Adobe EchoSign security overview

OVERVIEW

Adobe EchoSign is the electronic signature solution you can trust, from the company that brought you Adobe PDF and Adobe Acrobat software. Adobe uses the same technologies and security engineering processes relied on by financial institutions and governments around the world. With Adobe EchoSign, security is considered at every level—from the application code and networks to the physical facilities. Along with the most up-to-date technologies, Adobe EchoSign adheres to the latest best-practice policies for online security. That's why industry leaders including Aetna, BT Group, Dropbox, Google, and Proctor & Gamble choose EchoSign to get documents signed—easily, securely, on any device.

SAFE, PROTECTED CODE

Each release of Adobe EchoSign code, and the infrastructure that supports it, is developed with the Adobe Secure Product Lifecycle (SPLC) framework. The SPLC framework is a rigorous set of best practices, processes, and tools used throughout all phases of product development, resulting in more secure code that safeguards confidential information.

- **Planning**—During the planning phase, engineering teams are required to contact the Adobe Secure Software Engineering Team (ASSET) and complete the privacy and security risk questionnaire. This helps ASSET determine any risks to the product under development.
- **Design**—In the design phase, ASSET recommends privacy and security practices, and creates a test model based on the threat model.
- **Implementation**—During the implementation phase, the ASSET researcher and product engineering team collaborate to help ensure that secure coding guidelines are upheld and unsafe functions are avoided. The product engineering team performs static analysis tests. Code reviewers look for common issues and risks including those defined in the Damage, Reproducibility, Exploitability, Affected users, and Discoverability (DREAD) and Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) risk classification schemes.
- **Testing**—In the testing phase, the test plan developed in the design phase is implemented by a team of QA experts and the ASSET researcher. Bugs are identified, prioritized, and addressed. Finally, a security readiness review is performed to confirm all recommendations made in the threat model have been followed.
- **Shipping**—In the shipping phase, security documentation is finalized and stored on the product's internal wiki application.
- **Response**—During the response phase, external parties can report security vulnerabilities to the Adobe Product Security Incident Response Team (PSIRT). PSIRT coordinates with executives, engineering, and third-party vendors to respond to issues. PSIRT also provides guidance on proper incident response protocols, tracks issues, and identifies areas for improvement.

HARDWARE AND INFRASTRUCTURE

- EchoSign uses state-of-the-art, geo-dispersed data centers to provide data redundancy and availability.
- EchoSign servers are housed in protected Statement on Standards for Attestation Engagements (SSAE) 16 Type II Service Organization Controls 2 (SOC 2) data centers with redundant power and Internet connectivity.
- Physical entry into the facility is controlled by two-factor authentication: 1) a hand geometry scanner and 2) a keycard/badge. All access is monitored by security staff through closed-circuit video surveillance cameras installed at all entrance points.
- External third parties as well as internal resources are used to perform penetration tests and security assessments.
- EchoSign provides 100% transparent uptime data at *trust.echosign.com*. Uptime is continuously monitored by the Internet's leading third-party monitoring service, Pingdom.

SYSTEMS AND OPERATIONS

Adobe EchoSign adheres to security policies that are based on industry best practices and compliant with Health Insurance Portability and Accountability Act (HIPPA) and payment card industry (PCI) methodologies. Infrastructure security is achieved through a multilayered approach, including:

- Protected SSAE 16 Type II SOC 2 certified hosting facility
- Host-based and network firewalls
- A segmented network with servers on private, nonroutable IP spaces
- Real-time logging and monitoring
- Strict firewall policies
- Intrusion detection system

APPLICATIONS AND ACCESS

Audit trail

Adobe EchoSign automatically generates an audit trail that tracks every step in the signature process—from initial document preparation through signing and archiving. This comprehensive audit trail is stored securely and can be used, as needed, to prove who signed a document and when they signed it.

Authentication

All EchoSign web service APIs require the use of an API key, a unique secure identifier that grants a specific user or company access to the API. All document and user keys exist within the namespace of a particular API key. For example, you cannot use one API key to create a document and then use a different API key to retrieve the status of that document.

Access controls

Authorization to access different data sets is based on user roles within the application. User accounts are typically created by account administrators. Users must log in with their email address and password to gain access to the application. All data within EchoSign is access controlled with a role-based model; the user must be a participant in the contract (such as the sender or signer) in order to view or modify it.

Passwords and credentials

Within the application, administrators can configure password strength and complexity, frequency of change, past password comparison, and lockout policies.

Passwords are processed and stored using industry standard best practices. For example, each password key is calculated using thousands of "key stretching" iterations. Adobe EchoSign:

- Provides password expiration for login renewal
- Supports single sign-on (SSO) to a customer's corporate identity system using the industry standard Security Assertion Markup Language (SAML) protocol
- Enables IP address limits to be added to help ensure access is only allowed through the corporate network

Application-level encryption

Adobe EchoSign leverages Secure Sockets Layer (SSL) using 256-bit Advanced Encryption Standard (AES) encryption to safeguard confidential information that is contained in any EchoSign document.

Secure integration with external systems

Adobe EchoSign can be integrated via secure HTTPS Simple Object Access Protocol (SOAP) web services such as Salesforce.com, Microsoft CRM, SugarCRM, and NetSuite.

TRANSMISSION AND STORAGE

Adobe EchoSign relies on SSL AES encryption to safeguard the integrity of documents, both when in motion and when at rest:

- **In motion**—EchoSign leverages SSL using 256-bit AES encryption when accessing the application from the Internet.
- **At rest**—EchoSign leverages Linux Unified Key System (LUKS), using 128-bit AES on Logical Volume Manager (LVM) disk containers throughout the data center.

LEGAL AND COMPLIANCE REQUIREMENTS

For details on how Adobe EchoSign e-signatures meet legislative and compliance requirements, see *Adobe EchoSign legal and compliance FAQ*.

For more information

www.echosign.adobe.com/en/home.html

Adobe

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

These materials are intended to provide general information and are not a substitute for legal advice. Before taking action, you should seek the assistance of an attorney for advice on your use of this service or software. Access to these materials does not create an attorney-client relationship between you and Adobe Systems Incorporated.