DocuWare

White Paper
Electronic Signatures with DocuWare

Secure business processes through trust in documents

December 2021

This document was created using AuthorIT™.

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

DocuWare GmbH
Planegger Straße 1
D-82110 Germering
www.docuware.com

DocuWare

Contents

1 Secure business processes through trust in documents

Trust forms the basis for any cooperation or exchange of goods and information, be it within a personal or an official business setting. In contracts or other agreements, the binding symbol of this trust is a person's signature.

What was once exclusive to paper and pen is now achieved with an electronic signature, creating a binding commitment in the same way as the handwritten signature does – with business partners all over the world. Signatures create legal certainty for your documents even over long distances.

Almost all industries have adapted to workforces that collaborate from different locations, including home and mobile offices.

Cloud signatures contribute significantly to your business success by providing legal verification for documents while ensuring business continuity and productivity.

Demonstrate document integrity and authenticity

Every day we write or receive vast amounts of documents. Some of these do not require any documentary proof in a business or official setting. Other documents, such as certain contracts, must be legally watertight so that a court would also consider them to be binding. Depending on the industry, process, preference, your company's location and with whom it works, rules vary to establish legal certainty.

With electronic signatures, you create certainty for three essential factors:

- Authenticity: The document is genuine.
- Integrity: The contents of the document have not been changed.
- Origin: The person who created the document can be identified.

Electronic signatures for networked business and remote work

Business documents are no longer exclusive to physical corporate offices. They are also employed in home offices and mobile working. This distributed environment demands the need for binding principles and legal certainty even over long distances. Electronic signatures help employees fulfill their responsibilities immediately and from any location. After all, a process should not come to a standstill because an employee cannot sign a document when working on the move due to a lack of printing options.

Execute location-independent transactions in compliance with the law

Although legal models vary in strictness across regions, one thing is clear: the hardware security modules for generating digital certificates can be located in highly secure cloud infrastructures anywhere.

Where a physical smartcard and card reader was once necessary, today you can connect via verified signature providers that are certified in line with clear security standards. In this way, the data exchanged during the signature process is also secure.

Sign from any device

Through the integration of electronic signatures into automated workflows, companies can complete all processes in a legally secure manner, regardless of the device used. This includes signatures provided on computers, tablets, and mobile devices both company and customer owned.

The transaction data is secure and protected. With modern signatures, companies meet the compliance requirements of their respective regions, both in terms of information security and data protection.

Authentication and identity transmission

Many documents, such as contracts, are created and signed by one person within an organization and then countersigned by a person outside the organization. In these cases an advanced electronic signature is very often used. Recognized procedures for this are confirmation via access code, phone, SMS, or knowledge based authentication.

However, depending on the requirements of the signature, it may be necessary to verify the identity of the signatory beyond any doubt. In theses cases a qualified electronic signature is recommended. This verification is performed using a third-party provider who authenticates the user and thus ensures their identity when signing.

What to consider when making a decision

If you want to use electronic signatures in your company, you should consider these questions, among others:

- Is the signature solution suitable for proving the integrity and authenticity of the documents?
- Does the signing process take place in automated workflows in which employees with remote workstations can also be included?
- Does the solution offer signing on both customer and company owned devices?
- Does the solution allow you to sign with different security levels (advanced or qualified electronic signature)?
- Is the data of the signature process stored in a legally compliant manner in the desired data protection region?
- Does the signature service provider use highly secure HSM modules with proof of compliance?

2 Signing documents in the workflow with DocuWare

With DocuWare Signature Service, you apply an electronic signature to your documents in a workflow. Two factors ensure scalability and future-readiness for your company:

- By signing within workflows, you keep the time and effort needed by your employees as low as possible, while accelerating entire processes.
- You use remote signatures, also known as cloud signatures, and are therefore independent of the work location of those involved.

With cloud signatures, the signing process takes place in the cloud via the Internet, regardless of whether you work with DocuWare Cloud or with an on-premises system from DocuWare. No locally installed software or hardware is required.

