



WHITE PAPER

Adobe Sign Security Overview

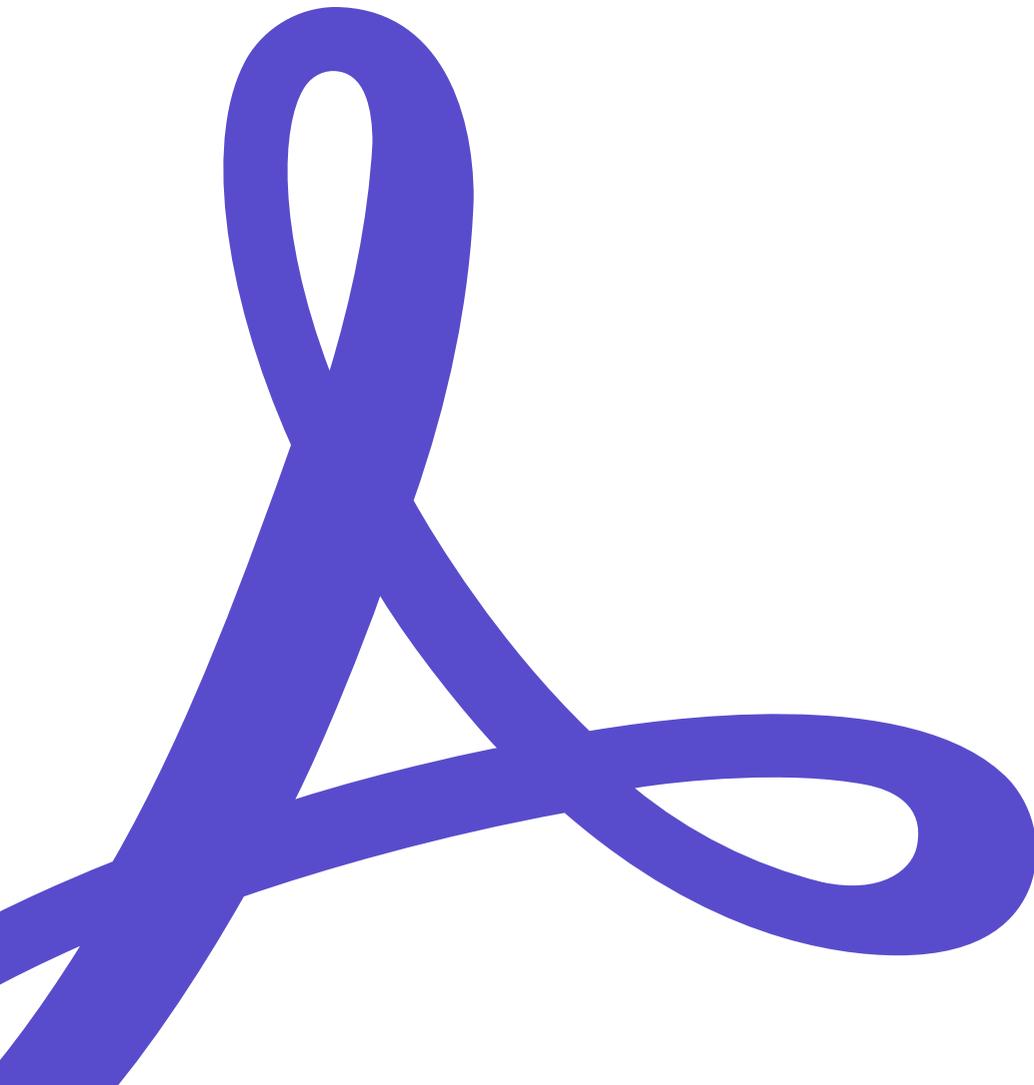


Table of Contents

Adobe Security	3
About Adobe Sign	3
Adobe Sign Solution Architecture	4
Adobe Sign Data Flow Narrative	6
Adobe Sign Security Architecture	8
Adobe Sign Identity Management	10
Adobe Sign Document Certification	12
Adobe Sign Hosting and Security	12
Data Center Physical and Environmental Controls	15
The Adobe Security Organization	17
Adobe Secure Product Development	17
Adobe Risk & Vulnerability Management	20
Adobe Corporate Locations	21
Adobe Employees	21
Conclusion	23

Adobe Security

At Adobe, we know the security of your digital experiences is important. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques into the products and services we offer.

