DOCUSIGN® SERVER

Version 2.0

Cuando en una organización los aplicativos a nivel centralizado requieren ejecutar procesos de emisión de firmas electrónicas, autenticación de mensajes, autenticación de estados de certificados digitales y de sellos de tiempo **DocuSign® Server** es la solución para integrar mecanismos de seguridad basados en tecnología de firma electrónica avanzada para aplicaciones gubernamentales, financieras y de comercio electrónico.

DocuSign® Server, 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.

Prolongación Paseo de la Reforma 625
Torre Lexus, Despacho 402
Col. Lomas de Santa Fé
CP 01330

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.
- ☑ **Verificación 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.
- ☑ **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.

CARACTERÍSTICAS

- ☑ **Interoperabilidad**
  DocuSign® Server cumple con los estándares tecnológicos que garantizan la interoperabilidad. Esta característica asegura la integración con cualquier aplicación existente.
- ☑ **Escabilidad**
  Su arquitectura modular asegura la estabilidad de la solución para presentes y futuros requerimientos.
- ☑ **Flexibilidad**
  DocuSign® Server está diseñado para ser integrado fácilmente a cualquier aplicación en la que se requiera integrar firma electrónica avanzada sin que tenga que hacer grandes esfuerzos de programación.
- ☑ **Integración de dispositivos de seguridad de hardware.**
  Para mejorar el desempeño y los niveles de seguridad en el ambiente de integración, DocuSign® Server proporciona soporte para dispositivos de seguridad de hardware.

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.

ESPECIFICACIONES TÉCNICAS

Algunos Algoritmos y Estándares Soportados

- ☑ Llaves públicas y privadas RSA a 1024/2048/4096 bits
- ☑ Certificados Digitales X509v3
- ☑ PKCS#7
- ☑ Algoritmos de Digestión MD5, SHA-1 y SHA-2
- ☑ Protocolo para consulta de estado de revocación de certificados digitales (OCSP-RFC3280).
- ☑ Estampillas de Tiempo (TSP-RFC3161).

Administración

- ☑ Las llaves se almacenan en una base de datos segura y opcionalmente pueden estar resguardas en dispositivos criptográficos de hardware (HSM).
- ☑ Todas las operaciones procesadas son registradas en una base de datos.
- ☑ El acceso a las operaciones está restringido a usuarios autorizados.

Algunos de los Dispositivos Criptográficos Soportados

- ☑ SafeNet Luna PCI 3000/7000
- ☑ SafeNet LunaSA
- ☑ SafeNet CA3/CA4

BENEFICIOS

Integración estratégica orientada a servicios

DocuSign® Server ofrece una solución para integrar funciones de seguridad en Arquitecturas Orientadas a Servicios (SOA) y XML. De este modo, se alinea con la práctica predominante en los sistemas de información corporativos y cierra una etapa de predominio de arquitecturas de software poco flexibles.

Auditoría y control centralizado

DocuSign ® Server centraliza tanto las políticas de confianza como el control y registro de logs. Esto permite regular el uso de criptografía en los procesos críticos de negocio y administrar, de forma totalmente transparente y auditada, Autoridades de Certificación (CA) y de Validación (VA), como la AC de Economía, del SAT o cualquier otra que el cliente confíe.

Mayor orientación a los procesos de negocio

En los procesos de toma de decisiones es clave conocer con exactitud tanto el nivel de confianza de la información como sus autores y atributos.

Flexibilidad en la integración de aplicaciones

Al cubrir la totalidad de los métodos de integración, DocuSign permite la adopción de diferentes estrategias.

- ☑ Los servicios de DocuSign se pueden
- ☑ Invocar de diferentes formas:
- ☑ Como servicios web (SOAP o REST);
- ☑ Mediante una API Java o .NET (integrada en las aplicaciones) que consume de forma transparente los servicios de DocuSign.
- ☑ Accediendo desde una pasarela e integración que evita modificar las aplicaciones y permite procesar datos de forma encadenada (mediante un lenguaje XML-Pipeline).