eSignature—Why and How

An LLI Whitepaper by Jutta Löwe, Baltasar Cevc, Dario Dill, Kai Jacob, Peter Karmann, Dr. Rainer Markfort, Lucija Kobal Nakić, Christian Rathgen, Dr. Jan Querfurth, Bernhard Waltl and Dr. Lutz Zimmer (edited by Dr. Roger Strathausen)

Introduction

The global pandemic has made it even clearer that the process of getting contracts or other documents signed or approved with a paper-based process, like handwritten signatures from the respective representatives, causes unnecessary delays. If you are lucky enough not to be the one running around with the sheets of paper, there are others who are doing it while they could be using their time much more constructively. The effort of wet signatures (paper-based process) remains a major driver of cost in legal inhouse departments. With this project, we would like to enable organizations to pragmatically move from wet signatures to a digital signature process.

There is no digitalization without digital signatures!

When planning and starting the implementation of eSignature, you might—like so many others—feel overwhelmed by all the information available and the many topics to consider. For example, you might ask: What is eSignature, precisely? Is it legally binding? Does it take effect (proof) in all countries, under all jurisdictions? How to best implement it? What does good governance look like? Is there a vendor list? What are pros and cons of specific vendors? What are the most important lessons other companies have learned?

Each company seems to have the same problems—and appears to re-invent the wheel once again. We aim to address this lack of guidance and provide useful, vendor-neutral material for a quick start. Specifically, this whitepaper aims to provide you with a first overview and a summary of the background of eSignature. We would like to put you in the position of better understanding the benefits and use cases of eSignature and what you should be aware of when implementing eSignature solutions.

Additionally, we created an eSignature starter kit which enables you to take the first steps while avoiding pitfalls for the long run.

Content

eSignature—What is it? What is it called?

First of all: Instead of re-iterating known problems from the paper-based world, look at the benefit of eSignature. The story of the eSignature is full of misunderstandings, misconceptions and confusion.

You should be prepared that in the field of signing documents in a non-analog way, there are many different understandings and definitions, many different wordings. If you talk with colleagues, e.g. from IT or Legal,

experienced or not, don't expect them to have the same understanding of eSignature as you have, especially when it comes to different jurisdictions.

1. Digital signature or electronic signature?

Is there a difference between digital signature or electronic signature, and if yes, what kind of difference? Some people do refer to the text with name and contact details at the end of an e-mail by using the word signature (block).

The so-called eIDAS Regulation[1] is using the term electronic signature, but it is used in general for "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"[2].

In this whitepaper, we use the term "eSignature" in a more general sense of the word. We distinguish between different levels of legal effects or security by adding additional terms or explanations, but we do not focus too much on assigning specific effects on specific terms. For instance, in Europe we are used to the terms basic, advanced and qualified electronic signature. Because of the specific features and effects, a qualified electronic signature possesses, we sometimes refer to the term "Non-Qualified eSignature" as eSignature not meeting the specific criteria of a qualified eSignature.

2. Different effects and purposes of eSignature

In order to understand the difference between various types of eSignatures, it is worth taking a closer look at the effect or purpose that a signature might have:

a) **Authorship:** Presumption that this document can be clearly attributed to its author.

b) **Authentication:** Presumption that the person identified and indicated as signatory actually is the person signing it.

c) **Approval:** Presumption that the author/signatory of this document has approved its content either in its own name or in the name and on behalf of another person.

d) **Integrity:** Presumption that this document has not been altered.

e) **Timestamping:** The vendor certifies at which time the signature has taken place.

f) **Non-repudiation:** In case of qualified electronic signature, this means that the signatory as owner of its qualified electronic signature cannot deny its signature.

3. Different kinds or levels of eSignatures

The different levels of eSignature reflect different levels of proof, identity and security, in general. You might consider this just a technical issue which should be covered by Information Security, but the level of security directly correlates with the level of evidence.

a) **Wet Ink Signature:** A handwritten signature on a paper document.

b) **Authenticated Wet Ink Signature:** A wet ink signature on a paper document with an official confirmation (by a notary or other approved authority) that it can be attributed to the person who has signed it.

