Transform business processes with electronic and digital signatures.

Adobe Sign lets you comply with local and international regulations using one scalable signature solution.

A White Paper

August 2018

TABLE OF CONTENTS

Transforming the way you sign on the dotted line.

Organizations around the world are urgently transforming their businesses, using digital technologies to deliver agility, efficiency, cost savings, and great customer experiences. Document signature processes represent one of the biggest opportunity areas to accelerate this shift. Workers spend countless hours hunting down approvals and ink signatures—and then print, scan, fax, or mail documents to get the job done. The resulting delays frustrate customers, business partners, and employees alike—and ultimately reflect poorly on the company's brand.

It's little wonder that organizations have embraced electronic and digital signatures. Today, leading companies in every industry and geography—including KLM, Groupon, Jaguar Land Rover, Ricoh, Unum, and LeasePlan Corporation—get fast, legal, and secure signatures electronically. The results are impressive. Ricoh accelerated turnaround time for sales contracts and trimmed five days off the process. LeasePlan reduced its average contract turnaround time from 23.5 days to 4 days and 2 hours—an 83% reduction in processing time.

The biggest question today isn't whether to adopt electronic signatures—it's how to go about it while ensuring ongoing compliance with changing regional and industry regulations. While the terms may seem similar, electronic and digital signatures actually describe two different approaches to signing documents—and those differences are linked with signature laws and regulatory requirements. To make the right choice for your organization, you'll want to learn about those differences, understand your unique legal or regulatory environment, and partner with a company you trust—to help you deliver value today and into the future.

This paper explores electronic and digital signatures in Adobe Sign and showcases how you can work with either approach or a combination of the two within a single solution. Adobe Sign is an Adobe Document Cloud solution that manages signature processes from end to end, integrates easily with existing business processes, and helps you comply with regional and industry regulatory requirements around the world. With over 20 years of experience developing and refining PDF and signature technologies, Adobe is uniquely positioned to help you build legal and compliant signature processes.

> *"The courts now recognize an advanced e-signature solution with high security and privacy standards like Adobe Sign. We've partnered with Adobe and created a set of best practices in the area."*
>
> **BART VAN DEN HEUVEL**
> Manager of corporate procurement
> LeasePlan Corporation

Electronic vs. digital signatures: What's the difference?

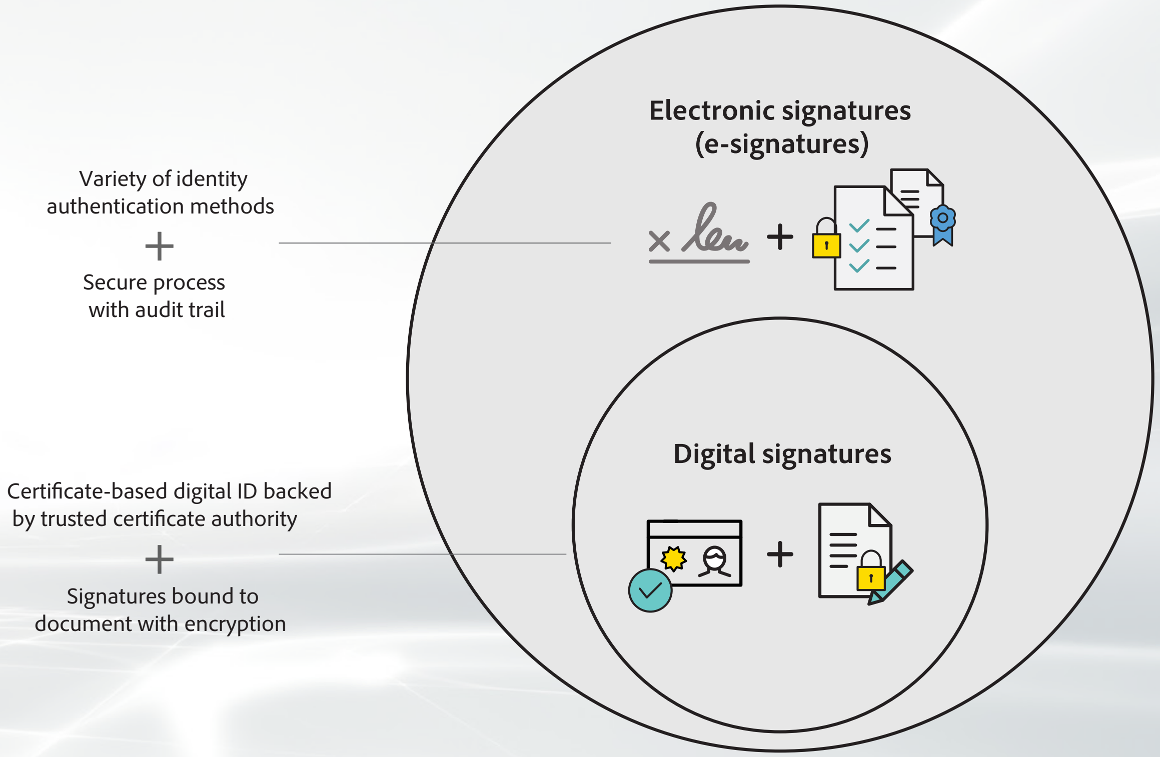
Electronic signatures (e-signatures) refer to any electronic process that indicates acceptance of an agreement or a record. Electronic signatures:

