



# Transform business processes with electronic and digital signature solutions from Adobe

With Adobe Sign, you can comply with laws and regulatory guidelines—using one scalable signature solution.

**Table of contents**

- 2: Electronic signature law
- 2: Electronic and digital signature approaches
- 5: Adobe Sign
- 6: Work with the digital document leader
- 7: Resources

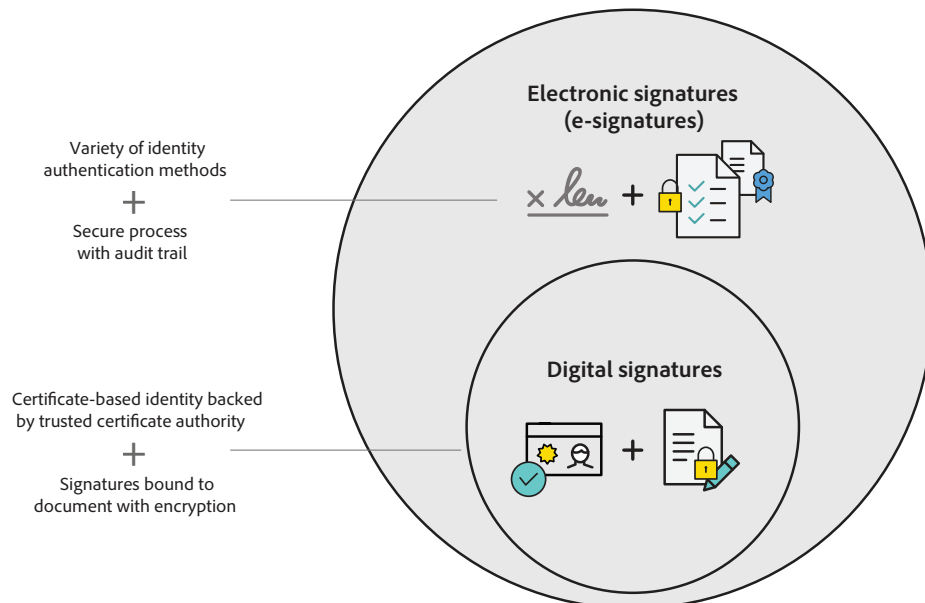
Organizations around the world are urgently transforming their businesses, using digital technologies to deliver agility, efficiency, cost savings and superior customer experiences. Document signature processes represent one of the biggest opportunity areas to accelerate this transformation. Workers 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, yielding 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 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 and shows how Adobe solutions let you work with either approach, or a combination of the two. *Adobe Sign* is an Adobe Document Cloud solution that manages signature processes from end to end, integrates easily with existing business processes and provides a quick return on investment. With over 20 years of experience developing and refining PDF and signature technologies, Adobe is uniquely positioned to help you build signature processes in compliance with local and global laws as well as regulatory guidelines.

## Electronic vs. digital signatures



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

- May use a wide variety of methods to authenticate signer identity, such as email, enterprise ID or phone verification
- 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 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)

*“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 signature law

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 passed the Electronic Signatures in Global and National Commerce (ESIGN) Act, making e-signatures legal for virtually all uses. The European Union passed an *electronic signature* directive in 1999 that member states used as the foundation for country-specific laws. Now, the European Union Electronic Identification and Trust Services (eIDAS) Regulation will take effect in July 2016—creating a single, standardized regulation for all 28 member states. 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 strongly prefers 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 which require digital signatures.

The types of electronic signatures defined in the eIDAS Regulation are a good example of differing approaches:

- **General electronic signatures**—Using a “minimalist” or “permissive” approach, this definition provides broad legal acceptance for the full range of electronic signature types. Signatures cannot be denied legal acceptance just because they are in electronic form.
- **Advanced Electronic Signatures (AdES)**—Requires that signatures be uniquely linked to—and capable of identifying—the signer. This requirement is typically met with certificate-based digital IDs.
- **Qualified Electronic Signatures (QES)**—Requires certificates to be issued by a certificate authority (CA) that is accredited and supervised by authorities designated by EU member states. These certificates must be stored on a qualified signature creation device (QSCD), such as a USB token, smart card or a cloud-based hardware security module (HSM).

