Adobe Sign technical overview

Security, compliance, identity management, governance, and document handling

Table of contents

Executive summary

Adobe Sign helps your organization replace paper-and-ink signatures and automate document-based business processes from end to end. This Adobe Document Cloud solution makes it easy to initiate, track, and manage digital document processes from web or mobile apps—or inside your enterprise systems. Recipients can sign or participate from anywhere, on any device, with no download or signups required. Adobe Sign complies with requirements for many industry and regulatory standards. As a robust cloud-based service, Adobe Sign securely handles large volumes of *electronic signature* (e-signature) processes, including:

- Managing user identities with capability-based authentication
- Certifying document integrity
- Verifying e-signatures
- Logging recipient acceptance or acknowledged receipt of documents
- Maintaining audit trails
- Integrating with your most valued business applications and enterprise systems

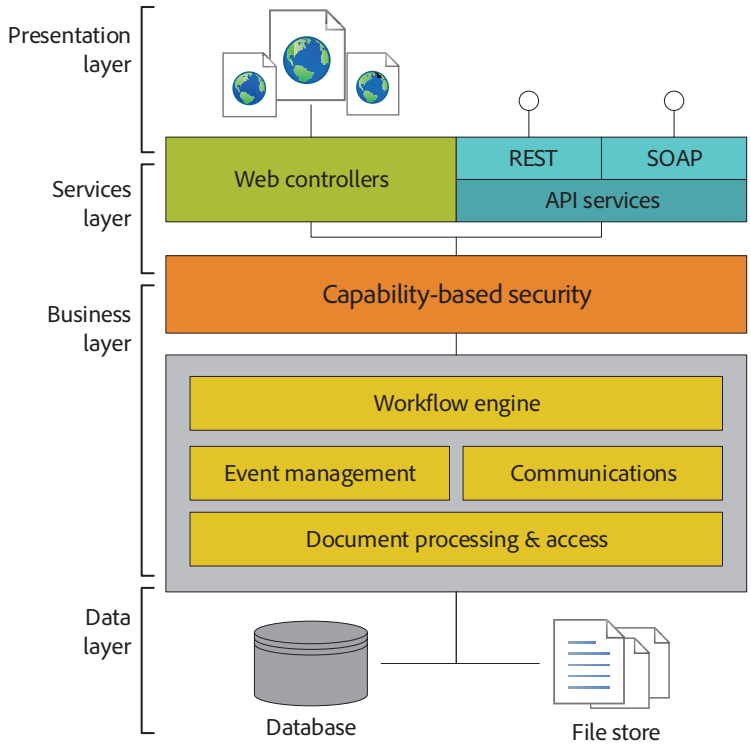
Adobe Sign supports both e-signatures and *digital signatures*. E-signatures are a way to indicate consent or approval on digital documents and forms. E-signatures are legally valid and enforceable in many industrialized nations around the world. A digital signature, by contrast, is a specific implementation of an e-signature that uses a certificate-based digital ID to verify signer identity and binds the signature to the document with encryption. Adobe Sign works with digital IDs stored on smart cards, USB tokens, and cloud-based hardware security modules (HSMs). And it supports open, standards-based signing with digital IDs across desktop, web, and mobile using the Cloud Signature Consortium specification.

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. In the European Union (EU), the Electronic Identification and Authentication Services (eIDAS) Regulation established a consistent legal framework and recognition for electronic signatures, seals, and documents across all 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 1999 (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, network protection, performance monitoring, service management, governance, and other key technical topics. For additional information on using differing signature types, 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 any of the key indicators fall outside of their defined monitoring thresholds. 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 load balancers. The services layer web servers also incorporate security-filtering rules to prevent common web attacks and firewall protection to strengthen access control.

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.

* Automatic recovery is limited to Amazon Web Services infrastructure.

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.

Integrations

Adobe Sign also 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*.

Security

At Adobe, security practices are deeply ingrained into our culture and software development, as well as our 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, 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:

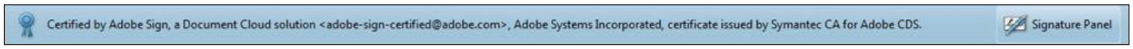
- **Adobe Sign ID**—A verified email address and password combination that is used by a licensed user to securely log in to an Adobe Sign account.
- **Adobe ID**—An Adobe ID may be used to access all licensed Adobe services, including Adobe Sign. Adobe continually monitors all Adobe ID accounts for unusual 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 help 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 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.

Acrobat DC version—black badge



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, Brazil, 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 v1.2 (plus other legacy versions) 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.

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.

