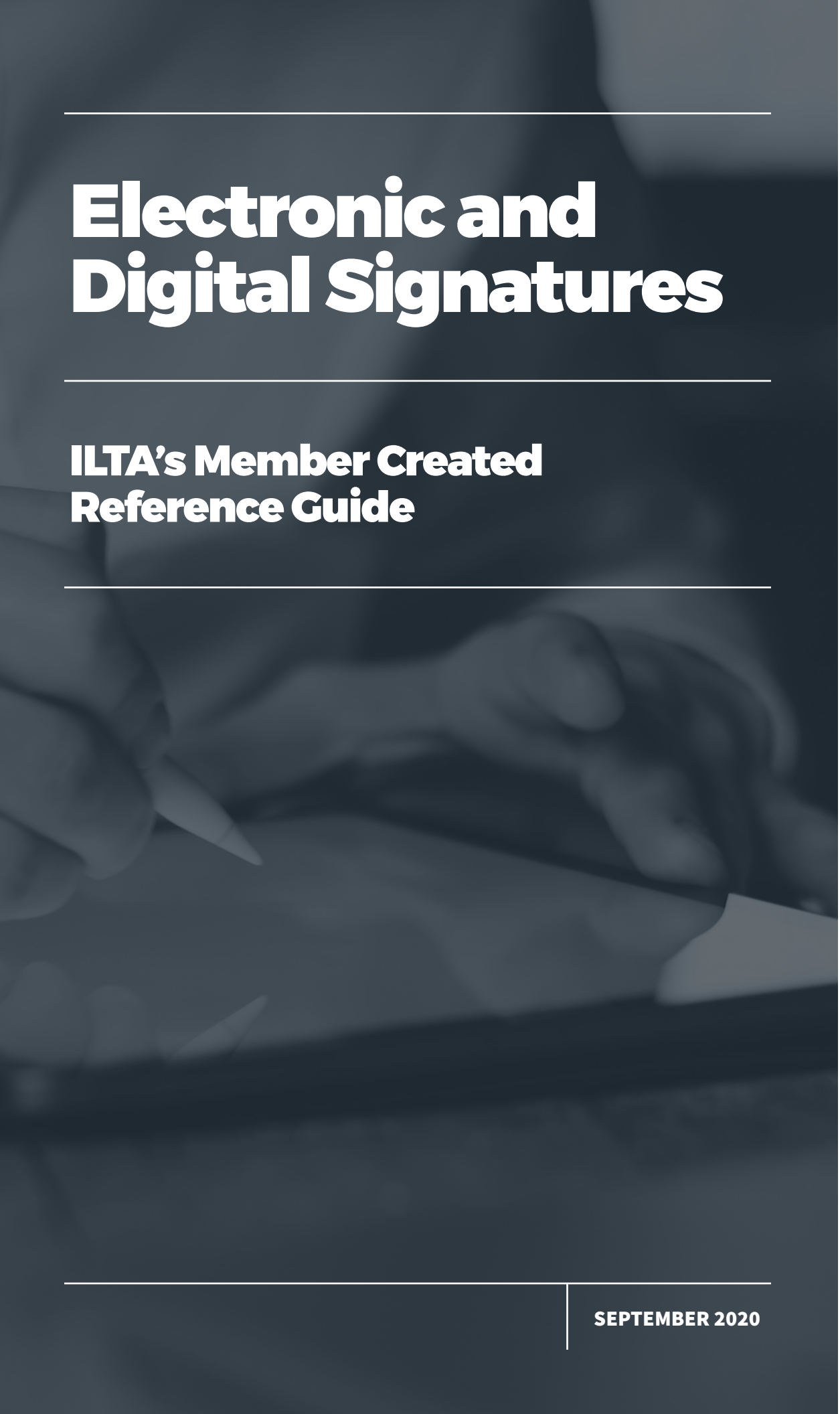

Electronic and Digital Signatures

ILTA's Member Created Reference Guide

SEPTEMBER 2020

Differences Between Electronic and Digital Signatures

AREN'T THEY THE SAME?

An electronic signature is an electronic symbol attached to a contract or other record, used by a person with an intent to sign. In contrast, a digital signature is a more secure and sophisticated type of electronic signature, providing assurance that the signatory is who they claim to be, and that the signed document is authentic

Both electronic and digital signatures are binding in many jurisdictions.

> ***Deciding what type of 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.***

A digital signature is a type of electronic signature that offers more security than a traditional electronic signature. When you sign a document with a digital signature, the signature links a "fingerprint" of the document to your identity. Then that information is permanently embedded into the document, and the document will show if someone comes in and tries to tamper with it after you have signed it.