This paper describes the defense-in-depth approach and security procedures implemented by Adobe to bolster the security of Adobe Sign and your data.

About Adobe Sign

Adobe Sign helps your organization replace paper-and-ink signatures and deliver 100% digital experiences across all types of signing workflows — from simple signatures to highly compliant qualified electronic signatures in the cloud. With Adobe Sign, you can easily send, sign, track, and manage signature processes anywhere, anytime using a browser or mobile device. Adobe Sign provides turnkey integrations and APIs to allow your organization to incorporate e-signature workflows into enterprise services, systems of record, and popular cloud productivity solutions, such as Microsoft 365.

Adobe Sign complies with many regional, industry, and regulatory standards including supporting certificate-based digital signatures for increased signer identification and security. As a robust cloud-based service, Adobe Sign securely handles large volumes of online signature processes, including:

- Managing user identities, authentication and access control
- 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

Additionally, Adobe Sign cloud signatures enable remote digital signatures backed by [digital certificates from trust service providers \(TSPs\)](#) with verified Cloud Signature Consortium (CSC) standard integrations to Adobe Sign.

For detailed information on e-signature legality around the world, please see [e-signature legality by country/region](#) in the Adobe Trust center and for more information on Adobe Sign, please go to www.adobe.com/go/adobesign.

Adobe Sign Solution 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.¹

The following layered architectural diagram depicts the logical division of Adobe Sign components and functionality:

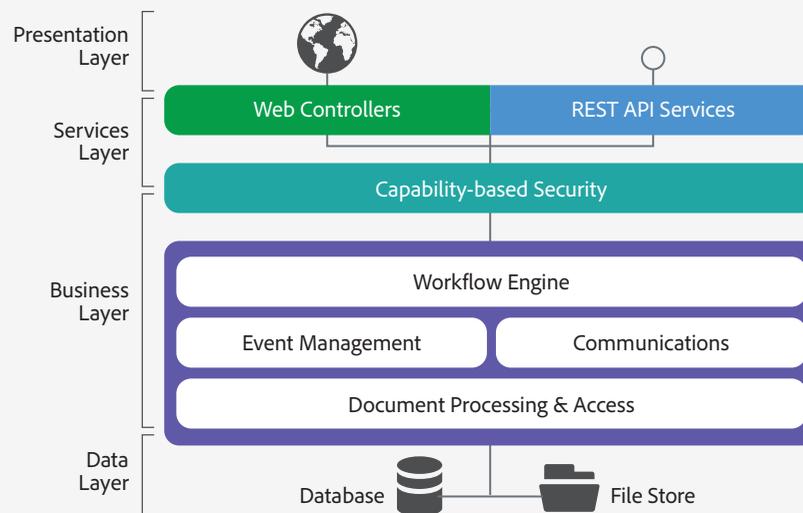


Figure 1: Adobe Sign solution architecture

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 cannot 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 recurrence.

Presentation Layer

The presentation layer manages the web user interface (UI) as well as the generation and rendering of documents for signature collection and other workflows, as well as for final certified PDF files.

Services Layer

The services layer handles the required controlling functions for the client and REST API services. The external-facing systems' web servers handle browser and API requests, and the email servers manage inbound and outbound communications traffic.

Using load balancers, the web servers distribute complex dynamic requests to the Adobe Sign application servers in the business layer. To prevent common web attacks, the services layer web servers also incorporate security-filtering rules as well as firewall protection in order to strengthen access control.

Business Layer

The Adobe Sign business layer handles the following functions:

- **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** — Controls and audits which resources are available and what operations are allowed to be performed on those resources by an authenticated user or application. Resources include any information in the form of documents, data, metadata, user information, reports and APIs.
- **Document processing and access** — Provides completely stateless functionality for converting different file formats into PDF, for encrypting and decrypting files and for 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.
- **Event management** — Records and preserves an audit trail for relevant information pertaining to each user and document at each step in the workflow process. At each stage in the workflow, Adobe Sign generates an event and distributes messaging via an asynchronous messaging system to the appropriate system resources.
- **Communications** — Notifies users of signature events and optionally of signed and certified document delivery 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).