The DocuWare Signature Service ensures that your documents are signed by a recognized, verified signature provider. The service offers you maximum speed and flexibility when using electronic signatures:

- Seamlessly integrate external signature providers such as Validated ID or DocuSign into your DocuWare workflows. The documents are automatically transmitted to the service provider and the recipient also automatically receives a notification when a document is available for signature.
- Collect signatures for a document from all relevant signers in a timely manner.
- Advanced or qualified? You choose the security level for the signature according to your requirements. The main difference is the authentication procedure. In the case of an advanced signature, for example, a two-factor authentication of the signatory (such as email or SMS) is sufficient. For a qualified signature, the certificate of a trust service provider is required for authentication.
- The qualified certificates for a qualified electronic signature are stored centrally with an external service provider so that they can be used at any time.
- You store the document together with the signature in the archive in an audit-compliant manner.

Flexible and legally compliant

With DocuWare, you can design electronic signing flexibly and meet all the specifications that your industry or the legislator makes for your processes. For example, use these options:

- Sign a single document in multiple places, for example, a contract on pages 1, 3 and 7.
- Combine multiple stapled files into one document and have them signed as individual sections. This way, the signer cost-effectively receives only one document consisting of multiple files as in one envelope. This is useful, for example, when a standard confidentiality agreement is to be signed with a contract. (DocuSign only)
- Set a deadline for signing. After the expiration of this period, counted from the sending of the signature request, the signer no longer has the possibility to sign the document.

- Set up reminder emails. If a signer has not signed a document within a certain period of time, they will receive a reminder.
- Ensure that the signer receives a copy of the signed document as an email attachment after signing.
- Apply an electronic company stamp, also called a seal, to your documents before sending them to the signer. This is how you prove the documents are genuine (authenticity) and unaltered (integrity). (Validated ID only)
  Such a seal works technically like an electronic signature and can have an advanced or a qualified certificate. The difference is: the electronic seal is always linked to a legal entity, i.e. a company, a public authority and other organizations. The electronic signature is always associated with a natural person.

3 How your processes benefit from electronic signatures

Signing in workflows is suitable for many business processes. The following scenarios are examples of a wide variety of business areas.

Paperless processing of contracts

Enter contracts seamlessly and without delay, for example leasing contracts for equipment.

Signing of employment contracts

With remote and distributed workforces, your HR department can have many types of employment contracts signed without delay and without the signatory being physically present. This not only saves costs for paper and postage, but also shortens the process enormously. If you are investing a lot of money in recruiting qualified employees, the signing of the employment contracts must not be delayed just because there is no digital signature process. Electronic signatures also enable new employees to complete the hiring and onboarding process 100% remotely.

Human resources

For corporate compliance, you can have employees electronically sign SOPs, work instructions, non-disclosure agreements, or other agreements in the workflow seamlessly and without delay. If your employees work in a remote office, electronic signatures can help ensure that everyone applies the same standard of trust. For audits and certifications, all evidence is available in the archive in a legally compliant manner and can be presented at the click of a button.

Provisioning of IT equipment

Equipment provisioning is a key component of an onboarding process and results in lost time and increased costs for inefficiencies. Automated workflows result in streamlined processes and electronic signatures allow employees to efficiently sign for the receipt of any equipment. This is also suitable for providing devices for home office work.

Loans for customers

A trading company or distributor grants its customers lines of credit. Related documentation and contractual agreements are automatically routed for customer review. Customer signatures are performed electronically on any available computer, tablet, or mobile device.

4 Signature service providers for DocuWare

DocuWare works with signature service providers such as Validated ID or DocuSign to sign documents in a DocuWare workflow. Both are trust service providers (TSPs). The signature procedures of Validated ID and DocuSign offer different authentication procedures that you can specify depending on the signature method you choose.

The signature methods are the Advanced Electronic Signature (AES) and the Qualified Electronic Signature (QES), which are explained in more detail in Compliance through electronic signatures worldwide (page 17).