SOC

The Service Organization Controls (SOC) is a series of IT controls for security, availability, processing integrity, confidentiality, and privacy (Type 2). Adobe Sign is SOC 2–Type 2 (Security & Availability) certified.

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. As part of Adobe Document Cloud, Adobe Sign has achieved attestation for PCI DSS compliance as a merchant and service provider.

SAFE-BioPharma

The SAFE-BioPharma® digital identification and digital signature standard was created by the biopharmaceutical industry and its regulators to provide global high-assurance identity trust for cyber transactions in biopharmaceuticals, biotech, and healthcare industries. Adobe Sign is SAFE-BioPharma certified.

HIPAA†

The Health Insurance Portability and Accountability Act (HIPAA) helps ensure sensitive patient information is protected by establishing standards for electronic healthcare transactions. Adobe Sign is ready to support HIPAA compliance for any organization that meets the definition of a covered entity as outlined by the U.S. Department of Health and Human Services (HHS) and signs a business associate agreement (BAA) 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. For details on how Adobe Sign is ready to comply with 21 CFR Part 11, please read the *Adobe Sign and 21 CFR Part 11* white paper.

GLBA[†]

The U.S. Gramm-Leach-Bliley Act (GLBA) provides regulations for financial institutions that help ensure the privacy of personal customer information. Adobe Sign is ready to comply with GLBA.

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. Under FERPA guidelines, Adobe Sign is ready to contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.

Infrastructure

Adobe Sign infrastructure resides in American National Standards Institute (ANSI) tier-4 datacenters managed by our trusted cloud service provider, Amazon Web Services (AWS). All hosting partners maintain very strict controls around datacenter access, fault tolerance, environmental controls, and security. 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, Japan, Australia, and the European Union. Additionally, as part of our commitment to security, Adobe reviews compliance attestations, such as SOC 2–Type 2 and ISO 27001 reports, on a regular basis. Additionally, Adobe actively monitors all Adobe Sign components using industry-standard intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Network protection

All Adobe Sign service providers employ network devices to monitor and control communications at the external boundary of the network as well as key internal boundaries within the network. These firewall and other boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. For AWS implementations, the AWS security group approves all ACL policies and automatically pushes them to each managed interface using the AWS ACL-Manage tool to help ensure that the most up-to-date ACLs are enforced.

Both providers also employ a variety of automated monitoring systems to assure a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at network ingress and egress points to protect against traditional network security vulnerabilities such as:

- Distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MITM) attacks
- Internet protocol (IP) spoofing
- Port scanning
- Packet sniffing by other tenants

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the hosted infrastructure for Document Cloud services.

[†] An Adobe service that is GLBA-ready, FERPA-ready, FDA 21 CFR Part 11 compliant, or HIPAA compliant means that the service can be used in a way that enables the customer to help meet its legal obligations related to the use of service providers. Ultimately, the customer is responsible for ensuring compliance with legal obligations, that the Adobe service meets its compliance needs, and that the customer secures the service appropriately.

Operations

Adobe employs standard operations practices such as performance monitoring to manage the health of the Adobe Sign service.

Performance monitoring

Adobe conducts extensive monitoring activities to ensure the health of the Adobe Sign service, including availability, volume, and performance checks. All health checks are based on defined and measurable thresholds that are preemptive indicators of a need for preventative measures. Health-check thresholds and processes are reviewed on a regular basis.

Adobe also conducts server-side logging of customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs do not store any personally identifiable information (PII) such as passwords or names, except for the Adobe ID if applicable. Only authorized Adobe technical support personnel, key engineers, and select developers have access to the logs to diagnose specific issues that may arise.

Service management

Adobe leverages industry-standard service management concepts such as change, incident, and problem management. Our processes and controls are also designed to support numerous compliance frameworks.

Change management

Adobe enforces a comprehensive, standards-compliant change management process with rigorous inspections to assess potential impacts and benefits for any changes to the Adobe Sign service. Most changes have no impact on the service. However, there are rare exceptions, such as the annual disaster-recovery procedures test that may impact the customer experience. In such special cases, Adobe will provide advance notification to any potentially impacted Adobe Sign customers.

Incident management

In the case of a service disruption, the Adobe Sign operations team will invoke Adobe's incident management process. When this process is invoked, 24x7x365 on-call engineers are brought together via online collaboration tools to triage, solve, and resolve the issue. The incident management process also has provisions to capture data on the chain of events leading to the incident resolution, as well as timing and impact information used to assess the impact to our service level agreements (SLAs). Any outstanding issues are transitioned to the problem-management team for ongoing governance.