Because that information is embedded in the document, you do not need to check back with the vendor if you want to verify that the signature is still secure unlike with electronic signature.

Standards that Qualify

WHAT ARE THE STANDARDS GOVERNING USE OF ELECTRONIC AND DIGITAL SIGNATURES?

Digital and electronic signatures following standards have the same legal implication as traditional hand-written signatures.

Digital Signature Standard

The Digital Signature Standard (DSS) was developed by the United States National Security Agency (NSA) and put into use by the National Institutes of Standards and Technology (NIST) in 1994. DSS makes use of the digital signature algorithm (DSA) to generate digital signatures that are assigned both private and public keys. Only the message sender has knowledge of their private key, while the recipient can use the public key to verify the integrity of the sender's digital signature.

eIDAS Regulation

Regulation (EU) No. 910/2014, referred to as the eIDAS Regulation was enacted by the European Parliament in July 2014 and fully adopted by the European Commission by September 8, 2015 as an expansion of Directive 1999/93/EC. It established an EU-wide legal framework for electronic signatures (as well as for electronic seals, electronic time stamps, electronic registered delivery services and website authentication). The intent of this regulation was to enable seamless and secure electronic interactions between citizens, businesses and governments to promote trust that would help build economic and social development through Digital Single Market. This standard provided a foundation to enable users the ability to safely access services and conduct both online and cross-border transactions with "one click."

Federal Act on Electronic Signatures, Electronic Signatures Act

Enacted by the Federal Assembly of the Swiss Confederation in December 2003, the Federal Act on Electronic Signatures (ZertES) addresses the requirements for the authenticity of electronic signatures. These requirements state that the electronic signature must: 1) be uniquely linked to its owner; 2) enable the owner's identification; 3) be created in a way that gives the owner complete control; 4) detect tampering and alert the owner and recipient of the message has been tampered in any way; 5) be created on a secure device through the use of private cryptographic keys; 6) provide verification through the use of a public cryptographic key.

WHEN SHOULD YOU EMPLOY A DIGITAL AND ELECTRONIC SIGNATURE?

NOTE:
You should not use an electronic or digital signature if there is a legal or regulatory reason to have a wet signature.

1. When you need to expedite document signing and improve efficiencies to current processes, such as HR onboarding or contract management.

2. When you have multiple, dispersed signatories and want to bring efficiencies to the process.

3. When you want to strengthen security. The use of digital signatures reduces the risk of duplication or alteration of the document itself and ensures that signatures are verified and legitimate because each of them is protected with a tamper-evident seal which alerts you if any part of the document has been changed after signing. Digital encryption and audit trails keep your signature secure, protecting your organization against fraud and keeping your information safe. This is particularly useful when dealing with private information. A digital signature would be used, therefore, for high risk, high value transactions.

4. When you want minimize the storage of paper. Digital files are stored virtually, eliminating the need to keep paper on site. It also eliminates the manual, and costly aspects of managing paper. It also reduces printing and mailing costs associated with paper.

WHEN IS A "WET" SIGNATURE NECESSARY?

Certain documents are required by law to contain a wet signature. You should always verify any laws or rules that govern the jurisdiction in which you want to employ the use of digital signatures. Below are some examples of documents that generally require a wet signature.

- Wills, codicils, testamentary trusts
- Adoption, divorce and family law
- Court orders or notices, and official court documents
- Notice of cancellation of utility service
- Any notice of cancellation of health or life insurance
- Notice of recall
- Uniform Commercial Code documents
- Documents required to accompany the transportation of hazardous materials

WITNESSING A SIGNATURE

Some jurisdictions place great emphasis on witnessing of a signature regardless of it being "wet" or electronic. It is important, therefore, to pay attention to any applicable execution formalities. In English law, for example, a deed can be signed with an electronic signature but if the relevant formalities (such as a witness being physically present) are not complied with, that document will not be validly executed. You should, therefore, consider the rules that govern witnessing and before choosing a technology provider ensure there is a workflow that factors in witnessing that meets your needs.

IS IT LEGAL TO USE A SIGNATURE FONT AS AN ELECTRONIC SIGNATURE ON LEGAL DOCUMENTS?

This is dependent upon the laws of the jurisdiction and of the particular court. In many instances a pleading may be signed with a typed font in this manner /s/ Signature, where "signature" is your typed-out name. This is generally used for electronically filed documents.

