Adobe Sign

U.S. Guide to Electronic Signatures.

An overview of federal and state law.

Overview.

Electronic signatures facilitate faster and more secure document signing for the public and private sector, with the flexibility to choose the option that is most efficient for each organization, department, or project. With the passage of the United States (U.S.) Electronic Signatures in Global and National Commerce (ESIGN) Act in 2000, electronic signatures became legal in every state and U.S. territory where federal law applies. When federal law does not apply, most U.S. states have adopted the Uniform Electronic Transactions Act (UETA).

In the U.S., there are two primary types of electronic signatures:

1. Electronic signature (e-signature) refers to any electronic process that indicates acceptance of an agreement or record. Most electronic signature solutions in the U.S. fall into this broad category. Electronic signatures use a wide variety of common electronic authentication methods to verify signer identity, such as email, corporate ID, password protection, or a PIN sent to a mobile phone. Proof of signing is demonstrated via a secured process that often includes an audit trail and a final tamper-evident digital certificate embedded into the completed signed document.
2. Digital signature uses a certificate-based digital ID to authenticate a signer's identity. Certificates used in digital signatures are usually issued by a certificate authority (CA) and demonstrate proof of signing by binding the digital certificate associated with each signature to the document using encryption.

The information provided in this guide is intended to assist in understanding the legal framework of electronic signatures for U.S. states and territories. Laws pertaining to electronic signatures are constantly evolving, so this guide should not serve as a substitute for professional legal advice.

CONTENTS

Electronic Signatures in Global and National Commerce (ESIGN) Act.

The ESIGN Act granted electronic signatures the same legal status as handwritten signatures throughout the U.S., greatly simplifying and expediting how organizations gather, track, and manage signatures, and approvals on agreements and documents of all kinds. Under the ESIGN Act, an electronic signature is defined as any electronic process associated with an agreement that indicates acceptance of that agreement. The ESIGN Act:

- Provides that any law with a requirement for a signature may be satisfied by an electronic signature.
- Allows electronically executed agreements to be presented as evidence in court.
- Prevents denial of legal effect, validity, or enforceability of an electronically signed document solely because it is in electronic form.

Under the ESIGN Act, an electronic signature is defined as "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." In simple terms, electronic signatures are legally recognized as a viable method to indicate agreement to a contract. For an electronic signature to be legally binding under the ESIGN Act, it is recommended that all electronic signature workflows include:

Intent to sign.

Similar to ink signatures, a signer must show clear intent to sign an agreement electronically. For example, signers can show intention by using a mouse to draw their signature, typing their name, or clicking an "Accept" button that is clearly labeled.

Consent to do business electronically.

Most electronic signature laws also require some form of consent to do business electronically. Many enterprise electronic signature solutions ask signers to "click to accept" a standard consent clause or provide an option to customize a consent clause such as:

> *The parties agree that this agreement may be electronically signed. The parties agree that the electronic signatures appearing on this agreement are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility.*

Opt-out clause.

If a signer elects to opt-out of signing an agreement electronically, clear instructions on how to sign an agreement manually should be easily accessible as part of the signature workflow.

Signed copies.

All signers should receive a fully executed copy of the agreement. Many electronic signature solutions automatically provide executed copies of agreements to signers as part of the approval workflow.

Record retention.

Record retention requirements are addressed via the ESIGN Act which legitimized the validity of electronic records as long as they accurately reflect the agreement and can be reproduced as required. Often this is addressed by providing a fully executed copy to the signer or permitting the signer to download a copy of the agreement.

Uniform Electronic Transactions Act (UETA).

In 1999, the Uniform Law Commission drafted the model Uniform Electronic Transactions Act or UETA to provide a legal framework for the use of electronic signatures in each state. UETA has been adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. However, three states—Illinois, New York, and Washington—have not adopted UETA, but have implemented their own statutes pertaining to electronic signatures. Some of these statutes include material changes to UETA recommended language and guidelines—such as details around consumer disclosures or regulations regarding certificate authorities.

The following key legal terms are outlined in UETA:

1. A record or signature can't be denied legal effect or enforceability simply because it's in electronic form.
2. A contract can't be denied legal effect or enforceability simply because an electronic record was used in its formation.
3. If a law requires a record to be in writing, an electronic record satisfies the law.
4. If a law requires a signature, an electronic signature satisfies the law.

In all states that have adopted UETA, the law generally does not apply to birth, wedding, or death certificates and wills, codicils, and testamentary trusts are also often exempt.

Illinois.

The state of Illinois (IL) has not adopted UETA. However, in 1999, Illinois enacted electronic signature law 5 ILCS 1 75/1-101. The Illinois law favors some types of electronic signatures as more trustworthy than others. Under the law, the most secure type of electronic signature is the "secure electronic signature." Secure electronic signatures are presumed valid under the law unless there is evidence to the contrary. Under the law, an electronic signature is deemed "secure" if:

1. It is created in a manner that can be considered commercially reasonable under the circumstances
2. It is applied by all parties in a trustworthy manner that can be verified
3. It can be reasonably and in good faith relied upon by all parties
4. Both parties agree that the signature is "secure"

The Illinois law also defines a digital signature as a "secure electronic signature" if:

1. It is created using an asymmetric algorithm certified by the Secretary of State
2. It is created using a valid certificate issued by a CA in accordance with standards set by the Secretary of State, within the scope specified in the valid certificate, and can be verified via the valid certificate public key.

New York.

The state of New York (NY) has not adopted UETA. However, since 2000, electronic signatures have been legally binding in New York under the Electronic Signatures and Records Act (ESRA). This law broadly established the legal equivalence of electronic and handwritten signatures. ESRA also created the role of the "electronic facilitator" within the NY Office of Information Technology Services. This department oversees all technology used to promote government efficiency and effectiveness, including electronic signatures and publishes a comprehensive best practices guide for those wishing to implement electronic signatures under ESRA.

In New York, electronic signatures have the same legal validity as handwritten signatures. They are admissible in a court of law as long as they comply with the rules of evidence. However, just as with all other electronic signature laws, no government organization nor citizen is required to use electronic records or signatures. Additionally, ESRA does not apply to any document providing for the disposition of an individual's person or property upon death or incompetence, or appointing a fiduciary of an individual's person or property. This includes wills, trusts, and "do not resuscitate" orders as well as powers of attorney and health care proxies.

Washington.

The state of Washington (WA) has not adopted UETA. However, Washington did enact the Washington Electronic Authentication Act to facilitate e-commerce and minimize fraud, as well as to ensure the security and integrity of "e-messages." It includes wording to ensure that electronic signatures are not refused legal recognition and regulates CAs. In Washington, the Secretary of State licenses and regulates CAs and oversees the rules and policies around using them. In order to be considered for government use, CAs must pass specific requirements and prove that they have a trustworthy system. The Secretary of State conducts periodic compliance audits of CAs and can even fine CAs in violation.

Resources.

For additional information, please see the following resources:

- Stephen Mason, *Electronic Signatures in Law* (4th edition, Cambridge University Press, 2016)
- Stephen Errol Blythe, Ph.D., J.D., Ph.D., *E-Commerce Law Around the World: A Concise Handbook* (Xlibris, Corp., February 24, 2011) Available on Amazon and Google Books
- The Standards and Procedures for Electronic Records and Signatures (SPeRS)
- Electronic Signature & Records Association
- Digital Evidence and Electronic Signature Law Review
- Electronic and digital signatures in Adobe Sign for government white paper

For more information.

https://adobe.com/go/adobesign

Adobe is pleased to provide information that can help businesses understand the legal framework of electronic signatures. However, Adobe cannot provide legal advice. Any information in this paper is not intended as legal advice and should not serve as a substitute for professional advice. You should consult an attorney regarding your specific legal questions.