Adobe Sign enterprise overview

Security, compliance, identity management, and document handling

Table of contents

1: Executive summary
2: Architecture
4: Security
6: Compliance
7: Integration
7: Infrastructure
7: For more information

Executive summary

Adobe Sign can help your organization replace paper-and-ink signature processes with 100% digital workflows. With this Adobe Document Cloud solution, you can easily send, sign, track, and manage signature processes and electronically sign (e-sign) digital documents on any device, from any location. Adobe Sign meets or can be configured to meet compliance requirements for many industry and regulatory standards. As a robust cloud-based service, Adobe Sign securely handles large volumes of e-signature processes, including:

- Managing user identities with capability-based authentication
- Certifying document integrity
- Verifying e-signatures
- Maintaining audit trails
- Integrating into your most valued business applications and enterprise systems

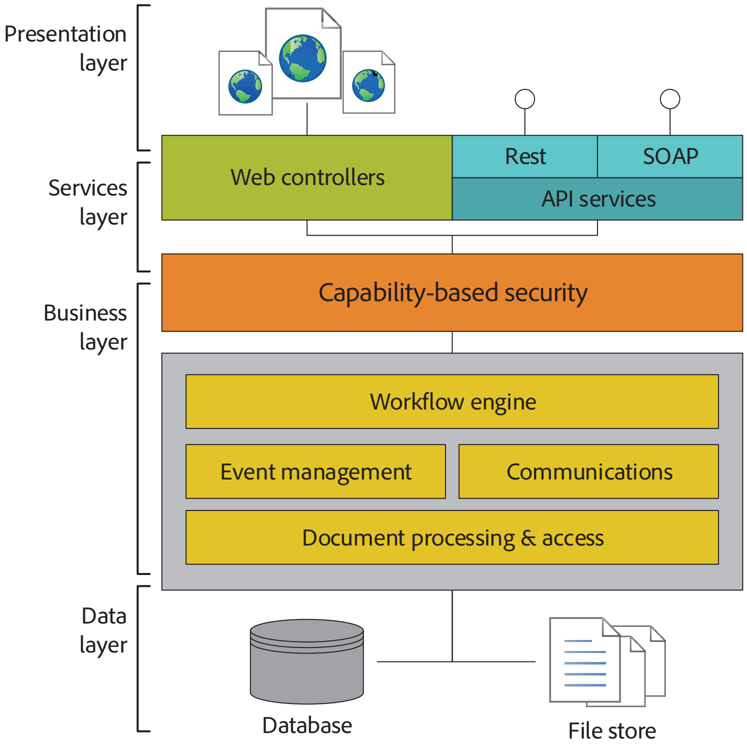
Adobe Sign supports both electronic signatures (e-signatures) and digital signatures. An e-signature is a legally binding way to indicate consent or approval on digital documents and forms. E-signatures are legally valid and enforceable in many countries around the world. A digital signature is a specific implementation of an e-signature that embeds a verified digital certificate into each e-signature. For organizations requiring this increased level of authentication, Adobe Sign can be used with Adobe Acrobat DC or Adobe Acrobat Reader DC to incorporate certified digital signatures into e-signed documents.

E-signature laws vary by country. In the United States, the Electronic Signatures in Global and National Commerce (ESIGN) Act is a federal law that facilitates the use of electronic records and e-signatures in interstate and foreign commerce transactions by providing for the validity and legal effect of contracts entered into electronically. Additionally, as of July 2016, the European Union (EU), the Electronic Identification and Authentication Services (eIDAS) regulation establishes a consistent legal framework and recognition for electronic signatures, seals, and documents across all 28 EU member states. When used according to applicable state and/or country law, Adobe Sign is fully compliant with both the U.S. ESIGN Act and EU eIDAS Regulation. This also enables compliance with other e-signature laws and regulations in other countries, such as the Australian Electronic Transactions Act (ETA) and Canadian Uniform Electronic Commerce Act (UECA).

This paper provides a high-level overview of Adobe Sign architecture, security, compliance, identity management, document handling, and other key technical topics. For additional information on using digital signatures, please see the *Transform business processes with electronic and digital signature solutions from Adobe* white paper.