DO YOU NEED A THIRD-PARTY SECURITY CERTIFICATE?

To ensure the security of internet commerce, many companies use a third party to validate the transaction. If you are using just an image of a signature, the use of a digital signature to validate a picture of your signature should be used.

Third party publicly trusted tools such as ssl.com can take care of the validation process and issue a document signing certificate, giving added assurance when digitally executing a document.

The certificate and creation of a digital audit trail is a beneficial record generally. Depending on the platform used, it will include a record of who signed the document, steps taken to authenticate the signatory, and a time-stamp. In English law, for example, this digital trail is admissible in evidence and useful should a dispute arise about authenticity.

WHAT ARE SOME GUIDELINES TO ASSIST IN IMPLEMENTING EFFECTIVE AND ENFORCEABLE E-SIGNATURE PRACTICES?

Find more information about global electronic signature laws:

global electronic signature laws »

digital signature laws »

1. Put your e-signature policy in writing, make it clear when e-signatures can be used and the requirements for such use, and put in place a robust workflow. It is easier to argue that an employee knew that it was important to check their email when that is included in your handbook.

2. Know the e-signature laws of the states/countries in which you do business. As already noted, most jurisdictions have enacted some sort of governing rules.

3. Go beyond the "black letter" law. Merely following the letter of a governing rule (such as the E-SIGN Act, may not be enough in the eyes of the court. If there is doubt, consult with an outside professional to make sure that your processes effectively establish authenticity and non-repudiation.

4. Ensure there is an internal governance system in place that is equipped to lead technology and legal developments and respond to questions from within your organization.

5. Have a comprehensive internal training program. Often your lawyers, for example, will be administering the signing process on behalf of clients so will need to be comfortable using the different features of the chosen platform.

WHAT CAN YOU SIGN WITH A FONT?

Electronic signature is more than just an image file that resembles a handwritten signature. It doesn't even need to look like the handwritten signature of the person signing the document. This feature carries limited weight when signing documents electronically. You can use a font when you don't need to verify the signer's identity and don't need to ensure that the signature wasn't forged. Note: a scanned signature or "tick box plus declarations" does not have the equivalent legal effect of a handwritten signature.

Tips to Enable from Home

HOW ELECTRONIC DIGITAL SIGNATURES COULD HELP BUSINESSES CONTINUE TO OPERATE WHILE WORKING FROM HOME.

Moving to electronic or digital signing a document requires only a portable device (laptop, mobile phone, tablet) with Internet access. With this in mind, every business could continue to operate while in an emergency or to allow better life management for its workforce.

Complex acts such as remote notary, could be performed while on the go, by using a combination of a web conference tool and mobile device.

Digital signing certificates accessible from the cloud (used for Qualified Signatures), allow even the most confidential act to be signed, while ensuring the identity of the signer. Examples are: employment contracts, tax applications, certain corporate documents, such as the assignment of nominative shares or stocks.

With Electronic Digital Signatures, there are no limits in improving existing workflows and speed up processes.

Tips for Attorney Adoption

INNOVATION IN SHORT ORDER - A SOLUTION THAT IS SUDDENLY A NECESSITY

Adoption of innovative ideas is not a universal attribute of all law firms. However, in the case of electronic / digital signatures, it is a technology tool that in normal circumstances would be an efficiency. A signatory that was not close geographically, or where there was not time to send, notarize, and return documents required electronic signatures – but those were outliers. Innovative companies were able to deploy the technology to meet their needs, but traditionally bent companies were slow to adopt. With the 2020 global workforce not in an office, the ability to execute legal documents quickly became a necessity.

Electronic / Digital signature programs gained traction across practice areas and throughout firms to create transaction documents, create PDF signature packets, compiling documents and building a document binder.

Adoption of a technology tool that meets needs without a viable alternative is easy at first blush, however the ability for a "quick sell" to users still requires a deployment that is smooth and allows users to pick up on the solution without strife - my introduction packet to our program came with 4 easy-to-understand handouts.

Good communication with attorneys is important to ensure consistent adoption. Advertise your preferred electronic or digital signature platform regularly, have a robust training program in place, and create comprehensive resources (store them, for example, on an easily accessible central intranet page). Consider, also, having a committee of legal and technology representatives from across your organization who attorneys can contact for help.

Given the visibility of this outward-facing program – the maintenance and support of the program along with continuous process improvement is commitment, but adoption at all life stages for change with this solution is virtually guaranteed.

Necessity is the Mother of Invention… (or is it Adoption, Plato?)