Validated ID

Validated ID usually sends an email to the signer with a link to the document. The signer can choose from the following authentication methods for signing, depending on how the request was submitted and the associated AES or QES signature method:

- Remote – authentication by SMS (AES)
  When a document is sent to Validated ID for signature, the recipient gets an SMS message allowing them to sign the document.
- Biometric – on-site authentication (AES)
  A customer signs on a tablet. Biometric data such as writing pressure and speed are recorded and embedded in the document with the signature. The devices used must be registered in advance and are thus known to the signature service provider (supported devices). Only in the case of the biometric option will a document be sent directly to a registered device for signature.
- Centralized – one-time authentication with the signature service provider (AES / QES)
  With this signature, Validated ID stores a certificate that confirms the user's identity after identifying the user. This allows users to authenticate themselves and sign documents with Validated ID from anywhere and at any time.

DocuSign

DocuSign sends an email to the signer with a link to the document. The person initiating a signature process can choose from the following authentication methods for signing, depending on how the request was submitted and the associated AES signature method:

- No special authentication (AES)
- Authentication by telephone call (AES)
- Authentication by access code, for example password (AES)
- Authentication by SMS (AES)
- Knowledge-based authentication (AES). In this method, available only in the U.S., signers answer specific questions about themselves, the answers to which are available from public records (e.g., current and previous addresses).

5 How electronic signatures work in DocuWare

For a document to be signed with the DocuWare Signature Service (such as a contract), it must first be stored in a file cabinet. The service is then started within a workflow task.

After this trigger, several steps take place between person 1 who requests a signature in a DocuWare workflow and person 2 who signs the document. Both can also be identical.

In principle, the signing process with the DocuWare Signature Service always looks the same:

1. The workflow sends information about the document and the signature to the Signature Service.
2. The DocuWare Signature Service loads the document from DocuWare and transfers it to the signature service provider.
3. The signature service provider informs the signing person by email.
4. The person signing opens the link sent with the document and starts the signature process.
5. The signature service provider authenticates the person signing the document.
6. The signature is linked to the document.
7. The signature service provider informs the signature service about the signed document.
8. The DocuWare Signature Service loads the document from the signature service provider and stores it in DocuWare.

A document can be signed by a single person or by several persons. The signing process is always the same for each signer, because an electronic signature is always bound to the person who executes the signature.

Which type of signature is chosen - so advanced (AES) or qualified electronic signature (QES) - always depends on the type of document, legal requirements if one or more persons should sign it, and at what signature security level. Read more about this in chapter Compliance through electronic signatures worldwide (page 17).

The various signing options

The signing procedures differ mainly in the authentication method. The authentication options described below assume that: Person 1 (P1) works in a company that uses DocuWare. Person 2 (P2) can be an internal colleague or an external business partner, but does not have to be a DocuWare user. It is always person 1 who requests the signature within a workflow and person 2 who signs.

Validated ID: Remote (AES)

Person 2 does not need to register with Validated ID.

Steps:

1. P2 tells P1 their name, email address, and SMS-enabled phone number.
2. P1 enters the data of P2 in the workflow form and thus requests the signature from Validated ID.
3. P2 receives an email with the link to the document and an SMS with a TAN, which they use to trigger the signature.

Validated ID: Biometric (AES)

Person 2 does not need to register with Validated ID.

Steps:

1. P1 sits at a company reception and visually checks the identity of visitor P2. P1 confirms the identity of P2 and enters their name in the form in a workflow task. The information is sent to a signature tablet.
2. P2 signs on the tablet, thus storing biometric data such as the writing pressure for possible later verification.

Validated ID: Centralized (AES)

Person 1 and person 2 work in the same company that has a contract with Validated ID. P2 is registered with Validated ID.

Steps:

1. P2 tells P1 their name, email address, and the user ID that P2 received from Validated ID upon authentication (which can be, for example, a passport number).
2. P1 enters the data of P2 in the workflow form and thus requests the signature.
3. P2 signs the document.

Validated ID: Centralized (QES)

Person 1 and person 2 work in the same company that has a contract with Validated ID. P2 is registered with Validated ID and has undergone separate identification with Validated ID for a qualified certificate.

Steps:

1. P2 tells P1 their name, email address, and the user ID that P2 received from Validated ID upon authentication (which can be, for example, a passport number).
2. P1 enters the data of P2 in the workflow form and thus requests the signature.
3. P2 signs the document with the qualified certificate.

DocuSign: No authentication (AES)

Person 2 does not need to register with DocuSign.

