Electronic and digital signatures in Adobe Sign for government white paper

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

Table of contents

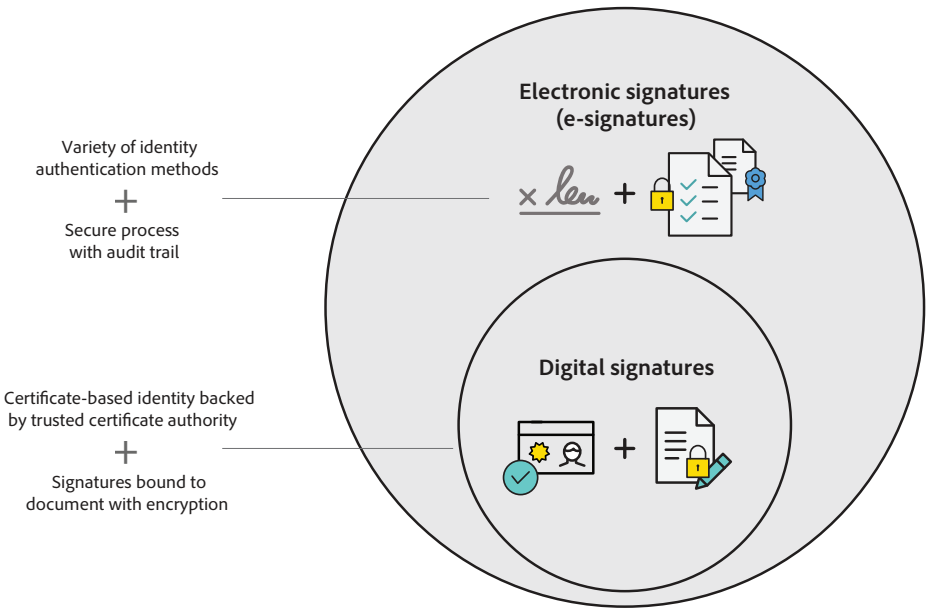
Government organizations around the world are actively transforming their agency businesses, using digital technologies to deliver agility, efficiency, cost savings and superior constituent experiences. Document signature processes represent one of the biggest opportunities to accelerate this transformation. Government 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 citizens, departments, suppliers and employees alike.

It's little wonder that government organizations have embraced electronic and *digital signatures*. Today, leading agencies such as the State of Hawaii and the Western Australian Local Government Association (WALGA) get fast, legal and secure signatures electronically. The results are impressive. WALGA has reduced their average time to have contracts signed from 2 weeks or longer to just 80 minutes.

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 agency, 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 goverment 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 your agency 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 same customer expectations in the commercial world are redefining constituent expectations in the public sector…"

Andrew Bartels and Chip Gliedman, Forrester Research, Inc.
US Government Spending And The BT Agenda, March 2015

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. In the European Union, the Electronic Identification and Trust Services Regulation, commonly referred to as eIDAS, 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 agency will depend on your unique regulatory environment, risk profile and specific 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, there are more prescriptive guidelines for specific government 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 agency, you will need to balance regulations and risk, and consider what level of effort is necessary to ensure your government transactions are both legal and secure. In general, properly configured e-signature processes are easier to implement, and meet legal and security requirements for many government 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.