1 Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (https://eur-lex.europa.eu/eli/reg/2014/910/oj, last accessed 2020-04-29)

2 Art. 3 (10) eIDAS

c) **Digital or Electronic Signature (in general):** Set of sounds, symbols or data linked to an electronic document which has been adopted or used by a person with the intention of identifying themselves and of accepting or adhering to the content of an electronic document.

d) **Features and functions for more security and evidence:** Since many vendors exist on the market, many different eSignature functionalities and bundles of different functionalities are offered. Some of them do have the purpose of fulfilling special legal requirements for some regions, like eIDAS Regulations within the EU. We don't want to stick to a certain jurisdiction. See also below for the Global Use of eSignature. Instead, we would like to mention the main functionalities we found useful and provide suggestions in order to balance usability, evidence and security.

   i. **Proof of integrity:** The document cannot be changed. You could fill out specific fields determined by the sender, and sign or reject the document. You could also delegate the signing to someone else if you are the wrong person.

   ii. **Authentication factors:** The most simple eSignature functionality is the request for signature by just sending it to an e-mail address of which you assume that the signatory has access to it. Without any additional security factor, the document could be signed by anybody who would have access to this e-mail address. This could be an intended process. We know many cases where the personal assistant of a signatory signs documents on behalf of the respective signatory. Adding more factors for authentication, like password for access and sending a special individual code to a different device (TAN to mobile), would enhance the security level of the authentication.

e) **Qualified Electronic Signature:** The signatory has to go through a verification process, e.g. a video identification procedure, where a certified trust provider verifies the identity. There is a two-factor-authentication process usually covering knowledge and ownership for using the qualified electronic Signature (QES). In Europe, this form of eSignature is considered to generally have the same effects as a signature on paper.

"Deciding what type of [e-*]signature you want to implement should be dictated by the type of documents you need to sign, the level of authenticity you need the document to uphold and local, state or country regulations that need to be met."[3] (* added by the authors for the sake of clarity)

We think it is much easier to understand the benefit of eSignature solutions if we do not dive too deep into the different types of eSignatures. First, you should understand the general benefit of it, and second, be made aware of some common functionalities and their effects.

eSignature Use Cases

The decision to implement eSignature and the question which functionalities to add very much depend on the use case or cases at hand. Since such implementation is a digital / IT project, we generally recommend starting small and doing some prototyping (in a broader sense) before rolling it out across an organization or for many documents.

To find a viable use case, we suggest asking a number of questions related to an existing and not too complex signature process:

3 https://www.iltanet.org/blogs/leigh-isaacs/2020/10/07/digital-and-electronic-signatures, last accessed 2021-04-29

1. Can you imagine improvement in terms of process, logistics, speed, cost, integrity, authenticity or proof by using eSignature?
2. Are there statutory, contractual, or internal form requirements conflicting with eSignature (that do not go away even after having challenged them)?
3. What is the risk appetite that your organization has in case third parties challenge the viability and validity of an eSignature?

After having answered these three basic questions, you should be in a position to reasonably decide whether you have a use case where it is worth trying eSignature. For a start, you should focus on a use case that doesn't require the highest security standards (e.g. in Europe: a qualified eSignature).

Here are few thoughts on these three questions:

1. When thinking about signature process improvements, you may want to consider the following aspects:
    a. How many documents, situations or signatures would the change to eSignature affect?
    b. What are the current costs related to physically storing wet ink signed documents (now and in the future)?
    c. Is there an even more appropriate process to improve the process (e.g. instead of digitizing signatures in an internal approval process, it may be possible to establish a simple approval workflow by way of a no-code or low-code automation tool already available in your organization)?
2. When thinking about form requirements, the following may be helpful considerations:
    a. For organization-internal situations as well as in simple B2B environments, strict form requirements are less likely to apply. The more consumers, or private customers, or public authorities are involved in the signature process, the more likely it is that form requirements are relevant.
    b. In unregulated industries and/or transactions, strict form requirements are less likely to apply than in regulated industries / transactions.
    c. The more advanced and mature the jurisdiction which governs the signature or any follow-up process, the less likely it is that form requirements will prevent eSignature. The more (different) jurisdictions are affected by the process, the more difficult it is to ensure that one eSignature process will comply with all form requirements.
3. When thinking about the risk appetite (and apart from the obvious like what are the financial amounts at stake), you may want to reflect on the following:
    a. What are the risks associated with your current signature processes as well as with your current information management, and will these risks really increase by implementing eSignature? (E.g. executing contracts only by way of exchange of scans of signed documents or storing all originally signed documents only as electronic scans may be worse than using basic eSignature.)
    b. How big is the practical risk that any interested party will challenge the eSignature process in court or in arbitration?
    c. How long will the document resulting from the eSignature process be legally relevant? (The currently state-of-the-art security and encryption concepts are considered secure (only) until

2027, and only in the absence of groundbreaking cryptanalytic improvements, e.g., quantum computers; thereafter, eSignatures with security features, in particular qualified eSignatures, produced before that date may require re-evaluation or even recertification security-wise).[4]

Global use of eSignature

Different countries do have different regulations regarding eSignature, especially for signing documents and declarations with legal effect, e.g. contracts. You can find a broad overview of eSignature related regulations in several jurisdictions in this Digital Signatures Tracker, created by Dentons.[5]

eSignature and its Complexity under International Law

In international legal relations, the complexity of questions concerning the effectiveness of eSignatures increases significantly.