Problem management

As part of the Adobe incident management process, a formal post-mortem problem-management meeting is scheduled to review the root cause of the incident and propose preventive actions. Since other incidental discoveries may occur during outages, the problem-management process is used to address these along with any vulnerabilities that have either contributed to an outage or have a high risk of causing an outage in the future. The output of a problem-management process is an analysis and summary of the incident, a detailed explanation of the root cause, impact analysis, and required corrective actions to help ensure that the problem is fully resolved.

Staffing

Adobe maintains a dedicated, geographically dispersed team of technical operations engineers utilizing a "follow-the-sun" model where working hours are allocated during regular business hours. This global team provides 24x7x365 on-call response support to assist the corporate Adobe incident response team with resolving any disruption to the service as quickly as possible. Most of Adobe's on-call technical operations engineers are located in the United States and Noida, India.

Governance

Whether monitoring for new vulnerabilities or mitigating potential threats, Adobe employs industry-standard practices to ensure the Adobe Sign risk management, mitigation, and incident resolution process is agile and thorough.

Risk management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. Adobe continuously monitors the threat landscape, shares knowledge with security experts around the world, and endeavors to swiftly resolve incidents. All Adobe Sign infrastructure providers use several tools to proactively detect, evaluate, and trace network-wide traffic and other potentially threatening anomalies, such as denial-of-service (DOS) attacks.

Penetration testing

Adobe approves and engages with third-party security firms to perform penetration testing designed to uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe will document these vulnerabilities, evaluate severity and priority, and then create a mitigation strategy or remediation plan for the Adobe Sign service.

Prior to each release, the Adobe Sign security team performs a risk assessment of the service to look for insecure network setup issues across firewalls, load balancers, and server hardware as well as application-level vulnerabilities. The risk assessment is conducted by highly trained security staff trusted with securing the network topology and infrastructure, as well as the Adobe Sign service. The security touchpoints include threat modeling exercises along with vulnerability scanning and static/dynamic analysis of the application.

Threat mitigation

To mitigate new vulnerabilities and threats that evolve on a daily basis, Adobe subscribes to industry-wide vulnerability announcement lists, such as US-CERT, Bugtraq, and SANS, as well as security alert lists issued by major security vendors. For cloud-based services, such as Adobe Sign, Adobe centralizes incident response, decision-making, and external monitoring to provide cross-functional consistency and fast resolution of issues.

If a significant vulnerability is announced that puts Adobe Sign at risk, the vulnerability is communicated to the appropriate teams within the Adobe Document Cloud organization to coordinate the mitigation effort. Additionally, if an incident occurs with the Adobe Sign service, incident response and development teams use industry-standard practices to identify, mitigate, and resolve the incident:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

To assist with forensic analysis of an incident, the Adobe Sign team captures a complete image (or memory dump) of an impacted machine(s), evidence safe holding, and chain-of-custody recording.

Disaster recovery

Adobe Sign datacenters are designed to deliver high availability and tolerate system or hardware failures with minimal impact. To help ensure business continuity, Adobe maintains regional disaster recovery plans for Adobe Sign in the U.S. and EU along with documentation in the form of an annual *run* book that outlines all the steps required to complete a datacenter failover. Additionally, Adobe strives to achieve the following disaster recovery parameters for its Adobe Sign customers:

- **Recovery point objective (RPO)**—Refers to the amount of data that could potentially be lost during disaster recovery. The timeframe is determined by the amount of time between data protection events. The RPO for Adobe Sign is 2 hours.

- **Recovery time objective (RTO)**—Relates to potential downtime. The metric refers to the amount of time it could take to recover from a data-loss event and how long it takes to return to service. The RTO for Adobe Sign is 8 hours.

Customer notification

Adobe Sign uptime data is available at *www.adobe.com/go/trust-dc*. Additionally, for both planned and unplanned system downtime, Adobe Sign also follows a notification process to inform customers about the status of the service.

If there is a need to migrate the operational service from a primary site to a disaster-recovery site, customers will receive several specific notifications including:

- Notification of the intent to migrate the services to the disaster-recovery site
- Hourly progress updates during the service migration
- Notification of completion of the migration to the disaster-recovery site

The notifications will also include contact information and availability for client support and customer success representatives. These representatives will answer questions and concerns during the migration as well as after the migration to promote a seamless transition to newly active operations on a different regional site.

Data isolation/segregation

All cloud services partners use strong tenant isolation security and control capabilities to segregate Adobe Sign customer data within the multitenant service. Security management processes and other security controls are also used to help ensure that customer data is appropriately isolated and protected.

For more information

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

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

Amazon Web Services security: *https://aws.amazon.com/security*

Adobe Sign Help/Enabling Single Sign-On with SAML: *http://www.adobe.com/go/adobesign_saml_configuration*

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

10/17