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 via REST API Services

Adobe Sign has turnkey integrations for a wide variety of business applications, enterprise systems and trust service providers (TSPs). Additionally, Adobe Sign exposes a comprehensive set of REST APIs that allow for custom integration with proprietary business systems or company websites via secure web services. To view the list of business applications and enterprise systems supported by Adobe Sign, please see the Adobe Document Cloud for Business [integrations overview page](#). For a list of trust service providers, please visit <https://www.adobe.com/trust/document-cloud-security/cloud-signatures-compliance.html>

Adobe Sign Data Flow Narrative

The following is how a user initiating the signing process for a document interacts with Adobe Sign. Step numbers correspond to the numbers in Figure 2, below:

1. **Define Repository Items:** Before using Adobe Sign for the first time, users can create and save reusable custom workflow definitions, library templates and web forms in the Adobe Sign repository. Any user with access rights to these assets can then send a library template, start a workflow or post a web form to initiate signature processes.
2. **Compose:** To initiate a send agreement workflow through Adobe Sign, the user defines the participants, the order in which they will participate and the different options that define their participation. The workflow agreement may also be initiated through an Adobe-provided integration or a partner or customer application built using the Adobe Sign API. Agreements may also be sent out in bulk based on an uploaded list of email addresses.

Next, the user uploads the source document(s) to which the agreement pertains. Document/s may be uploaded from a third-party cloud storage system, a customer or partner integration, from an existing library template, or from the user's desktop.

3. **Create Agreement:** Once a document is uploaded, it becomes an agreement within Adobe Sign. If the agreement is a library template form with predefined fields, Adobe Sign instantiates these fields into the agreement. If the agreement is not a library template form, the user must place the required fields into the agreement in order to guide the signer through the signing experience.

Adobe Sign allows users to place form fields in their logical position in the agreement and add information and context to the agreement using typed form fields, such as email address, first name, last name, and title. This process is called “authoring.”

At a minimum, every agreement must have a signature field. The signature field can be placed through authoring or automatically by Adobe Sign. If the user chooses to place the signature field automatically, Adobe Sign places it at the bottom of the agreement (if there is enough whitespace) or by adding an additional signing page to the agreement. This information can be exported later and used in downstream processes.

4. **Distribute Links:** When the user completes authoring the agreement, it is sent to all designated participants via email, web form, or by using the Adobe Sign API in a custom application.
5. **Gather Signatures:** Based on the agreement parameters, signers are asked to submit approval, provide a signature, and/or fill in form field values. These form fields may be optional or required, based on the originating user’s instructions, and can be masked or formatted in a variety of ways. All values, along with the current agreement state (e.g., who has signed and who must sign next) are maintained in Adobe Sign data storage in the cloud. Attachment documents may be collected at this stage.
6. **Fully Signed Agreement:** After all signers complete the signing workflow, the fully signed agreement is made available to all participants in the signing process and automatically stored in Adobe Sign cloud storage. Users may download all artifacts related to the signing, including the signed agreement (certified PDF), an audit report (certified PDF) and a separate report of form field data values (exportable in CSV format), using Adobe Sign clients or optionally move or copy the agreement into their chosen systems of record through Adobe Sign APIs or a partner document vaulting service.



Figure 2: Adobe Sign Data Flow

Adobe Sign Security Architecture

The following network diagram depicts Adobe Sign security architecture including external-facing servers, cloud servers, and client access:

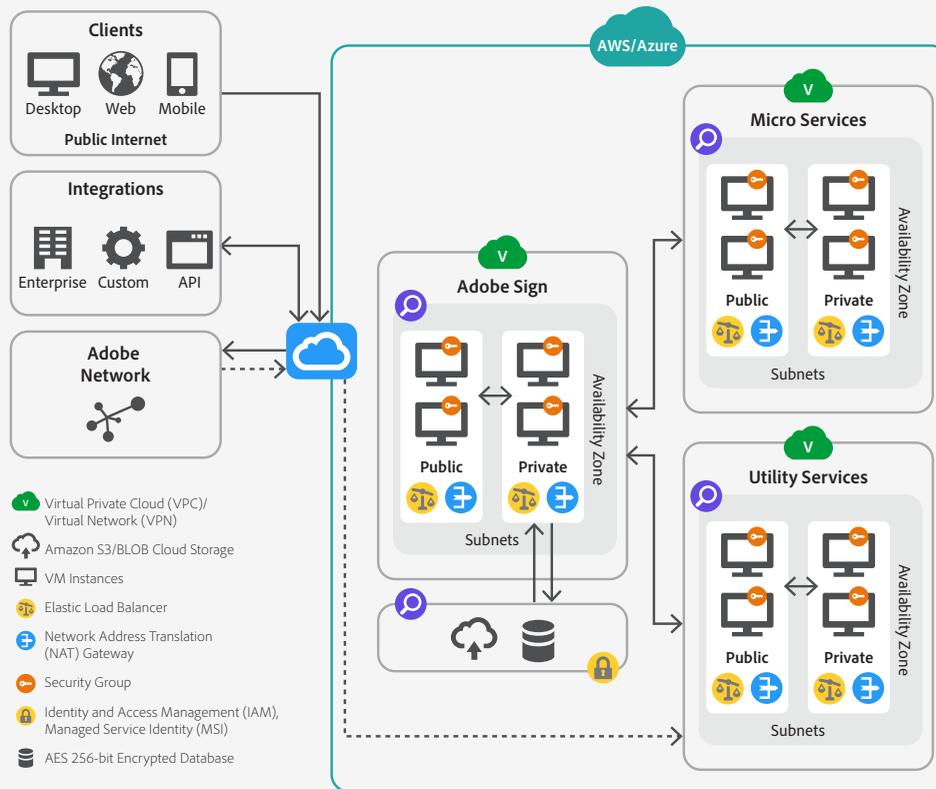


Figure 3: Adobe Sign Network Security Architecture

External-Facing Servers

The external-facing systems within the hosted network architecture of Adobe Sign services include *web servers* to handle browser and API requests and *email servers* that handle inbound and outbound email traffic. The web servers and associated load balancers are responsible for distributing dynamic requests to the application servers. The web servers also include built-in security filtering rules to deny common web attacks and firewall protection to help ensure strong access control.

Virtualized Cloud Networks

The Adobe Sign network security architecture also relies on several virtualized cloud networks. In the AWS environment, these are referred to as Virtual Private Clouds (VPCs), while Microsoft Azure uses the term Virtual Networks (VNETs).

A VPC/VNet is a logically isolated network, inaccessible from the outside except through tightly constrained entry and egress points. Within each VPC/VNet there are subnets, which contain a range of IP addresses. Subnets may be either public or private. A public subnet is connected to the Internet; A private subnet is not connected to the Internet. VPCs/VNETs used by the Adobe Sign service include:

- A core VPC/VNet supporting central Adobe Sign business processes.
- A microservice VPC/VNet to support secondary services, such as digital signature integration with the Cloud Signature Consortium, signature validation and background removal of signature images.
- A utility services VPC/VNet to manage event monitoring and other administrative functions.

All these services run on scalable, secure virtual cloud servers that are accessible only via the tightly secured subnet and VPC/VNET network restrictions.

To support high availability, VPC/VNet instances are divided into multiple, redundant availability zones (AZs). AZs are physically isolated from each other to ensure that power, network or other infrastructure failures in one AZ do not affect operation in the others. All data is replicated across all AZs and across multiple servers within each AZ.

Network access within a VPC/VNet instance is locked down via security group rules. Similar to a virtual firewall, the security groups allow Adobe to further control inbound and outbound traffic to the VPC/VNet instance, enabling Adobe to help ensure sure that only validated users are performing authorized actions. Additionally, the Adobe Sign network security architecture includes intrusion detection sensors at key locations to help ensure system integrity and visibility across the service.

Client Access

The Adobe Sign service is accessible from a variety of client endpoints, including browsers and mobile apps. When a client connects to Adobe Sign in its assigned region, it connects through an Internet gateway to a specific VPC/VNet. All the client connections occur over a HTTPS connection utilizing TLS1.2 with a minimum of AES 128-bit encryption.

Data encryption

Adobe Sign employs [PCI DSS approved encryption algorithms](#) to encrypt documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.

Documents at rest can only be accessed with appropriate capability-based security permissions through the application data access layer in a private subnet. Adobe Sign senders also have the option to add a private password in order to further secure a document. Document encryption keys are stored and managed in a secure environment with restricted access.

