

SeguriServer versión 6.12

Manual de Administración

Revisión 1.0

Seguri▶ata

SeguriData Privada, S.A. de C.V.

Av. Insurgentes Sur #2375, 3er. piso,
Col. Tizapán, Del. Alvaro Obregón,
C.P. 01000, México, D.F.

Tel. +52 (55) 3098-0700

Fax. +52 (55) 3098-0702

<http://www.seguridata.com>

Derechos Reservados © SeguriData IP S.A. de C.V., Av. Insurgentes Sur #2375, 3er. piso, Col. Tizapán, Del. Alvaro Obregón, C.P. 01000, México, D.F.. Derechos Reservados © SeguriData Privada S.A. de C.V., Av. Insurgentes Sur #2375, 3er. piso, Col. Tizapán, México, D.F., México, 1998. Este producto constituye una obra intelectual protegida por las leyes nacionales y tratados internacionales en materia de derechos de autor, y queda prohibida su reproducción o uso total o parcial, que no sean autorizadas por su titular.

Contenido

Capítulo 1. ¿Cómo utilizar este manual?

1.1 Organización de este manual	1 - 1
1.2 Simbología y convenciones	1 - 1
1.2.1. Recomendaciones y Advertencias	1 - 1
1.3 Objetivo del Manual	1 - 2

Capítulo 2. Los componentes de SeguriServer

2.1 Componentes de SeguriServer	2 - 1
---------------------------------	-------

Capítulo 3. La Consola de Administración de SeguriServer

3.1 Acceso al Módulo de Administración	3 - 2
3.2 Administración de Certificados de Usuarios de la Autoridad Certificadora	3 - 3
3.3 Certificación de Usuarios	3 - 4
3.3.1. Consulta de Certificados	3 - 18
3.4 Registro de Usuarios en un servidor LDAP	3 - 22
3.5 Autoridades Subordinadas	3 - 22
3.5.1. Agregar Autoridades Subordinadas	3 - 24
3.5.2. Consulta de Autoridades Subordinadas	3 - 36
3.6 Agentes Certificadores	3 - 37
3.6.1. Agregar Agentes Certificadores	3 - 39
3.6.2. Eliminar Agentes Certificadores	3 - 53
3.6.3. Consulta de Certificados de Agentes Certificadores	3 - 54
3.7 Obtención de CRLs	3 - 55
3.7.1. Consulta de CRLs	3 - 56
3.8 Configuración	3 - 56
3.8.1. Parámetros de Acceso a la Autoridad Certificadora	3 - 57
3.8.2. Parámetros de Acceso a la Consola de Administración	3 - 58

Apéndice A. Uso de PKCS12

CAPÍTULO 1

¿Cómo utilizar este manual?

1.1 Organización de este manual

El Manual del Administrador está orientado al personal que operará la Autoridad Certificadora, SeguriServer, a través de la aplicación del Administrador para la emisión y revocación de certificados digitales.

Se asume que el usuario cuenta con conocimientos sobre Infraestructuras de Llave Pública, Autoridades Certificadoras, así como la operación de Microsoft® Windows y el funcionamiento de la red.

Si el usuario no tiene experiencia previa en el uso de Certificados Digitales y/o con Autoridades Certificadoras se recomienda leer el Capítulo 2: Documentos Digitales Seguros.

En el CD de distribución de SeguriServer encontrará una copia de este manual en formato PDF.

1.2 Simbología y convenciones

En todo el manual se hace uso de una simbología específica para hacer más sencilla la identificación del tipo de información que se expone, así como de convenciones tipográficas, para hacer más clara la documentación.

1.2.1 Recomendaciones y Advertencias

En los lugares que resulte mas oportuno, se insertarán comentarios sobre el contenido del texto.

Importante

Este tipo de anotaciones contiene sugerencias y aclaraciones que facilitan el uso de la aplicación.

Precaución

Este tipo de anotaciones advierten sobre posibles riesgos en las operaciones descritas en el texto y que pueden causar pérdida de funcionalidad o datos.

1.3 Objetivo del Manual

Explicar los procedimientos de administración de SeguriServer: Subordinación de Autoridades, Gestión de Agentes, Gestión de Certificados de Usuario y Generación de Listas de Certificados Revocados.

CAPÍTULO 2

Los componentes de SeguriServer

2.1 Componentes de SeguriServer

SeguriServer esta formado por un grupo de aplicaciones que en conjunto proporcionan la funcionalidad de una autoridad certificadora. Algunos de los componentes se instalan por separado debido a su función específica, ofreciendo una flexibilidad total para cualquier infraestructura de seguridad.

Los componentes de SeguriServer son:

- *Servicio de Certificación*
Este componente es el motor de administración de certificados y es un servicio del sistema. Se instala en el equipo de la autoridad certificadora.
- *Consola de Configuración*
Este componente permite configurar los parámetros de operación del servicio de certificación de SeguriServer. Se instala en el equipo de la autoridad certificadora.
- *Consola de Administración*
Este componente ofrece una interfaz para administrar los certificados generados por la autoridad. Se instala en el equipo de la autoridad certificadora.
- *Consola del Respondedor OCSP*
Este componente permite configurar el servicio del Respondedor de OCSP. Se instala en el equipo de la autoridad certificadora, sin embargo se puede transferir manualmente a otro equipo.
- *Consola del Agente Certificador*
Este componente permite administrar certificados de manera remota desde un equipo distinto al de la autoridad certificadora. Se instala de manera independiente.

- *Consola del Ejecutivo de Registro*
Este componente permite organizar y solicitar certificados a un agente certificador. Se instala de manera independiente.
- *Web Services*
Es un componentes externo de SeguriServer, que puede integrarse a programas de terceros para: tramitar certificados digitales, revocar certificados y hacer búsquedas personalizadas en la base de datos de la Autoridad Certificadora.
- *CGIs*
Es un módulo externo de SeguriServer que permite a través del protocolo HTTP:
 - Generar requerimientos de certificación
 - Instalar certificados digitales
 - Consultar el certificado de la Autoridad Certificadora
 - Consultar la lista de certificados revocados
 - Hacer búsquedas de certificados y revocar certificados

En el siguiente diagrama se muestran los componentes que conforman a SeguriServer. (Figura 2.1).

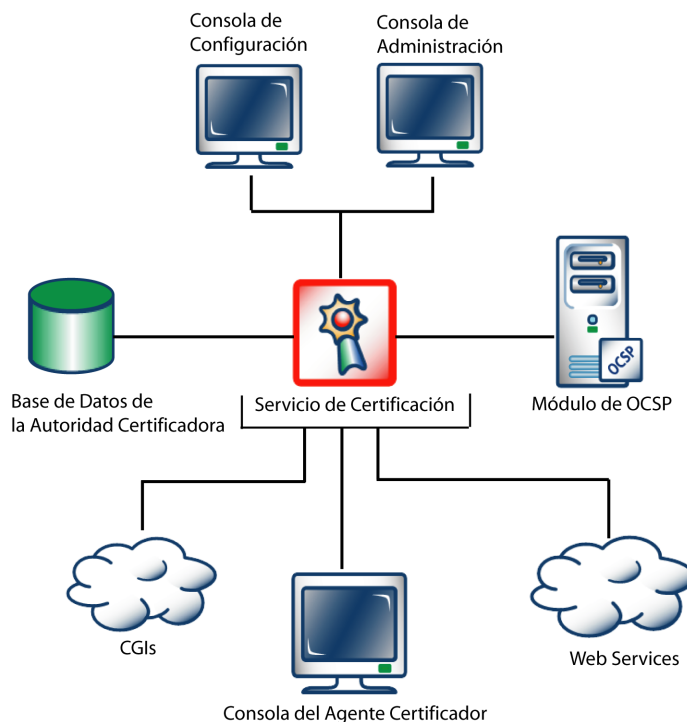


Figura 2.1 Diagrama de los Componentes de SeguriServer

/ Importante

Todos los componentes del diagrama anterior se instalan con el programa de instalación de SeguriServer, el cual se encuentran en el CD de distribución, excepto el componente *Agente Certificador* y *CGIs* que son instaladores independientes de SeguriServer.

CAPÍTULO 3

La Consola de Administración de SeguriServer

En una infraestructura de seguridad, la autoridad certificadora es la encargada de la certificación de usuarios y del control de éstos.

Para cumplir con esta función, SeguriServer cuenta con un módulo de administración que permite realizar actividades como:

- Generación, consulta y revocación de certificados
- Administrar Autoridades Certificadoras subordinadas
- Administrar Agentes Certificadores
- Definición, creación y consulta de una CRL
- Cambio de la clave de acceso y certificado del administrador

La consola permite realizar las labores de administración, operando directamente con la autoridad certificadora.

/ Importante

Por lo general, SeguriServer atiende peticiones para generar certificados, a partir de requerimientos de usuarios, mediante un Agente Certificador. Sin embargo es posible, administrar certificados desde la consola de administración.

3.1 Acceso al Módulo de Administración

Para acceder al módulo de administración de SeguriServer, es necesario ejecutar la aplicación a través de

Inicio > Programas > SeguriData > SeguriServer > Administrador

Al iniciar la aplicación, aparecerá una ventana que controlará el acceso al módulo de administración. (Figura 3.1).

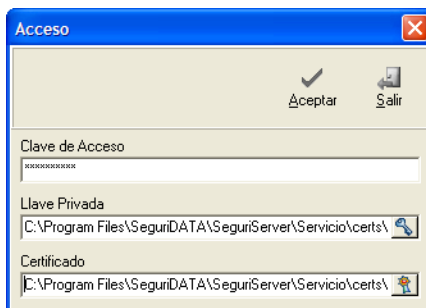


Figura 3.1 Ventana de Acceso

Indique la Clave de Acceso que corresponde a la llave privada del Administrador de la Autoridad, así como la ubicación del Certificado y de la Llave Privada.

Haga clic en el botón Aceptar.

Al completar el acceso, aparecerá la consola de Administración. (Figura 3.2).

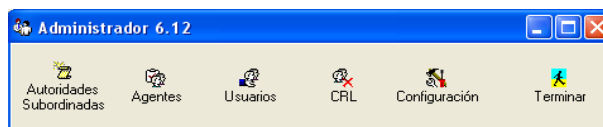


Figura 3.2 Consola de Administración

3.2 Administración de Certificados de Usuarios de la Autoridad Certificadora

Por lo general, la autoridad certificadora atenderá las peticiones de un agente certificador quien enviará requerimientos de certificación, generando y devolviendo los certificados correspondientes.

Sin embargo, es posible realizar diversas tareas de administración de certificados a través de la consola de administración de SeguriServer.

Las tareas que se pueden llevar a cabo son:

- Certificación de Usuarios
- Consulta de Certificados
- Revocación de Usuarios
- Registro de Usuarios en un servidor LDAP

Para acceder al módulo en que se realizan estas tareas, haga clic en la opción Usuarios de la consola de Administración. (Figura 3.3).

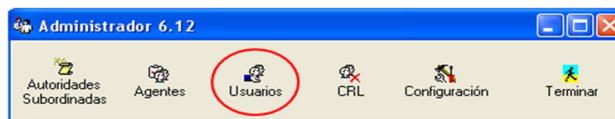


Figura 3.3 Opción Usuarios

Aparecerá la ventana de administración de usuarios. (Figura 3.4).

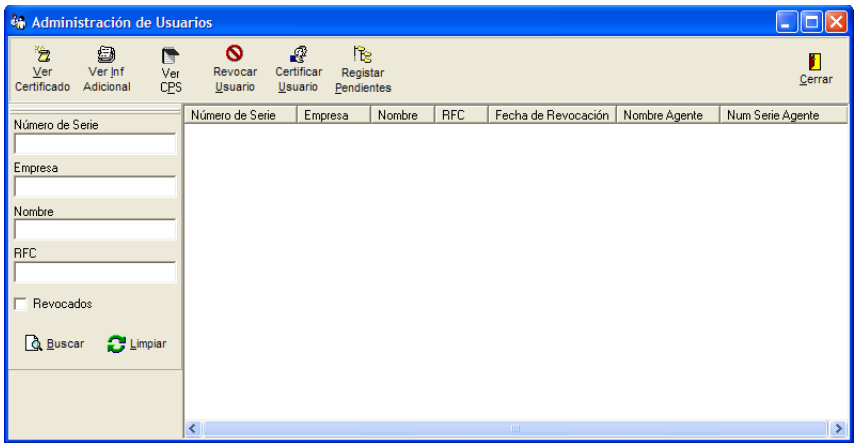


Figura 3.4 Administración de Usuarios

3.3 Certificación de Usuarios

Para la creación y registro de un certificado en la autoridad certificadora, es necesario contar con el requerimiento creado por el usuario que solicita dicho certificado. Para crear un certificado, siga el siguiente procedimiento:

- 1. Haga clic en el botón Certificar Usuario en la ventana de Administración de Usuarios, como se muestra en la Figura 3.5.

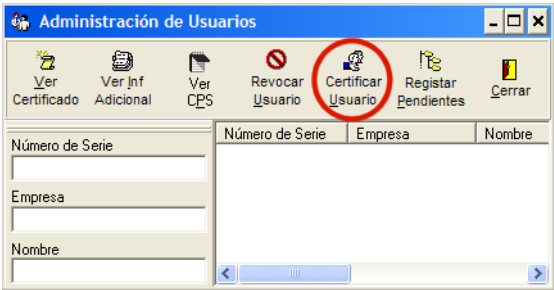


Figura 3.5 Certificar Usuarios

2. Aparecerá una ventana en la cual se selecciona el requerimiento del usuario, así como las características del certificado que se generará. (Figura 3.6).

Dato	Valor
Razón Social	SeguriData Privada S.A.
Área	QA
Nombre	Agente1
CP	01000
País	MX
RFC	LEMH690329KR7
ID	LEMH690329MDFYRL05
Clave de anulación	12345678

Período de Validez | Tipo de Certificado

Válido a partir de: 11/12/2007 Válido hasta el: 10/12/2008

Certificado: [Text Field]

Figura 3.6 Selección del Requerimiento

Haga clic en el botón Requerimiento, que presenta el selector de archivos para seleccionar el archivo que contiene el requerimiento (.req) del usuario.

Al terminar, regresará a la ventana de certificación y se mostrarán los datos del requerimiento.

3. A continuación indique los parámetros que se solicitan en la parte inferior de la ventana. (Figura 3.7).

Período de Validez | Tipo de Certificado

Válido a partir de: 10/12/2007 Válido hasta el: 09/12/2008

Certificado: [Text Field]

Figura 3.7 Período de Validez

Seleccione las fechas de validez del certificado a través de los campos Válido a partir de: y Válido Hasta:

En el campo Certificado haga clic en el botón a la derecha, que presenta el selector de archivos para indicar la ruta y el nombre del certificado a generar.

4. Haga clic en la pestaña Tipo de Certificado que presenta la siguiente ventana. (Figura 3.8).

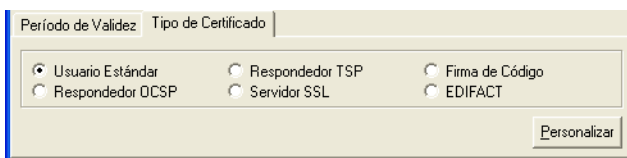


Figura 3.8 Tipo de Certificado

Seleccione alguno de los siguientes tipos de certificado, según corresponda:

- **Usuario Estándar.** Genera certificados para personas físicas; es la opción que más usaría un administrador: emitir certificados a personas físicas. El seleccionar esta opción enciende lo mínimo necesario para un certificado estándar.
- **Respondedor OCSP.** Permite que el certificado sea usado por un respondedor OCSP para firmar sus respuestas.
- **Respondedor TSP.** Permite que el certificado sea usado por un servidor de estampillas de tiempo para firmar sus respuestas.
- **Servidor SSL.** Crea un certificado para un servidor Web que permita conexiones seguras (SSL) a sus clientes.
- **Firma de Código.** Permite otorgar un certificado a una persona física ó moral que va a utilizar su certificado para firmar aplicaciones confiables.
- **EDIFACT.** Permite que el certificado pueda ser usado para encriptar mensajes de EDIFACT.

5. Si desea personalizar el tipo de certificado, haga clic en el botón Personalizar, que presenta la siguiente ventana. (Figura 3.9).

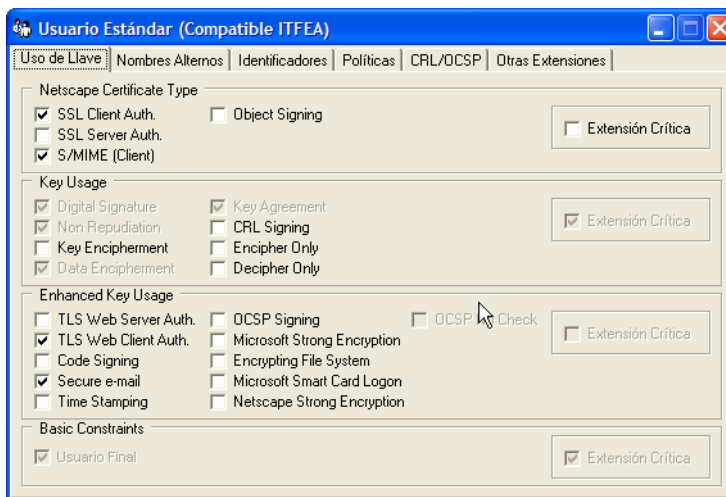


Figura 3.9 Uso de Llave

En esta ventana el usuario deberá habilitar/deshabilitar las banderas de las extensiones según lo requiera:

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.1.

Tabla 3.1 Parámetros de Uso de Llave

Nombre de la Extensión	Atributos	Descripción
<i>Netscape Certificate Type</i>		Esta extensión es definida por Netscape y es un grupo de banderas que sirven para distinguir el uso que se debe dar al certificado.
	SSL Client Auth.	Indica que el certificado se puede usar para autenticar a un usuario en una conexión SSL.
	SSL Server Auth.	Indica que el certificado en cuestión es un certificado con el que se puede establecer una sesión SSL para autenticar a un servidor web.

Tabla 3.1 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
Key Usage	S/MIME Client	Indica que el certificado se puede usar para validar firmas de mail.
	Object Signing	Indica que la AC podrá emitir certificados que sirvan para firmar software ejecutable
		Esta extensión nos indica por medio de banderas el uso que se la va a dar a la llave. Está definida por el grupo PKIX.
	Digital Signature	Firma Digital
	Non Repudiation	No repudio. Es decir, sirve para validar firmas realizadas por la AC y ésta no se puede retractar de haberlas generado
	Data Encipherment	Cifrado de datos.
	Key Agreement	Acuerdo de llave. Sirve para establecer un canal seguro de comunicación (SSL)
	Cert Signing	Firma de certificados. Es decir, será capaz de emitir certificados
	CRL Signing	Firma de listas de certificados revocados
	Encipher Only	Indica que el certificado se debe usar sólo para cifrar información.
Enhanced Key Usage	Decipher Only	Indica que el certificado se debe usar sólo para descifrar información.
		Uso extendido de llave. Esta extensión sirve para indicar usos de llave más a la medida de las aplicaciones. Los usos extendidos de llave están definidos comúnmente en estándares RFC. Los presentes usos extendidos de llave son los más comunes que se encuentran en uso.
	TLS Web Server Auth.	Indica que el certificado se puede usar para autenticar a un servidor en una comunicación SSL ó TLS.

Tabla 3.1 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
	TLS Web Cliente Auth.	Indica que el certificado se puede usar para autenticar a un cliente en una comunicación SSL ó TLS.
	Code Signing	Indica que el certificado se puede usar para firmar aplicaciones.
	Secure e-mail	Firma de e-mail.
	Time Stamping	Emisión de estampillas de tiempo.
	OCSP Signing	Firma de estatus de certificados en línea (OCSP).
	Microsoft Strong Encryption	Indica a las aplicaciones de Microsoft que utilicen llaves y/ó algoritmos de exportación para encriptar información que tiene como destinatario el poseedor del certificado.
	Encrypting File System	Indica a los sistemas operativos de Microsoft que el certificado se puede usar para encriptar archivos.
	Microsoft Smart Card Logon	Indica a las aplicaciones de Microsoft que este certificado de puede usar para realizar un logon.
	Nestcape Strong Encryption	Indica a los browsers de Netscape que utilicen algoritmos y/o llaves de exportación para encriptar información que va destinada al poseedor de este certificado.
<i>Basic Constraints</i>		Limitantes básicas. Nos indica los límites (niveles de subordinación) que pueden depender del certificado de la AC.
	Usuario Final	Indica que el poseedor de este certificado no puede subordinar certificados.

6. Haga clic en la pestaña Nombre Alternos/Identificadores para especificar los datos de la extensión Nombres Alternos del Sujeto. (Figura 3.10).

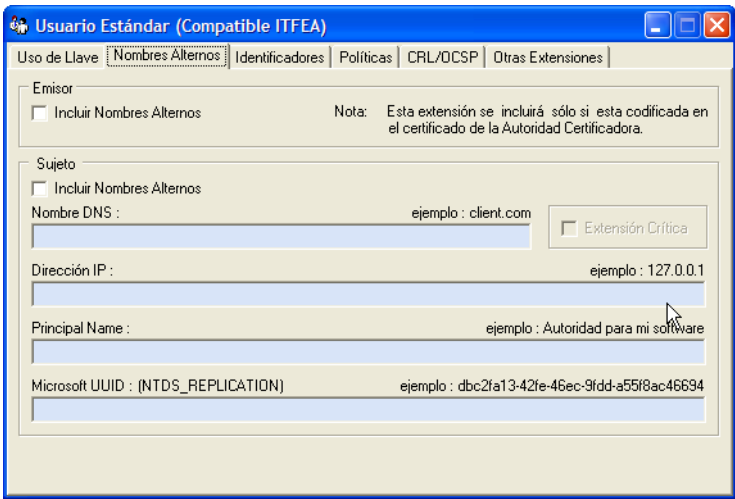


Figura 3.10 Nombres Alternos

Indique los parámetros correspondientes, como se indica en la Tabla 3.2.

Tabla 3.2 Parámetros de Nombres Alternos/Identificadores

Nombre de la Extensión	Atributos	Descripción
Emisor		Esta opción nos permite indicar si se incluirán los nombres alternos de la autoridad en el certificado del usuario.
	Incluir Nombres Alternos	Si se selecciona esta opción, los nombres alternos que tenga el certificado de la autoridad se replicarán en el certificado del usuario como nombres alternos de la autoridad.
Sujeto		Los nombres alternos del sujeto son “etiquetas” distintas del “nombre común” que se asignan al poseedor de un certificado. Recordemos que un certificado puede ser para un equipo ó un site.
	Nombre DNS	Es el nombre del equipo por el que lo localiza un DNS.
	Dirección IP	Es la IP asignada al equipo.

Tabla 3.2 Parámetros de Nombres Alternos/Identificadores (Continuación)

Nombre de la Extensión	Atributos	Descripción
	Principal Name	Indica el “nombre principal” como se define en Kerberos (RFC 1510)
	Microsoft UUID: (NTDS_REPLICATION)	Es el Identificador universal único (UUID) asignado a un proceso ó equipo.

7. Haga clic en la pestaña Identificadores para que se presente la siguiente ventana. (Figura 3.11).

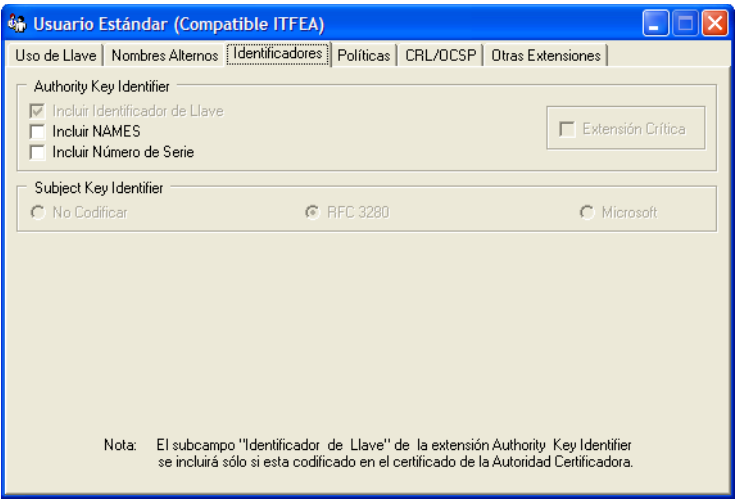


Figura 3.11 Identificadores

Indique los parámetros correspondientes, como se indica en la Tabla 3.3.

Tabla 3.3 Parámetros de Identificadores

Nombre de la Extensión	Atributo	Descripción
<i>Authority Key Identifier</i>		En ocasiones es útil incluir en los certificados de los usuarios información característica del certificado la autoridad que lo emitió, como por ejemplo: la digestión de la llave pública, los Nombres completos que la describen y/o el número de serie.

Tabla 3.3 Parámetros de Identificadores

Nombre de la Extensión	Atributo	Descripción
Subject Key Identifier	Incluir Identificador de Llave	Si se selecciona esta opción, se incluye la digestión de la llave pública de la autoridad.
	Incluir NAMES	Si se quieren incluir los nombres de la autoridad en la extensión que identifica al emisor, se debe seleccionar esta opción.
	Incluir Número de Serie	Seleccionando esta opción se incluye el número de serie del certificado de la autoridad.
		Es un identificador único de 20 bytes asignado a la llave pública contenida en el certificado. Los 20 bytes pueden ser calculados como lo indica el RFC3280 (incluyendo sólo los bits de la llave pública) ó como lo calcula Microsoft (incluyendo el algoritmo de la llave pública). Seleccione el correspondiente.

8. Haga clic en la pestaña Políticas para que se presente la siguiente ventana que permite indicar los datos de la extensión Certificate Policy Statement. (Figura 3.12).

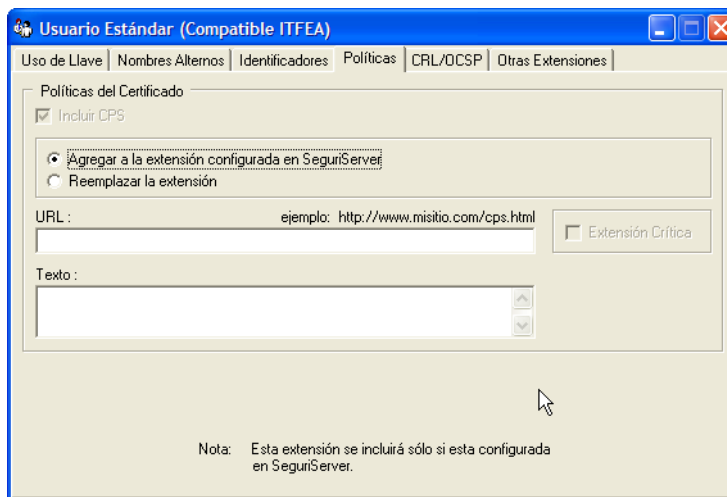


Figura 3.12 Políticas

En caso de incluir la extensión CPS, el usuario debe proporcionar el identificador y al menos uno de los campos restantes.

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.4.

Tabla 3.4 Parámetros de Configuración de las Políticas

Nombre de la Extensión	Atributos	Descripción
<i>Políticas del Certificado</i>		Las políticas de un certificado se refieren a las políticas de emisión y uso a los que se debe apegar un certificado. Las políticas se pueden publicar en un site en internet y adicionalmente se puede poner un resumen de no más de 200 caracteres que sea incluido en el certificado.
	Incluir CPS	Si desea que el certificado contenga las políticas de certificación, seleccione esta opción.

Tabla 3.4 Parámetros de Configuración de las Políticas (Continuación)

Nombre de la Extensión	Atributos	Descripción
	Agregar a la extensión configurada en SeguriServer	Si en el servicio de SeguriServer se configuraron políticas de certificación y se selecciona esta opción, estas políticas se agregarán a las configuradas en SeguriServer.
	Reemplazar la Extensión	El seleccionar esta opción substituirá el URL y/o texto de la política que está configurada en SeguriServer por la que provea el administrador.
	URL	Es una URL donde se encuentra publicada la política de certificación. El objetivo es que sea legible para una persona que acepta el certificado
	Texto	Es un texto breve que resume la política de certificación. Su objetivo es que alguien que no tenga acceso a internet ó no quiera ir a ver la política completa en internet, tenga una idea básica de las políticas de certificación.

9. Haga clic en la pestaña CRL/OCSP para que se presente la siguiente ventana que permite indicar las extensiones CRL Distribution Point y Authority Info Access. (Figura 3.13).

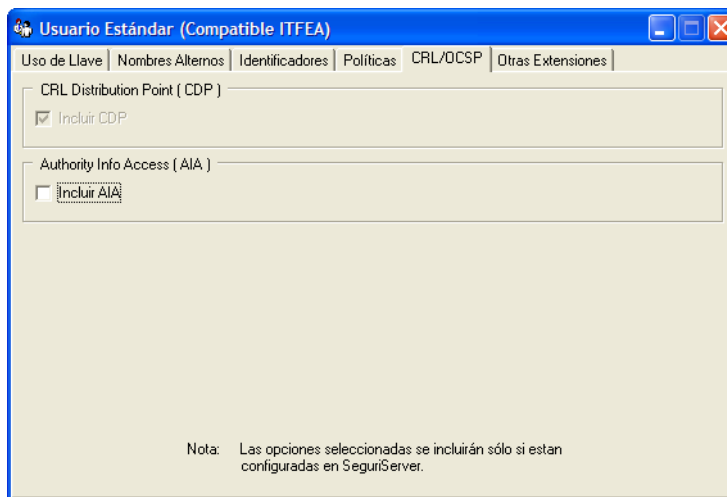


Figura 3.13 CRL/OCSP

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.5.

Tabla 3.5 Parámetros de Configuración del CRL/OCSP

Nombre de la Extensión	Atributos	Descripción
<i>CRL Distribution Point (CDP)</i>	Incluir CDP	Esta extensión indica a las personas y aplicaciones que acepten el certificado dónde pueden consultar un CRL donde eventualmente aparecería si el certificado está revocado o no. Marque esta casilla si desea incluir CDP en el certificado.
<i>Authority Info Access (AIA)</i>	Incluir AIA	Esta extensión indica URLs donde se encuentran servicios que puede dar la Autoridad emisora del certificado. Marque esta opción si desea incluir AIA en el certificado.

10. Haga clic en la pestaña Otras Extensiones que presenta la siguiente ventana que permite indicar los datos de las extensiones Autoridad EDIFACT, Comentario Netscape, URL Netscape, Microsoft Enroll Certificate Template Name y Microsoft CA Key Index Pair. (Figura 3.14).

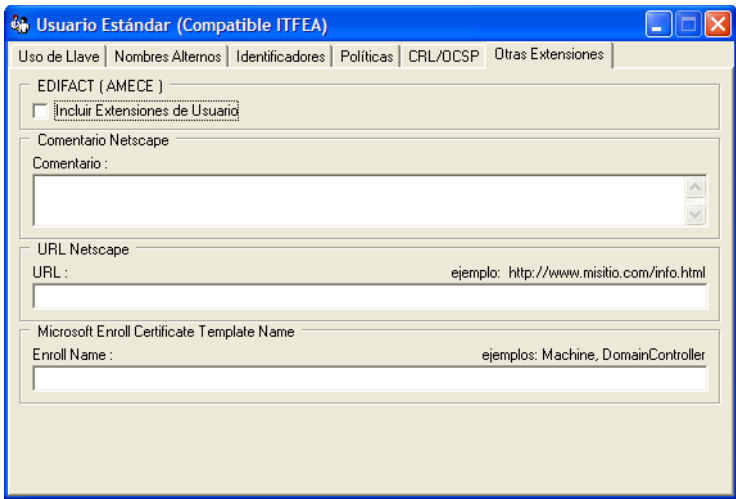


Figura 3.14 Otras Extensiones

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.6.

Tabla 3.6 Parámetros de Configuración de Otras Extensiones

Nombre de la Extensión	Atributos	Descripción
EDIFACT (AMECE)		Este campo solicita que se generen las distintas extensiones (definidas por el comité de seguridad de AMECE) para señalar que el certificado que se está generando será una AC ó un usuario final y que incluya a su vez las extensiones necesarias para poder convertir el certificado X.509 a un certificado EDIFACT.
	Incluir Extensiones de Usuarios	Indica que se incluyan las extensiones necesarias para poder hacer convertible el certificado X.509 a un certificado de EDIFACT (certificado de autoridad).

Tabla 3.6 Parámetros de Configuración de Otras Extensiones (Continuación)

Nombre de la Extensión	Atributos	Descripción
<i>Comentario/URL Netscape</i>		Estas extensiones, definida por Netscape indican a un browser de netscape que si es solicitada información adicional del certificado muestren un comentario ó lo lleven a un url donde está publicada información al respecto del certificado.
	Comentario	Texto a desplegar si se solicita información del certificado.
	URL	URL a direccionar si se solicita más información del certificado.
<i>Microsoft Enroll Certificate Template Name</i>		En aplicaciones de Microsoft®, en ocasiones es necesario indicar un rol que tendrá el certificado emitido.
	Enroll Name	El nombre del rol se debe indicar en este campo.

3.3.1 Consulta de Certificados

En ocasiones será necesario localizar certificados dentro de la base de datos de la autoridad. Las consultas de certificados se realizan utilizando los campos que se encuentran en la parte derecha de la ventana de administración de usuarios: Número de Serie, Empresa, Nombre y RFC. (Figura 3.15).

The screenshot shows a window titled "Administración de Usuarios". At the top, there is a toolbar with icons and labels for various actions: "Ver Certificado", "Ver Inf Adicional", "Ver CPS", "Revocar Usuario", "Certificar Usuario", and "Registrar Pendientes". Below the toolbar, on the left side, are input fields for "Número de Serie", "Empresa", "Nombre", and "RFC". There is also a checkbox labeled "Revocados". At the bottom of this section are two buttons: "Buscar" (with a magnifying glass icon) and "Limpiar" (with a circular arrow icon). On the right side of the window, there is a table with four columns: "Número de Serie", "Empresa", "Nombre", and "RFC". The table is currently empty. At the bottom of the window, there is a horizontal scrollbar.

Figura 3.15 Criterios de Búsqueda

Si adicionalmente se marca la casilla Revocados, la búsqueda se realizará sobre certificados revocados únicamente.

Para iniciar la búsqueda haga clic en el botón Buscar.

El botón Limpiar, borra todos los criterios de búsqueda, en caso de requerir una consulta con criterios distintos.

El resultado de la búsqueda aparecerá listado en el lado derecho de la ventana de administración de usuarios. (Figura 3.16).

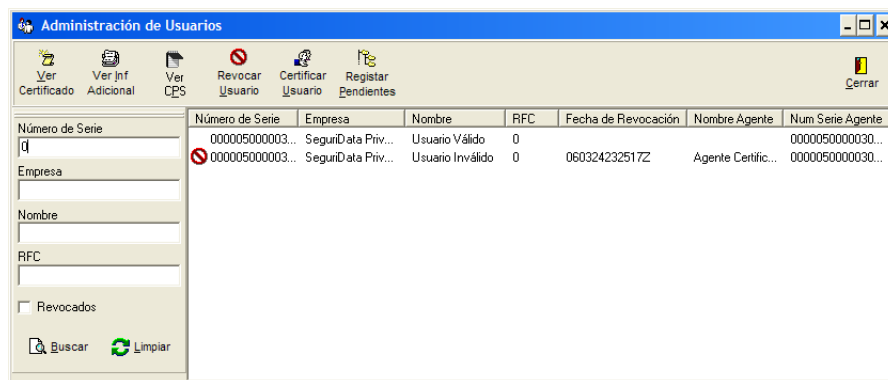


Figura 3.16 Resultado de la Búsqueda

Para consultar los detalles de un certificado en particular, selecciónelo y haga clic con el botón derecho del ratón, para que se presente el menú emergente. (Figura 3.17).

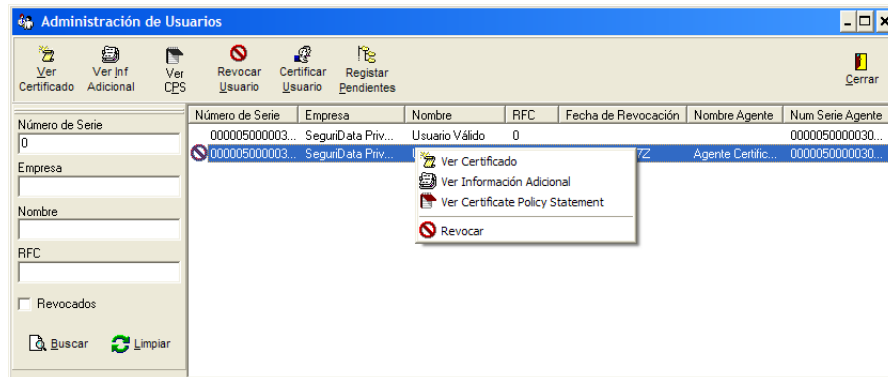


Figura 3.17 Detalles de un Certificado

Seleccione alguna de las siguientes opciones:

- Ver Certificado. Presenta una ventana con el detalle del certificado seleccionado. (Figura 3.18).

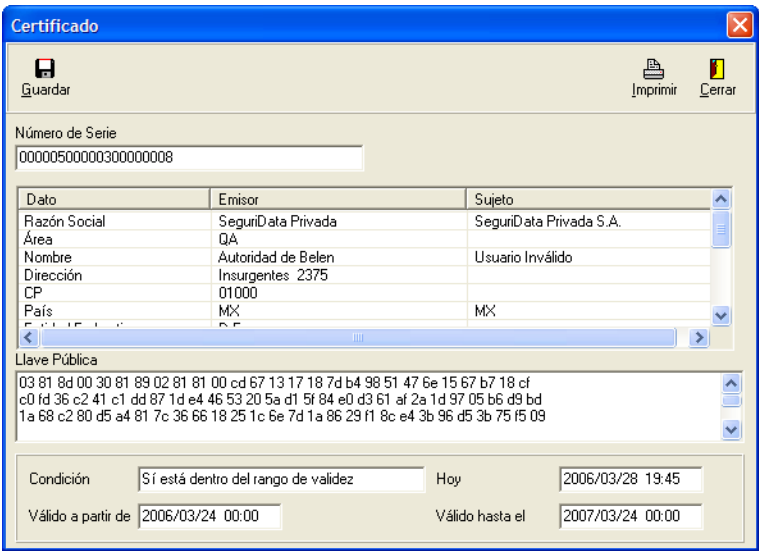


Figura 3.18 Detalle de un Certificado

- Ver Información Adicional. Presenta una ventana con información no contenida en el certificado, pero que esta relacionada con el mismo.

- Ver Certificate Policy Statement. Permite ver los detalles de la información específica de reglas que indican el vínculo entre el certificado y una comunidad ó tipo de aplicación particulares con requerimientos de seguridad comunes que se generará. (Figura 3.19).

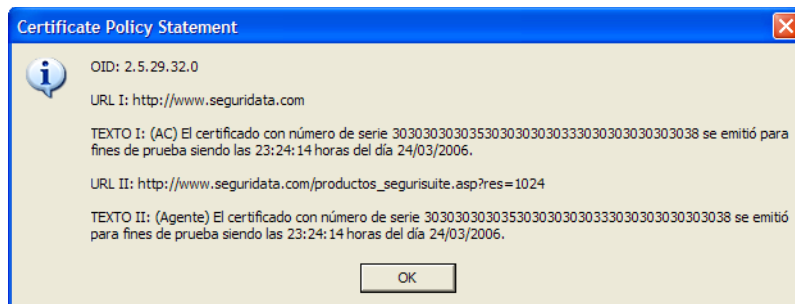


Figura 3.19 Información de Certificate Policy Statement

- Revocar. Permite revocar un certificado seleccionado, presentando la confirmación de la revocación. (Figura 3.20).

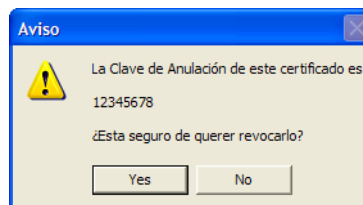


Figura 3.20 Mensaje

Para cerrar la ventana haga clic en el botón Cerrar.

Warning

La revocación del certificado **NO** es reversible y una vez que se completa el proceso, no existe manera de revertirlo.

3.4 Registro de Usuarios en un servidor LDAP

Si se ha configurado un servidor LDAP bajo el servicio de certificación, al momento de crear un certificado a partir de un requerimiento, SeguriServer lo registra en el servidor LDAP.

Sin embargo puede suceder que por alguna razón, como una falla en el enlace, el servidor LDAP no haya podido atender la transacción de SeguriServer y por lo tanto es necesario actualizar los usuarios que estén en la base de datos de la autoridad certificadora y que estén pendientes de registro en LDAP.

Para realizar esta sincronización de registro, deberá hacer clic en el botón Registrar Pendientes. (Figura 3.21).

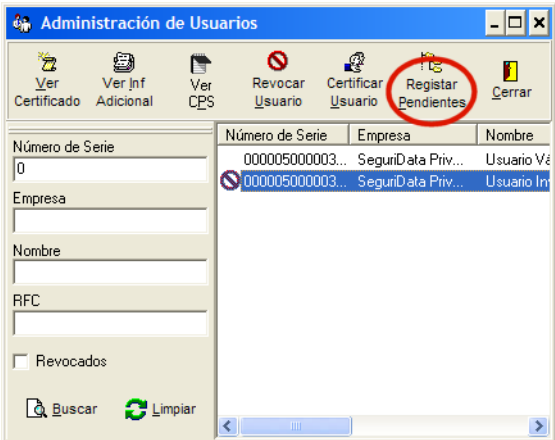


Figura 3.21 Registrar Pendientes

Al terminar, regresará a la ventana de administración de usuarios.

3.5 Autoridades Subordinadas

En una infraestructura de seguridad, en ocasiones es conveniente subordinar una autoridad certificadora a otra ya existente. Esto hace que los certificados emitidos por la autoridad subordinada reflejen que está reconocida por otra autoridad, y que por tanto, esta última también respalda los certificados.

Para realizar este proceso es necesario contar con el certificado de la autoridad certificadora que se desea subordinar.

Para acceder al módulo en que se realiza el registro de las autoridades subordinadas, seleccione la opción Autoridades Subordinadas, de la consola de Administración.

(Figura 3.22).

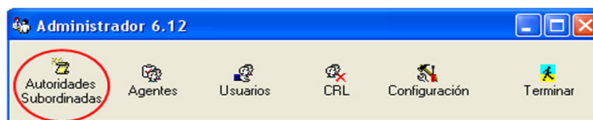


Figura 3.22 Autoridades Subordinadas

Se presentará una ventana para realizar el registro y consulta de los certificados de las autoridades subordinadas. (Figura 3.23).

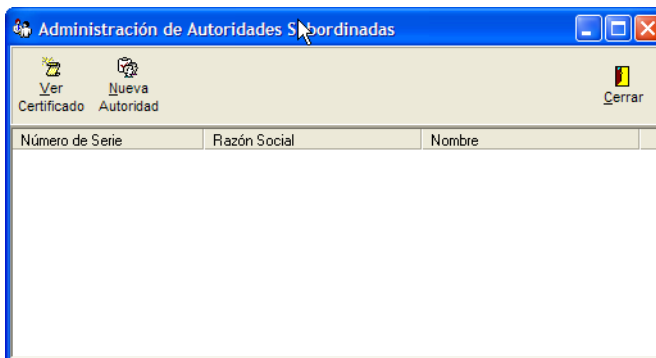


Figura 3.23 Area de Trabajo para las Autoridades Subordinadas

Las autoridades subordinadas registradas en SeguriServer se mostrarán en la parte inferior de la ventana, mostrando el Número de Serie, Razón Social y Nombre correspondiente a una autoridad por renglón.

3.5.1 Agregar Autoridades Subordinadas

Para definir una nueva autoridad subordinada, haga clic en el botón Nueva Autoridad. (Figura 3.24).

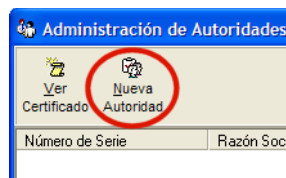


Figura 3.24 Nueva Autoridad

Se mostrará el selector de archivos, con el cual deberá elegir el certificado de la autoridad que se desea subordinar.

A continuación SeguriServer mostrará los datos de la Autoridad a Subordinar. Figura 3.25.

Nueva Autoridad

Subordinar Regresar

Número de Serie
j000040000800000001

Dato	Emisor	Sujeto
Razón Social	SeguriData Privada S.A. de C.V.	SeguriData Privada S.A. de C.V.
Área	R&D	R&D
Nombre	Autoridad de Pruebas ITFEA 6.0	Autoridad de Pruebas ITFEA 6.0
Dirección	Insurgentes Sur 2375	Insurgentes Sur 2375
CP	01000	01000
País	MX	MX

Llave Pública
03 81 8d 00 30 81 89 02 81 81 00 b2 c1 74 e2 80 a0 8c 28 f1 bb c2 ca a0 59 0c 30
c5 03 cf f0 35 a5 5f ea f0 24 68 c9 8e 90 76 31 25 0a d8 a8 44 ea f6 6e 4a 37 a6 29
bd 6a ca 10 20 12 72 0c 87 83 95 13 b1 79 af 34 15 10 71 09 17 e1 5f 30 83 ad 3a 10

Condición Hoy
Válido a partir de Válido hasta el

Extensiones Ruta Nuevo Certificado

Figura 3.25 Nueva Autoridad

Si desea personalizar el tipo de certificado, haga clic en el botón Personalizar, que presenta la siguiente ventana. (Figura 3.26).

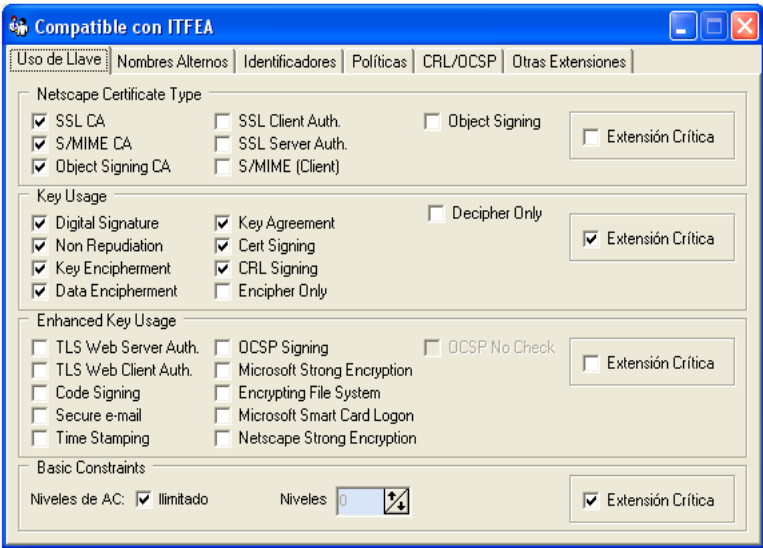


Figura 3.26 Uso de Llaves

/ Importante

Esta ventana puede variar ya que depende de las extensiones que se encuentren codificadas en el certificado a subordinar.

En esta ventana el usuario deberá habilitar/deshabilitar las banderas de las extensiones según lo requiera:

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.7.

Tabla 3.7 Parámetros de Uso de Llave

Nombre de la Extensión	Atributos	Descripción
<i>Netscape Certificate Type</i>		Esta extensión es definida por Netscape y es un grupo de banderas que sirven para distinguir el uso que se debe dar al certificado.

Tabla 3.7 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
<i>Key Usage</i>	SSL CA	Indica que la Autoridad Certificadora puede emitir certificados SSL.
	S/MIME CA	Indica que la Autoridad Certificadora puede emitir certificados para validar firmas de e-mail.
	Object Signing CA	Indica que la Autoridad Certificadora puede emitir certificados para firma de Software ejecutable.
	SSL Client Auth.	Indica que la AC puede autenticarse en una conexión SSL.
	SSL Server Auth.	Indica que el certificado de la AC puede utilizarse para establecer una sesión SSL para autenticar a un servidor.
	S/MIME (Cliente)	Indica que el certificado de la AC se puede usar para validar firmas de e-mail.
	Object Signing	Indica que el certificado de la AC puede firmar software ejecutable.
		Esta extensión nos indica por medio de banderas el uso que se le va a dar a la llave. Está definida por el grupo PKIX.
	Digital Signature	Firma Digital
	Non Repudiation	No repudio. Es decir, sirve para validar firmas realizadas por la AC y ésta no se puede retractar de haberlas generado
	Data Encipherment	Cifrado de datos.
	Key Agreement	Acuerdo de llave. Sirve para establecer un canal seguro de comunicación (SSL)
	Cert Signing	Firma de certificados. Es decir, será capaz de emitir certificados
	CRL Signing	Firma de listas de certificados revocados
	Encipher Only	Indica que el certificado se debe usar sólo para cifrar información.

Tabla 3.7 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
Enhanced Key Usage	Decipher Only	Indica que el certificado se debe usar sólo para descifrar información.
		Uso extendido de llave. Esta extensión sirve para indicar usos de llave más a la medida de las aplicaciones. Los usos extendidos de llave están definidos comúnmente en estándares RFC. Los presentes usos extendidos de llave son los más comunes que se encuentran en uso.
	TLS Web Server Auth.	Indica que el certificado se puede usar para autenticar a un servidor en una comunicación SSL ó TLS.
	TLS Web Cliente Auth.	Indica que el certificado se puede usar para autenticar a un cliente en una comunicación SSL ó TLS.
	Code Signing	Indica que el certificado se puede usar para firmar aplicaciones.
	Secure e-mail	Firma de e-mail.
	Time Stamping	Emisión de estampillas de tiempo.
	OCSP Signing	Firma de estatus de certificados en línea (OCSP).
	Microsoft Strong Encryption	Indica a las aplicaciones de Microsoft que utilicen llaves y/o algoritmos de exportación para encriptar información que tiene como destinatario el poseedor del certificado.
	Encrypting File System	Indica a los sistemas operativos de Microsoft® que el certificado se puede usar para encriptar archivos.
	Microsoft Smart Card Logon	Indica a las aplicaciones de Microsoft que este certificado se puede usar para realizar un logon.
	Nestcape Strong Encryption	Indica a los browsers de Netscape que utilicen algoritmos y/o llaves de exportación para encriptar información que va destinada al poseedor de este certificado.

Tabla 3.7 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
Basic Constraints		Limitantes básicas. Nos indica los límites (niveles de subordinación) que pueden depender del certificado de la AC.
	Usuario Final	Indica que el poseedor de este certificado no puede subordinar certificados.

Haga clic en la pestaña Nombres Alternos/Identificadores para especificar los datos de la extensión Nombres Alternos del Sujeto. (Figura 3.27).

The screenshot shows a window titled 'Compatible con ITFEA' with several tabs: 'Uso de Llave', 'Nombres Alternos', 'Identificadores', 'Políticas', 'CRL/OCSP', and 'Otras Extensiones'. The 'Nombres Alternos' tab is active. It contains two main sections: 'Emisor' and 'Sujeto'. Both sections have a checkbox labeled 'Incluir Nombres Alternos'. In the 'Emisor' section, there is a note: 'Nota: Esta extensión se incluirá sólo si esta codificada en el certificado de la Autoridad Certificadora.' The 'Sujeto' section has four text input fields: 'Nombre DNS' (example: client.com), 'Dirección IP' (example: 127.0.0.1), 'Principal Name' (example: Autoridad para mi software), and 'Microsoft UUID' (example: dbc2fa13-42fe-46ec-9fdd-a55f8ac46694). There is also a checkbox labeled 'Extensión Crítica'.

Figura 3.27 Nombres Alternos

Indique los parámetros correspondientes, como se indica en la Tabla 3.8.

Tabla 3.8 Parámetros de Nombres Alternos/Identificadores

Nombre de la Extensión	Atributos	Descripción
Emisor		Esta opción nos permite indicar si se incluirán los nombres alternos de la autoridad en el certificado del usuario.

Tabla 3.8 Parámetros de Nombres Alternos/Identificadores (Continuación)

Nombre de la Extensión	Atributos	Descripción
Sujeto	Incluir Nombres Alternos	Si se selecciona esta opción, los nombres alternos que tenga el certificado de la autoridad se replicarán en el certificado del usuario como nombres alternos de la autoridad.
		Los nombres alternos del sujeto son "etiquetas" distintas del "nombre común" que se asignan al poseedor de un certificado. Recordemos que un certificado puede ser para un equipo ó un site.
	Incluir Nombres Alternos	Si la autoridad certificadora tiene nombres alternos, éstos se incluirán como nombres alternos del emisor del certificado en cuestión.
	Nombre DNS	Es el nombre del equipo por el que lo localiza un DNS.
	Dirección IP	Es la IP asignada al equipo.
	Principal Name	Indica el "nombre principal" como se define en Kerberos (RFC 1510)
	Microsoft UUID: (NTDS_REPLICATION)	Es el Identificador universal único (UUID) asignado a un proceso ó equipo.

Haga clic en la pestaña Identificadores para que se presente la siguiente ventana. (Figura 3.28).

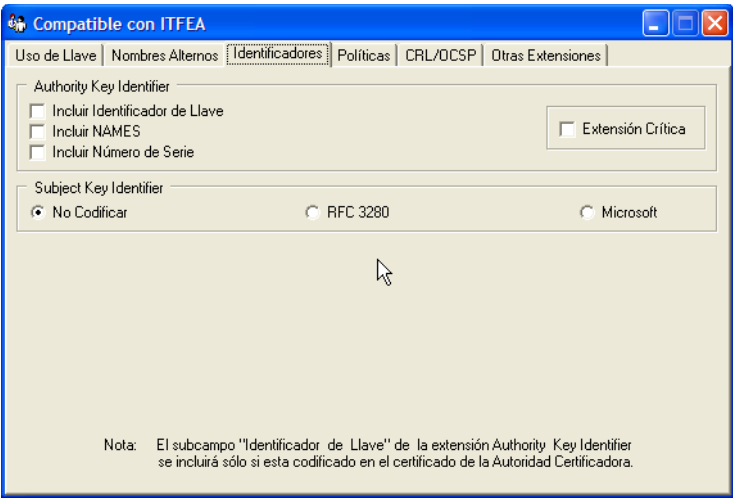


Figura 3.28 Identificadores

Indique los parámetros correspondientes, como se indica en la Tabla 3.9.

Tabla 3.9 Parámetros de Identificadores

Nombre de la Extensión	Atributo	Descripción
<i>Authority Key Identifier</i>		En ocasiones es útil incluir en los certificados de los usuarios información característica del certificado la autoridad que lo emitió, como por ejemplo: la digestión de la llave pública, los nombres completos que la describen y/o el número de serie.
	Incluir Identificador de Llave	Si se selecciona esta opción, se incluye la digestión de la llave pública de la autoridad.
	Incluir NAMES	Si se quieren incluir los nombres de la autoridad en la extensión que identifica al emisor, se debe seleccionar esta opción.
	Incluir Número de Serie	Seleccionando esta opción se incluye el número de serie del certificado de la autoridad.

Tabla 3.9 Parámetros de Identificadores

Nombre de la Extensión	Atributo	Descripción
Subject Key Identifier		Es un identificador único de 20 bytes asignado a la llave pública contenida en el certificado. Los 20 bytes pueden ser calculados como lo indica el RFC3280 (incluyendo sólo los bits de la llave pública) ó como lo calcula Microsoft® (incluyendo el algoritmo de la llave pública). Seleccione el correspondiente.

Haga clic en la pestaña Políticas para que se presente la siguiente ventana que permite indicar los datos de la extensión Certificate Policy Statement. (Figura 3.29).

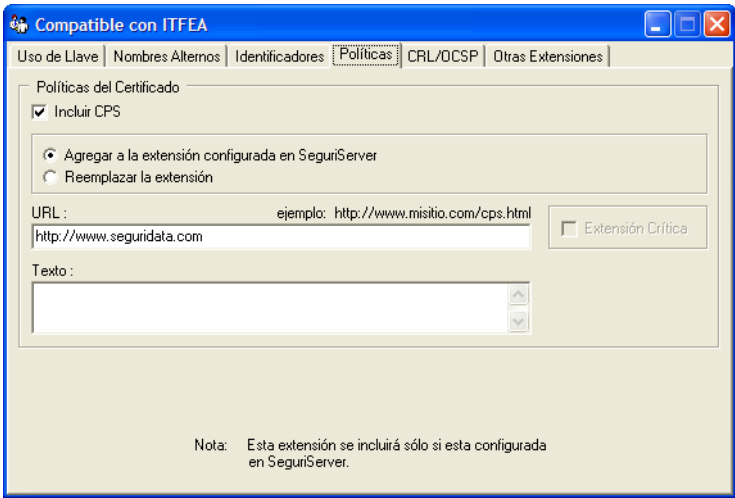


Figura 3.29 Políticas

En caso de incluir la extensión CPS, el usuario debe proporcionar el identificador y al menos uno de los campos restantes.

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.10.

Tabla 3.10 Parámetros de Configuración de las Políticas

Nombre de la Extensión	Atributos	Descripción
<i>Políticas del Certificado</i>		
		Las políticas de un certificado se refieren a las políticas de emisión y uso a los que se debe apegar un certificado. Las políticas se pueden publicar en un site en internet y adicionalmente se puede poner un resumen de no más de 200 caracteres que sea incluido en el certificado.
	Incluir CPS	Si desea que el certificado contenga las políticas de certificación, seleccione esta opción.
	Agregar a la extensión configurada en SeguriServer	Si en el servicio de SeguriServer se configuraron políticas de certificación y se selecciona esta opción, estas políticas se agregarán a las configuradas en SeguriServer.
	Reemplazar la Extensión	El seleccionar esta opción substituirá el URL y/o texto de la política que está configurada en SeguriServer por la que provea el administrador.
	URL	Es una URL donde se encuentra publicada la política de certificación. El objetivo es que sea legible para una persona que acepta el certificado
	Texto	Es un texto breve que resume la política de certificación. Su objetivo es que alguien que no tenga acceso a internet ó no quiera ir a ver la política completa en internet, tenga una idea básica de las políticas de certificación.

Haga clic en la pestaña CRL/OCSP para que se presente la siguiente ventana que permite indicar las extensiones CRL Distribution Point y Authority Info Access. (Figura 3.30).

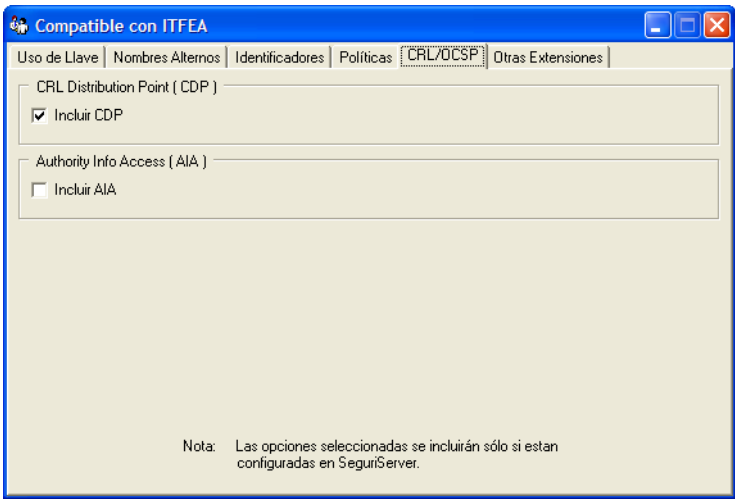


Figura 3.30 CRL/OCSP

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.11.

Tabla 3.11 Parámetros de Configuración del CRL/OCSP

Nombre de la Extensión	Atributos	Descripción
<i>CRL Distribution Point (CDP)</i>	Incluir CDP	Esta extensión indica a las personas y aplicaciones que acepten el certificado dónde pueden consultar un CRL donde eventualmente aparecería si el certificado está revocado o no. Marque esta casilla si desea incluir CDP en el certificado.
<i>Authority Info Access (AIA)</i>	Incluir AIA	Esta extensión indica URLs donde se encuentran servicios que puede dar la Autoridad emisora del certificado. Marque esta opción si desea incluir AIA en el certificado.

Haga clic en la pestaña Otras Extensiones que presenta la siguiente ventana que permite indicar los datos de las extensiones Autoridad EDIFACT, Comentario Netscape, URL Netscape y Microsoft Enroll Certificate Template Name y Microsoft CA Key Index Pair. (Figura 3.31).

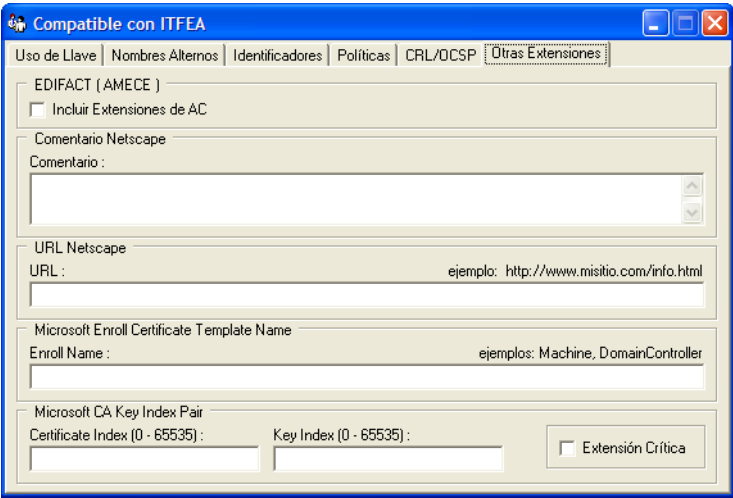


Figura 3.31 Otras Extensiones

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.12.

Tabla 3.12 Parámetros de Configuración de Otras Extensiones

Nombre de la Extensión	Atributos	Descripción
EDIFACT (AMECE)		Este campo solicita que se generen las distintas extensiones (definidas por el comité de seguridad de AMECE) para señalar que el certificado que se está generando será una AC ó un usuario final y que incluya a su vez las extensiones necesarias para poder convertir el certificado X.509 a un certificado EDIFACT.
	Incluir Extensiones de Usuarios	Indica que se incluyan las extensiones necesarias para poder hacer convertible el certificado X.509 a un certificado de EDIFACT (certificado de autoridad).

Tabla 3.12 Parámetros de Configuración de Otras Extensiones (Continuación)

Nombre de la Extensión	Atributos	Descripción
<i>Comentario/URL Netscape</i>	Comentario	Estas extensiones definida por Netscape indican a un browser de netscape, que si es solicitada información adicional del certificado muestren un comentario ó lo lleven a un url donde está publicada información al respecto del certificado.
	URL	Texto a desplegar si se solicita información del certificado. URL a direccionar si se solicita más información del certificado.
<i>Microsoft Enroll Certificate Template Name</i>	Enroll Name	En aplicaciones de Microsoft®, en ocasiones; es necesario indicar un rol que tendrá el certificado emitido. El nombre del rol se debe indicar en este campo.
	Certificate Index (0-65535)	Esta extensión la utilizan las aplicaciones de Microsoft® para distinguir entre las diferentes versiones de certificado cuando éste se renueva. Este campo indica la secuencia de renovación del certificado. La versión inicial debe ser "0". Siempre que exista un nuevo certificado, este índice se debe incrementar, ya sea si cambiaron los nombres en el certificado ó algún otro campo ó si cambió la llave pública.
<i>Microsoft CA Key Index Pair</i>	Key Index (0-65535)	Este campo indica si la llave pública ha sido substituida por una nueva. Su valor inicial debe ser 0. Si el nuevo certificado contiene una llave nueva, el valor del Key Index debe ser igual al del nuevo valor que se asignará al Certificate Index. Si la llave permaneció sin cambios, su valor también debe permanecer igual al del certificado anterior.

A continuación indique la ruta y el nombre del certificado a generar, haciendo clic en el botón a la derecha del campo Ruta Nuevo Certificado. (Figura 3.32).

Nueva Autoridad

Subordinar Regresar

Número de Serie
j000040000800000001

Dato	Emisor	Sujeto
Razón Social	SeguriData Privada S.A. de C.V.	SeguriData Privada S.A. de C.V.
Área	R&D	R&D
Nombre	Autoridad de Pruebas ITFEA 6.0	Autoridad de Pruebas ITFEA 6.0
Dirección	Insurgentes Sur 2375	Insurgentes Sur 2375
CP	01000	01000
País	Méx	Méx

Llave Pública
03 81 8d 00 30 81 89 02 81 81 00 b2 c1 74 e2 80 a0 8c 28 f1 bb c2 ca a0 59 0c 30
c5 03 cf f0 35 a5 5f ea f0 24 68 c9 8e 90 76 31 25 0a d8 a8 44 ea f6 6e 4a 37 a6 29
bd 6a ca 10 20 12 72 0c 87 83 95 13 b1 79 af 34 15 10 71 09 17 e1 5f 30 83 ad 3a 10

Condición: Hoy:

Válido a partir de: Válido hasta el:

Extensiones: Personalizar

Figura 3.32 Ruta del Nuevo Certificado

Por último haga clic en el botón Subordinar.

3.5.2 Consulta de Autoridades Subordinadas

Cuando se han dado de alta Autoridades Subordinadas, se pueden consultar los datos de estás. Para esto, deberá de seleccionar el renglón correspondiente a la autoridad subordinada que se desea consultar, seguido de un clic en el botón Ver Certificado. (Figura 3.33).

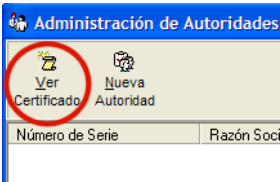


Figura 3.33 Ver Certificado

Se presentará una ventana con el detalle del certificado seleccionado, como se muestra en la Figura 3.34.

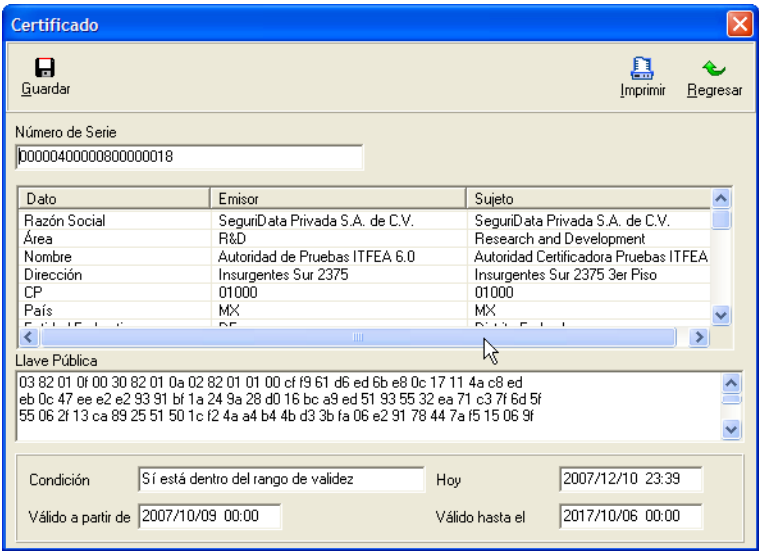


Figura 3.34 Detalle del Certificado

3.6 Agentes Certificadores

La autoridad certificadora es el eje sobre el cual funciona una infraestructura de seguridad, proporcionando el servicio de generación de certificados. Por razones muy diversas como puede ser el resguardo del equipo en que está la autoridad certificadora o el volumen de certificados que se deben generar, no es recomendable que los certificados se generen a través de la consola de administración.

SeguriServer está habilitado para atender peticiones de certificación desde un puerto de comunicaciones, lo cual permite que además de la consola de administración, SeguriServer atienda las transacciones solicitadas por uno o más Agentes Certificadores. (Figura 3.35).

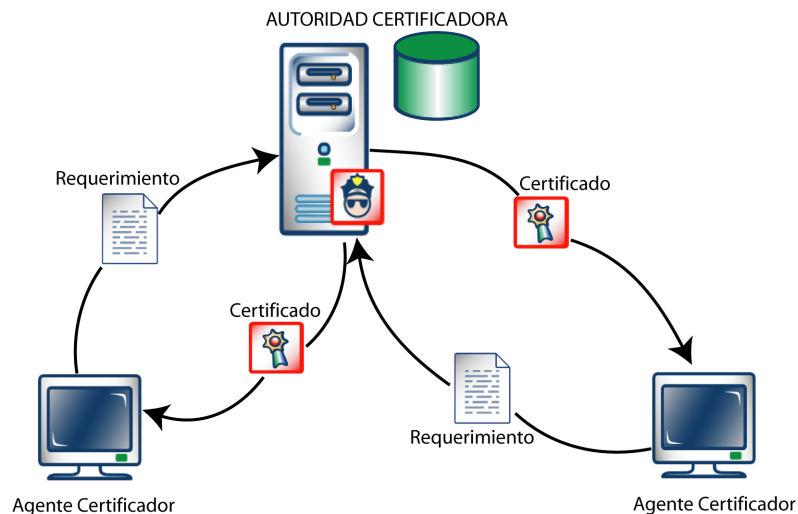


Figura 3.35 Diagrama de Agentes Certificadores

El Agente Certificador corresponde a un Agente Registrador dentro de la relación de confianza de una infraestructura de seguridad y por tanto las solicitudes de certificación que recibe la autoridad certificadora, se aceptarán como totalmente confiables.