- Use a variety of common electronic authentication methods to verify signer identity, such as email, social IDs, passwords, or a phone PIN. Standard e-signatures use single factor authentication. Enhanced e-signatures use multifactor authentication to increase security when needed.
- Demonstrate proof of signing using a secure process that often includes an audit trail along with the final document.

Digital signatures use a specific method to sign documents electronically. Digital signatures:

- Use a certificate-based digital ID to authenticate signer identity.
- Demonstrate proof of signing by binding each signature to the document with encryption—validation is done through trusted Certificate Authorities (CAs) or Trust Service Providers (TSPs).

Electronic signature types


Electronic signatures
(e-signatures)
Variety of identity authentication methods
+
Secure process with audit trail
Digital signatures
Certificate-based digital ID backed by trusted certificate authority
+
Signatures bound to document with encryption

The ins and outs of electronic signature laws.

Electronic signatures are legally binding in nearly every industrialized nation, and even less developed countries are beginning to enact e-signature laws. In 2000, the United States (U.S.) passed the Electronic Signatures in Global and National Commerce (ESIGN) Act, making e-signatures legal for virtually all uses. In the European Union (EU), the Electronic Identification and Trust Services (eIDAS) regulation took effect in July 2016. It established a new legal structure for electronic identification, signatures, seals, and documents—creating a single digital market across the entire EU. To learn more about signature laws, read Global Guide to Electronic Signature Laws: Country by Country.

The right approach to building a compliant electronic signature process for your business will depend on your unique regulatory environment, risk profile, and specific business requirements. There's a marked contrast, for example, in legal approaches between the United States and the European Union. U.S. law allows for a broad definition of electronic signatures and does not prescribe a specific technology. In contrast, the EU eIDAS regulation distinguishes between three types of electronic signature approaches, and requires digital signatures for some types of documents. In addition, some business sectors, such as biopharmaceutical and government, have developed more prescriptive guidelines for specific business processes that require digital signatures.

Worldwide, there are generally two types of electronic signature laws:

Minimalist laws—Many countries, including the United States, Australia, New Zealand, and Canada, have minimalist or permissive laws, which allow for the broad enforceability of e-signatures with few legal restrictions and give e-signatures the same legal status as handwritten signatures.

Multi-tier laws—Countries with multi-tier laws generally permit the broad use of e-signatures but provide greater evidentiary weight to signatures that use different types of certificate-based digital IDs to authenticate signers. Regions and countries that have adopted multi-tier laws include the European Union, China, India, and South Korea. In the European Union, for example, only signatures using digital IDs from qualified providers are automatically given the same status as handwritten signatures.

