DocuSign

Implementing Electronic Signatures and Digital Signatures with DocuSign

Whitepaper

Electronic and digital signatures around the world

Electronic signatures are broadly accepted throughout the world as an electronic replacement to handwritten signatures. Most laws define an electronic signature as electronic data that's logically associated with a document and used by the signer to indicate their agreement. For most use cases, customers and locations, a 'simple' electronic signature is sufficient. However, some transactions in certain countries, in heavily regulated industries or with governmental entities may require or prefer digital signatures, a type of electronic signature that offers a heightened level of identity assurance and security.

Digital signatures are based on a technology standard called Public Key Infrastructure (PKI), a widely accepted format that provides the highest levels of security and broad acceptance. PKI is a set of requirements involving the use of certificates and cryptographic keys that allow (among other things) the creation of digital signatures.

With PKI, each digital signature transaction involves a pair of keys—one private, one public. The private key isn't shared and is used only by the signer to electronically sign documents. The public key is openly available and used by those who need to validate the signer's electronic signature.

To protect the integrity of the signature, PKI requires that the keys be created, conducted and saved in a secure manner and often requires the services of a reliable Certificate Authority (CA). DocuSign is a CA in some key jurisdictions, including the European Union.

Around the world, there are international standards that govern the use of electronic and digital signatures as well as the methods used to authenticate a signer, like eIDAS. To learn the facts about current e-signature laws, visit the DocuSign eSignature Legality Guide.

The eIDAS regulation

In the European Union, all electronic signatures are governed by regulation 2014/910, known as eIDAS. The eIDAS regulation is applicable throughout the European Union and recognizes three types of electronic signatures: electronic signatures, advanced electronic signatures (AES) and qualified electronic signatures (QES). Customers can use DocuSign eSignature solutions to deliver all three.

The eIDAS regulation

These three electronic signatures offer increasing levels of legal protection, and as the level of assurance increases, the implementation requirements become more stringent. eIDAS doesn't prescribe which signature should be used for which scenario. As a consequence, the level of signature that organizations select is based on established and local industry usage, specific laws (e.g., German employment law) and the organization's risk tolerance.

Electronic signature is a signature in electronic form, appropriate for most use cases and simple to implement. Identity verification or authentication of signatories can be added, but isn't required.

Advanced electronic signature (AES) adds an identity verification requirement. Signatures must be uniquely linked to, and capable of identifying, the signer. In the event of a dispute involving an AES, the burden of proving the validity of the signature lies with the signer.

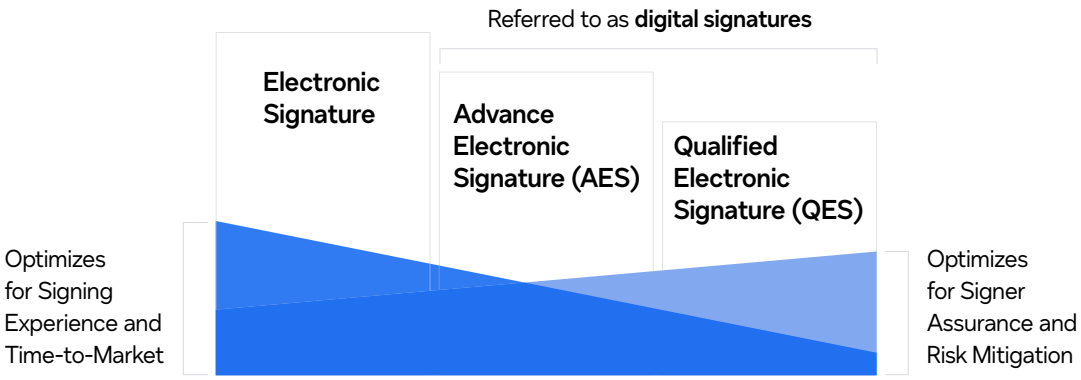
Qualified electronic signature (QES) requires face-to-face identity verification. The face-to-face identification can be live, in-person or via an audio/video connection. A QES is unique in that it's considered legally equivalent to a handwritten signature under eIDAS. A QES also shifts the burden of proof. The burden of proving the invalidity of the signature lies with the challenging party . Finally, the law on QES requires that every member state accept the validity of a QES even if it was executed in another member state of the EU.

While QES has a special legal status in the EU (more on that in the section below on QES), all three electronic signature levels ensure that the legal effect, and the admissibility of the electronic signature can't be refused just because the signature is in electronic form (eIDAS, Article 25-1).

Therefore, from a legal point of view, the differences between an electronic signature, AES and QES relate mainly to the ID verification process and where the burden of proof lies, as noted above. When a dispute does arise, the Certificate of Completion that DocuSign generates for each signing experience serves as an audit trail and proof of the transaction regardless of the type of signature used.

In the sections that follow, we explore in more detail the three electronic signatures, as defined by eIDAS regulation, as well as how DocuSign supports each of them.