Adobe Sign 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 including:

- **Sender**—Licensed user who is granted specific Adobe Sign permissions by their administrator to create document-signing workflows and send documents for signature, approval or viewing.
- **Signer**—Verified user who is 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, which is comprised of exclusive identifiers specific to the transactions.
- **Approver**—Verified user who is provided access by a sender to approve a document.
- **Other**—Verified user who is 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- and multi-factor authentication.

Typically, a licensed user will log into 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).

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.
- **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.

For more information on enabling single sign-on with SAML in Adobe Sign, please see http://www.adobe.com/go/adobesign_saml_configuration

For more information on Adobe Identity Management Services (IMS), please see <https://www.adobe.com/content/dam/acom/en/security/pdfs/AdobeIdentityServices.pdf>

Location of Identity Data

User identity data is stored within the same data center associated with the customer's geographical location. Typically, Adobe Sign customers use Adobe IMS and the Adobe Admin Console for user management. In this scenario, user identity data is also replicated in highly available Adobe IMS data centers located in US-East (Virginia), US-West (Oregon), EU-West (Ireland), and Singapore.

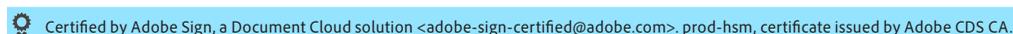
Signer Identification Verification

Basic identity verification 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 verification. First-level verification is often used for signer, approver or other user types. To improve security and help prevent malicious individuals from spoofing the system, multi-factor authentication methods, including telephone, SMS text, knowledge-based authentication (KBA), and Government ID verification, can also be added depending on availability in the customer's geographical location. For more information on the latest signer identity verification methods, please see <https://helpx.adobe.com/sign/using/signer-identity-authentication-methods.html>.

Adobe Sign Document Certification

At each stage in the workflow, Adobe Sign secures the document to help ensure both document integrity and proof of origin. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents and audit trails with a digital signature before distributing to any recipient.

The certification signature is created with the SHA-256 hashing algorithm that calculates a unique cryptographic fingerprint from the final signed PDF. Displayed graphically as the blue banner with a certification badge at the top of the final signed PDF, this digital signature verifies document integrity (see Figure 4 below), provides assurance that the document was generated within Adobe Sign, and 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, if document confidentiality is also needed.

A blue banner with a white certification badge icon on the left. The text reads: "Certified by Adobe Sign, a Document Cloud solution <adobe-sign-certified@adobe.com>. prod-hsm, certificate issued by Adobe CDS CA." data-bbox="177 340 780 356"/>

Certified by Adobe Sign, a Document Cloud solution <adobe-sign-certified@adobe.com>. prod-hsm, certificate issued by Adobe CDS CA.

Figure 4: Adobe Sign Document Certification Banner

To generate the keys used to lock and certify the final signed PDF, Adobe Sign uses certificates issued by multiple trusted certificate authorities (CAs) and timestamp authorities (TSAs). In certain circumstances, Adobe Sign can be configured to apply the certification signature using a specific certificate based on regional or compliance requirements. PKI keys used to certify the final PDF are stored in hardware security modules to meet the highest level of security and compliance.

Adobe Sign Hosting and Security

The Adobe Sign service infrastructure resides in American National Standards Institute (ANSI) Tier 4 data centers managed by our trusted cloud hosting providers, Amazon Web Services (AWS) and Microsoft Azure. Adobe's cloud service infrastructure partners maintain very strict controls around data center access, fault tolerance, environmental controls and network security. Only approved, authorized Adobe employees, cloud service provider employees and contractors with a legitimate, documented business are allowed access to the secured sites. More information about our data centers used for Adobe Sign services can be found on the [Adobe Support website](#).

For more information on Amazon Web Services security, please see <https://aws.amazon.com/security>

For more information on Microsoft Azure security, please see <https://azure.microsoft.com/en-us/services/security-center/>

For more information on Microsoft Azure Government security, please see <https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-plan-security>.

Adobe Sign Network Management

Adobe understands the importance of securing the data collection, data content serving and reporting activities over the Adobe Sign network. To this end, the network architecture is designed with security as a top priority, including segmentation of development and production environments and authenticated RBAC.

Secure Management

All management connections to the servers occur over encrypted channels only accessible from the Adobe corporate network. All access requires two-factor authentication.