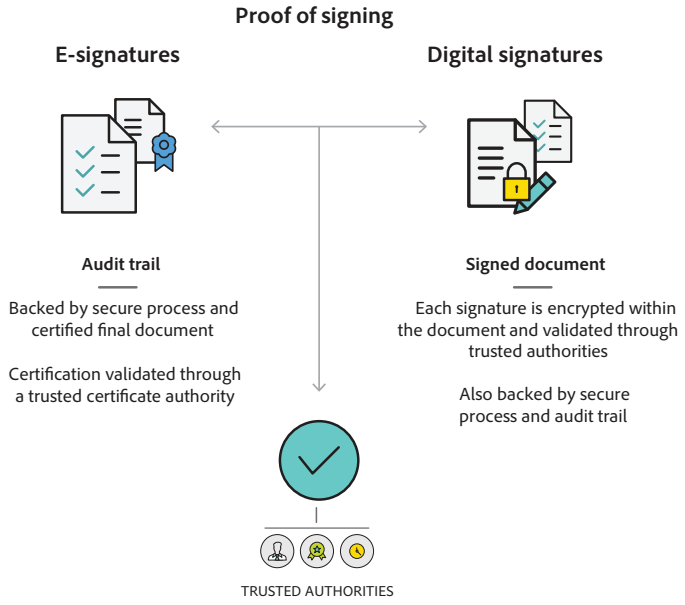
"Our average turnaround time for signed contracts with Adobe Sign is 1.3 hours. Considering that it used to take at least two weeks, and sometimes even months with paper contracts, this is a huge improvement."

Nikki Brennan, Contract Coordinator, WALGA

E-signatures

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. 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 government 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

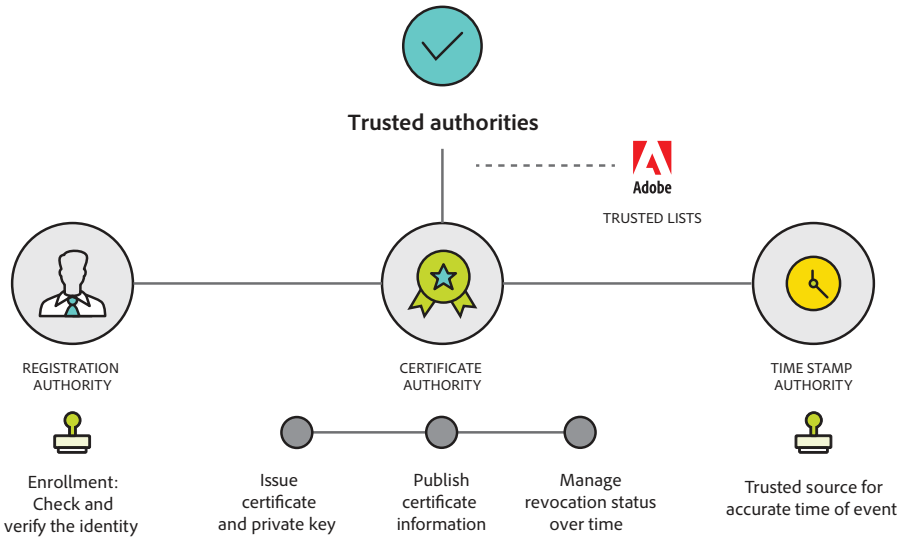
Digital signature processes in Adobe Sign are compliant with more rigorous requirements, such as advanced (AdES) and qualified (QES) electronic signatures in eIDAS—and provide comprehensive support for working with accredited certificate authorities (CAs) and qualified signature creation devices (QSCDs).

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 and lists



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 member states of the European Union; the governments of Japan, Brazil, Switzerland, India and Uruguay; the U.S. Department of Defense; as well as the postal services of Germany, France, Italy, Hong Kong and South Africa.

"Since deploying Adobe Sign, we've completed hundreds of contracts. Previously, each of these contracts, which average 110 pages long, would be printed in triplicate. Moving to a paperless workflow with Adobe Sign has saved us more than 50,000 pieces of paper, approximately AU $56,000 so far, and has significantly impacted our sustainability, professionalism, and process efficiencies."

