



PSC Advantage

DocuSign®

PSC Advantage
Version 2.0

Advantage Security S de RL de CV
Av Prolongación Paseo de la Reforma 625
Paseo de las Lomas, Santa Fe
CP 01330
Tel. 01 52 55 50 81 43 60

Tabla de contenido

DOCUSIGN®.....	4
DESCRIPCION.....	4
CARACTERÍSTICAS FUNCIONALES	4
Ambiente de Trabajo	6
Integración con varios lenguajes de programación.....	6
Permite Obtener	7
Realiza la autenticación	7
Estándares que Soporta.....	7
Incluye la capacitación sobre el uso de DocuSign®	7
OPERACIONES DISPONIBLES	8
Generación de Firma Electrónica.	8
Verificación de firma electrónica.	8
Solicitud de sellos de tiempo.....	8
Certificación de sellos de tiempo y constancia NOM151.	8
Generación de firma electrónica PCKS7.	8
Autenticación de firma electrónica PCKS7.	8
Firmado y encriptado (Ensobretado).	8
Autenticación ensobretado.....	8
Servicios de Autenticación.	8
Consulta de estado de revocación de certificados digitales.	9
Distribución	9
Consola Gráfica	9
Operación del Servicio por TCP.....	9
Operación con múltiples Autoridades Certificadoras	9
Bases de Datos que Soporta	9
Resguardo de Firmas Electrónicas - Archiving	9

ARQUITECTURA OPERACIÓN CENTRALIZADA.....	10
Interfaces de Desarrollo	10
Modulo de Administración	10
ARQUITECTURA	11
COMPONENTES CLIENTE	11
ActiveX	12
Java Applet	13

DOCUSIGN®

DESCRIPCION

DocuSign® es una solución diseñada para trabajar desde equipos de escritorio, portátiles y web para generar firmas electrónicas avanzadas, así como el cifrado de cualquier tipo de documento o mensaje de datos, de forma ágil y segura para los usuarios.

Puede ser integrado a aplicaciones de negocio donde se desea crear un entorno confiable de intercambio de información para establecer relaciones de negocio entre usuarios y aplicaciones al interior o exterior de una institución.

Su esquema de operación está basado en peticiones que las aplicaciones de negocio ejecutan a través de Servicios Web y XML, lo cual permite la interoperabilidad con infraestructuras tecnológicas soportadas bajo diversas plataformas.

CARACTERÍSTICAS FUNCIONALES

Compatible con estándares abiertos de firmas electrónicas

DocuSign genera firmas electrónicas con el estándar abierto PKCS#7 definido en el RFC 2315 y el Cryptographic Message Syntax (CMS) definido en el RFC 3369.

Cuenta con un módulo generador de firma electrónica, que le permiten al cliente la generación del firmado electrónico en transacciones y si requiriera, también cifrar la transacción.

Múltiples Firmantes

Un mismo documento puede ser firmado por varios firmantes (firma unilateral y multilateral de cadena de datos y archivos también).

Altamente Escalable

Proporciona escalabilidad en la infraestructura en cuanto a la capacidad de atención de múltiples transacciones simultáneas

Firma Formularios Web

La API de DocuSign puede integrarse en formularios web, para garantizar la integridad, confidencialidad y no repudio de sus transacciones.

Verificación de firmas electrónicas

Verifica la firma electrónica, utilizando algoritmos de estándares abiertos y de forma implícita valida la integridad de la información.

Verificación de estatus de certificado digital

Revisa el estatus del certificado que corresponde a la llave privada que firma un archivo, esta revisión la realiza a través de Listas de Revocación de Certificados CRL's o con el protocolo OCSP, permitiendo con ello identificar certificados válidos, caducados y revocados.

Adicional soporta un respondedor de confianza para OCSP

Repositorios Criptográficos

Soporta múltiples repositorios criptográficos de certificados digitales, como tokens, tarjetas inteligentes, CAPI de Windows a través de interfaces PKCS#11, también incluye su propio keystore nativo.

Cifrado

También se puede cifrar datos (entre ellos, cadena de caracteres) y archivos con AES, 3DES, DES

Utiliza llaves públicas RSA y DSA para el cifrado

Descifra con llave privada RSA PKCS#8

Asegura un archivo para múltiples ensobretadores, procesando previamente la firma

Obtiene un arreglo de estructuras con información de los ensobretadores, procesando previamente la firma.