Architecture

The Adobe Sign architecture is designed to scale and handle large volumes of transactions without performance degradation. To provide a high level of availability and scalability, all Adobe Sign transactional data is stored in multiple distributed redundant database clusters with automatic failover and recovery.* The following layered architectural diagram depicts the logical division of Adobe Sign components and functionality:



Adobe Sign high-level logical architecture

Each logical layer in the Adobe Sign application is monitored by an extensive suite of tools that keeps track of key indicators, such as average time to convert documents into PDFs or resource usage. The monitoring dashboard allows Adobe Sign operations engineers to easily view the overall health of the service. Real-time notifications alert operations engineers if an incident occurs or a resource process falls outside of a monitoring threshold. If an issue can't be averted, Adobe Sign keeps extensive diagnostic and forensic logs to help engineers resolve the issue quickly and address the root cause to avoid a potential reoccurrence.

Presentation layer

The presentation layer manages the web user interface (UI) as well as the generation and display or rendering of documents for signature, final certified PDF files, and workflow components.

Services layer

The services layer handles the required controlling functions for the client services and web services API interfaces, such as the REST Gateway and SOAP API. The external-facing systems web servers handle browser and API requests, and the email servers manage inbound and outbound communications traffic. The web servers distribute complex dynamic requests to the Adobe Sign application servers in the business layer through the use of hardware load balancers. The services layer web servers also incorporate security-filtering rules to prevent common web attacks and firewall protection to strengthen access control.

* Automatic recovery is limited to Amazon Web Services infrastructure.

Business layer

The Adobe Sign business layer handles the workflow, capability-based security, document conversion and imaging services, event management, logging and monitoring, file access and manipulation, and communications functions.

Workflow engine

The Adobe Sign workflow engine executes and manages all the business processes and steps that a document needs throughout the signature process. The workflow engine uses a declarative XML-based definition language to describe the preconditions for executing customer-specific flows and the sequence of events required to complete a signature or approval process.

Capability-based security

The Adobe Sign capability-based security defines, controls, and audits which resources are available and what operations are allowed by an authenticated user or application on those resources. Resources include any information in the form of documents, data, metadata, user information, reports, and APIs.

Event management

The Adobe Sign event management records and preserves an audit trail for relevant information pertaining to each user and document at each step in the workflow process. As each stage in the workflow occurs, Adobe Sign generates an event and distributes messaging via an asynchronous messaging system to the appropriate system resources.

Communications

Adobe Sign uses email for signature event notifications and optional delivery of signed and certified documents at the end of the process. To minimize spam and phishing, Adobe Sign enables authenticated email with Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), and Sender Policy Framework (SPF).

Document processing and access

To increase performance, the Adobe Sign document processing engine provides completely stateless functionality for converting different file formats into PDF, encrypting and decrypting files, and rasterizing images for viewing through a web browser. For document processing actions, Adobe Sign relies on an asynchronous, queue-based messaging system to communicate across system resources. Additionally, all document processing and access to network-attached storage (NAS) occurs in the background, allowing Adobe Sign processing to appear instantaneous for users at each step in the workflow.

Data layer

The data layer is responsible for transactional database access, the asynchronous messaging system database, and the document store. Transactional data stored in the data access layer includes the original customer document, intermediate document versions generated during the signature process, document metadata, users, events, and the final signed PDF document processed by Adobe Sign.

Security

At Adobe, security practices are deeply ingrained into our culture, software development, as well as service operations processes. Adobe Sign employs industry standard security practices—for identity management, data confidentiality, and document integrity—to help protect your documents, data, and personal information.

For additional information about Adobe security processes, community engagement, and the Adobe Secure Product Lifecycle, please see *www.adobe.com/security*.

Identity management

Adobe Sign uses a role-based model for identity management that handles authentication, authorization, and access control throughout the Adobe Sign system. Capability-based security and authentication processes are defined and enabled for an organization by an Adobe Sign administrator. Adobe Sign defines general user roles for:

- **Sender**—Licensed user granted specific Adobe Sign permissions by their administrator to create document signing workflows and send documents for signature, approval, or viewing.
- **Signer**—Verified user provided access by a sender to sign a specific document. By default, Adobe Sign sends an email to the signer that includes a unique URL to the document to be signed that is comprised of exclusive identifiers that are specific to the transaction.
- **Approver**—Verified user provided access by a sender to approve a document.
- **Other**—Verified user provided specific access by a sender to view a document or audit trail.