Steps:

1. P2 tells P1 their name and email address.
2. P1 enters the data of P2 in the workflow form and thus requests the signature from DocuSign.
3. P2 receives an email with a link to the document in DocuSign, where they sign it.

DocuSign: Authentication via SMS (AES)

Person 2 does not need to register with DocuSign.

Steps:

1. P2 tells P1 their name, email address, and SMS-enabled phone number.
2. P1 enters the data from P2 in the workflow form and thus requests the signature from DocuSign.
3. P2 receives an email with a link to the document in DocuSign. P2 receives a TAN from DocuSign via SMS, which they use to trigger the signature.

DocuSign: Authentication via telephone call (AES)

Person 2 does not need to register with DocuSign.

Steps:

1. P2 tells P1 their name, email address and telephone number.
2. P1 enters the data of P2 in the workflow form and thus requests the signature from DocuSign.
3. P2 receives an email from DocuSign with a link to the document as well as information received by phone call, e.g. a code, with which P2 triggers the signature.

DocuSign: Authentication via access code (AES)

Person 2 does not need to register with DocuSign.

Steps:

1. P2 tells P1 their name and email address.
2. P1 enters the data of P2 and a code (e.g. password) in the workflow form and thus requests the signature from DocuSign.
3. P2 receives an email with a link to the document in DocuSign.
4. P2 actively transfers the code to P1. This can be done verbally (face-to-face conversation, telephone call) or via a prior agreement (for example, date of birth or a membership number can always be used as the code).
5. P2 uses the code to trigger the signature.

DocuSign: Knowledge-based authentication (U.S. only, AES)

Person 2 does not need to register with DocuSign.

Steps:

1. P2 tells P1 their name and email address.
2. P1 requests the signature and transmits the name and email address of P2 to DocuSign.
3. P2 receives an email with a link to the document and must answer a personalized, knowledge-based multiple-choice question from DocuSign.

6 Licensing

To use the DocuWare Signature Service with Validated ID or DocuSign, you sign a service contract with one of them. Depending on whether you work with DocuWare Cloud or a locally installed system, you need the following license elements.

	DocuWare Cloud	On-premises systems
Signature Service	Included	Add-on license *Electronic Signature Integration* needed
Client licenses	The Signature Service requires its own DocuWare Client license	The Signature Service requires its own DocuWare Client license
Further DocuWare licenses	---	- Workflow Manager - Valid maintenance and support contract
Signature volume	Has to be purchased additionally from the provider or – for Validated ID – also from DocuWare	Has to be purchased additionally from the provider or – for Validated ID – also from DocuWare
Signature certificate	Has to be purchased additionally	Has to be purchased additionally

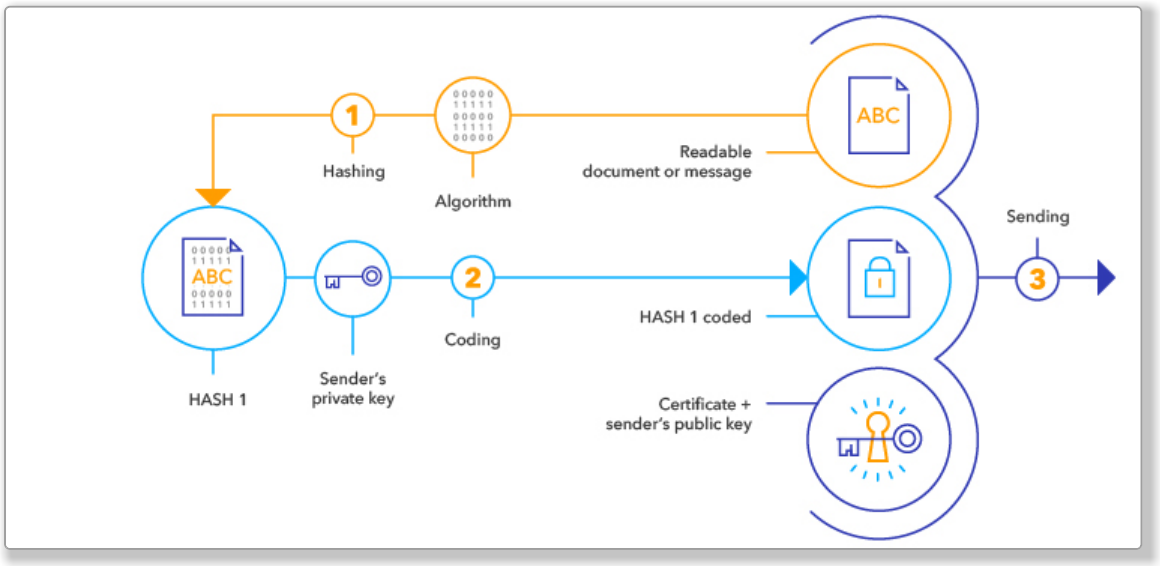
7 What happens technically during electronic signing

When you add an electronic signature to a document, the process involves more than just adding a signature at the bottom of a text. Most of the steps take place behind the scenes, controlled by software.

In simple terms, every form of electronic signature consists of data that is added to a document or file. With the qualified electronic signature, this added data is generated by hardware security modules (HSM) in a particularly secure technical environment. In regions with a tiered system of legal regulation for signatures as a trust service, such as in the EU, a specially authorized and qualified body has also issued the signatory's authenticated proof of identity, the digital certificate.

Signing takes place in what is known as a public key infrastructure, in which an encryption procedure with two software keys is used. One is the private one, which only the encrypting authority knows, and one is the public one. The latter is provided along with the document in the signature certificate for the recipient.

There are three steps in the process:



1. **Calculating the hash value**
   A mathematical function is used to calculate a checksum from the data of the document or file, which is called a hash value. This is like the document's fingerprint.
2. **Encrypting the hash value**
   This hash value is encrypted with the signer's private key.
3. **Connecting the encrypted hash value + certificate with the document**
   The encrypted hash value and the certificate are attached to the document. The certificate contains the public key to decrypt the hash value, the information that this key is associated with the identity of the signer, and the validity of the certificate.

8 Data security, data protection and secure authentication

You can use cloud signatures like those provided by DocuWare Signature Service completely independently of whether you use a cloud or on-premises system for your document management and workflows. The term cloud signature only describes that the Signature Service, like DocuWare Cloud, is hosted in Microsoft Azure data centers. With cloud signatures as with the DocuWare Signature Service, you are on the safe and legally compliant side with both solutions.

Data security: signature process in highly secure crypto-processors

In the past, companies could only create qualified electronic signatures if the hardware for this – the signature creation device – was under their control, i.e. the hardware crypto module and the necessary smartcard and card reader.

Today, the secure signature creation device (SSCD) can be located at a signature service provider, which stores and applies the certificate and keys for the signature creator. These providers provide a highly secure cloud-signing platform via the Internet, where businesses, official bodies, or private individuals can sign their documents.

The actual signing process takes place in hardware security modules, which the signature service provider operates in a secure cloud server infrastructure. Hardware security modules (HSMs) are special crypto-processors that ensure the protection of signatures and software keys.

The signature service providers that DocuWare works with use HSMs that meet the U.S. FIPS 140-2 Level 3 standard for cryptographic modules.

Data protection: the data remains in your region

Signature data contains personal and confidential data. Therefore, it should be ensured that this data remains within the data protection region whose data protection law is applicable, even during the signing process. This is guaranteed with the signature service providers with whom DocuWare works.

Validated ID uses highly secure data centers in Ireland and the Netherlands, which are subject to the European General Data Protection Regulation (GDPR), and an additional data center in the United Kingdom for customers there.

DocuSign uses several highly secure data centers in both the U.S. and the EU for the signature service.

9 Compliance through electronic signatures worldwide

Electronic signatures are an established means of legally secure documents worldwide. However, legal requirements vary between regions and countries. Every company must clarify the respective legal requirements for transactions protected with electronic signatures.

It's important to distinguish between the venue and the applicable law in accordance with the principle of freedom of contract. The *venue* is the place whose court may be appealed to in case of doubt. The *applicable law* refers to the national law under which the document would be decided in the event of a dispute. The applicable law governs both the content of the document and its electronic signatures.