## Electronic and digital signature approaches

To find the right signature approach for your business, you will 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 requirements. Adobe Sign supports both approaches in one flexible, scalable solution, letting you choose one or the other—or a combination of the two.

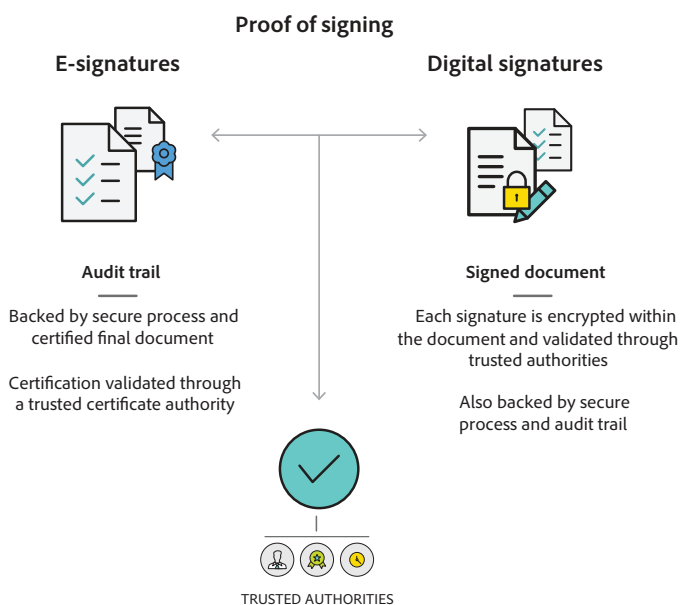
*“Our average turnaround time for signed contracts with Adobe Sign is 1.3 hours. Considering that it used to take at least two weeks, and sometimes even months with paper contracts, this is a huge improvement.”*

Western Australian Local Government Association (WALGA)

## E-signatures

E-signature processes in Adobe Sign are compliant with e-signature laws, such as the U.S. E-SIGN 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. Basic authentication is achieved by sending an email request to a specific person. Because most signers have unique access to one email account, this is considered the first level of authentication. To improve security and help prevent malicious individuals from spoofing the system, you can also include another verification step before signers open the document. Using methods such as enterprise IDs, social IDs, passwords, or phone or knowledge-based authentication (KBA)\*, the identity of signers can be authenticated with higher assurance before they sign the document. To further enhance 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 that provides clear, easily producible evidence of each party's signature.



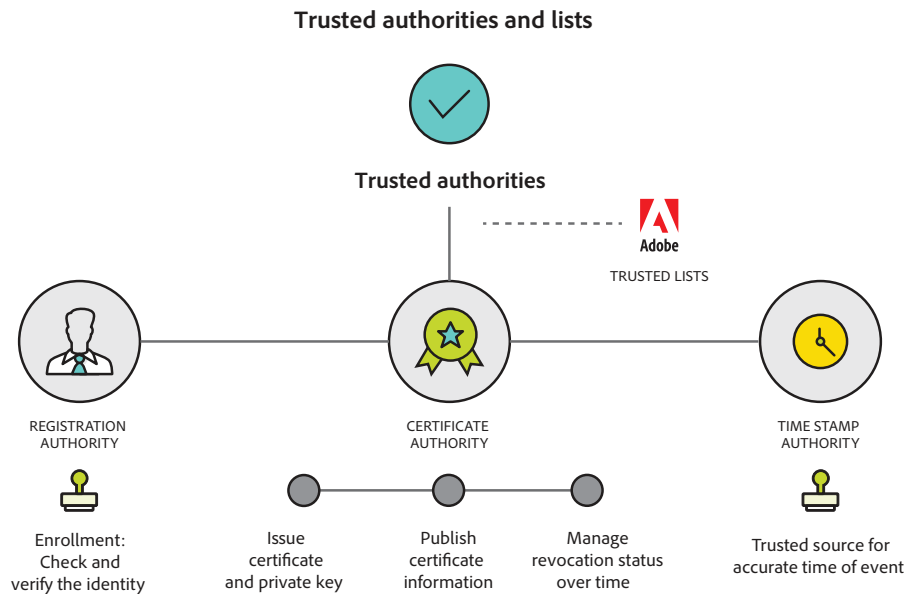
## Digital signatures

*Digital signature* processes in Adobe Sign are compliant with more rigorous requirements, such as advanced (AdES) and qualified (QES) electronic signatures in eIDAS—and provide comprehensive support for working with accredited certificate authorities (CAs) and qualified signature creation devices (QSCDs).

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 that 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.

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

To achieve the highest levels of security and global interoperability, digital signature processes work with certificate IDs that are issued by trusted authorities that meet defined requirements. These authorities, in turn, are part of a standards-based, industry-wide effort to allow verification of signer identities and document authenticity on a global scale.



**Trusted authorities**—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.

There are three main types of trusted authorities:

- **Registration authority (RA)**—Signer identities are typically verified in person 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 trusted TSAs to establish an accurate time for each signing event.

Adobe Sign lets you work with your choice of authorities to sign and time stamp documents, so you can comply with laws or regulations governing your specific country or industry. 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 trusted service providers. Examples of participants include: the U.S. federal government; all 28 member states of the European Union; the governments of Japan, Brazil, Switzerland, India and Uruguay; the U.S. Department of Defense; postal services of Germany, France, Italy, Hong Kong and South Africa; as well as SAFE-BioPharma and IdenTrust, serving the international pharmaceutical and finance markets respectively.

*“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.”*

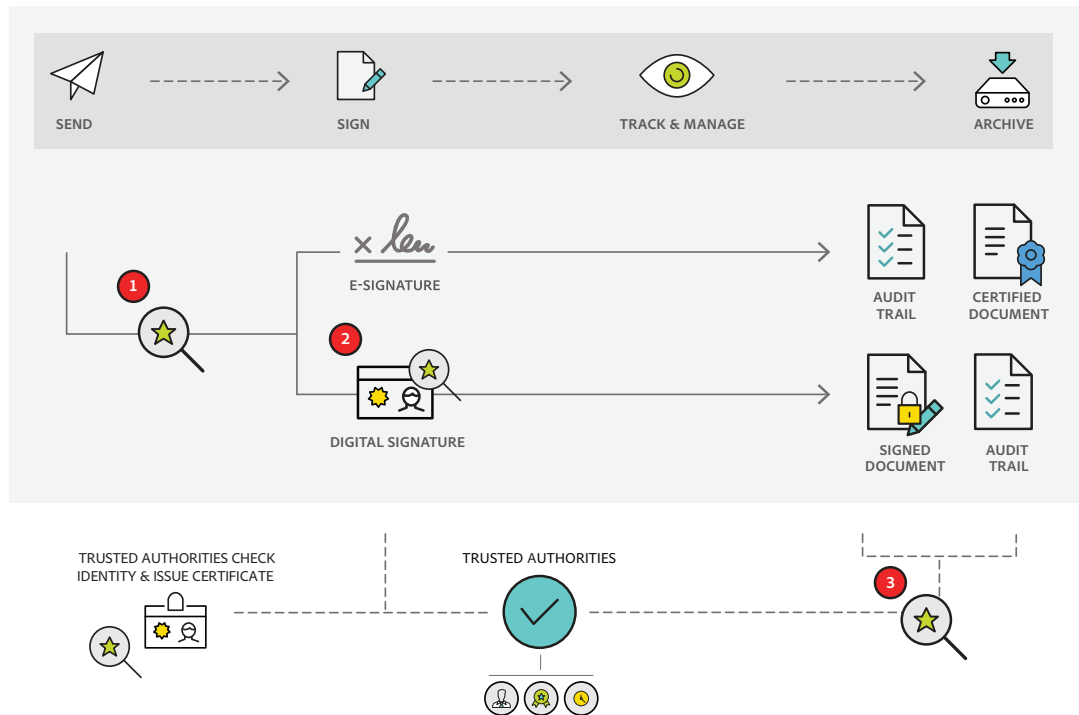
Christine Francis  
Business operations  
development manager of  
shared services, Unum

## Adobe Sign

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 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 trusted authorities.

### E-signatures and digital signatures in Adobe Sign



## 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.

		E-signatures	Digital signatures
<b>Consent to e-sign</b>	Explicit consent can be captured during the process	✓	✓
<b>Authenticate</b>	Basic authentication with email ID	✓	✓
	Multifactor authentication, e.g., enterprise ID, phone verification, knowledge based, password and more	✓	✓
	Certificate issued by CA	—	✓
	Secure signature creation device, e.g., USB token, smart card, or cloud-based HSM	—	✓
<b>Sign</b>	Type, draw, use image or click to approve	✓	—
	Use private key from certificate to bind signature to document	—	✓
<b>Time stamp</b>	Built-in or third-party TSA	✓	✓
<b>Ensure document integrity</b>	Certified by Adobe	✓	✓
	Digitally signed by all participants	—	✓
<b>Track all events</b>	Audit trail certified by Adobe	✓	✓
<b>Validate through trusted authorities</b>	Tamper-evident seal	✓	✓
	Time stamp	✓	✓
	Signer's identity and signature	—	✓
<b>Secure the process</b>	ISO 27001, SOC 2 Type 2, PCI DSS certification and Adobe SPLC compliance	✓	✓
	FDA 21 CFR Part 11		✓
<b>Comply with regulations</b>	Supports compliance with HIPAA, FERPA, GLBA, PIPEDA, and many more	✓	✓
	Supports compliance with Food and Drug Administration (FDA) 21 CFR Part 11		✓
<b>Store data in your region</b>	Data centers located in North America and Europe, with more coming soon	✓	✓

## Work with the digital document leader

Adobe is the global leader in secure digital documents. From the invention of PDF more than 20 years ago—to the creation of digital signatures in PDF—to becoming the first global vendor to support EU Trusted Lists—Adobe has been at the forefront of digital transformation with signatures. We help advance signature standards around the world through our involvement with *ISO*, *OASIS*, *IETF* and *ETSI* and other standards groups.

The highest rated e-signature app in the Salesforce community since 2006, tens of thousands of organizations have adopted Adobe Sign services to manage document signing processes and deliver exceptional customer experiences.

Key benefits of Adobe Sign:

**World-class capabilities**—Manage end-to-end signature processes. Easily 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 workers 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 using the CA and TSA of your choice with support for the full range of signature creation devices including smart cards, USB tokens and cloud-based HSMs.

**Standards-based global signing**—Adobe adheres to global standards to help ensure our solutions work around the world with a wide range of providers. As the first major software vendor to incorporate support for EUTL in globally available solutions, Adobe Sign supports a broad range of certificate and time stamp providers, including approved CAs from the EUTL and the AATL.

**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 v3.0 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 and Europe help you address data sovereignty concerns. Once you choose a data center for your region or country, all administrative data, document processing, and document data and metadata remain in that region or country for the entire data lifecycle. Additional data centers are planned in the Australia and the Asia Pacific region in 2016.

**Superior turnkey integrations**—Easily add e-signing that works natively in your systems of record with richly featured, preintegrated solutions. Adobe Sign turnkey integrations and robust APIs allow you to embed electronic signature processes into your organization's enterprise systems and applications. Turnkey integrations include Salesforce, Workday, Microsoft Dynamics CRM, Ariba, SAP, Apptus and more.

**Exceptional customer experience**—Adobe solutions let you 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 solution brief](#)
- [Global overview of electronic signature law](#)
- [Global Guide to Electronic Signature Law: Country by country](#)
- [Developing an effective electronic signature policy](#)
- [Blog: EU Trusted List in Adobe Acrobat](#)

### For more information

Solution details:

<https://adobe.com/go/adobesign>



Adobe Systems Incorporated  
345 Park Avenue  
San Jose, CA 95110-2704  
USA  
[www.adobe.com](http://www.adobe.com)

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.

Adobe, the Adobe logo and Acrobat are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2016 Adobe Systems Incorporated. All rights reserved. Printed in the USA.