Service Monitoring

Adobe monitors all servers, routers, switches, load balancers, and other critical network equipment on the Adobe Sign network 24 hours a day, 7 days a week, 365 days a year (24x7x365). The Adobe Network Operations Center (NOC) receives notifications from the various monitoring systems and will promptly attempt to fix an issue or escalate the issue to the appropriate Adobe personnel. Additionally, Adobe contracts with multiple third parties to perform external monitoring.

Further, Adobe Sign uses state of the art technologies and industry leading providers for application-specific monitoring and alerting. SLIs and SLOs are constantly tracked and violations result in alerts with the right severity.

Data Availability

Adobe Sign data is stored in a combination of databases and cloud storage repositories. Databases are replicated across multiple availability zones, and further backed up periodically. Cloud storage repositories provide their own redundancy mechanisms with very high levels of durability, offering 99.999999999% (11 9's) durability over a year. In addition, for Adobe Sign regions that offer disaster recovery, all data is replicated to a secondary region.

Change Management

Adobe uses a change management tool to schedule modifications, helping increase communication between teams that share resource dependencies and inform relevant parties of pending changes. In addition, Adobe uses the change management tool to schedule maintenance blackouts away from periods of high network traffic.

Patch Management

In order to automate patch distribution to host computers within the Adobe Sign organization, Adobe uses internal patch and package repositories as well as industry-standard patch and configuration management. Depending on the role of the host and the criticality of pending patches, Adobe distributes patches to hosts at deployment and on a regular patch schedule. If required, Adobe releases and deploys emergency patch releases on short notice.

Adobe Sign instances and product updates, including security updates, are applied through the deployment pipeline (see above section on the deployment model for more details).

Access Controls

Only authorized users within the Adobe intranet or remote users who have completed the multi-factor authentication process to create a VPN connection can access administrative tools. In addition, Adobe logs all Adobe Sign production server connections for auditing. For Adobe Sign environments, Adobe makes built-in security features available to implement permissions and access control using groups and privileges.

Adobe administrators do not have access to customer agreements, except under narrow circumstances such as when needed for troubleshooting customer issues. Only administrators whose job function requires such access are assigned a role enabling access, and any access requires approval both from the customer as well as from an administrator with a designated approval role. In addition, this access is subject to 2FA, and is logged.

Logging

In order to help protect against unauthorized access and modification, Adobe captures and manages network logs, OS-related logs, and intrusion detections using a combination of industry-standard and Adobe-proprietary tools. Adobe periodically reviews log storage capacity and expands storage capacity if, and when, required. Adobe hardens all systems that generate logs and restricts access to logs and logging software to authorized Adobe personnel. Adobe retains raw logs for one year and all logs are managed and accessed only by Adobe personnel.

Data Center Physical and Environmental Controls

The below description of data center physical and environmental access controls includes controls that are common to all Adobe data center locations. Some data centers may have additional controls to supplement those described in this document.

Physical Facility Security

Adobe physically secures all hardware in Adobe-owned or -leased hosting facilities against unauthorized access. All facilities that contain production servers for Adobe Sign include dedicated, 24-hour on-site security personnel and require these individuals to have valid credentials to enter the facility. Adobe requires PIN or badge credentials—and, in some cases, both—for authorized access to data centers. Only individuals on the approved access list can enter the facility. Some facilities include the use of man-traps, which prevent unauthorized individuals from tailgating authorized individuals into the facility.

Fire Suppression

All data center facilities must employ an air-sampling, fast-response smoke detector system that alerts facility personnel at the first sign of a fire. In addition, each facility must install a pre-action, dry-pipe sprinkler system with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

Controlled Environment

Every data center facility must include an environmentally controlled environment, including temperature humidity control and fluid detection. Adobe requires a completely redundant heating, ventilation, and air conditioning (HVAC) system and 24x7x365 facility teams to promptly handle environmental issues that might arise. If the environmental parameters move outside those defined by Adobe, environmental monitors alert both Adobe and the facility's Network Operations Center (NOC).

Video Surveillance

All facilities that contain product servers for Adobe Sign must provide video surveillance to monitor entry and exit point access, at a minimum. Adobe asks that data center facilities also monitor physical access to equipment. Adobe may review video logs when issues or concerns arise in order to determine access.