Choosing the right approach for your processes.

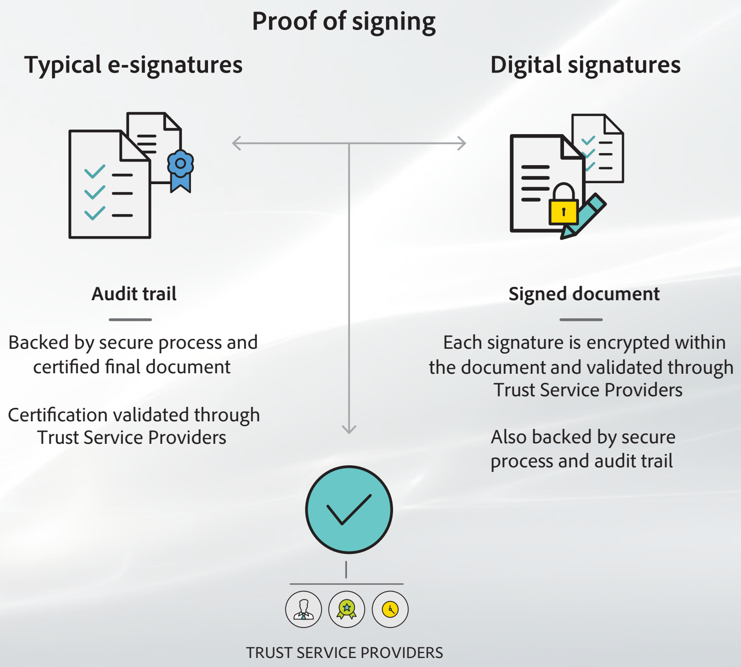
To find the right signature approach for your business, you'll need to balance regulations and risk, and consider what level of effort is necessary to make your business transactions both legal and secure. In general, properly configured e-signature processes are easier to implement, and meet legal and security requirements for many business processes. Digital signatures have additional technical demands, but provide an advanced form of authentication that meets more stringent, highly regulated compliance requirements. Adobe Sign supports both approaches in one flexible, scalable solution, letting you chose one or the other—or a combination of the two.

Typical signer authentication for everyday approvals.

E-signature processes in Adobe Sign are compliant with e-signature laws, such as the U.S. ESIGN Act and EU eIDAS regulation. With support for both single factor and multifactor authentication, Adobe Sign gives you a range of options to verify signer identities. Standard authentication is achieved by sending an email request and private link to a specific person. Because most signers have unique access to one email account, this is considered the first level of authentication. To strengthen security and help prevent hackers from spoofing the system, you can use "enhanced authentication," which adds another verification step before signers open the document. Senders can choose from a variety of methods—such as social IDs, passwords, phone PINs, and knowledge-based authentication (KBA)*—to reconfirm the signers' identity. To further improve legal compliance, you can also build processes that require an explicit consent to do business electronically before engaging in the signature process.

Adobe Sign manages the document securely throughout the process and certifies the signed document with a tamper-evident seal to confirm its integrity. Each key step in the signature process is logged, such as: when the agreement was sent, opened, and signed; IP addresses or geolocations of signers; and the specific form of authentication used for each signer or approver.

The result is captured in a secured audit trail. Both the signed document and audit trail are delivered to all parties and securely stored in Adobe Document Cloud, providing clear, easily producible evidence of each party's signature.



Proof of signing

Typical e-signatures

Digital signatures

Audit trail

Backed by secure process and certified final document

Certification validated through Trust Service Providers

Signed document

Each signature is encrypted within the document and validated through Trust Service Providers

Also backed by secure process and audit trail

TRUST SERVICE PROVIDERS

> *"Our average turnaround time for signed contracts with Adobe Sign is 1.3 hours. Considering that it used to take at least two weeks, and sometimes even months with paper contracts, this is a huge improvement."*

Western Australian Local Government Association (WALGA)

* Knowledge-based authentication available in the United States only.