User authentication

Adobe Sign supports multiple methods to authenticate a user's identity, including both single factor and multifactor authentication plus additional options to verify a user's identity. Typically, a licensed user will log in to Adobe Sign using a verified email address and password that maps to an authenticated identity, such as an Adobe ID. Administrators may also choose to configure password strength and complexity, frequency of change, past password comparison, and lockout policies (such as login renewal expiration).

Basic authentication to Adobe Sign is achieved by sending an email request to a specific person. Because most users have unique access to one email account, this is considered the first level of authentication. First level of authentication is often used for signer, approver, or other user types. To improve security and help prevent malicious individuals from spoofing the system, multifactor authentication methods such as telephone, SMS text, or knowledge-based authentication (KBA) can also be added depending on availability in your geographical location.

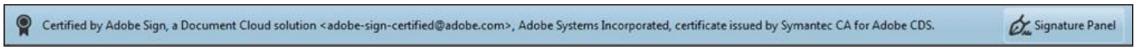
Adobe Sign supports the following types of user authentication options:

- **Adobe Sign ID**—A verified email address and password combination that is used by a licensed user to securely log in to an Adobe Sign account.
- **Adobe ID**—An Adobe ID may be used to access all licensed Adobe services, including Adobe Sign. Adobe continually monitors all Adobe ID accounts for unusual or anomalous activity to quickly mitigate any potential security threats.
- **Google ID**—User identification authenticated by Google, such as Google Mail or Google Apps.
- **Single sign-on (SSO)**—Enterprises seeking a tighter access control mechanism can enable Security Assertion Markup Language (SAML) SSO to manage Adobe Sign users through their corporate identity system. Adobe Sign can also be configured to recognize and integrate with leading identity management vendors, including Okta and OneLogin.

Document certification

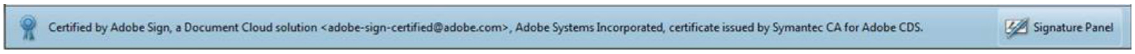
At each stage in the workflow, Adobe Sign maintains a secure checksum of the document to ensure both document integrity and confidentiality. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents with a digital signature before distributing it to all participants.

The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length cryptographically sound hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity (see the following figure) and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.



Certified by Adobe Sign, a Document Cloud solution <adobe-sign-certified@adobe.com>, Adobe Systems Incorporated, certificate issued by Symantec CA for Adobe CDS.

Acrobat DC version—black badge



Certified by Adobe Sign, a Document Cloud solution <adobe-sign-certified@adobe.com>, Adobe Systems Incorporated, certificate issued by Symantec CA for Adobe CDS.

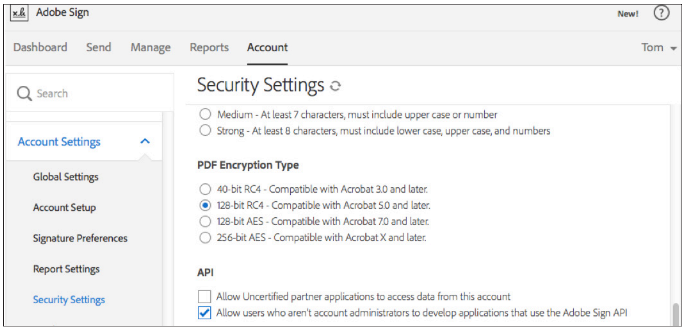
Acrobat X and XI—blue badge (versions 10 and 11)

Adobe Sign document certification banners and badges

To generate the keys used to lock and certify the final signed PDF, Adobe Sign uses specific certificates issued by trusted certificate authorities (CAs) and timestamp authorities (TSAs). In certain circumstances, Adobe Sign can be configured to issue certified documents using government-required CAs, such as in Switzerland and India. PKI keys used to certify the final PDF are stored in a hardware security module to prevent online attacks and tampering.

