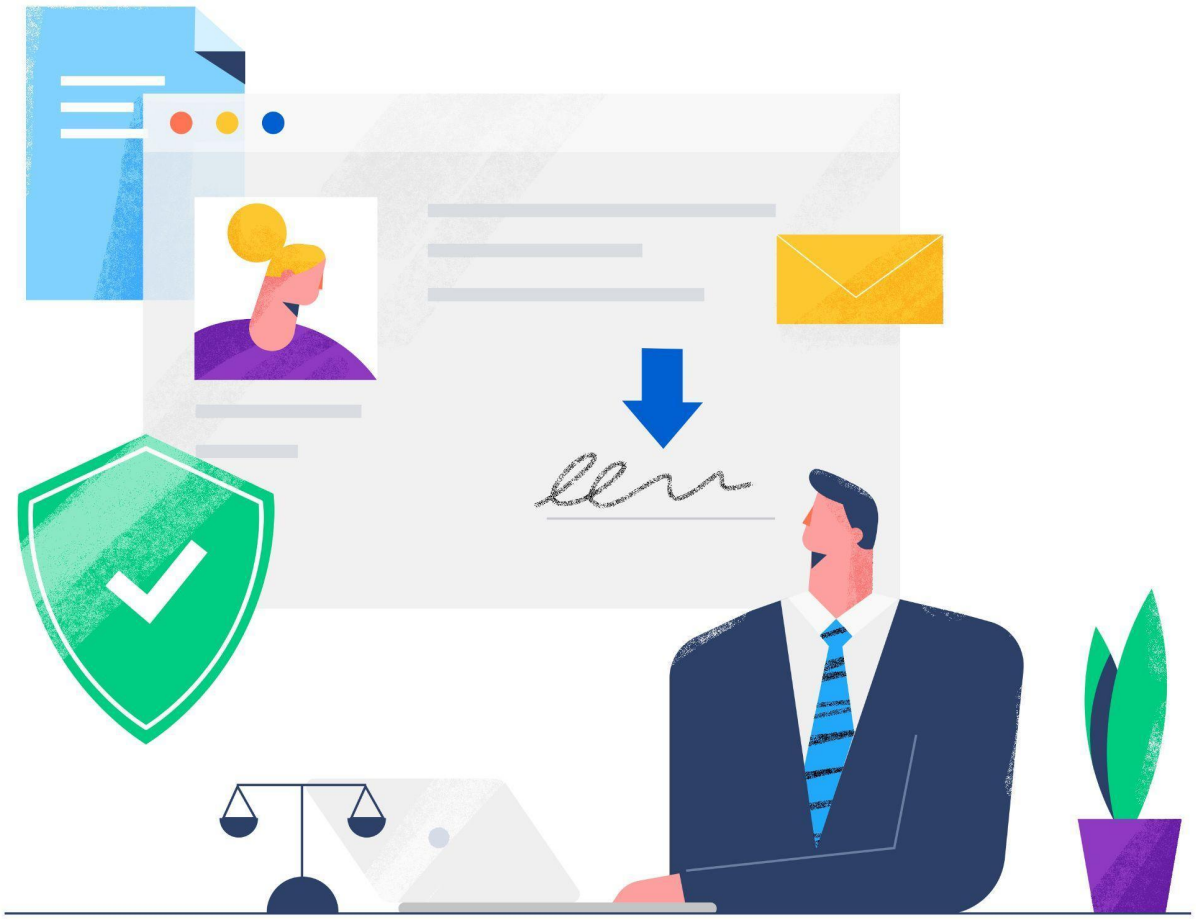
Sign electronically with legal validity

A complete introduction for companies operating in the EU and Switzerland



Skribble

Contents

How electronic signatures are relevant for companies

The missing piece of the puzzle for seamless digital business processes

The typewriter became Microsoft Word, the CD gave way to Spotify and the DVD evolved into Netflix. The digital transformation has made many things faster, more affordable and easier. And the same applies to companies, at least in terms of the majority of everyday business processes.

However, there is one step in everyday operations that remains fully reliant on paper and ink: the legally binding signing of documents and contracts – both internally and externally with customers and partners. Companies today still resort to tried-and-tested analogue processes for this step. Until recently, the same legal foundation was not guaranteed in digital form, or only with enormous additional effort.

