Adobe Sign enterprise - una reseña

Seguridad, observancia, manejo de identidad y manejo de documentos.

Tabla de Contenidos

1: Resumen Ejecutivo
2: Arquitectura
4: Seguridad
6: Observancia
7: Integración
7: Infraestructura
7: Más Información

Resumen Ejecutivo

Adobe Sign puede ayudar a su organización a reemplazar los procesos de papel y tinta con flujos de trabajo 100% digitales. Con esta solución de Adobe Document Cloud, puede de forma sencilla enviar, firmar, dar seguimiento y administrar procesos de firma y firmar digitalmente documentos desde cualquier dispositivo en cualquier lugar. Adobe Sign cumple o puede ser configurado para cumplir con las normas reguladoras de muchas industrias. Al ser un servicio robusto basado en la nube, Adobe Sign de forma segura maneja grandes volúmenes de procesos de firma electrónica incluyendo:

- Manejo de identidades de usuarios con autenticación basada en capacidades.
- Certificación de la integridad de un documento.
- Validación de Firmas Electrónicas.
- Mantenimiento de rastros para auditoría.
- Integración con sus sistemas de negocio y aplicaciones empresariales.

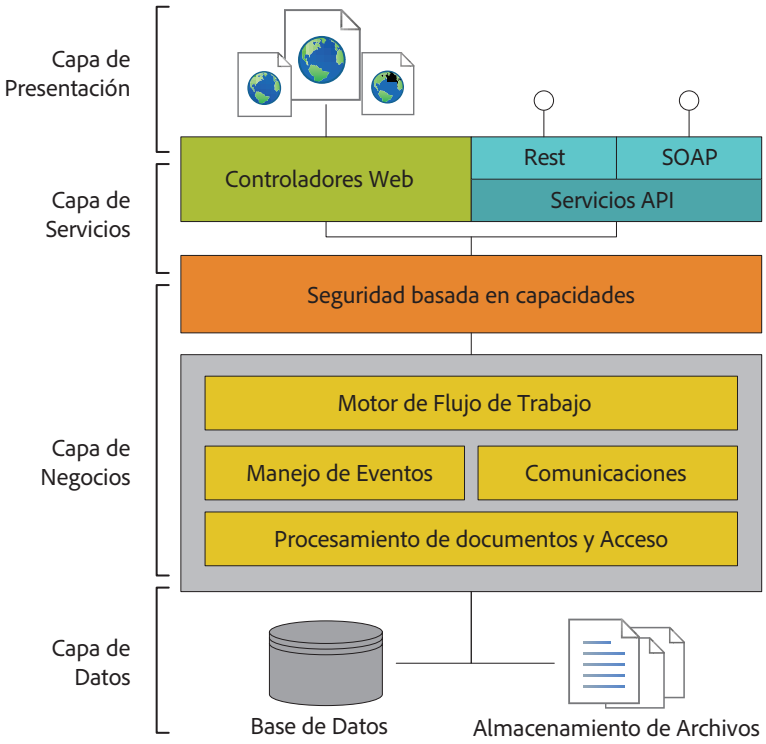
Adobe Sign soporta tanto las firmas electrónicas (e-signatures) y firmas digitales. Una firma electrónica es legalmente vinculante para indicar el consentimiento o aprobación en documentos digitales y formas. Las firmas electrónicas son válidas legalmente y exigibles en muchos países del mundo. Una firma digital es una implementación especial que incorpora un certificado digital verificado en cada firma electrónica. Para organizaciones que requieren este nivel de autenticación, Adobe Sign puede ser utilizado con Adobe Acrobat DC o Adobe Acrobat Reader DC para incorporar firmas digitales certificadas en los documentos firmados de forma electrónica.