Legal models for signatures

The legal models for electronic signatures scale from less to highly regulated. The requirements are less regulated in North America, where a range of technological solutions and security levels are accepted as legally secure. The countries of the European Union, for which the eIDAS regulation forms the legal framework, have medium or tiered regulation. Only a few countries have particularly strong or restrictive regulation.

Low regulation	Tiered regulation	Restrictive regulation
U.S.A. Canada Australia New Zealand	EU Japan China South Korea	Brazil India Israel Malaysia

It's worth focusing on the two most widely used legal models: low regulation and tiered regulation.

Low regulation

In the U.S., Canada, Australia and New Zealand, electronic signatures are generally accepted and provide the same legal effect as manual signatures. All types of electronic signatures are legal and enforceable and are considered equivalent.

Example of the U.S.

Electronic signatures are legally permissible and well established in the United States. The Uniform Electronic Transactions Act (UETA) 1999 and the Electronic Signatures in Global and National Commerce Act (ESIGN) 2000 recognize the validity and enforceability of electronic signatures. Both laws expressly provide that a signature, contract or other record in connection with a commercial transaction may not be denied legal validity solely because it is in electronic form.

Tiered regulation

Example of the European Union

The legal framework for electronic signatures in the EU is the eIDAS Regulation. The abbreviation stands for "Electronic IDentification, Authentication and Trust Services," in the European Single Market. The regulation has been in force since 2016.

eIDAS provides a tiered legal model to make electronic transactions more secure, trustworthy and simple. As an EU regulation, it is a kind of European law and supersedes the national legislations of the EU member states. Each EU member state had to adapt its laws to the content of the regulation. In Germany, for example, eIDAS was implemented in the German Trust Services Act, among other things.

eIDAS applies throughout the European Economic Area (EEA), which includes Norway, Iceland and Liechtenstein. However, non-European companies doing business with EU companies should also consider eIDAS. For example, many U.S. companies have branches or customers in the EU and in this case must also comply with the eIDAS requirements.

eIDAS distinguishes between three levels of electronic signatures, which have different documentary proof: the simple, the advanced, and the qualified electronic signature.

- **Simple: informal with low legal risk**
  For many documents we use the simple electronic signature. In an email and many contracts, the typed name and/or the bitmap image of the handwritten name is sufficient. There is no specific form required by law for such documents and there is little risk of their legal validity being challenged. With DocuWare, you can provide a simple electronic signature with a stamp.
- **Advanced: medium legal risk**
  In the event of a dispute where it must be possible to identify the signatory of a document or the creator of the signature, you need an advanced electronic signature. It is widely used for commercial contracts in the B2B sector. eIDAS prescribes certain rules for this signature level, such as the signature creator must be identified by using an electronic signature certificate. The advanced signature has medium documentary proof.
- **Qualified: greatest security**
  For some documents, such as certain contracts, for example German law requires a handwritten signature. In these cases, the qualified electronic signature is used, which, with some exceptions, is equivalent to a handwritten signature in court and has the highest documentary proof.

Advanced electronic signatures can be accepted by other EU member states, whereas qualified ones must be accepted throughout the EU. However, each member state regulates for itself whether a business or official transaction requires an electronic signature and the level at which it must be provided.

Qualified certificates are provided by trust service providers (TSP), which must meet special security requirements for this purpose. These providers have received qualified status after an official audit by a national authority and are listed in the EU list of eIDAS Trusted Lists (LOTL).

For electronic seals, which you can use with DocuWare and Validated ID, the eIDAS regulation makes the same specifications. The seal differs from the signature only in that the certificate is associated with a legal entity instead of a natural person.

Example of Japan

Japan also has a tiered legal model for the regulation of electronic signatures. The Japanese Electronic Signatures and Certification Business Act (Act No 102 of 31 May 2000) has been in force since April 2001, according to which a qualified electronic signature is considered a legally compliant electronic signature. An advanced electronic signature is possible, but on its own it has less documentary proof.

DocuWare supports all scenarios and legal requirements

With the DocuWare Signature Service, you can use electronic signatures efficiently in your company and ensure greater compliance. In cooperation with the signature service providers Validated ID and DocuSign, DocuWare offers you a wide range of secure procedures for this purpose.

Check which of your documents need which level of compliance according to legal requirements. Based on this, decide which of the many signing options you want to use.