Backup Power

Multiple power feeds from independent power distribution units help to ensure continuous power delivery at every Adobe-owned or Adobe-leased data center facility. Adobe also requires automatic transition from primary to backup power and that this transition occurs without service interruption. Adobe requires each data center facility to provide redundancy at every level, including generators and diesel fuel contracts. Additionally, each facility must conduct regular testing of its generators under load to ensure availability of equipment.

Availability and Notification

Adobe Sign is hosted on Amazon Web Services (AWS) and Microsoft Azure continuously active Availability Zone (AZ) data center configurations. All Adobe Sign data centers are highly resilient, designed to deliver high availability and tolerate system or hardware failures with minimal impact. Each data center runs on its own physically distinct and independent infrastructure to help ensure business continuity in case of an outage. More information about our data center configurations, including our recovery point objective (RPO) and recovery time objective (RTO) commitments, can be found on the [Adobe Support website](#).

Adobe Sign uptime data is available at on the [Adobe Status website](#). 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.

The Adobe Security Organization

As part of Adobe's commitment to the security of its products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe Sign team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

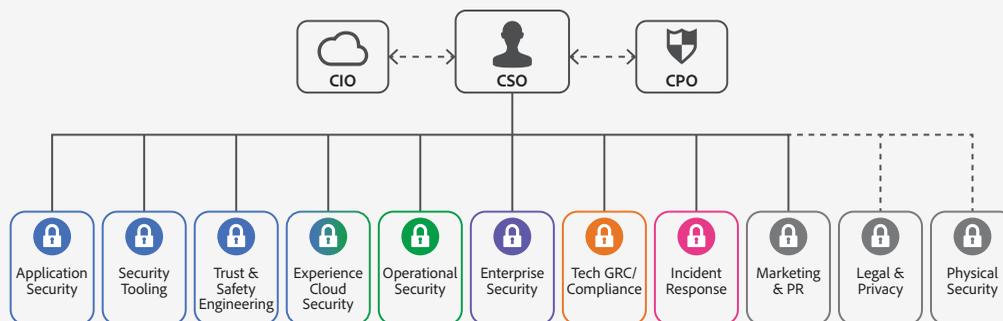


Figure 6: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Sign organization employs the Adobe Software Product Lifecycle (SPLC) process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC activities include, depending on the specific Adobe Sign component, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Sign security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

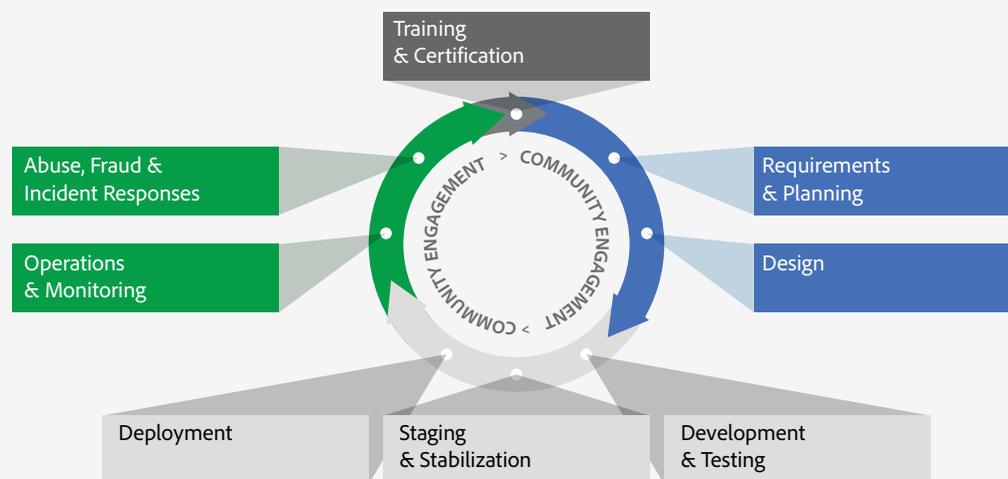


Figure 7: The Adobe Software Product Lifecycle (SPLC)

More information about the Adobe security organization and the SPLC can be found at www.adobe.com/security

Adobe Software Security Certification Program

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

Various teams within the Adobe Sign organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company in general. For more information, please see the [Adobe Security Culture white paper](#).