La legislación sobre firmas electrónicas difiere en cada país. En los Estados Unidos, el *Electronic Signatures in Global and National Commerce Act (ESIGN)* es una Ley Federal que facilita el uso de registros electrónicos y formas electrónicas en transacciones comerciales locales e internacionales acordadas de forma electrónica. Adicionalmente, desde Julio del 2016, en la Unión Europea, el *Electronic Identification and Authentication Services (eIDAS)* establece un marco legal consistente para el reconocimiento de firmas electrónicas, sellos y documentos dentro de los 28 países miembros de la U.E. Cuando se utiliza de acuerdo con la legislación aplicable, Adobe Sign cumple tanto con el ESIGN de los Estados Unidos, así como el eIDAS de la Unión Europea. Esto permite también la observancia de otras leyes y regulaciones en otros países como el *Australian Electronic Transactions Act (ETA)* y el *Canadian Uniform Electronic Commerce Act (UECA).*

Este documento ofrece una reseña de alto nivel de la arquitectura, seguridad, observancia legal, manejo de identidades, manejo de documentos y otros puntos técnicos de importancia. Para más información en el uso de firmas electrónicas, por favor vea el documento: Transform business processes with electronic and digital signature solutions from Adobe

Arquitectura

La arquitectura de Adobe Sign está diseñada para ser escalable y manejar un gran volumen de transacciones sin degradación en el rendimiento. Para ofrecer un alto nivel de disponibilidad y escalabilidad, todos los datos transaccionales de Adobe Sign se almacenan en diversos clusters redundantes de bases de datos con recuperación automática*. El siguiente diagrama arquitectónico muestra la división lógica de los componentes y funcionalidad de Adobe Sign.



Arquitectura Lógica de Alto Nivel de Adobe Sign

Cada capa lógica en la aplicación de Adobe Sign esta monitoreada por una suite de herramientas que mantiene un registro de los indicadores principales, como el tiempo para convertir documentos en PDF's o el uso de recursos. El panel de monitoreo permite a los Ingenieros de Operaciones de Adobe Sign ver fácilmente la salid del servicio. Las alertas en tiempo real alertan a los Ingenieros si ocurre algún incidente o si ocurre un proceso fuera de lugar. Si la situación no puede ser remediada, Adobe Sign mantiene registros de diagnóstico y forenses para que los Ingenieros puedan resolver el problema rápidamente y atiendan el problema de raíz para evitar que vuelva a ocurrir.

Capa de Presentación

La capa de presentación maneja la interfase de usuario web (UI) así como la generación y muestra de documentos para firma, archivos PDF finales certificados y componentes del flujo de trabajo.

Capa de Servicios

La capa de servicios maneja las funciones necesarias para los servicios del cliente y servicios web, interfases API, como el Gateway REST y el API SOAP. Los servidores web exteriores manejan las solicitudes de navegadores y API y los servidores de correo manejan el tráfico de comunicaciones interno y externo. Los servidores web distribuyen las solicitudes dinámicas complejas a los servidores de aplicación de Adobe Sign en la capa de negocio, a través de balanceadores de carga en hardware. Los servidores de la capa de servicios también incorporan reglas de filtrado de seguridad para prevenir ataques comunes y protección de firewall para fortalecer el control de acceso.

* La recuperación automática está limitada a la Infraestructura de Amazon Web Services.

Capa de Negocios

La capa de negocios de Adobe Sign maneja el flujo de trabajo, la seguridad basada en capacidades, conversión de documentos y servicios de imagen, manejo de eventos, registro y monitoreo, acceso de archivos y manipulación y funciones de comunicación.

Motor del Flujo de Trabajo

El motor del flujo de trabajo de Adobe Sign ejecuta y maneja todos los procesos de negocio y pasos que requiere un documento a través del proceso de firma. El motor de flujo de trabajo utiliza un lenguaje declarativo basado en XML para describir las pre-condiciones para ejecutar flujos de trabajo específicos del cliente y la secuencia de eventos requerida para completar un proceso de firma o de aprobación.

Seguridad basada en capacidades

La seguridad basada en capacidades de Adobe Sign define, controla y audita los recursos disponible y las operaciones permitidas para un usuario autenticado o aplicación. Los recursos incluyen cualquier información en forma de documentos, datos, metadata, información de usuario, reportes y API´s.