Robust authentication for stricter requirements.

Digital signature processes in Adobe Sign are compliant with more rigorous requirements, such as advanced (AdES) and qualified (QES) electronic signatures in the EU eIDAS—and provide comprehensive support for working with accredited Certificate Authorities (CAs) and Trust Service Providers (TSPs). They also work with qualified signature creation devices (QSCDs), such as smart cards, USB tokens, and cloud-based hardware security modules (HSMs).

Documents signed digitally in Adobe Sign provide evidence of each participant's signature within the document itself. During the signing process, the signer's certificate is cryptographically bound to the document using the private key uniquely held by that signer. During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signer's identity through the CA and help ensure no changes were made to the document since it was signed. Audit trails can also provide additional, valuable information such as the signer's IP address or geolocation.

Understanding Trust Service Providers.

To achieve the highest levels of security, digital signature processes use a technology approach called Public Key Infrastructure (PKI) for encryption, signing, and certificate authentication. Digital IDs are issued by CAs and TSPs that meet defined requirements. These providers, in turn, are part of a standards-based, industry-wide effort to allow verification of signer identities and document authenticity on a global scale.

Industries and governments publish lists of authorities that meet defined requirements. Adobe uniquely enables global validation for the entire industry through publication and management of trusted lists. Global and regional lists, like the Adobe Approved Trust List (AATL) and the European Union Trusted Lists (EUTL), are fully supported in Adobe solutions.

Trust Service Providers offer a range of secure identity and transaction services, including:

- Registration Authority (RA)—Signer identities are verified to qualify for an ID.
- Certificate Authority (CA)—Once verified, a CA issues a private key and the corresponding certificate, and then manages it over time. The private key is controlled by a password or PIN uniquely known to the signer.
- Time Stamp Authority (TSA)—Digital signature processes also engage with TSAs to establish an accurate time for each signing event.

Adobe Sign lets you work with your choice of TSPs to sign and time stamp documents, so you can comply with laws or regulations governing your specific country or industry. Additionally, you can also use a qualified time stamp from Adobe or the TSP of your choice to comply with long-term digital record retention requirements. During the validation process, Adobe also confirms that the authorities being used in the document are trusted providers—approved through global, regional or industry-specific accreditation. Trust lists, such as AATL and EUTL, serve the entire industry, providing an authoritative source of Trust Service Providers.. Examples of participants include:

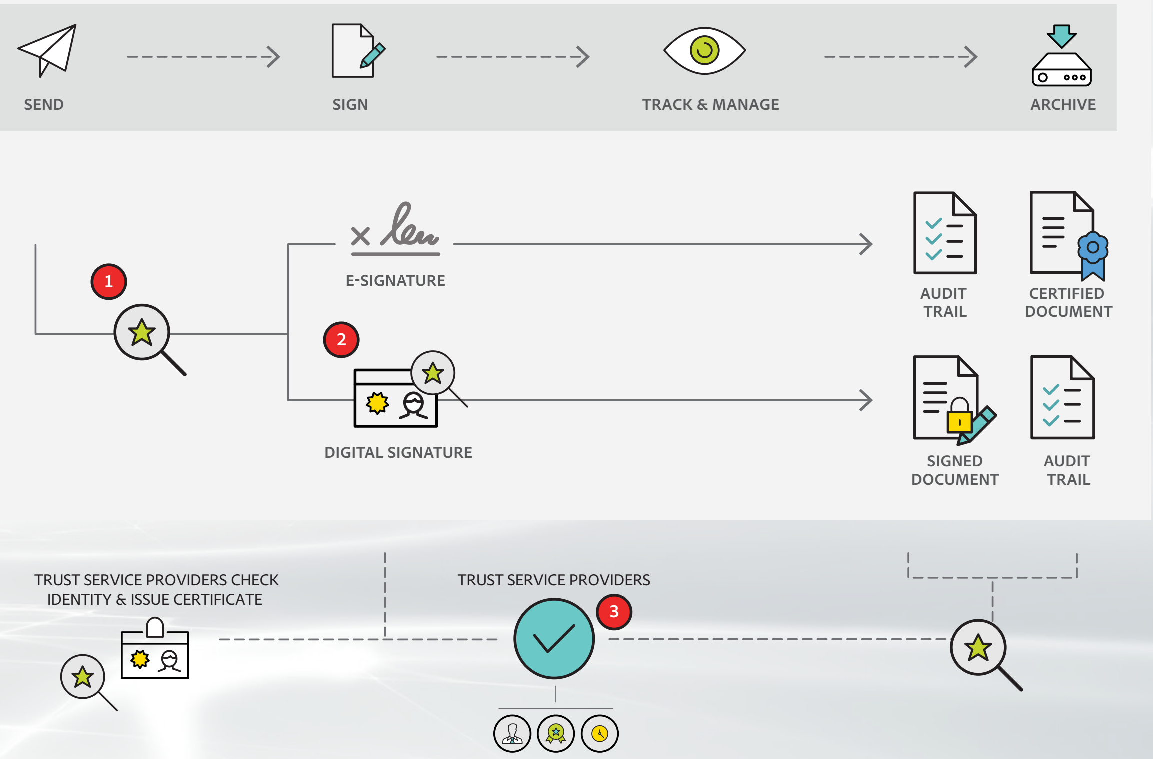
- The U.S. federal government and Department of Defense
- All 28 member states of the European Union
- The governments of Japan, Brazil, Switzerland, India, and Uruguay
- Postal services of Germany, France, Italy, Hong Kong, and South Africa
- SAFE-BioPharma and IdenTrust

One solution. Multiple options.

Adobe Sign is uniquely designed to support the broadest range of electronic and digital signature requirements, so you can do business locally or globally—and choose the best approach for each of your business processes. With Adobe Sign, you can build end-to-end workflows that include typical e-signatures, digital signatures, or both. Adobe Sign also provides industry-leading support for signer authentication and validation.

1. Before opening your document, signers authenticate their identity using single factor or multifactor methods.
2. Signers add digital signatures using a password or PIN-protected private key from their certificate to bind their signature to the document.
3. Signer and document authenticity are validated through the trust service providers who issue digital IDs to signers. Adobe Sign works with with over 200 TSPs globally, including a growing ecosystem of providers who support cloud-based digital signatures for anytime, anywhere experiences on web and mobile devices.

E-signatures and digital signatures in Adobe Sign



> *"With Adobe Sign, instead of it taking a day to send out a policy form on paper and then waiting a week or longer for the completed form to come back, 70% of returned forms are received within 24 hours. The process is easier all around and translates to a much better customer experience."*

CHRISTINE FRANCIS
Business operations development manager of shared services
Unum

Comparing signature types in Adobe Sign.

Whether your signers use e-signatures or digital signatures, Adobe Sign supports essential requirements to help you build fully compliant business processes.

		Typical e-signatures	Digital signatures
Consent to e-sign	Explicit consent can be captured during the process	✓	✓
Authenticate	Single factor e-signature authentication with email ID and a secure, tracked process	✓	✓
	Enhanced, multifactor e-signature authentication (e.g., email plus social ID, phone PIN, knowledge based, password, and more)	✓	✓
	Digital signature authentication with digital ID and private PIN	—	✓
Sign	E-sign using a web browser or mobile device. No downloads or signups required.	✓	✓
	Sign with a digital ID using your desktop computer. Work with smart cards, USB tokens, HSMs, and over 200 CAs globally.	—	✓
	Sign with a cloud digital ID using your web browser or mobile device. Take advantage of open standards for cloud-based digital signatures.	—	✓
Ensure document integrity	Certified by Adobe	✓	✓
	Digitally signed by all participants	—	✓
Track all events	Audit trail certified by Adobe	✓	✓
Validate through Trust Service Providers	Signer's identity and signature	—	✓
	Tamper-evident seal	✓	✓
	Adobe time stamp with long-term validation or third-party time stamp.	—	✓
Secure the process	ISO 27001, SOC 2 Type 2, PCI DSS and SAFE-BioPharma certified. Adobe SPLC compliance	✓	✓
	Conforms to Adobe Software Product Life cycle (SPLC) standards	✓	✓
Comply with regulations	Such as HIPAA, FERPA, and GLBA.	✓	✓
	Supports compliance with FDA 21 CFR Part 11	✓	✓
Store data in your region	Data centers located in North America, Europe, Australia, India, and Japan	✓	✓

