



A GUIDE TO ELECTRONIC SIGNATURES



WHITE PAPER

TABLE OF CONTENTS

What are the different types of E-Signatures? 4

 Digital Signature 4

Legality and Enforceability 5

 US 5

 European Union 6

 Other Countries 6

What Cannot be E-Signed? 7

Benefits of E-Signatures 7

Foxit eSign. 9

A GUIDE TO ELECTRONIC SIGNATURES

Enterprises from almost every industry have taken great initiative to realize paperless workflows in an effort to eliminate the clutter, restrictions and costs associated with paperwork. Most crucially, going paperless helps businesses boost efficiency and productivity.

Yet one critical component that interrupts that efficiency is the way we convey approval or consent – that is, with a signature. The signature is, by and large, the most authoritative means to provide evidence of identity and to express acknowledgement or consent between parties. For companies that conduct their business electronically, the need for a handwritten signature can bring productivity back to a crawl.

Fortunately, electronic signature technology is a much more efficient way to approve digital agreements and transactions. Major advancements have been made to make e-signatures fast, secure, and traceable. Legislation has also been passed in many countries to make e-signatures legal to use as a replacement for handwritten signatures, paving the way for broader adoption. By 2026, the e-signature market is projected to reach 6.1 billion USD, with a CAGR of 28.77% during this forecast period (2019-2026)¹. This guide takes a look at e-signature technology, its legal status, and its known benefits.

¹ <https://www.fortunebusinessinsights.com/industry-reports/digital-signature-market-100356>



WHAT ARE THE DIFFERENT TYPES OF E-SIGNATURES?

The electronic signature represents a broad category that encompasses a variety of signing solutions. Below, we examine the most commonly used forms of e-signature used in business:

Electronic signature is an electronic symbol or process attached to an agreement and used by a person with the intent to sign the agreement or contract. Examples include clicking an “Accept” or “Agree” button, or signing on a touchpad after a credit card purchase, or typing your name onto a signature line. This is the most common type of e-signature for quick and easy signing, and the one you are most likely to encounter while browsing online.

Enhanced electronic signature is similar to an electronic signature, but requires an extra layer of ID verification to prove that the signer is indeed the one signing. An enhanced e-signature process will first ask the signer to verify their identity by entering a password, SMS verification code, company-provided PIN, government-issued personal ID, or another method of authentication before the document can be viewed or opened. Enhanced electronic signatures are commonly used in highly regulated markets such as in government and healthcare organizations.



DIGITAL SIGNATURE

A digital signature is a subset of the e-signature category and has the most layers of security for compliance. This type of e-signature uses encrypted digital certificates to verify the identity of the signer and that the document hasn't been tampered with.

Digital signatures generally use a protocol called public key infrastructure (PKI), which uses mathematical algorithms to generate a pair of numerical keys, one private key (for the signer) and one public key. When a signer signs a document, a signature is created using the private key. Next, the mathematical algorithm creates and encrypts data to match the signed document. This encrypted data is the digital signature, which is accompanied by a timestamp of the signing. When the signer sends the signed document over, the other party receives the document along with the public key. The public key must be able to decrypt the digital signature. If it can't, it is considered invalid, because this indicates that either the signature on the document does not belong to the rightful signer, or the signature or document has been tampered with after it was signed.

Digital signatures offer high degree of security, so many countries with more stringent signing laws give digital signatures the same status as handwritten signatures. Simple e-signatures may also be legal in less regulated industries or markets.



LEGALITY AND ENFORCEABILITY

A common hindrance to adopting e-signatures is uncertainty about whether they are legally binding or enforceable. However, many jurisdictions around the world have passed legislation to ensure that e-signatures are legally admissible for business transactions.

One of the earliest legal recognitions of the electronic signature was when the United Nations Commission on International Trade Law (UNCITRAL) published the Model Law on Electronic Commerce (MLEC) in 1996. MLEC outlined a set of internationally accepted rules aimed at removing legal obstacles for electronic commerce, which helped spur the acceptance and development of e-signatures around the world. In 2001, UNCITRAL passed a dedicated text Model Law on Electronic Signatures, which is backed by 34 jurisdictions to date².



US

In the United States, there are two major laws relating to e-signatures in place. At the state level, the Uniform Electronic Transaction Act (UETA) was signed in 1999 to harmonize state laws concerning the validity of e-signatures. UETA is adopted by 47 states, along with the District of Columbia, Puerto Rico and the U.S. Virgin Islands. The other states – Illinois, New York, and Washington – have implemented their own local laws that recognize e-signatures for legal usage. The Electronic Signatures in Global and National Commerce Act (ESIGN), a similar e-signature law at the federal level, was signed in 2000, allowing interstate commerce. Both laws helped lay out the legal framework for electronic signatures. Under ESIGN, signatures “may not be denied legal effect, validity, or enforceability solely because it is in electronic form”³.

Under both laws, an e-signature is legally recognized as long as four criteria are met:

1. Intent to sign - parties must clearly show intention to sign the document.
2. Consent to do business electronically - parties must indicate consent to conduct business electronically. For instance, parties may be asked to click an “Accept” button on a clause to do e-business.
3. Association of signature with the record - when signed electronically, the system used to capture the transaction must keep an associated record that reflects the way the signature was produced, including time and date stamps.
4. Record retention - a record of the signing must be kept and made reproducible to parties who signed the contract.

² <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/overview-status-table.pdf>

³ <https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf>

The US practices an open-technology approach, meaning there is no law requiring the usage of a specific signing technology to produce legally binding e-signatures.