Manejo de Eventos

El manejo de eventos de Adobe Sign guarda y conserva un trazo de auditoría relacionada con cada usuario y documento en cada paso del flujo de trabajo. Al momento que ocurre cada paso del flujo de trabajo, Adobe Sign genera un evento y distribuye mensajes a través de un sistema asíncrono de mensajería a los recursos apropiados del sistema.

Comunicaciones

Adobe Sign utiliza el correo electrónico para notificaciones de eventos de firma y la entrega opcional de los documentos firmados y certificados al final del proceso. Para minimizar el spam y el phishing, Adobe Sign permite el correo autenticado con *Domain Keys Identified Mail* (DKIM), Autenticación vía mensaje basado en domino, Reporte y Conformación (DMARC) y *Sender Policy Framework* (SPF).

Procesamiento de documentos y acceso

Para aumentar el rendimiento, el motor de procesamiento de documentos de Adobe Sign proporciona funcionalidad libre de estado para convertir distintos formatos de archivo a PDF, encriptando y desencriptando archivos y rasterizando imágenes para ser vistas en un navegador web. Para las acciones de procesamiento de documentos, Adobe Sign confía en un sistema de mensajería asíncrono basado en colas para comunicarse entre los recursos del sistema. Adicionalmente todo el procesamiento de documentos acceso a el *Network Attached Storage* (NAS) sucede en segundo plano, permitiendo que el procesamiento de Adobe Sign parezca instantáneo para los usuarios en cada paso del flujo de trabajo.

Capa de Datos

La capa de datos es responsable del acceso a la base de datos transaccional, la base de datos del sistema asíncrono de mensajería y el almacén de documentos. Los datos transaccionales almacenados en la capa de datos incluye el documento original del cliente, versiones intermedias de documentos generados durante el proceso de firma, metadata de documentos, usuarios, eventos y el PDF final firmado procesado por Adobe Sign.

Seguridad

En Adobe las prácticas de seguridad están incrustadas en nuestra cultura, desarrollo de software, así como los procesos de operación de servicio. Adobe Sign utiliza prácticas de seguridad estándar en la Industria - para manejo de identidad, confidencialidad de datos e integridad de documentos - para ayudar a proteger sus documentos, datos e información personal.
Para información adicional sobre los procesos de seguridad de Adobe, interacción con la comunidad y el ciclo de vida de Producto Seguro de Adobe, visite *www.adobe.com/security*

Manejo de Identidad

Adobe Sign utiliza un modelo basado en roles para el manejo de identidades que se encarga de la autenticación, autorización y control de acceso en el sistema de Adobe Sign. La seguridad basada en capacidades y los procesos de autenticación están definidos y habilitados para una organización por un administrador de Adobe Sign. Adobe Sign define roles generales de usuario para:

- **Remitente -** Usuario licenciado que tiene permisos específicos en Adobe Sign otorgados por el administrador para crear flujos de trabajo y enviar documentos para firma, aprobación o consulta.
- **Destinatario -** Usuario verificado a quien se da acceso por el remitente para firmar un documento específico. Por defecto, Adobe Sign envía un correo al destinatario que incluye una dirección para firmar el documento que contiene identificadores específicos de cada transacción.
- **Autorizador -** Usuario verificado a quien se da acceso por el remitente para aprobar un documento.
- **Otro -** Usuario verificado a quien se da acceso por el remitente para ver un documento o auditarlo.

Autenticación de Usuario

Adobe Sign soporta múltiples métodos para autentificar la identidad del usuario, incluyendo autenticación de un solo paso y de pasos múltiples con opciones adicionales para verificar la identidad del usuario. Típicamente, un usuario licenciado ingresa a Adobe Sign usando un correo electrónico verificado y contraseña que mapea a una identidad autenticada como un Adobe ID. Los administradores pueden configurar los requisitos de la contraseña y su complejidad, frecuencia de cambio, comparación con contraseñas anteriores y políticas de bloqueo (como expiración de renovación de login).