Construye compendio PKCS#7

Con el campo de información integrada en un bloque de memoria.

Simple sin el campo de información en un bloque de memoria.

Con el campo de información y es almacenado en un archivo.

Decodifica compendio PKCS#7

En memoria y retorna los parámetros de información localizados como referencias.

Crea un nuevo archivo con el campo de datos y retorna los parámetros de información como referencias.

Opera es equipos con Sistema Operativo Windows Server 2003 o superior, así como cualquier variante de Linux/Unix

Integración para la solicitud de Estampillas de Tiempo

Permite solicitar Estampillas de Tiempo a una TSA conforme al RFC 3161

Permite la Integración para la solicitud de Constancias para la NOM151

Permite solicitar y almacenar Constancias NOM151 para la conservación de mensajes de datos.

PSC Advantage es un Prestador de Servicios de Certificación, título brindado por la Secretaría de Economía, para brindar este servicio.
<http://www.firmadigital.gob.mx/tabla.html>

Ambiente de Trabajo

DocuSign trabaja en ambientes Java, .NET y C++

Integración con varios lenguajes de programación

- Java

- C, C++, C#, Visual Basic
- Plataforma .NET

Permite Obtener

El contexto de la llave pública RSA o DSA del certificado para realizar operaciones criptográficas.

La digestión de un arreglo de bytes aplicando algoritmos MD5, SHA-1 SHA-2

La digestión de un archivo aplicando algoritmos MD5, SHA-1, SHA-2 La firma RSA digital con digestión md5 y sha1 de un arreglo de bytes.

La firma RSA digital con digestión md5 y sha1 de un archivo.

Arreglo de estructuras con información de los ensobretadores localizados en el documento asegurado.

Realiza la autenticación

De una firma digital contra un arreglo de bytes y el documento original.

De una firma digital contra un archivo como documento original

De un archivo utilizando la llave descifrada generada

Estándares que Soporta

- | | |
|--------------------|--|
| • CMS | • PKCS#10 |
| • RSA | • PKCS#12 |
| • SHA1 | • OCSP (On Line Certificate Status RFC 2560) |
| • SHA2 | • CRL (Certificate Revocation List RFC 3280) |
| • XML Signature | • TSP (Time Stamping Protocol RFC 3161) |
| • MD5 | |
| • X.509 - RFC 5280 | |
| • PKCS#1 | |
| • PKCS#5 | |
| • PKCS#7 | |

Incluye la capacitación sobre el uso de DocuSign®

A la entrega de la licencia de DocuSign® se capacita a la gente de desarrollo que el cliente indique, entregándoles la documentación sobre la misma.

OPERACIONES DISPONIBLES

Generación de Firma Electrónica.

Mediante esta opción es posible generar una firma electrónica para cualquier cadena o archivo que la aplicación de negocios proporcione. A través de esta firma es posible garantizar la integridad y autoría de mensajes de datos procesados por los sistemas

Verificación de firma electrónica.

Mediante esta opción se verifica la validez de una firma electrónica contra los mensajes de datos originales a partir de los cuales se obtuvo.

Solicitud de sellos de tiempo.

Esta opción permite obtener una estampilla de tiempo, de acuerdo al estándar RFC 3161, a partir de un documento electrónico la cual es solicitada a una Autoridad Emisora de Estampillas de Tiempo (TSA) confiable como DocuSign TSA

Certificación de sellos de tiempo y constancia NOM151.

Esta opción permite autenticar documentos electrónicos a través de un sello de tiempo conforme al estándar RFC 3161.

Generación de firma electrónica PCKS7.

Esta opción genera una firma electrónica utilizando el estándar PKCS7, con cual se incluye la información del firmante.

Autenticación de firma electrónica PCKS7.

Esta opción lleva a cabo la validación de una firma electrónica generada con el estándar PKCS7.

Firmado y encriptado (Ensobretado).

Con esta opción los mensajes de datos son cifrados con base al estándar PKCS7 de tal forma que se asegura la confidencialidad de la información.

Autenticación ensobretado.

Con esta opción la información cifrada es validada y recuperada para destinatarios autorizados.

Servicios de Autenticación.