Nikki Brennan, Contract Coordinator, WALGA

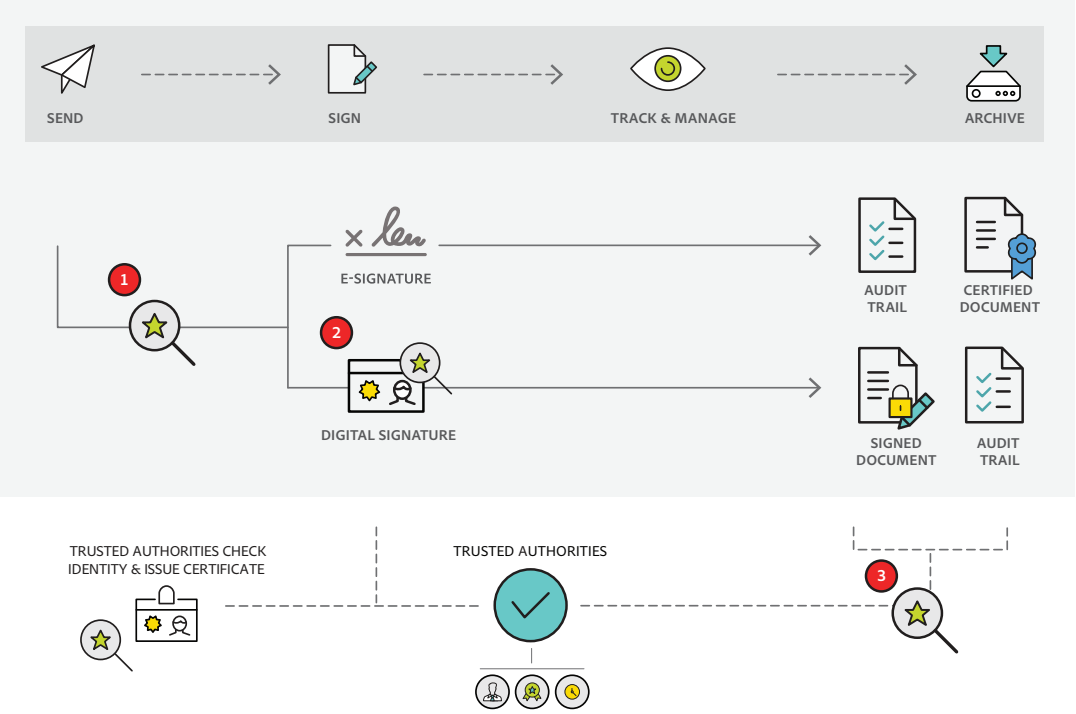
Adobe Sign

Adobe Sign is uniquely designed to support the broadest range of electronic and digital signature requirements so you can conduct government business locally or globally—and choose the best approach for each of your agency 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 government processes.

		E-signatures	Digital signatures
Consent to e-sign	Explicit consent can be captured during the process	✓	✓
Authenticate	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	—	✓
Sign	Type, draw, use image or click to approve	✓	—
	Use private key from certificate to bind signature to document	—	✓
Time stamp	Built-in or third-party TSA	✓	✓
Ensure document integrity	Certified by Adobe	✓	✓
	Digitally signed by all participants	—	✓
Track all events	Audit trail certified by Adobe	✓	✓
Validate through trusted authorities	Tamper-evident seal	✓	✓
	Time stamp	✓	✓
	Signer's identity and signature	—	✓
Secure the process	ISO 27001, SOC 2 Type 2, PCI DSS certification and Adobe SPLC compliance	✓	✓
Comply with regulations	Supports compliance with industry-specific regulations such as HIPAA, FERPA, GLBA and many more	✓	✓
	Supports compliance with Food and Drug Administration (FDA) 21 CFR Part 11	—	✓
Store data in your region	Data centers located in North America, Europe, Australia and Japan	✓	✓

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.

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 enterprise storage 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 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.

Flexible APIs and superior turnkey integrations—Easily add e-signing that works natively in your existing systems. 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 digital government experiences—Adobe solutions let you delight citizens, suppliers and more with fast response times and speedy contract signing processes. Constituents 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 agency, contact your Adobe government sales representative today.

Resources

Discover even more by consulting these additional resources:

- *Adobe Sign solution brief for government*
- *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*
- *Adobe Sign technical overview*

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

9/16