There's a signer assurance spectrum for the three levels of signatures



Electronic signatures

An **"electronic signature"** is defined (eIDAS Art 3-10) very broadly as **"data in electronic form, which are attached or logically associated with other data in electronic form and which the signatory uses to sign."**

An electronic signature is appropriate for most use cases, such as internal documents, business-to-consumer transactions or agreements with existing partners or signers. It's simple and has few requirements associated with it, making it an efficient form of e-signature for most agreements.

Advanced electronic signatures

An AES is defined (eIDAS Art 3-11 and 26) more precisely than an electronic signature. In particular, an AES must:

- Identify the signatory
- Be uniquely linked to the signatory
- Be created using electronic signature creation data that the signatory can, with a high confidence level, use under their sole control

DocuSign offers two AES options, depending on whether the identification of the signer is carried out by DocuSign or someone delegated by DocuSign (e.g., a DocuSign customer).

AES with identity verification performed by DocuSign ID Verification

DocuSign supports AES by adding DocuSign ID Verification to DocuSign eSignature. With this solution, DocuSign identifies the signer by presenting an official proof of identity online.

How it works:

- When signers receive the document, they're asked to provide proof of identity, with the option to submit an electronic ID or a photo of their passport, identity card or driver's license using their computer or mobile device.
- DocuSign then:
    - Checks the authenticity of the identity document, extracts the name and compares it to the signer name specified by the sender
    - Generates a digital certificate validating the signer's identity
    - Allows the signer to use the digital certificate to sign the document and creates a Certificate of Completion associated with the transaction
- Senders can also choose to retain elements of identity data (including a copy of the ID document) and export that data to their own systems of record for audit or compliance purposes.

AES with identity verification delegated to a third party

As an accredited Trust Services Provider (TSP) in the EU, DocuSign also supports AES by combining DocuSign eSignature with delegation of the AES signer identity verification to the DocuSign customer requesting the signature.

With this option, DocuSign customers are responsible for identifying the signer.

How it works:

- Before creating the envelope, the DocuSign customer verifies the identity of the signer and collects their phone number, which is used to send a one-time password via text message
- The sender prepares the document to be signed by selecting the AES option from their sending experience screen
- The sender is prompted to add the signer's phone number, upon which DocuSign sends the signer a one-time password prompt and the document to sign (the sender can also send an access code to the signer using a source outside of DocuSign)
- The signer opens the document on their device and is prompted to sign
- Once the signer adopts their signature, a prompt asks them to enter their one-time password or access code
- The signer's AES signature is confirmed and DocuSign generates a Certificate of Completion
- The certificate, which is associated with the signature, contains proof of the authentication process used to confirm the identity, the signer's IP address and email and the timestamp of different steps in the transaction
- DocuSign also stores, as required by law, proof of the identity verification

---

Qualified electronic signatures

Under EU law, a QES is legally equivalent to a handwritten signature (Article 25.2). In certain EU member states, a QES is mandated by law for specific use cases. Additionally, organizations may choose it for certain agreements. A QES offers non-repudiation and shifts the burden of proof in the event of a dispute. In this instance, the burden of proving the invalidity of the signature lies with the challenging party (i.e., the party that's contesting the validity of the QES).

A QES is a convenient option in cross-border transactions within the EU, because a QES issued in one EU member state must be recognized as such in another. On the other hand, a QES requires the signer's identity to be verified face-to-face or through an equivalent process performed by a certified agent. In the past, this presented a barrier to adoption. However, the emergence of artificial intelligence and online identification services is making this face-to-face requirement more and more affordable, enabling signers to identify themselves using their smartphone camera.

DocuSign ID Verification Premier

Tightly integrated into the DocuSign eSignature workflow, IDV Premier is our identity verification solution with the highest level of compliance and security. Through AI-enabled advanced liveness detection, selfie comparisons and asynchronous reviews by approved agents, IDV Premier helps organizations achieve the rigorous biometric identification requirements for QES in a much faster timeframe for a superior signer experience.

How it works:

- DocuSign presents the document to the signatory for signature. Before being able to access the document, the signer will need to confirm their identity by performing various video checks:
    - **Liveness checks:** In order to ensure that the signer and their ID document are physically present at the time of capture, the signer will be asked to record random parts of the ID document. This also helps mitigate against any risks of Deep Fakes.
    - **Selfie comparison video:** While recording themselves, the signer will be asked to perform certain easy tasks. This step confirms that the signer taking the selfie matches the photo on their ID.
    - **Asynchronous review:** The ID and video recordings are then sent to a certified agent who reviews everything within minutes.
- Once all the checks have been completed and the identity of the signer is confirmed by the agent, the signer can then access the document.
- Before returning the document to the sending party, the signer will need to enter a one time passcode sent to their phone number. This final step signals the signers intent.

DocuSign ID Check Remote for QES

DocuSign offers remote video identity verification conducted by certified agents through our preferred partnership with IDNow. Integrated into DocuSign eSignature, the video face-to-face identification happens the first time the signer uses the IDnow service, after which, the signer may create an account that can be reused for future QES signings for two years without the need for additional video identification.