This has now changed: with the introduction of secure and simple trust technologies, electronic signatures, which have been granted equal status by lawmakers years ago, but so far proved difficult to implement technically, are now becoming an attractive option for companies. They offer great potential for efficiency and cost savings.

“Some companies estimate the internal costs of traditional signing at CHF 25 to 100 per contract and may sign several thousand contracts per year, which equals quite some significant saving potential.”

brand eins / IT service providers 2021

Electronic signatures allow companies to reduce the costs of their signature processes by up to 80%*. This is due to lower direct costs and increased efficiency; contracts with customers and partners, along with internal company documents, no longer have to take the via printer and paper before they get legally valid signatures.

At the same time, this increases the potential for more business, as deals with customers can be concluded more quickly, which in turn improves the customer experience, resulting in a win-win situation for all parties involved.

The advantages of e-signing for companies at a glance:

Close deals faster
All parties can access the latest contract version in seconds and then sign with just a few clicks.

Cut costs
You can reduce your signing-related expenses by up to 80%* through streamlined processes and lower direct costs.

Work more efficiently
You offer your employees, clients and partners time-saving paperless processes and full media continuity.

Minimise risks
You work with recognised standards that are legally binding worldwide, instead of switching to digital alternatives without any legal weight.

Sign anywhere
Employees working from home or customers based in Asia can sign from anywhere with a smartphone or computer.

Check automatically
You can verify within seconds whether things have been signed correctly, whether the signature is authentic and whether the document has been altered.

* Skribble ROI calculator (average values based on Skribble analysis and customer feedback)

Legal validity and security of electronic signatures

Electronic signatures can replace handwritten signatures while remaining legally valid

In order to understand the legal validity of electronic signatures, it can help to take a brief detour into contractual law: Swiss and EU law differentiates between contracts without and contracts with a written form requirement.

For contracts without a written form requirement, the contracting parties are free to choose the form of the contract themselves. In this way, for example, a contract without formal requirements can also be concluded orally. Contracts with a written form requirement in the analogue world have to be provided on paper and signed by hand.

This same division applies in the digital world: documents without a written form requirement can be concluded in any way, e.g. via a video call. For contracts with a written form requirement, the legislator has amended the requirement for ink and paper by adding a digital form with the same legal weight: the qualified electronic signature (QES).

“A qualified electronic signature has the same legal validity as a handwritten signature.”

eIDAS, Art. 25, para. 2, REGULATION (EU) No. 910/2014

The equal status of the qualified electronic signature (QES) with the handwritten signature in the EU is set out in the “Regulation on electronic identification and trust services for electronic transactions in the internal market” (eIDAS Regulation) of July 23, 2014. This states: “A qualified electronic signature has the same legal validity as a handwritten signature.” (eIDAS, Art. 25, para. 2, REGULATION (EU) No. 910/2014). In Germany, the qualified electronic signature (QES) is equivalent to the

handwritten signature, and therefore, the written form in accordance with Section 126a of the German Civil Code (BGB): “If the legally prescribed written form is to be replaced by an electronic version, the issuer of the declaration must add his or her name to the declaration and provide the electronic document with a qualified electronic signature.” (Art. 126a BGB)

“If the legally prescribed written form is to be replaced by an electronic version, the issuer of the declaration must add his or her name to the declaration and provide the electronic document with a qualified electronic signature.”

German Civil Code (BGB), Art. 126a

In Switzerland, these are the "Federal Act on Electronic Signatures" (ZertES) of March 18, 2016 and the Swiss Code of Obligations (OR). The latter states: “A qualified electronic signature is equivalent to a handwritten signature, which is based on a qualified certificate issued by a recognised provider of certification services within the meaning of the Federal Act of 19 December 2003 on the Electronic Signature” (Art. 14, para. 2bis OR)

For contracts without a written form requirement, the law defines two standards that companies can use as the basis: the advanced electronic signature (AES) and the simple electronic signature (SES). More information is available in the chapter on e-signature standards.

According to EU and Swiss law, the e-signature keeps its legal weight beyond national borders.

The signature laws of the EU and Switzerland are to a large extent similar. There are certain differences, e.g. in the identification requirements for signing with QES. However, the courts in both jurisdictions generally recognise each other's QES.

Some individual companies and authorities explicitly require a QES in line with the legislation of a specific country. In this case, a QES based on EU law may not be sufficient. However, this tends to be an exception only.