La autenticación básica en Adobe Sign se logra enviando una solicitud por correo a una persona específica. Como la mayoría de los usuarios tienen acceso único a una cuenta de correo, esto se considera el primer nivel de autenticación. El primer nivel de autenticación se usa para prevenir que individuos mal intencionados hagan spoofing con el sistema, los métodos multifactor como teléfono, mensajes de texto o autenticación basada en conocimiento pueden ser agregados dependiendo de la disponibilidad en su ubicación geográfica.

Adobe Sign soporta los siguientes tipos de autenticación:

- **Adobe Sign ID -** Una dirección de correo verificada y una contraseña que combinadas se utilizan por un usuario para ingresar de forma segura a una cuenta de Adobe Sign.
- **Adobe ID -** Puede utilizarse un Adobe ID para ingresar a los servicios licenciados de Adobe incluyendo Adobe Sign. Adobe monitorea de forma constante todas las ID de Adobe para detectar actividad anormal para poder mitigar de forma rápida amenazas potenciales de seguridad.
- **Google ID -** Identificación de usuario autenticada por Google, como Google Mail o Google Apps.
- **Single sign-on (SSO) -** Las empresas que requieren un control de acceso más robusto pueden habilitar el lenguaje Security Assertion Markup (SAML) SSo para administrar a los usuarios de Adobe Sign a través de su sistema corporativo de identidad. Adobe Sign también puede ser configurado para reconocer e integrar con los proveedores más importantes de administración de identidad, incluyendo a Okta y OneLogin.

Certificación de Documentos

En cada paso en el flujo de trabajo, Adobe Sign mantiene un checksum seguro del documento para asegurar la integridad y confidencialidad del documento. Adobe Sign utiliza la infraestructura de llave pública (PKI) para certificar los archivos finales firmados con una firma digital antes de distribuirlos a los participantes.

La firma digital se crea con un algoritmo hashing que toma información específica del archivo PDF firmado para mostrar una línea de tamaño fijo codificada en hex de forma criptográfica con números y letras.

Esto se muestra como la barra azul y la certificación en el encabezado del documento PDF final firmado, la firma digital verifica la integridad del documento (ver la siguiente imagen) y ofrece la certeza de que el documento no ha sido alterado desde que el certificado fue aplicado. El PDF final certificado puede ser asegurado con una contraseña adicional en caso de ser necesario.

Versión de Acrobat DC - Distintivo Negro.

Versión de Acrobat X y XI - Distintivo Azul (versiones 10 y 11)

Distintivos de certificación de Adobe Sign

Para generar las llaves utilizadas para bloquear y certificar el documento final en PDF, Adobe Sign utiliza certificados específicos emitidos por autoridades de certificación (CAs) y Autoridades de Timestamp (TSAs). En algunos casos, Adobe Sign puede ser configurado para generar documentos certificados utilizando CAs requeridos por el gobierno, como en Suiza y la India. Las llaves PKI utilizadas para certificar los PDF finales están almacenadas en un módulo de seguridad en hardware para prevenir ataques en línea y modificaciones.

Encriptación

Adobe Sign encripta los documentos y activos en reposo usando encriptación AES 256-bit y soporta HTTPS TLS v1.0 (o mayor) para ayudar a asegurar que los datos en tránsito también se encuentran protegidos. Los documentos en reposo sólo pueden ser accesados con permisos establecidos en la seguridad basada en capacidades a través de la capa de acceso de datos. Todas las llaves de encriptación de los documentos se encuentran almacenadas en un entorno seguro con acceso restringido y son rotadas como sea necesario. Adicionalmente, los remitentes tienen la opción de asegurar un documento con una contraseña privada adicional.

Configuración de niveles de encriptación de PDF en el panel de control de Adobe Sign.

Observancia

Como una solución de firma electrónica global diseñada para que los destinatarios verificados interactúen con documentos en cualquier lugar y dispositivo, Adobe Sign cumple o puede ser configurado para observar los requisitos regulatorios de muchas industrias. Los clientes mantienen control sobre sus documentos, datos y flujos de trabajo y pueden escoger como dar cumplimiento a las regulaciones locales o nacionales. Para saber más acerca de la legislación aplicable en una región específica por favor consulte: *Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability*

ISO 27001

El standard ISO 27001 fue publicado por la *International Organization for Standardization* (ISO) y la International Electrotechnical Commission (IEC). Esta contiene los requerimientos para sistemas de administración de seguridad de la información (ISMS) que pueden ser auditados para una autoridad certificadora independiente y acreditada.
Adobe Sign está certificado en ISO 27001:2013

SSAE 16 SOC 2

El *Statement on Standards for Attestation Engagements* (SSAE) No. 16 para *Service Organization Controls* (SOC) son controles de TI para seguridad, disponibilidad, integridad de proceso y confidencialidad (Tipo 2). SSAE 16 SOC 2 esta diseñado para ayudar a cumplir con la ley *Sarbanes-Oxley Act* (SOX). Adobe Sign tiene una certificación SOC 2 Type 2 (seguridad y disponibilidad).

PCI DSS

El *Payment Card Industry Data Security Standard* (PCI DSS) es un standard propietario de seguridad de datos para empresas que manejan tarjetas de crédito de los esquemas principales para incrementar el control sobre los datos del tarjetahabiente y reducir fraudes. Adobe Sign está calificado como observante del PCI DSS 3.0 como proveedor de servicios mercantiles.

HIPAA †

El *Health Insurance Portability and Accountability Act* (HIPAA) ayuda a asegurar que la información sensible de los pacientes esté protegida al establecer estándares para transacciones de salud. Adobe Sign puede ser configurado para ser utilizado de forma que cumpla con las normas HIPAA por cualquier organización que lo requiera de acuerdo con el *Department of Health and Human Services* (HHS), y que firme un acuerdo de asociado de negocios con Adobe.

21 CFR Part 11 †

El *Code of Federal Regulations, Title 21, Part 11: Electronic Records; Electronic Signatures* (21 CFR Part 11) establece las regulaciones que la *U.S. Food and Drug Administration* (FDA) establece para registros y firmas electrónicas. Adobe Sign puede ser configurado para que las organizaciones cumplan con lo establecido en 21 CFR Part 11.

GLBA †

El U*.S. Gramm-Leach-Bliley Act* (GLBA) ofrece regulaciones para instituciones financieras para garantizar la información personal de los clientes. Adobe Sign puede ser configurado para que las entidades financieras observen los requerimientos de GLBA.

FERPA †

El *U.S. Family Educational Rights and Privacy Act* (FERPA) está diseñado para preservar la confidencialidad de la los registros de estudiantes en los E.U. y su información. Adobe Sign puede configurarse para manejar datos regulados de estudiantes de forma que observen los requerimientos de FERPA.

† Los clientes son los responsables de asegurarse que Adobe Sign esté configurado y asegurado de forma que permita a la organización cumplir con las obligaciones legales específicas como HIPAA, FERPA, GLBA y 21 CFR Part 11.

Integración

Adobe Sign cuenta con integraciones llave en mano para múltiples aplicaciones de negocio y empresariales, incluyendo a Salesforce, Apttus, Workday, Ariba y productos Microsoft. Adicionalmente Adobe Sign cuenta con una gama amplia de APIs que permiten la integración con sistemas de negocio propietarios o páginas web vía HTTPS seguro o servicios SOAP o REST. Para ver la lista de integraciones soportadas por Adobe Sign visite: *Página de Integraciones*

Infraestructura

La infraestructura de Adobe Sign reside en data centers de primer nivel operados por nuestros proveedores de servicios de nube Rackspace y Amazon Web Services. Sólo trabajadores autorizados y aprobados por Adobe, empleados y contratistas con una función legítima tienen acceso a los sitios seguros tanto en Norte América como en la Unión Europea.

Para más información

Detalles de la Solución: *www.adobe.com/go/adobesign*

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

Ayuda Adobe Enterprise / Configuración de Single Sign-On: *helpx.adobe.com/enterprise/help/configure-sso.html*

Adobe

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

4/16