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.
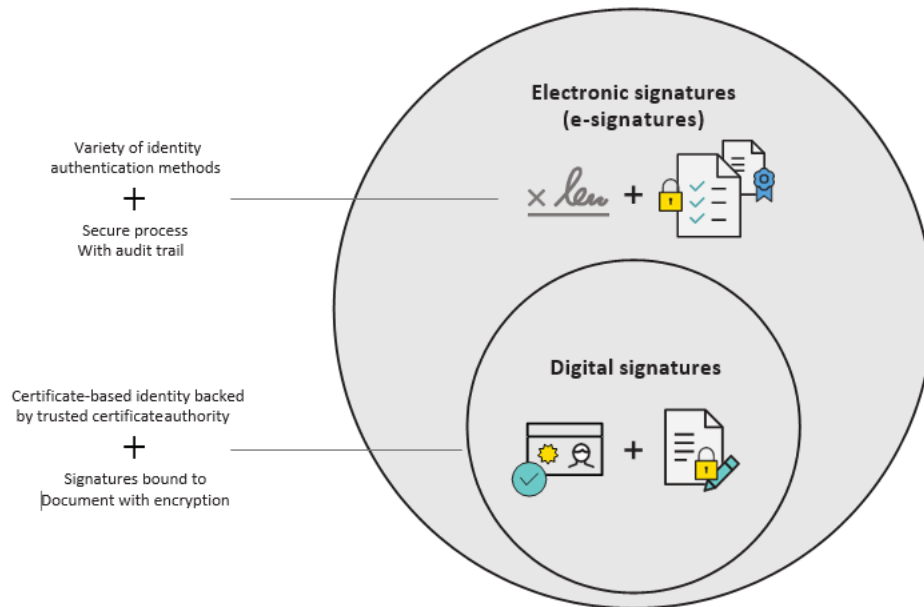
Government organizations around the world are actively transforming their agency businesses, using digital technologies to deliver agility, efficiency, cost savings and superior constituent experiences. Document signature processes represent one of the biggest opportunities to accelerate this transformation. 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 government 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 signatures
(e-signatures)**

Variety of identity
authentication methods

+

Secure process
With audit trail

Digital signatures

Certificate-based identity backed
by trusted certificateauthority

+

Signatures bound to
Document with encryption

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:
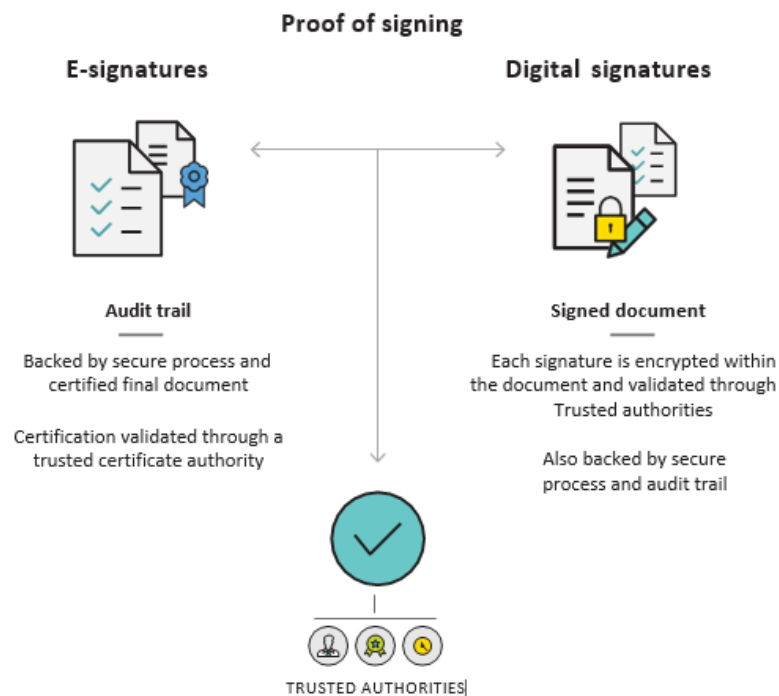
- Use a certificate-based ID to authenticate signer identity
- Demonstrate proof of signing by binding each signature to the document with encryption—validation is done through trusted certificate authorities (CAs)

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.

Proof of signing

| E-signatures | Digital signatures |

Audit trail

Backed by secure process and certified final document

Certification validated through a trusted certificate authority

Signed document

Each signature is encrypted within the document and validated through Trusted authorities

Also backed by secure process and audit trail

TRUSTED AUTHORITIES

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 HS

- 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.