EUROPEAN UNION

The EU passed similar regulations for electronic transactions called Electronic Identification, Authentication and Trust Services (eIDAS), which went into effect in 2014. Under eIDAS, an e-signature is defined as “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”⁴. The intent behind the regulation was to better facilitate digital growth among the EU’s 27 member states. eIDAS repealed the previous law, the eSign Directive, which did little to ensure that the recognition of an e-signature in one EU state also applied to another member state. Under eIDAS, member states need only follow one set of rules across the board. Three forms of e-signatures are officially recognized under eIDAS:

1. Electronic Signature - under eIDAS, electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form.
2. Advanced Electronic Signature (AdES) - this e-signature type must be uniquely linked to and capable of identifying the signer. Signers also must be able to use signature creation data that is solely under their control and is capable of detecting tampering.
3. Qualified Electronic Signature (QES) - QES uses certificate-based from an EU trusted service provider as well as qualified signature creation devices (QSCD). QES carries the same legal effect as handwritten signatures.

The eIDAS regulation also adopts an open-technology approach.



OTHER COUNTRIES

Other countries have recognized the legality and enforceability of e-signatures. Each country has their own local laws pertaining to the type of e-signatures that are permissible under the law (Electronic signature, advanced electronic signature, or digital signature). When doing international business, be sure to understand relevant e-signing laws of all countries involved.

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>



WHAT CANNOT BE E-SIGNED?

While electronic signatures are considered legally binding by law, the actual usage is at the sole discretion of the party requiring consent in an agreement. Some situations even require the signer to be physically present to sign, rendering an e-signature incompatible or unnecessary. Restrictions vary from country to country. Below is a list of possible use cases that may be exceptions to e-signature laws, or where the situation is incompatible with digital transactions:

- Wills, codicils and testamentary trusts
- Marriage and adoptions
- Divorce papers and court orders
- Power of attorney
- Mortgage agreements and certain real estate transactions
- Documents requiring notarization

BENEFITS OF E-SIGNATURES



Time saved - To sign a document remotely, the process might look something like this: print out the document, sign it, scan the signed version, upload it to your computer, and email it to the other party. It's a time-consuming task that requires access to hardware such as printers and scanners. If the physical document with signature is required, then postage or couriering is involved, further extending timeframes. Legally binding e-signatures eliminate all of this as signing a document can be done directly from your computer, tablet or phone. Completing transactions with e-signatures reduces signings from days and weeks to mere minutes.



Money saved - Besides time consumption, there's also an associated cost to using a physical signature, which entails the use of paper, printers, scanners, fax machines, ink, and postage (for mailing documents). This is also less environmentally friendly. With multiple transactions happening throughout the day for some departments, expenses can add up quickly just to get a quick stroke of a pen. Electronically signing a document eliminates these costs entirely.



Mobile signing - In today's ultra-connected world where remote offices and cross-border transactions are commonplace, requiring a physical signature simply isn't realistic for facilitating deals efficiently. Electronic signatures require only an internet connection, which greatly streamlines the process. Anyone with access to the internet or cellular data can quickly review and sign a contract, whether at home, on the go, or even at the gym.



Oversight - One benefit of digitization lies in its ability to leave behind a trail of information. Unlike paper signatures, which mostly leave no evidence trail, electronic signatures instantly identify the signer and produce a timestamp of an opened and signed document. This provides a reliable audit trail of the transaction, giving you a clearer view of who signed your document, the time and date the signature was collected, and who has yet to sign. The digital nature of an e-signature helps you track and manage every document that requires signatures.



Automation - When collecting multiple signatures on the same piece of paper, the collector has to get them one at a time before moving on to the next – a significant halt to efficiency. Many e-signature solutions are designed to solve this problem. When producing a document to be e-signed, these solutions automatically move around from signee to signee until all the required signatures have been collected on a single document, logging the progress throughout. If no particular signature order is required, then the document will return back to the collector when all signatures have been returned. In either case, when a document sits in a signatory's inbox for too long, the collector can send remote gentle reminders to keep the progress going. A saved agreement workflow can even be created for recurring agreements that require the same necessary parties to sign every time.



Templates - Similar legal language is often shared from contract to contract within a company's sales contract, even if the negotiated terms are different. Thus, underwriting a contract to be signed by wet signature can become tedious and time-consuming to complete. An e-signature document on the other hand can be generated using company-approved templates. With templates vetted by your organization's legal team, sales reps simply need to populate terms of the contract, and a standard contract will be produced accordingly, drastically reducing errors and minimizing back-and-forth between parties. This can be used for other types of consistent contracts as well.



Archiving - Because of its digital nature, e-signed documents and forms have the ability to be housed in a centralized computer repository after a transaction has been completed. Teams that heavily operate on agreements and sales cycles will appreciate being able to organize and refer back to previous contracts, taking note of expiring agreements, in order to prepare for renewal processes, without having to search through paper documents in file cabinets.



FOXIT ESIGN

Foxit eSign is Foxit's groundbreaking signing solution to help organizations greatly accelerate their agreement workflows, offering the easiest, fastest, and most secure way to sign, send, track and store documents. No matter where your clients are located, requesting for signatures is as quick as sending an email. Contracts facilitated through Foxit eSign are legally compliant and fully trackable, paving the way for your department to effortlessly sign or route important deals with peace of mind. After your contracts have been prepared – whether from scratch or via template – simply upload them to Foxit eSign to sign or send to recipients. With the combined power of Foxit eSign and Foxit PDF Editor, edit your contracts and collect signatures with complete ease – and reach time to agreement in record speeds while you're at it.

Foxit is a leading software provider of fast, affordable, and secure PDF solutions. Foxit has over 650 million users and has sold to over 425,000 customers located in more than 200 countries. The company has offices all over the world, including locations in the US, Asia, Europe, and Australia. For more information please visit, foxit.com.