PSC Advantage

DocuSign® TSA

PSC Advantage

Versión 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® TSA 2
DESCRIPCION 2
CARACTERÍSTICAS FUNCIONALES 2
ARQUITECTURA 4
Modulo de Administración 5
Modulo de Desarrollo/Comunicación Servicios Web 5
Software Base para su Instalación 5

DOCUSIGN® TSA

DESCRIPCION

DocuSign® TSA (Timestamping Authority) es una solución diseñada para administrar la generación de evidencias electrónicas o sellos de tiempo que certifican que una serie de datos existe y no ha sido alterada desde una fecha y hora específica, asegurando la confidencialidad y privacidad de los datos.

DocuSign® TSA cumple con las especificaciones establecidas en el RFC 3161 y puede ser configurada como una entidad confiable para operar como una notaría en línea para certificar la existencia de cualquier tipo de datos en formato electrónico.

Con la integración de sellos de tiempo para la operación de transacciones en línea, así como en cualquier documento electrónico, se incrementa la confiabilidad y certeza en la operación de cualquier aplicación.

En un entorno donde se ha implementado firma electrónica avanzada, DocuSign® TSA proporciona los mecanismos para certificar que una firma electrónica, ha sido generada en tiempo y de esta forma garantizar la no repudiación del instante en que fue firmada la información.

CARACTERÍSTICAS FUNCIONALES

Permite definir múltiples entidades emisoras de sellos de tiempo en un mismo equipo.

Incorpora el protocolo TSP (Time Stamping Protocol) definido en la especificación RFC 3161 , el cual implementa certificados digitales X.509 y tecnología de firma electrónica avanzada para la emisión de sellos de tiempo.

Incorpora mecanismos para administrar las peticiones de sellos de tiempos a través de cuentas de usuarios y contraseñas.

Incorpora mecanismos de comunicación alternativos para la petición de sellos de tiempo basados en servicios Web XML.

Cuenta con funciones para monitorear y generar reportes de la emisión de sellos de tiempo.

Facilidad de integración a través librería DocuSign ® API o aplicaciones propietarias.

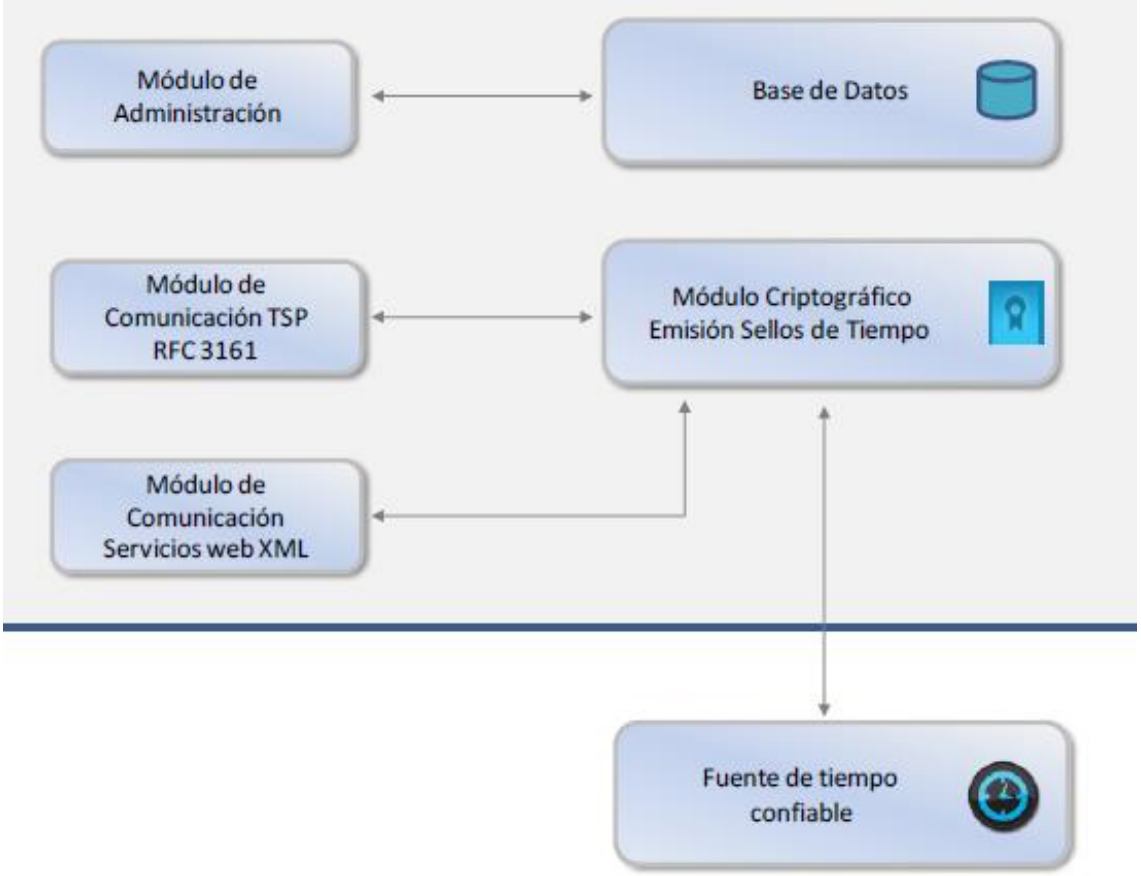
Capacidad de generar sellos de tiempo a partir de identificadores únicos de la información llamados compendios, los cuales son calculados con base a algoritmos MD5, SHA-1 y SHA-2, RSA, PKCS, X509-IETF RFC 3280, PKCS#5, TSP – IETF RFC 3161

Capacidad de integrar dispositivos criptográficos HSM (hardware security module) para el resguardo de la llave raíz responsable de emitir los sellos de tiempo.

Capacidad de operar sobre una infraestructura de cómputo sincronizada a fuentes de tiempo confiables.

El formato que ocupa para indicar la fecha es en formato Internet Date/ Time UTC (AAMMDDhhmmss)

ARQUITECTURA



DocuSign® TSA tiene la capacidad de operar en un ambientes distribuidos, lo cual permite definir niveles la estrategia de disponibilidad y continuidad de los servicios.

Puede soportar su operación en alta disponibilidad (Clúster)

DocuSign® TSA es altamente escalable

Permita Administrar las Estampillas de Tiempo con otra TSA (Time Stamping Autorithy) ya sea por software o por hardware permitiendo almacenar las evidencias y generar las pistas de auditoría correspondientes.

Modulo de Administración

Cuenta con una consola gráfica de configuración para administrar su operación y configuración.

Permite la consulta y extracción de la información

Permite la Generación de reportes, personalizables a la necesidad del cliente.

Permite la Operación y Comunicación del Servicio basada en TCP

Se comunica a la Base de Datos definida por el cliente-

Cuenta con un módulo de auditoría y seguimiento de las operaciones realizadas.

Modulo de Desarrollo/Comunicación Servicios Web

Cuenta con API's basados en lenguajes de programación C, y Java, y NET proporcionando funciones de:

Solicitud de Generación de Estampillas de Tiempo
Autenticación de Estampillas de Tiempo

Software Base para su Instalación

Sistema Operativo
Windows 2003, 2005 o 2008, Linux Red Hat

Base de Datos
Microsoft SQL Server 2000 SP3
Oracle 9i, 10g y 11g.
IBM DB2
MySQL