“The effort to prove that a signature actually originates from the person indicated is less in the case of an e-signature compared to a handwritten signature on paper.”

The same also applies to signatures outside the EU and Switzerland: the QES based on EU or Swiss law is generally also recognised by courts whose countries have not anchored the QES firmly in their legislation, or at least not in the same way. The effort to prove that a signature actually originates from the person indicated is less in the case of an e-signature compared to a handwritten signature on paper.

Along with legal certainty, technical security and data protection play a key role.

Legal certainty is one of three security aspects that are key when it comes to e-signing. The other two are the technical security of an e-signature solution along with data security and data protection.

For example, it is worth taking into account the encryption technology used. Ideally, documents are encrypted with an individual AES-256 key, which is allocated to the user by means of asymmetric cryptography. In terms of data protection, the location of the data and the security standards of the data centre are other critical aspects.

How electronic signatures work

It's the data linked to the e-signature and not the visual aspects that ensure legal weight

Newcomers to the world of electronic signatures may have to get used to a few things. Unlike the handwritten signature by pen, the digital world doesn't consider the visual aspect to be decisive for the legal weight of a signature. But we'll get to that later.

An electronic signature is primarily a legal term. It is used to describe electronic data that is linked to other electronic data and used by a person to sign (electronic) documents. The law differentiates between various e-signature standards that make it possible to verify the identity of the signer and the integrity of the signed document with varying levels of certainty.

By contrast, there is the concept of the digital signature. A digital signature is a mathematical process used to validate the authenticity of digital messages or documents based on asymmetric cryptography.

"The electronic signature is a legal term. The digital signature is a mathematical process."

A digital signature can therefore be used to generate an electronic signature with a high level of security. The law does not necessarily require this for every e-signature standard. However, the following applies to every secure e-signature: When signing electronically, a data package is attached to the PDF document – a so-called signature certificate.

The signature certificate provides information about the identity of the signer – and therefore answers the question "Who signed?"

Other security elements and specifically the signature time – "When did they sign?" – and the integrity of the document – "Was the content modified?" – are also included in the signature certificate.

Visual aspects, such as the insertion of a scanned, handwritten signature, on the other hand, do not play any legally relevant role in e-signing.

Despite their legal irrelevance: visual aspects are still important in e-signing

Although they achieve the same objective, the way electronic signatures work has surprisingly little to do with signing by hand. It isn't the visual aspect of the signature that gives a signed document its legal weight, but rather the invisible data linkages in the background.

Visual signatures therefore remain important, as they convey the signed document the usual look and feel. In turn, this establishes trust and gives the document a personal touch, something that is particularly relevant when dealing with customers. For this reason, most companies use a visual signature when signing electronically.

There are also cases where the digital visual signature is appealing but has little legal validity, such as when "signing on glass". This type of e-signature – by hand with a pressure-sensitive pen on a touch display – has nothing to do with real digital signatures and therefore little legal weight. It refers to the digitalised form of the handwritten signature.

"Signing on glass is a digitalised form of the handwritten signature – a copy. This is not equal a real digital signature with legal weight."

In spite of this, signing on glass and other forms of digitalised signatures (e.g. the insertion of a scanned signature) can be legally valid: for documents without a formal requirement, the company is able to decide freely which type of declaration of intent it wants to use.

For example, companies use this type of digitalised signatures if they are concluding customer contracts (without a written form requirement) directly on site.

The legal weight of digitalised handwritten signatures is, however, minimal. It is hardly possible to draw any conclusion about the identity of the signer. Once a contract exhibits an increased liability risk, companies usually opt for the use of real digital signatures with legal weight.

It is important to note here that digitalised forms of the handwritten signature such as scans or signing on glass are not legally valid on contracts with a written form requirement.

The three e-signature standards and where they are used

Choosing the right e-signature standard depends on the required legal weight

The law differentiates between three e-signature standards:

- The qualified electronic signature (QES)
- The advanced electronic signature (AES)
- The simple electronic signature (SES)

The three standards vary in terms of where they are used, their requirements and their legal weight.

The choice of e-signature standard will depend on which laws govern formal requirements as well as internal company guidelines. Feasibility and costs are also taken into consideration. The lower standards tend to be cheaper and, due to their lower requirements, easier to implement.

The law stipulates that, in the digital world, documents with written form requirement must be signed with QES. The QES is the world's highest e-signature standard with maximum legal weight,which basically holds up in any court of law.

