

## **Notaría Electrónica que da fé de la existencia de sus transacciones**

### **Descripción**

SeguriNotary proporciona servicios de Notaría Electrónica para dar constancia de que una transacción electrónica ocurrió en una fecha y hora específicos.

### **Módulos**

SeguriNotary consta de tres módulos:

- Módulo Cliente. Está compuesto por una biblioteca de funciones (API) que permiten hacer llamados al Módulo de Notaría Electrónica desde cualquier lenguaje de programación para solicitar la creación de un Recibo Criptográfico de una transacción.

Este módulo recibe como parámetro el contenido de la transacción, le aplica un algoritmo de digestión (MD5) obteniendo la digestión o huella digital de la transacción, conectándose posteriormente al Módulo de Notaría Electrónica para solicitar el recibo.

También se incluye dentro de este módulo, una función de auditoría que permite validar si una cierta transacción ha sido alterada con respecto a la información que se proporcionó para generar el recibo.

Esta función es especialmente importante cuando se requiere validar la integridad de la información de una transacción en un tiempo posterior al de su generación.

- Módulo de Notaría Electrónica. Recibe las solicitudes de generación de recibos criptográficos y genera el recibo que incluye:

- nombre del servicio emisor,
- un número secuencial único que identifica al recibo,
- la digestión de la transacción,
- la fecha y hora de su generación, y
- la firma digital de esta información generada con la Llave Privada en custodia de la Notaría.

Adicionalmente en este módulo, se implementan mecanismos que evitan que un recibo sea insertado de manera fraudulenta en un tiempo en el que no fué generado.

Todos los recibos generados por la Notaría son almacenados en una Base de Datos Relacional, lo que permite explotar la información con fines estadísticos.

La firma del recibo se realiza utilizando RSA como algoritmo de firmado, bajo el estándar PKCS #1.

Se considera que el Módulo de Notaría Electrónica se apegue a los Time Stamp Protocols que se encuentran en desarrollo publicados por parte del PKIX Working Group.

Estos protocolos se adoptarán en SeguriNotary, una vez que estén terminados.

- Módulo de Auditoría. Permite generar procesos de auditoría que validan la integridad de la Base de Datos de la Notaría, detectando cualquier inconsistencia en los recibos criptográficos.

Este módulo, genera reportes estadísticos con respecto al comportamiento de la Notaría, permitiendo identificar horas y días pico de servicio para anticipar la necesidad de actualizar el equipo de cómputo en el cual reside la Notaría.

El Módulo de Auditoría se ejecuta por solicitud del administrador y opera bajo Microsoft® Windows de 32 bits y requiere tener acceso a la Base de Datos de la Notaría Electrónica.

### **Requerimientos**

El servidor de SeguriNotary está diseñado para ejecutarse bajo:

- Microsoft® Windows NT/2000/XP/2003

El acceso al servicio se puede realizar desde las siguientes plataformas:

- Microsoft® Windows de 32 bits
- Linux
- Unix

**SeguriData**

**www.seguridata.com**  
**Insurgentes Sur 2375 3er. Piso**  
**Colonia Tizapán**  
**01000, México, D.F.**  
**Tel +52(55)3098 0700**  
**Fax +52(55)3098 0702**  
**ventas@seguridata.com**