How it works:

- DocuSign presents the document to the signatory for signature and, if the person is using ID Check Remote for the first time, starts a video session that connects them to an agent who asks them for their mobile phone number and proof of identity

- The agent:

    - Verifies the identity of the signer by comparing the name on the document with the name specified by the sender

    - Confirms that the photo shown on the document corresponds to the person present in the video chat

    - Checks the authenticity of the ID document by examining the security features visible in white light

- DocuSign then:

    - Obtains consent from the signer to sign through two-factor authentication (access to their personal account and a one-time code sent by SMS to the their mobile phone)

    - Applies the digital signature to the document

    - Generates a qualified electronic certificate associated with the signatory and the transaction

    - Executes the qualified electronic signature on behalf of the signatory in accordance with article 30 and Annex II-3 of the eIDAS regulation

    - Generates the Certificate of Completion associated with the signature

DocuSign ID Check In-Person for QES

This option is well suited to cases where the sender (usually a DocuSign customer) has already met the signer in a face-to-face meeting before the signing action or is meeting the signatory face-to-face at the time of the signing action, as in the case of an in-person sale.

With this option, DocuSign delegates the identity verification to the DocuSign customer. As part of this process, the sender also captures the phone number of the recipient, which is used to confirm signing intention through a one-time access code sent via SMS.

How it works:

- DocuSign presents the document to the signer for signature
- The signatory applies the representation of his signature on the agreement
- DocuSign asks the signer to capture a photo of their proof of identity (passport, identity card or driver license) using their smartphone's camera
- DocuSign then:
    - Checks the authenticity of the identity document, extracts the name and compares it to the signatory's name specified by sender
    - Obtains their consent to sign by sending an access code to the mobile phone that was provided by the sender when creating the envelope
    - Generates a qualified electronic certificate associated with the signatory and the transaction
    - Executes the qualified electronic signature on behalf of the signatory on a qualified signature creation device operated remotely
    - Generates the Certificate of Completion associated with the signature

QES using an existing qualified certificate

Beyond its own product offerings, DocuSign accepts and supports all QES stored on physical electronic IDs (eIDs), smart cards and USB tokens issued by qualified providers on the **EU Trust Services List.**[1] The EU Trust List tracks all Qualified Trust Service Providers (QTSP) across the European Union, and the DocuSign eSignature interface allows the signer to produce a digital signature using a device with a qualified certificate.

This option is designed for businesses whose employees are issued a smart card or USB token with a qualified certificate or whose customers carry a device that contains a qualified certificate.

Several EU member states provide their citizens with digital certificates on a smart card or eIDs, such as Germany, Belgium, Estonia and Spain, so they can be used to sign agreements with an eIDAS-compliant digital signature.

Digital signatures with certificates issued by trust service providers

In addition to the options above, DocuSign generates digital signatures using digital certificates issued by TSPs. Since these TSPs are accredited by national certification bodies around the world, the signatures obtained by using their digital certificates are legally binding and comply with the local regulations and standards for what an advanced or a qualified signature represents.

DocuSign supports signing with digital certificates in two ways:

- **In the European Union, DocuSign issues eIDAS-compliant digital certificates:** DocuSign is a QTSP on the EU Trust List and is accredited by the French National Authority. Thanks to the European Union's Internal Market Principle, digital certificates issued by DocuSign France are valid, legally binding and accepted by every one of the 27 EU Member States.

- **Integrated with local TSPs around the world:** By supporting signing with certificates issued by TSPs accredited by local authorities in dozens of countries, DocuSign offers the ability to generate digital signatures that are legally binding, and compliant with local regulations. This local, digital signature compliance allows DocuSign customers to sign agreements around the world using a trusted, single solution.

[1]The Member States of the European Union and European Economic Area publish trusted lists of qualified trust service providers in accordance with the eIDAS Regulation. The European Commission publishes a list of these trusted lists, the List of Trusted Lists (LOTL). The European Commission, through the CEF Digital program, provides this tool for anyone to browse the national trusted lists and the LOTL.

Conclusion

Electronic signatures are a fast and simple way of signing agreements and can be used in nearly all the same instances as handwritten signatures. Digital signatures, a type of electronic signature, offer a heightened level of identity assurance, like electronic "fingerprints." They securely associate a signer with a document in a recorded transaction in the form of a coded message.

DocuSign supports electronic and digital signatures around the world, including the three signature levels defined by the European Union through the eIDAS regulation: electronic signatures, advanced electronic signatures and qualified electronic signatures. This allows companies of all sizes to complete approvals, agreements and transactions faster while staying compliant with eIDAS.

This support also includes cloud-based digital certificates that contain public keys for the digital signatures and specify the identities associated with the keys. These certificates are used to confirm that the signature belongs to the person who signed the document. Along with the digital certificate that all Certificate Authorities provide, DocuSign also generates a Certificate of Completion that serves as an audit trail and proof of the transaction for all signing parties.

Altogether, DocuSign provides a smooth signing experience for organizations who must comply with eIDAS and other similar regulations around the world. For more information on e-signature requirements around the world, see the eSignature Legality Guide and consult your organization's legal counsel.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
Visit www.docusign.com
Call +1-877-720-2040