Adobe Sign 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, such as the General Data Protection Regulation (GDPR) in the EU. For more information on Adobe privacy policies, please see www.adobe.com/privacy

To learn more about e-signature laws in a specific region and the most up-to-date information about Adobe Sign compliance, please see www.adobe.com/trust.html

Adobe Common Controls Framework

Adobe Sign adheres to the Adobe Common Controls Framework (CCF), a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,350 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

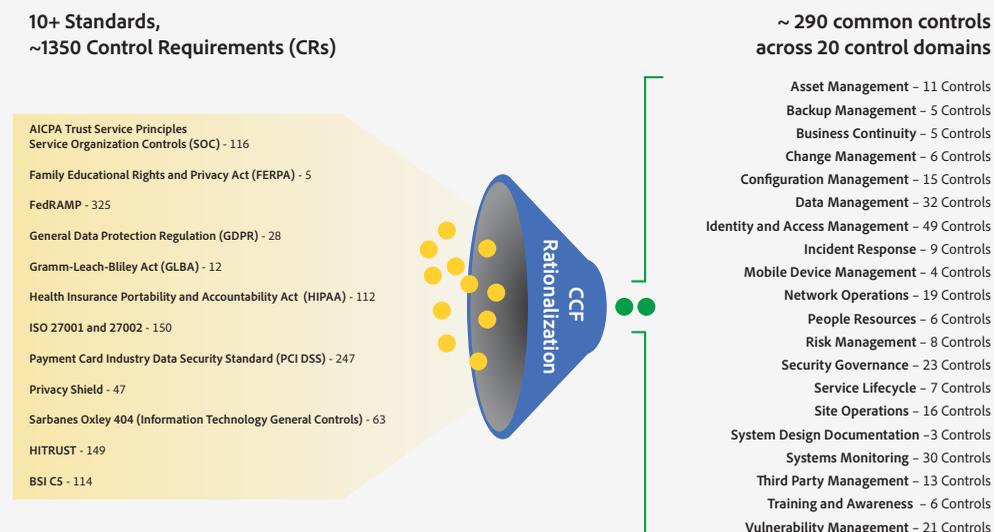


Figure 8: The Adobe Common Controls Framework (CCF)

FedRAMP

The Adobe Sign offer described in this document is currently FedRAMP authorized at the Tailored level. A security-enhanced instance of Adobe Sign is also “In Process” in the FedRAMP Marketplace at the Moderate level. It will be hosted on Microsoft Azure Government Cloud and designated for the sole use of U.S. federal, tribal, state, and local government customers, as well as U.S. government contractors.

Adobe Risk & Vulnerability Management

Adobe strives to ensure that its 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, swiftly resolves incidents when they occur, and feeds this information back to its development teams to help achieve the highest levels of security for all Adobe products and services.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can 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 documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan. Adobe conducts a penetration test annually and before every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

Internally, the Adobe Sign security team performs a risk assessment of all Adobe Sign components annually and prior to every release. The Adobe Sign security team partners with technical operations and development leads to help ensure high-risk vulnerabilities are mitigated prior to each release. For more information on Adobe penetration testing procedures, see the [Adobe Secure Engineering Overview white paper](#).

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

For more details on Adobe's incident response and notification process, please see the [Adobe Incident Response Overview](#).

Forensic Analysis

For incident investigations, the Adobe Sign team adheres to the Adobe forensic analysis process that includes, as appropriate, complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody record. We offer a data retention feature that helps automate deletion of Adobe Sign agreement data at a customer-specified interval after agreement completion. We also provide an administrative interface for customers to manually delete selected data.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Physical Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

All files uploaded to the service offering are scanned for known threats before committing them to the cloud. Any files that fail the scan are discarded and an error is generated. Adobe also scans all inbound and outbound corporate email for known malware threats.

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Adobe Sign, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

Background Checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background, work history, court records, including criminal conviction records and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee Termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can no longer access to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Data Center Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Facility Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Customer Data Confidentiality

Adobe treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the [Adobe Terms of Use](#) and the [Adobe Privacy Policy](#).

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Sign and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security our customers' data.

For more information please visit the [Adobe Trust Center](#).



© 2021 Adobe. All rights reserved.

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries.