

Para la Creación de una Autoridad de Certificación que emita y administre Certificados Digitales

Descripción

SeguriServer es un software diseñado para crear una Autoridad Certificadora; emite y administra certificados digitales, proporcionando a la Autoridad Certificadora las funciones necesarias para adaptar los certificados a sus propias políticas. SeguriServer le proporciona los servicios de Autoridad Certificadora y de Autoridad Registradora que su institución necesita, además puede trabajar en Cluster para ambientes que requieran alta disponibilidad. SeguriServer proporciona a la Autoridad Certificadora las funciones necesarias para adaptar los certificados a las políticas de cualquier Autoridad Certificadora. Además permite la revocación de certificados y la generación de listas de certificados revocados. Contiene la funcionalidad necesaria para la generación del certificado raíz.

Funcionalidad

SeguriServer se apega a los estándares internacionales PKIX para proporcionarle la funcionalidad necesaria para:

- Generar requerimientos de certificación bajo el estándar PKCS #6, #9, y #10.
- Procesar requerimientos de certificación por medio de Autoridades Registradoras. El sistema de Autoridad Registradora de SeguriServer

permite almacenar el certificado y la llave privada en tarjetas inteligentes (SmartCards) y/o Tokens Criptográficos.

- Emitir certificados:
 - X.509 v3
 - S/MIME
 - EDIFACT
 - SSL
 - OCSP Responder
- Revocar certificados en línea ó mediante Autoridades Registradoras ó mediante la consola de la Autoridad Certificadora.
- Emitir Listas de Certificados Revocados CRLs.
- Verificación de estatus de certificados en línea, a través del Módulo OCSP y consultas para aplicaciones de alto riesgo.
- Soporte a directorios LDAP.
- Auditoría a través de un Módulo que permite verificar la integridad y autenticidad de transacciones hechas por la Autoridad Certificadora durante su operación normal.
- Personalización del certificado de acuerdo a módulos de entrada y de salida que permiten a la institución incluir información adicional, modificar o procesar cada certificado.
- Licencia ilimitada para clientes de la Autoridad Registradora que deseen generar pares de llaves y requerimientos de certificación. Se pueden generar llaves RSA de 512

bits para compatibilidad con software restringido o 1024 bits para mayor seguridad. Si el usuario desea se pueden también generar llaves de 2048 bits.

- Todas las transacciones son firmadas en la base de datos de la Autoridad Certificadora, lo que permite verificar la integridad y autenticidad de la misma.

La Autoridad Certificadora

SeguriServer presenta en todo momento una interfaz gráfica a través de la cual se accede a todas sus funciones. Así mismo permite el almacenamiento y lectura de los certificados digitales desde una tarjeta inteligente.

La Autoridad Certificadora puede iniciar generando su certificado raíz. En este proceso la llave privada de la Autoridad Certificadora queda encriptada y en custodia de un conjunto de n custodios de los cuales m deben estar presentes en labores de certificación, utilizando hardware Criptográfico FIPS 140-1 nivel 3. Para el proceso de emisión de certificados digitales, la Autoridad de Certificación 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 de los usuarios, y tras

aceptar su petición genera un “precertificado”, que se entrega a la Autoridad Certificadora que lo firma definitivamente, obteniendo así el certificado digital.

Durante el proceso de emisión de un certificado digital, la Autoridad Registradora puede elegir el periodo de validez de los certificados.

La Autoridad de Certificación puede certificar a uno o más sujetos como Autoridad Registradora. De esta forma la Autoridad de Certificación puede procesar los “precertificados” que sus agentes le aporten.

Todos los certificados digitales emitidos, sin importar su condición, quedan reflejados en la herramienta de administración de la Autoridad Certificadora, evitando duplicidades en números de serie y de Llaves Públicas.

Desde esta misma interfaz es posible visualizar cualquier certificado digital que se ha expedido.

Simplemente seleccionando un certificado, este se desplegará mostrando toda su información.

Una vez desplegado el certificado digital, la Autoridad Certificadora puede proceder a revocar un certificado.

Un certificado digital puede ser revocado en cualquier momento, pero solo por la Autoridad Certificadora. Las Autoridades registradoras pueden hacer la solicitud de revocación. Los certificados revocados alimentan el CRL, cuya generación se hace de acuerdo a un período de publicación configurable.

El CRL se puede generar con la frecuencia que se requiera. Así mismo su distribución se puede llevar a cabo por diferentes medios, incluyendo páginas web.

SeguriServer proporciona una interfaz web para solicitud y consulta de certificados

Registradores

Cuando se cuenta con Autoridades Registradoras, se puede activar la función de certificación automática de los “precertificados” que envían las citadas Autoridades Registradoras.

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, así como la integridad del mismo.

Si se cumplen estos puntos, se genera el certificado digital, éste queda registrado en la Autoridad Certificadora y se envía de inmediato a la Autoridad Registradora que solicitó su certificación.

SeguriServer incluye el software de las Autoridades Registradoras.

Este software procesa los requerimientos de certificación de los usuarios transformándolos en “precertificados” que son remitidos a la Autoridad Certificadora, quien finalmente emite el certificado digital.

Cuenta con su propia interfaz de administración gráfica en la cual de manera sencilla puede acceder a un requerimiento para “precertificarlo”, o a un CRL para actualizar sus propios registros. Cuando la Autoridad Certificadora funciona automáticamente, las Autoridades Registradoras pueden enviar sus “precertificados” a la Autoridad Certificadora por medio de Internet. La respuesta de la Autoridad Certificadora es inmediata, de forma que la Autoridad Registradora cuenta con el certificado digital del sujeto en pocos segundos.

El modo de registradores permite incrementar el número de los mismos proporcionando una escalabilidad de la infraestructura.

SeguriServer ofrece una interfase para las Autoridades Registradoras a

través de una PC común.

Usuario Final

Para los usuarios finales SeguriServer incluye el software para la generación de requerimientos de certificación, así como del par de llaves criptográficas. Los usuarios pueden descargar esta pequeña aplicación desde Internet, o bien se les puede facilitar a través de correo electrónico o en un disquete, ya que es muy ligera y no requiere instalaciones. Consiste en un formulario que el usuario debe llenar; posteriormente se genera una semilla aleatoria para la creación de las llaves tomando como pauta los movimientos del ratón del propio usuario.

El usuario final guarda su llave privada protegiendo su acceso a través de un password de hasta 255 caracteres. De esta forma la generación de las llaves criptográficas es privada y secreta. La generación de las llaves puede realizarse en un dispositivo criptográfico (SmartCard o Token).

Hardware

El módulo de Autoridad Certificadora de SeguriServer es capaz de utilizar para sus operaciones criptográficas un dispositivo de hardware que cumpla con la norma FIPS-140-1 Nivel 3. La llave privada de la Autoridad Certificadora y el motor criptográfico pueden residir en el dispositivo. SeguriServer contiene el software de administración del dispositivo mediante el cual se definen las políticas de uso y custodia de la llave privada. Se puede definir un conjunto de n custodios y exigir un quórum de m de ellos para poder activar a la Autoridad Certificadora. Cada custodio cuenta con una llave magnética. El sistema de Autoridad Registradora puede utilizar tarjeta

inteligente o Tokens USB, lo cual permite un control absoluto sobre su computadora o bien realizar su labor en una computadora compartida en donde no tenga ningún control.

Acceso

En cuanto a métodos de acceso, la Autoridad Certificadora puede funcionar mediante diferentes formas:

- . Consola, basado en HTML/http
- . Conexión directa desde las Autoridades Registradoras.

Requerimientos Mínimos

Para el óptimo funcionamiento de SeguriServer es necesario contar con un equipo de las siguientes características:

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

APIs

SeguriServer cuenta con APIs desde donde programadores institucionales pueden automatizar operaciones y agregar valor específico a SeguriServer.

Adicionalmente los módulos de entrada y de salida permiten, mediante callbacks, personalizar y procesar los certificados digitales.

The logo for SeguriData, featuring the word "Seguri" in blue and "Data" in black, with a red dot above the '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