifically the "private key" associated with the certificate that needs to be generated and stored securely using hardware. We've also simplified the certificate-generation process, as the full process is too complex for the purposes of this white paper.*

These local signing options are great when you want full control of the signing process, such as:

- When you own and manage the hardware and access to it
- When you can let employees sign without access to the internet

But managing secure hardware requires financial and human resources, as well as expertise in using these specific products. Managing hundreds or thousands of USB tokens in a corporate environment can be troublesome, especially since digital certificates expire and need to be renewed. Plus, USB tokens can be lost, they can't be plugged in to mobile devices, and many organizations do not allow USB ports to be used by employees.

Once again, technology comes to the rescue. With the explosion of cloud solutions, the possibility to host digital certificates in cloud HSMs helped to simplify the user experience and maintain good control over digital certificates.

Moving your digital certificates to a cloud service for your document signatures may sound like an obvious choice, but you remain in charge of managing access and content. It's always important to check that:

- Your company and/or industry policies allow this practice
- Your signing application supports signing processes with a certificate that is not stored locally
- Your cloud HSM service uses a communication protocol that is compatible with your signing application

Now you might think "A-ha! This scenario must be **remote signing** because the digital certificate is stored remotely." From a purely technical perspective, this is true. However, since the eIDAS regulation was created and with the development of technological standards to accompany this legal framework, remote signing has become a specific term representing a signing process where the certificate is hosted and managed by the TSP itself.

In a remote signing scenario as defined under eIDAS, the TSP bears an even more important role than before. It is responsible for:

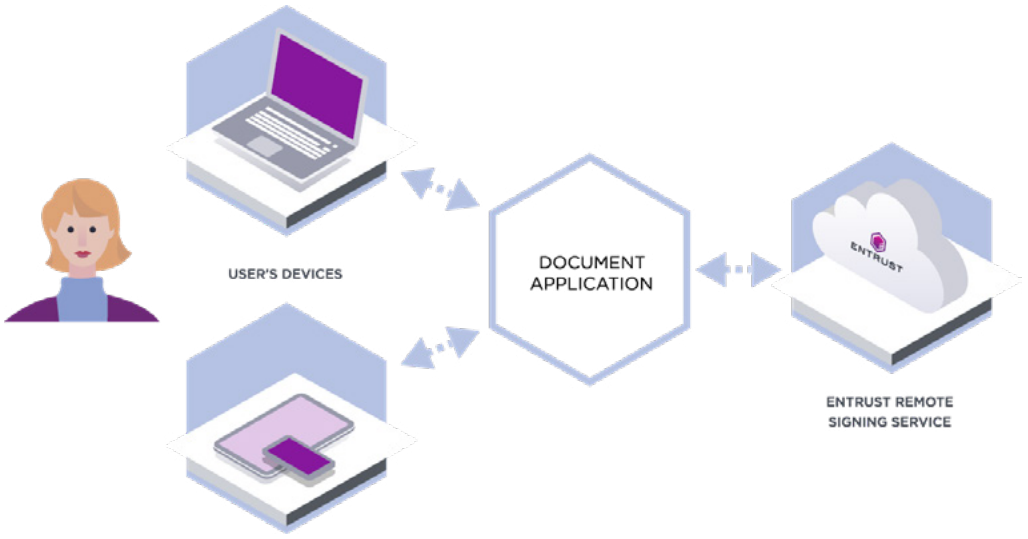
- Verifying identities
- Issuing digital certificates (and therefore maintaining a PKI)
- Securely storing the certificates
- Assigning each certificate to its rightful owner
- Ensuring only the owner can access their certificate

In a regulated environment like the European Union with eIDAS, TSPs must do all of these tasks using specific hardware, protocols, and standards, and they must get regularly audited. If they don't, they won't be considered a qualified TSP and won't be allowed to provide certificates for qualified signatures.

TSPs must strongly authenticate people who need to access their digital certificate for a signature. Authentication logs are securely recorded so TSPs can show when access to a digital certificate was requested and granted. Strong authentication typically involves one-time passwords via SMS or mobile app, email links, or even biometrics.

With today's new technology and new protocols, digital certificate owners don't need to connect separately to the TSP in order to retrieve their certificate. Instead, this is typically done by the document/signing application, which is connected directly to the TSP's remote signing service, making the user experience much smoother.

An example of remote signing using Entrust as TSP



Remote signing is gaining a lot of attention worldwide thanks to the strong layer of protocols that were created in order to standardize this practice. Many countries are adopting this model to provide digital signing services to their citizens, and we're seeing more and more companies looking for remote signing services because of the convenience it provides, since the entire signing service is handled by the TSP.

CONCLUSION

Taking the next step

This white paper was designed to help non-technical people understand the important concepts around electronic and digital signatures in a simpler way. We hope that you now feel more familiar with:

- The different types of electronic signatures and the naming conventions
- The specific benefits of digital signatures driven by related laws and regulations
- The PKI technology behind digital signatures and how they relate to TSPs, trust, and digital certificates
- The concepts of local signing and remote signing, which are specific to digital signing and depend on who is managing the certificate storage and access

Entrust is a global certification authority (CA) and a trust service provider (TSP). We live and breathe PKI and trust solutions, and are committed to providing digital signing products and services for all use cases you may have. Whether you're looking to buy Adobe-trusted digital certificates for document signing, buy secure hardware for your certificates, subscribe to a remote signing service, or even become a TSP, we have all the necessary components and expertise to help you achieve your goals.

Get in touch with us. We'd be happy to discuss your digital signing projects with you.

For more information

+44 (0) 118 953 3000
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223