Adobe: The digital document leader.

With 6 billion transactions a year, Adobe is the global leader in secure digital document solutions and standards-based electronic signatures. Adobe Sign allows you to deliver exceptional, simple signing experiences while ensuring compliance with local and global signature laws. We're trusted and used by Fortune 1000 companies, government, healthcare, and financial institutions to help automate signing and approvals across a wide range of departments and business processes.

Key benefits of Adobe Sign

Standards-based signing—We invented PDF— and the digital signatures that work in PDF— then worked with industry-recognized standards organizations ISO and ETSI to turn them into open standards. Adobe solutions work with over 200 CAs around the world, and we're the only global vendor to support every European Union TSP accredited to issue qualified digital IDs. We're also advancing global standards again for digital signing using mobile devices and the web with the Cloud Signature Consortium. Our real-world cloud signature solutions let you work with high-assurance digital IDs from industry leaders that are easy to use, easy to deploy, and help you comply with regulatory requirements.

World-class capabilities—Adobe Sign makes it easy to manage end-to-end business processes. Quickly send documents out for signature and get the job done in record time. Documents are stored in your business system, a repository of your choice, or Adobe Document Cloud—and backed by strict security, so your employees can store, access, track, and manage documents from anywhere in real time.

Maximum flexibility—Use one single, scalable solution to create end-to-end signing processes that include digital signatures, e-signatures, or a combination of the two. Adobe Sign gives you flexibility to build workflows in accordance with your specific compliance, industry and risk profile. Build digital signature processes within your organization or in the cloud using Adobe Sign plus the CA or TSP of your choice with support for the full range of signature creation devices including smart cards, USB tokens and cloud-based HSMs.

Comprehensive security controls—Adobe takes the security of your digital experiences very seriously. Adobe Sign meets rigorous security standards—including ISO 27001, SOC 2 Type 2, and HIPAA, as well as PCI DSS used in the Payment Card Industry. We also employ Adobe Secure Product Lifecycle (SPLC) practices, a demanding set of several hundred specific security activities—spanning software development practices, processes, and tools—integrated into multiple stages of the product lifecycle.

An enterprise-grade solution—Powerful administration tools in Adobe Sign help you manage user and group preferences, restrictions, and languages quickly and easily. Ultra-high availability data centers in North America, Europe, Australia, India, and Japan keep business running smoothly.

Superior prebuilt integrations—Easily add electronic signatures that work natively in your systems of record with richly featured, preintegrated solutions. Adobe Sign integrations and robust APIs let you embed signature processes within your organization's enterprise systems and applications. Integrations include Salesforce, Workday, Microsoft Dynamics CRM, Ariba, SAP, Apptus, and more.

Exceptional customer experience—Delight customers with fast response times and speedy contract signing processes. Customers can sign without printing or faxing documents, installing software, creating new logins, or scanning anything. The entire process can take just minutes from start to finish, so everyone can finish quickly and get on with their day.

To learn more about how Adobe Sign can benefit your organization, contact your Adobe sales representative today.

Resources

Discover even more by consulting these additional resources:

- Adobe Sign Cloud Signature Solution Brief
- Global Guide to Electronic Signature Law: Country by country
- Developing an effective electronic signature policy
- Adobe Sign Solution Brief

For more information

Solution details:
https://adobe.com/go/adobesign

Adobe