Encryption

Adobe Sign encrypts documents and assets at rest using AES 256-bit encryption, and supports HTTPS TLS v1.0 (or higher) to help ensure that data in transit is also protected. Documents at rest can only be accessed with appropriate capability-based security permissions through the application data access layer. All document encryption keys are stored in a secure environment with restricted access and are rotated as necessary. Additionally, senders have the option to further secure a document with a private password.



Security Settings

○ Medium - At least 7 characters, must include upper case or number
○ Strong - At least 8 characters, must include lower case, upper case, and numbers

PDF Encryption Type

○ 40-bit RC4 - Compatible with Acrobat 3.0 and later.
● 128-bit RC4 - Compatible with Acrobat 5.0 and later.
○ 128-bit AES - Compatible with Acrobat 7.0 and later.
○ 256-bit AES - Compatible with Acrobat X and later.

API

□ Allow Uncertified partner applications to access data from this account
☑ Allow users who aren't account administrators to develop applications that use the Adobe Sign API

Setting PDF security encryption levels in the Adobe Sign dashboard

Compliance

As a global e-signature solution designed for verified signers to interact with digital documents from any location or any device, Adobe Sign meets or can be configured to meet compliance requirements for many industry and regulatory standards. Customers maintain control over their documents, data, and workflows and can choose how to best comply with local or regional regulations. To learn more about e-signature laws in a specific region, see the *Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability*.

ISO 27001

The ISO 27001 standard is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It contains requirements for information security management systems (ISMS) that can be audited by an independent and accredited certification authority. Adobe Sign is ISO 27001: 2013 certified.

SSAE 16 SOC 2

The Statement on Standards for Attestation Engagements (SSAE) No. 16 for Service Organization Controls (SOC) are a series of IT controls for security, availability, processing integrity, and confidentiality (Type 2). SSAE 16 SOC 2 is designed to help organizations comply with the Sarbanes-Oxley Act (SOX). Adobe Sign has a SOC 2 Type 2 (security & availability) attestation.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes to increase controls around cardholder data management and reduce fraud. Adobe Sign has achieved attestation for PCI DSS 3.0 compliance as a merchant and service provider.

HIPAA[†]

The Health Insurance Portability and Accountability Act (HIPAA) helps ensure sensitive patient information is protected by establishing standards for electronic health care transactions. Adobe Sign can be configured to be used in a way that supports HIPAA compliance by any organization that meets the definition of a covered entity as outlined by the Department of Health and Human Services (HHS), and signs a business associate agreement with Adobe.

21 CFR Part 11[†]

The Code of Federal Regulations, Title 21, Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11) establishes the U.S. Food and Drug Administration (FDA) regulations on electronic records and electronic signatures. Adobe Sign can be configured to be used in a way that allows organizations to comply with 21 CFR Part 11.

GLBA[†]

The U.S. Gramm-Leach-Bliley Act (GLBA) provides regulations for financial institutions to ensure the privacy of personal customer information. Adobe Sign can be configured in a way that allows financial institutions to comply with GLBA requirements.

FERPA[†]

The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. student education records and directory information. Adobe Sign can be configured to handle regulated student data in a way that allows educational institutions to comply with FERPA requirements.

[†] Customers are ultimately responsible to ensure that Adobe Sign is configured and secured in a manner that allows the organization to comply with specific legal obligations such as HIPAA, FERPA, GLBA, and 21 CFR Part 11.

Integration

Adobe Sign has turnkey integrations for a wide variety of business applications and enterprise systems, including Salesforce, Apttus, Workday, Ariba, and Microsoft products. Additionally, Adobe Sign exposes a comprehensive set of APIs that allow for custom integration with proprietary business systems or company websites via secure HTTPS, SOAP, or REST web services. To view the list of integrations supported by Adobe Sign, see the *integrations overview page*.

Infrastructure

Adobe Sign infrastructure resides in top-tier data centers managed by our trusted cloud service providers, Rackspace and Amazon Web Services. Only approved, authorized Adobe employees, cloud service provider employees and contractors with a legitimate, documented business are allowed access to the secured sites in North America and the European Union.

For more information

Solution details: *www.adobe.com/go/adobesign*

Adobe security: *www.adobe.com/security*

Adobe Enterprise Help/Configure Single Sign-On: *helpx.adobe.com/enterprise/help/configure-sso.html*

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

4/16