In the context of international law, the question of eSignature is primarily dealt with under the aspect of the formal validity of legal transactions. Usually, international contracts are concluded by using eSignature between parties who are located in different places and different states at the time of the conclusion of the contract. In Germany and other EU member states, the Rome I Regulation applies[6]. Incidentally, this also applies to so-called third countries that are not members of the EU. The Rome I Regulation only regulates under which national (material) law the question of the effectiveness of the form is to be assessed. The specific requirements for the form are ultimately assessed according to the national (material) regulations of the respective state.

The Rome I Regulation (Art. 11) provides various connecting criteria for the assessment of the applicable national law:

- The contract statute (lex causae): The national law applicable according to the rules of the respective private international law; either on the basis of a choice of law or the private international law of the lex fori.
- The form of place (lex loci actus): the national law of each of the places where one of the parties or its representative makes its declaration.
- The habitual residence of the parties.

These different connecting criteria regarding (i) the contractual statute, (ii) the respective place of submission and (iii) the respective habitual residence of the parties apply to the form of both declarations. The principle of validity has the effect that an offer which is invalid in form at the place where it is made becomes valid in form according to the law at the place where it is accepted; the principle of validity also has the effect that, if applicable, the lenient consequence of a lack of form applies. Thus, it may be that more than two different national legal systems must be examined with regard to the question whether declarations signed by means of eSignature are formally effective or not. If the declaration is effective according to one legal system and if no internationally mandatory national regulations exist that prevent form effectiveness, the contract has been validly concluded.

4 For more details, see the January 2020 paper by the SOG-IS Crypto Working Group at EU Level called SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, section 1.1, available at https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf, last accessed 2021-04-29.

5 https://publisher.dentons.com/experience/dashboard/e-signatures-tracker, last accessed 2021-04-29

6 Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)

Rome I Regulation includes statutory rules which raise legal presumptions or determine the burden of proof as to the form (Art. 18 para. 1). When it comes to the modes of proof, all levels of evidence are relevant that are recognized by the law of the forum or by any of the laws referred to above (Art. 18 para. 2).

eSignature and tax pitfalls

You need to be diligent if the place where the document shall be signed is of importance to a certain tax regime. Often, relevant aspects are where a company has its tax residence or creates a permanent establishment, as that generally leads to local taxation. Taxation might be triggered by regular activities within one jurisdiction or, for example, by resolutions of the management board, respectively. An example: Under German law, the headquarters of a company are located at the place where fundamental business decisions are made. This is the place where the management board reconvenes to discuss matters of strategic importance, makes up its mind, and takes decisions. Some companies decided to move their headquarters to Luxembourg or Austria or to any other place with a favorable tax regime in order to save taxes. These companies need to make sure (and be able to prove to the tax authorities) that relevant business decisions have been made at such a place. The place where a document (e.g. a board resolution) is signed is a strong indicator for the place of decision making. Therefore, when using eSignature, these aspects should be considered. This may require checking how the eSignature tool tracks the location of the signatories. Also, major agreements with important customers which would create essential revenue need to be considered from a tax perspective.

Success stories—lessons learned

In this part, we asked colleagues who went through the process of implementing an eSignature solution about their experiences—here are the answers of one of them:

If you think about implementing eSignature, be assured you are not the first one. We would like to share some valuable experience from those who have already mastered the challenge.

1. How would you briefly describe the scope?

   After an unsuccessful first attempt to build our own eSignature solution (which is best described as a Click-to-Accept approach), we decided to go for one of the well-known suppliers in the market. Having invested quite some time and resources with our first try, the goal for our second attempt was set: global deployment of as many use cases as possible in the shortest possible time-frame—nothing less than that.

2. What was great and what are the lessons learned in general?

   We have learned that empowerment of employees is the basis of any eSignature deployment! While we knew we had the full backing of our Board of Directors to deploy the solution, we were allowed to set our own pace. The deployment was led by a small independent team and carried out with the help of many inspired colleagues around the globe who wanted to benefit from the ease of eSignature.

3. In your view, what are the key success factors?

   Knowing the WHY and being able to draw a picture of the future state allows all affected users to grasp the story and get on board. With this appealing vision in mind, we were able to also change HOW we do things. Processes changed, and new roles were established, both locally to organize for

adopting the new way of eSigning, but also in our central team which is responsible for the training, administration and continuous improvement of our eSignature solution.

4. What was the biggest failure and what is your hack to get over it?

   Certainly, the hours spent for creating our own solution were wasted, not because the solution was badly designed or not fit for purpose; what led to low adoption was a very small feature: there is a difference in "clicking" a button and "drawing a signature"" (or applying a look alike signature) in a tool. Switching from "click" to "draw" helped us to overcome the resistance.

5. What would you do differently?

   Next time, we wouldn't waste too much time with the make or buy decision and would simply buy a suitable solution. And, depending on the market power of my company, maybe go for a multi-vendor strategy, or at least let the users decide which solution they prefer, instead of forcing the global workforce into one preferred supplier's product.

6. What were the biggest constraints?

   The cultural barriers, which currently don't play such an important role anymore, after COVID and home office for more than 1 year. When we faced resistance, my boss advised us: lead and they will follow—and they did follow. With eSignature, the contracting processes becomes so much smoother and more enjoyable.

What to consider during vendor selection and project planning?

eSignatures come in different flavors, there is a large variety of vendors on the market. As usual, first start to better understand the challenge you want to solve. Then, you can align the requirements and the offerings. Some features of tools or other vendor-specific criteria might be easier to evaluate than others—in such cases, we suggest that you first start with the easier ones to reduce your initial list. While there might be some situation-specific circumstances, you can in general quickly evaluate vendor location/jurisdiction requirements (if you have some, e.g. because of a policy of only using specific vendors in your jurisdiction) and the required signature types. Similarly, if you have one necessary core integration, that is something to check early. Depending on your use case, the commercials of the procurement might be easy or challenging to evaluate. Out of that pre-selection, you can produce a short list of potential vendors which you can then investigate more deeply.

Criteria to decide between vendors will usually involve:

- Covered jurisdictions and signature standards
- Regulatory requirements (e.g. potential additional privacy requirements with foreign providers)
- Usability and interfaces (e.g. are the relevant people already used to a certain ecosystem, are interfaces for mobile and/or desktop available)?
- Does the tool provide features which cover your use cases?
- Security standard which also refers to the provided functions
- Pricing (what is billed, e.g. per document, per envelope, per user, combination or other?)
- Integration into other systems (e.g. CLM/ERM, HR, SSO or trust service providers, if necessary)
- Integration capabilities of the tool (API etc.)

Questions you should answer for yourself:

- Which use cases do you have? For which of them would eSignature be possible?
- Who are the experts to be involved early? Align with legal, tax, privacy experts
- Who will be your pilot users, and what do they need? How should the overall project evolve, and what should it cover?
- Which people will work with the tools? How many of them will there be? Where will they be located?
- What is the (estimated) number of signatures your company will have?
- Which formal requirements apply to the use cases?
- Which internal and risk requirements does your company have?

Please note: Certain scenarios might only work with certain providers. The more complex your requirements become, the likelier it is that you will need more than one provider. Whether you will accept signing with a "foreign" tool (based on the invitation of your contractual partner) is also something you will want to consider; however, that is part of the eSignature policy rather than of vendor choice (as you are only a user, not a customer in such cases).

Further reading on vendor choice:

- Contract Lifecycle Management – How to select the right platform?
- Our Vendor List gives an overview of important features, commercials and other information for a list of providers.

* * * * *

The Liquid Legal Institute is an open and interdisciplinary platform promoting a new way of thinking and working in the legal sector. Being neutral and non-profit, it enables stakeholders to address digitalisation, new business models and technological innovations within the field of law. We are a group of multi-disciplinary enthusiasts from various countries promoting new realities in law and implementing Liquid Legal in practice. For this purpose, we leverage insight from other disciplines and address specifics of the law. We focus on tangible action, gathering knowledge, creating methodology kits, setting standards and further activities that use an open mindset to make law practice better for everyone involved.

We believe in the power of collaboration, co-innovation and simplification. We base or work on actual needs and invite all stakeholders to bring in their perspectives and set the bar for tomorrow's legal!

Find out more and join us today!
Just visit https://www.liquid-legal-institute.org/

Jutta Löwe, Baltasar Cevc, Dario Dill, Kai Jacob, Peter Karmann, Dr. Rainer Markfort, Lucija Kobal Nakić, Christian Rathgen, Dr. Jan Querfurth, Bernhard Waltl and Dr. Lutz Zimmer: eSignature—Why and How