"In the digital world, documents with written form requirement must be signed with QES."

The maximum legal weight of QES comes about by an independent and state-certified trust service provider (TSP) who issues a certificate that guarantees the authenticity of the signed document as well as the identity of the signer with utmost certainty.

In order to minimise risks, companies may also resort to QES even when the law does not require it. As such, this is often the case for documents containing agreements on large sums of money.

Alternatively, they may choose AES, which boasts a similar level of legal weight but has lower requirements, generally resulting in lower costs and easier implementation.

For documents without a formal requirement and with a low liability risk, SES is used. This standard has the lowest legal weight, but is also the cheapest and easiest to implement.

How much legal weight does my e-signature need?

The law distinguishes between the qualified electronic signature (QES), the advanced electronic signature (AES) and the simple electronic signature (EES). The three standards vary in terms of area of application and legal weight.

Legal weight	Basic	High	Maximum
Area of application	**Documents** without legal form requirement and with low liability risk. **Examples*:** • Offer for suppliers • Order • Confidentiality agreement • Permanent rental or employment contract • Service contract	**Documents** without legal form requirement and with calculable liability risk. **Examples*:** • Rental agreement • Purchase agreement • Partnership agreement • Patent, trademark or copyright contract • Personal insurance	**Documents** with legal form requirements or high liability risk. **Examples*:** • Consumer credit contract • Temporary employment or rental contract • Audit report • Consumer loan contract • Consumer loan agreement
Trust and security	**Low level of identity security and simple signature triggering (LOA 1 to 2)** **Example:** • Identification by means of email address verification • 1-click signature activation	**Identity verified using official identity document, triggering of signature with one factor authentication (LOA 3)** **Example:** • Identification for signing contracts with telecommunications providers • Declaration of intent with mTAN	**Identity verified by authorised entities, triggering of signature by means of two factor authentication (LOA 4)** **Example:** • Identification by trained person (in person or by video call) • Declaration of intent with password and mTAN
Legal certainty and regulatory basis	**Low requirement level** Integrity of signed document ensured through advanced organisation certificate according to Adobe Approved Trust List (AATL) AATL compliant	**High requirement level** Personal electronic signature AATL compliant	**Maximum requirement level** Equal to a handwritten signature according to EU law (eIDAS) AATL compliant

* The choice of the e-signature standard depends on applicable formal requirements and internal policies and may differ from the listed examples. Consult a legal advisor for your specific case.

Identification for electronic signatures

Every electronic signature must be capable of being uniquely assigned to one person

For an electronic signature to be conclusive, it has to give evidence of identity of the signer – this being the only way a court can accept the signed document as valid in the event of a dispute. .

The procedure for ensuring this identifiability differs depending on the e-signature standard used. The higher the standard, the higher the requirements concerning identification.

In the case of the qualified electronic signature (QES), the identity of the signer is verified once in advance using an official identification document. This verification takes place in person or via video call. Bank identification through an online banking account is also possible. The identity checks for QES are stipulated precisely by the law.

“The higher the requirements for identifying the signer, the higher the legal weight of the signature.”

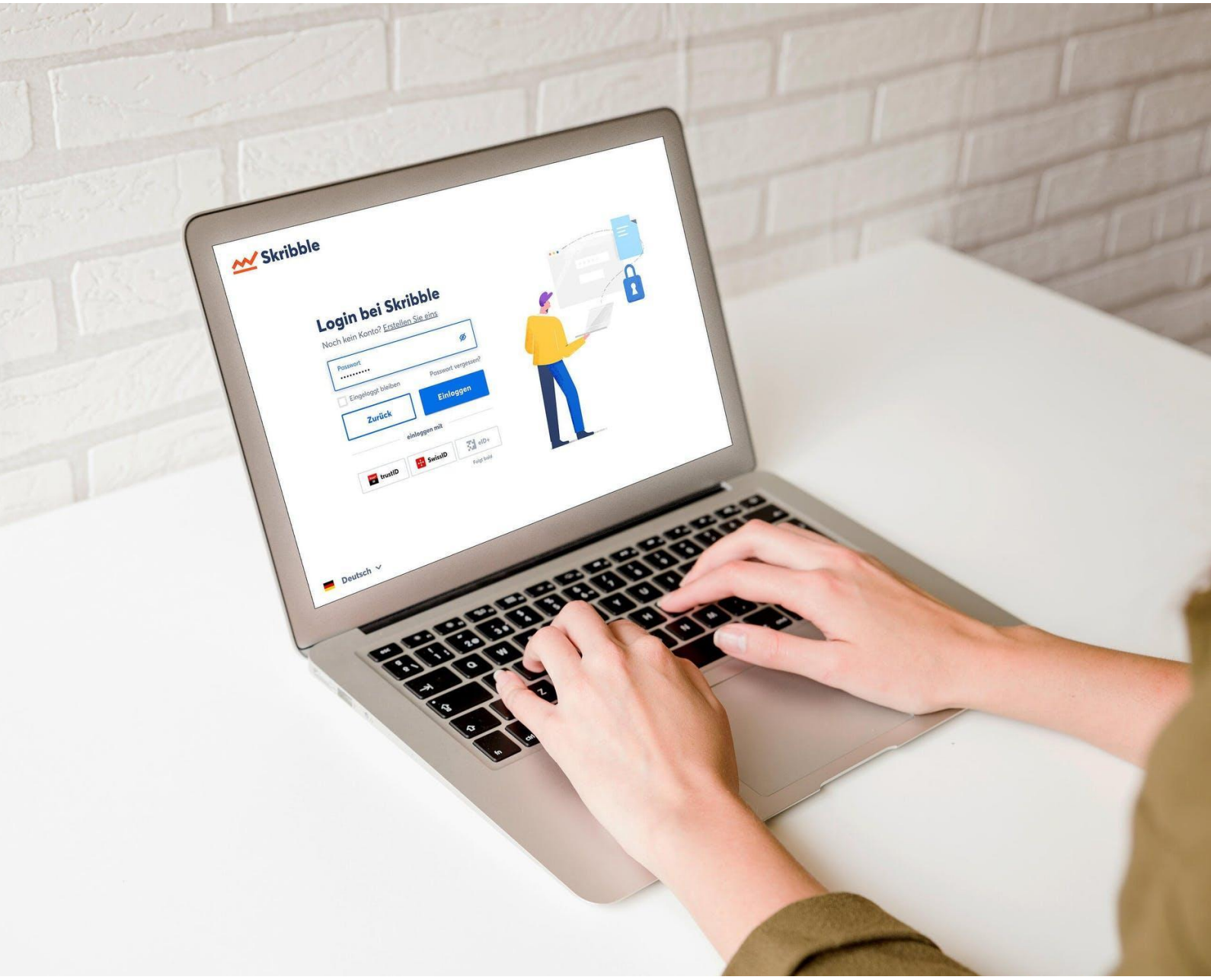
In the case of the advanced and simple electronic signature (AES and SES), the identity of the signer does not have to be verified with absolute certainty in advance, but rather needs to be capable of being reconstructed afterwards. The law leaves the exact definition of the measures largely to the market.

The verified identity characteristics for AES and SES vary between providers and come with more or less legal weight. This includes (but is not limited to):

- E-mail address (low legal weight – SES)
- Business e-mail address, with the employer guaranteeing that an identity check was carried out during recruitment
  (high legal weight – AES)
- Mobile phone number (with the telecommunications provider guaranteeing that an identity check was performed during contract signing (high legal weight – AES)
- Machine capture of an official document without human verification (high legal weight – AES)

Annex

About Skribble



Signing with Skribble – legally valid, simple, secure

Trusted by 2,500+ companies with the highest requirements for data protection and security.

Skribble is the global provider for electronic signatures that comply with Swiss data protection regulations and the GDPR. As a universal solution for electronic signing, Skribble offers the ideal, legal electronic signature for every type of contract.

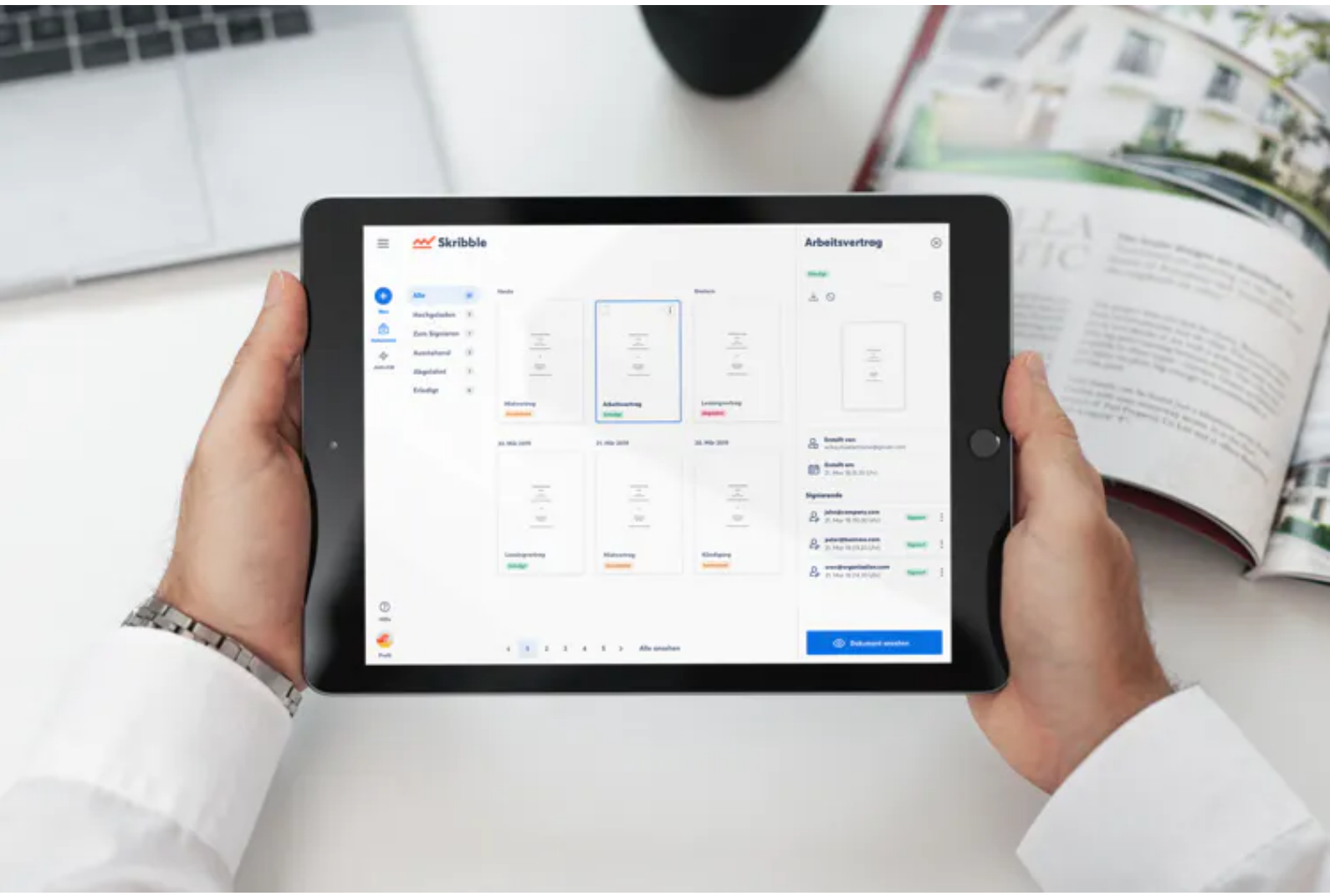
The basis is formed by legally regulated standards, including the qualified electronic signature (QES) – the only form of electronic signature that is legally equivalent to the handwritten signature according to EU and Swiss law.

“Skribble has given me enormous peace of mind in my daily work. We can now get contracts with affiliates in Austria, Central & Eastern Europe signed in a timely and more secure manner.”

Jaroslav Molik, Reinsurance Manager, Uniqa RE

Want to know more?
You can find customer use cases and further information on our website. www.skribble.com

Our e-signature experts will be happy to assist you.
You can reach us at info@skribble.com or by phone at +4915735992797 (Germany) / +41 44 505 16 64 (Switzerland)/800769413 (Italy) / 08002264357 (Netherlands).



“The service portfolio of the other providers was on the one hand too complex and on the other hand not mature enough to meet our high requirements – especially with regard to legal aspects.”

Markus Schneider, Vice President of Purchasing, SEG Automotive

Skribble AG
info@skribble.com
www.skribble.com

Germany
Pforzheimer Str. 128A
DE-76275 Ettlingen
Tel.: +4915735992797

Switzerland
Förrlibuckstrasse 190
CH-8005 Zurich
Tel.: +41 44 505 16 64