

Soluciones Electrónicas para su empresa en un solo paquete.

SeguriServer

Descripción

Es un software diseñado para crear una Autoridad Certificadora que emita y administre certificados digitales, proporcionando las funciones necesarias para adaptar los certificados a sus políticas.

SeguriServer también cuenta con la función de Autoridad Registradora para procesar los requerimientos de certificación que son enviados a la Autoridad Certificadora para emitir un certificado digital compatible con Hardware Criptográfico como tarjetas inteligentes o tokens criptográficos USB.1

Funcionalidad

SeguriServer utiliza estándares PKIX que proporcionan la funcionalidad necesaria para:

- Generar requerimientos de certificación
- Procesar requerimientos de certificación
- Emitir y revocar certificados
- Soporte a directorios LDAP

La Autoridad Certificadora

SeguriServer cuenta con una interfaz a través de la cual se puede acceder a la administración de los certificados digitales. Como módulo opcional cuenta con la llave privada de la Autoridad Certificadora, que puede trabajar bajo esquemas de custodios mismos que deberían estar presentes en labores de

certificación.

Para el proceso de emisión de certificados digitales, la Autoridad Certificadora puede seguir dos procesos:

1. A partir de requerimientos de certificación aportados por usuarios finales
2. A través de Autoridad Registradora, quien recibe los requerimientos de certificación entregados manualmente por usuarios finales a quienes sean Autoridades de Registro.

Todos los certificados digitales emitidos quedan registrados en la base de datos de la Autoridad Certificadora, evitando duplicidades en números de serie y Llaves Públicas, permitiendo su consulta a través de la consola de administración.

Registradores

Cuando se cuenta con Autoridades Registradoras, se puede activar la función de certificación automática de los "precertificados." Esta modalidad permite recibir a través de Internet "precertificados" que son verificados para comprobar que contengan la firma digital de alguno de los Agentes de Certificación dados de alta, proporcionando una escalabilidad de la infraestructura. SeguriServer ofrece una interfase gráfica fácil de usar para las Autoridades Registradoras, a través de una PC común.

SeguriServer

Para la creación de una Autoridad Certificadora que emita y administre certificados digitales

SeguriSign

Integridad, Autenticidad y Confidencialidad para transacciones y documentos electrónicos en ambientes web

SeguriNotary

Proporciona servicios de Notaría Electrónica para dar constancia de que una transacción ocurrió en fecha y hora específicos, a través de una estampilla de tiempo.

Usuario Final

Para los usuarios finales, incluye el software para la generación de requerimientos de certificación, así como un par de llaves criptográficas. Los usuarios pueden descargar esta pequeña aplicación desde Internet, o bien se les puede facilitar a través de correo electrónico, ya que es muy ligera y no requiere instalaciones.

Hardware

El módulo de Autoridad Certificadora es capaz de utilizar para sus operaciones criptográficas un dispositivo de hardware que cumpla con la norma FIPS-140-1 Nivel 3.

Acceso

- Conexión directa desde las Autoridades Registradoras

Requerimientos Mínimos

- Microsoft® Windows 2000 Server o superior
- En el caso de Cluster, se requiere Microsoft® Windows 2000 Advanced Server

APIs

SeguriServer cuenta con APIs desde donde programadores institucionales pueden automatizar operaciones y agregar valor específico a SeguriServer con funcionalidad a las aplicaciones propietarias o hechas a la medida.

SeguriSign

Descripción

Es una aplicación que permite garantizar la autenticidad de transacciones y documentos electrónicos transmitidos o concentrados en un servidor para su consulta posterior.

La protección que SeguriSign proporciona a las transacciones y documentos no se limita al hecho de garantizar que su contenido no se ha modificado, sino que puede hacerlo accesible únicamente al destinatario que se haya seleccionado.

Funcionalidad

Permite realizar funciones de firmado y ensobretado digital de transacciones, documentos o mensajes con criptografía de llave pública RSA.

Operación

El proceso se realiza a través de un navegador que se enlaza de manera segura con el Web Server, el cual entrega el documento o transacción al SeguriSign Server para su autenticación y registro. Una vez procesado el documento es posible obtener un recibo electrónico de la operación.

Llaves y Certificados Digitales

SeguriSign requiere que los usuarios y los destinatarios cuenten con una llave privada y su correspondiente certificado digital X.509, emitido por una Autoridad Certificadora.

Requerimientos

Microsoft® Windows XP y Microsoft® Windows 2003

SeguriNotary

Descripción

Proporciona servicios de Notaría Electrónica para dar constancia de que una transacción electrónica ocurrió en cierta fecha y hora, amparando un contenido específico.

Módulos

Módulo Cliente. 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. Recibe las solicitudes de generación de recibos criptográficos de las transacciones y los genera.

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

Requerimientos de la aplicación

Microsoft® Windows 2000 Server o superior

The logo for SeguriData features the word "Seguri" in a blue, sans-serif font, followed by "Data" in a larger, bold, black, sans-serif font. A small red dot is positioned above the letter 'i' in "Seguri".

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