Soporta el uso de varios servicios de Autenticación de Firmas en el mismo equipo, cada servicio puede administrarse de manera independiente.

Consulta de estado de revocación de certificados digitales.

En esta opción se consulta el estado que guardan los certificados digitales con respecto a su validez haciendo consultas hacia las Entidades Emisoras de Certificados Digitales empleando el protocolo OCSP.

Distribución

Puede ser instalado, operado y administrado en sistemas distribuidos como Clústeres y Granjas lo cual garantiza la disponibilidad del servicio y/o el balanceo de cargas

Consola Gráfica

Cuenta con una consola gráfica de configuración para facilitar al administrador su operación.

Operación del Servicio por TCP

Permite establecer el puerto TCP de operación del servicio, para comunicación de aplicaciones de acuerdo a las definiciones del cliente.

Operación con múltiples Autoridades Certificadoras

Permite la operación con múltiples Autoridades Certificadoras, el cliente puede determinar a qué Autoridad o Autoridades reconoce como Confiable(S).

Bases de Datos que Soporta

Microsoft SQL, Oracle, MySQL,

Resguardo de Firmas Electrónicas - Archiving

Permite el almacenamiento seguro de evidencias a través del tiempo, lo cual permite refrendar la firma electrónica avanzada, evitando con ello, la obsolescencia de los algoritmos empleados, cumpliendo estándares internacionales.

ARQUITECTURA OPERACIÓN CENTRALIZADA

Almacena las llaves privadas en una base de datos segura o en dispositivos criptográficos de seguridad a nivel de hardware (HSM) ejecutando operaciones basadas en firma electrónica avanzada a partir de peticiones recibidas desde otras aplicaciones.

Los servicios de DocuSign® se pueden

- Invocar de diferentes formas:
 - Como servicios web (SOAP)
 - DocuSign API/OCX/Applet/ActiveX

Interfaces de Desarrollo

DocuSign cuenta con herramientas y servicios que permitan al cliente su integración a aplicaciones propietarias o de terceros, soporta su operación en Sistemas Operativos tanto Windows como UNIX y LINUX.

Las API's DocuSign están basadas en lenguajes de programación "C", "Java", "C#" y Visual Basic.

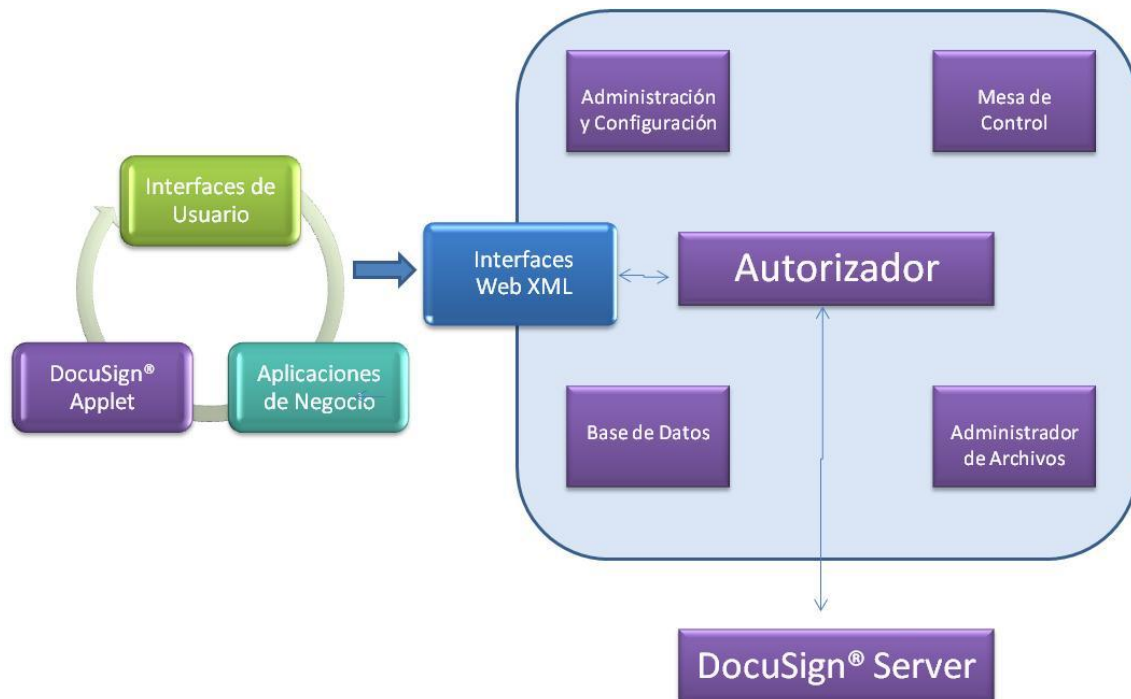
La funcionalidad que proporcionan son:

- Autenticación de Transacciones Firmadas y/o Cifradas.
- Obtención del documento o transacción original.
- Obtención del documento o transacción firmada en formato PKCS#7.
- Solicitud de evidencias relacionadas a una transacción de firma.
- Gestión de procesos de firma multilateral basados en CMS y firmas XML

Modulo de Administración

- Módulo a través del cual se hace la administración de las transacciones.
- Permite la consulta y extracción de información.
- Permite la generación de reportes de acuerdo a las transacciones procesadas.
- Registra y mantiene bitácoras que permitan el monitoreo de los servicios mediante logs o transacciones de error registradas en base de datos.

ARQUITECTURA



COMPONENTES CLIENTE

DocuSign® API/OCX/Applet/ActiveX

Soluciones desarrolladas para que cualquier aplicación pueda solicitar a un usuario que desde un equipo con sistemas operativos Windows/Linux/Unix capaces de ejecutar el entorno de ejecución de JAVA (JRE 1.5 o superior), para que pueda aplicar firma electrónica a documentos, sin comprometer con ello, las llaves del usuario.

Las funciones de firma electrónica se realizan utilizando certificados digitales contenidos en almacenes de certificados de Windows, /Linux/Unix archivos PKCS#12 y archivos con llave privada en formato PKCS#8, PKCS#5 a través de por proveedores criptográficos (CSP Cryptographic Service Providers) DocuSign® API/Applet/OCX/Activex puede interactuar con tarjetas inteligentes o tokens USB. Generación de firmas digitales con base a especificación PKCS#1 y PKCS#7

- Integración de funciones de digestión con algoritmos MD5, SHA-1, SHA-2
- Integración de funciones para autenticación de firmas digitales.
- Validación de certificados digitales X.509
- Decodificación de atributos y extensiones de certificados digitales X.509
- Integración de funciones para validación de estados de certificados digitales con base al protocolo OCSP RFC 2560 y listas de certificados revocados (CRLs)
- Integración de funciones para la solicitud de sellos de tiempo con base al RFC 3161
- Integración de funciones para solicitud de constancias de conservación de mensajes de datos con base a la NOM-151.

ActiveX

Soporta su operación con Sistema Operativo Windows XP o superior

Soporta su operación con Navegadores Web:

- Internet Explorer 5 o superior 32 y 64 bits
- Netscape Navigator 7.1 o superior (Active X enabled)
- Mozilla FireFox 1.4 y 1.5

Brinda servicios criptográficos mediante alguna de las siguientes tecnologías:

- MS CAPI.

Librerías propietarias de encriptación y servicios criptográficos.

- Cryptographic Service Providers.
- Smart Cards y/o Tokens Criptográficos

Soporta sus diferentes operaciones con los siguientes estándares o algoritmos criptográficos.

X.509 (RFC 3280)	PKCS#5	PKCS#12
PKCS#1 (RSA)	PKCS#7	SHA1

Java Applet

Soporta su operación con Sistema Operativo:

Windows XP o superior

UNIX (Mac, Solaris, Red Hat)

Soporta su operación con Navegadores Web:

- Internet Explorer 5 o superior 32 y 64 bits
- Netscape Navigator 4 o superior
- Mozilla FireFox 1.4 o superior
- Chrome
- Safari

Soporta operaciones de:

- Firmado y/o cifrado de cadenas de texto.
- Firmado y/o cifrado de cualquier tipo de archivos

Soporta en sus diferentes operaciones al menos los siguientes estándares o algoritmos criptográficos.

- X.509 (RFC 3280)
- PKCS#1 (RSA)
- PKCS#5
- PKCS#7
- PKCS#11
- PKCS#12
- SHA1
CMS
- SHA 2
- MD5