Las operaciones de administración, accesibles a través de la consola de administración de SeguriServer, son:

- Agregar Agentes Certificadores
- Eliminar Agentes Certificadores
- Consultar el Certificado del Agente Certificador
- Consultar el Certificate Policy Statement

Para realizar cualquiera de estas operaciones, haga clic en la opción Agentes de la consola de Administración. (Figura 3.36).

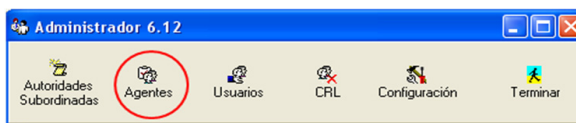


Figura 3.36 Agentes

A continuación se presentará la siguiente ventana. (Figura 3.37).

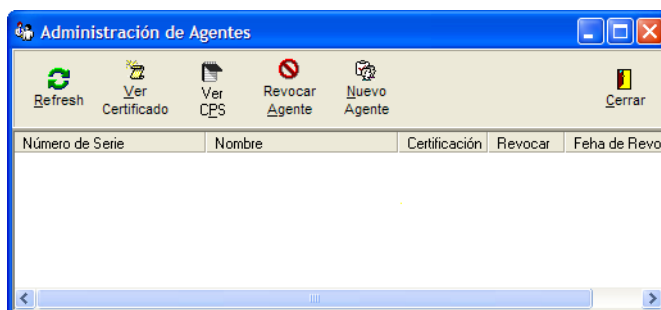


Figura 3.37 Administración de Agentes

3.6.1 Agregar Agentes Certificadores

Para definir a los agentes certificadores válidos para la autoridad certificadora, se deberá dar de alta a cada uno de ellos por medio de la consola de administración de SeguriServer.

Este procedimiento, necesita un requerimiento por parte del Agente Certificador, el cual se deberá generar únicamente con el programa de requerimientos que acompaña a la aplicación del agente, accesible desde:

Inicio > Programas > SeguriData > SeguriServer > Agente > Requerimiento de Certificación

Warning

El programa de requerimientos para agentes certificadores genera un requerimiento con características especiales. Los certificados generados a partir de un requerimiento creado con cualquier otra aplicación, **NO** serán aceptados por SeguriServer para identificar a un agente certificador.

El llenado es similar al de cualquier otro requerimiento.

El archivo donde se encuentra el requerimiento del Agente Certificador, se deberá entregar al administrador de la autoridad certificadora para crear el certificado correspondiente.

Una vez que el administrador de la autoridad certificadora recibe el requerimiento, deberá de abrir la ventana para administración de agentes certificadores. (Figura 3.38).

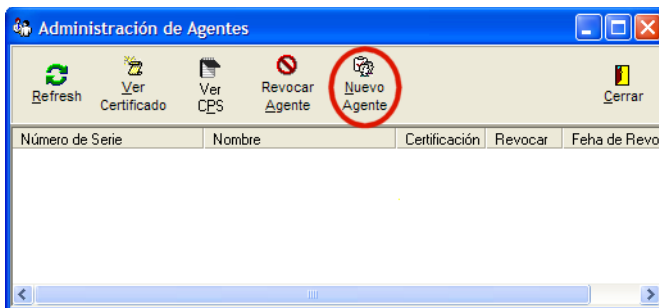


Figura 3.38 Nuevo Agente

Haga clic en el botón Nuevo Agente que presenta la siguiente ventana. (Figura 3.39).

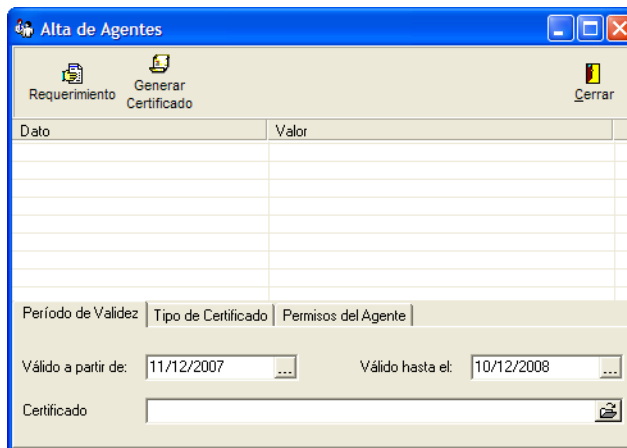


Figura 3.39 Alta de Agentes

Haga clic en el botón Requerimiento, que presenta el selector de archivos para facilitar la ubicación del requerimiento del Agente.

A continuación proporcione la siguiente información:

1. Deberán de indicarse las fechas en los campos Válido a partir de y Válido hasta el. (Figura 3.40).

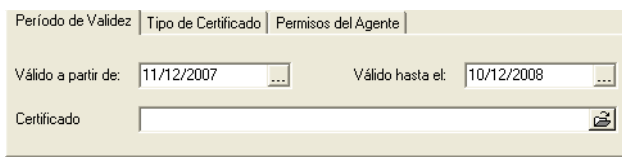


Figura 3.40 Vigencia del Certificado

En el campo Certificado indique la ruta y nombre del archivo donde se guardará el certificado ya generado.

2. Seleccione la pestaña Tipo de Certificado, para que se presente la siguiente ventana. (Figura 3.41).

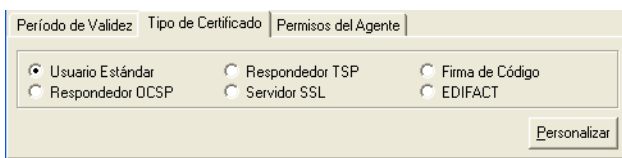


Figura 3.41 Tipo de Certificado del Agente

Seleccione alguno de los siguientes tipos de certificado, según corresponda:

- Usuario Estándar. Esta opción está pensada para generar certificados para personas físicas; es la opción que más usaría un agente certificador: emitir certificados a personas físicas. El seleccionar esta opción enciende lo mínimo necesario para un certificado estándar.
- Respondedor OCPS. Permite que el certificado sea usado por un respondedor OCSP para firmar sus respuestas
- Respondedor TSP. Permite que el certificado sea usado por un servidor de estampillas de tiempo para firmar sus respuestas
- Servidor SSL. Crea un certificado para un servidor Web que permita conexiones seguras (SSL) a sus clientes
- Firma de Código. Esta opción está pensada para otorgar un certificado a una persona física ó moral que va a utilizar su certificado para firmar aplicaciones confiables.
- EDIFACT. Permite que el certificado pueda ser usado para encriptar mensajes de EDIFACT

3. Si desea personalizar el tipo de certificado, haga clic en el botón Personalizar, que presenta la siguiente ventana. (Figura 3.42).

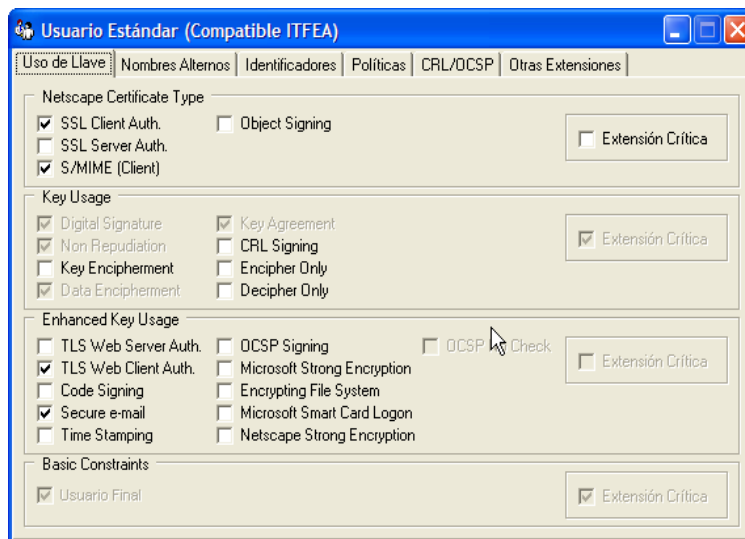


Figura 3.42 Uso de Llave

En esta ventana el usuario deberá habilitar/deshabilitar las banderas de las extensiones según lo requiera:

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.13.

Tabla 3.13 Parámetros de Uso de Llave

Nombre de la Extensión	Atributos	Descripción
<i>Netscape Certificate Type</i>		Esta extensión es definida por Netscape®, y es un grupo de banderas que sirven para distinguir el uso que se debe dar al certificado.
	SSL Client Auth.	Indica que el certificado se puede usar para autenticar a un usuario en una conexión SSL.
	SSL Server Auth.	Indica que el certificado en cuestión es un certificado con el que se puede establecer una sesión SSL para autenticar a un servidor web.

Tabla 3.13 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
Key Usage	S/MIME Client	Indica que el certificado se puede usar para validar firmas de mail.
	Object Signing	Indica que la AC podrá emitir certificados que sirvan para firmar software ejecutable
		Esta extensión nos indica por medio de banderas el uso que se la va a dar a la llave. Está definida por el grupo PKIX.
	Digital Signature	Firma Digital
	Non Repudiation	No repudio. Es decir, sirve para validar firmas realizadas por la AC y ésta no se puede retractar de haberlas generado
	Data Encipherment	Cifrado de datos.
	Key Agreement	Acuerdo de llave. Sirve para establecer un canal seguro de comunicación (SSL)
	Cert Signing	Firma de certificados. Es decir, será capaz de emitir certificados
	CRL Signing	Firma de listas de certificados revocados
	Encipher Only	Indica que el certificado se puede usar para validar firmas de mail.
Enhanced Key Usage	Decipher Only	Indica que el certificado se debe usar sólo para descifrar información.
		Uso extendido de llave. Esta extensión sirve para indicar usos de llave más a la medida de las aplicaciones. Los usos extendidos de llave están definidos comúnmente en estándares RFC. Los presentes usos extendidos de llave son los más comunes que se encuentran en uso.
	TLS Web Server Auth.	Indica que el certificado se puede usar para autenticar a un servidor en una comunicación SSL ó TLS.

Tabla 3.13 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
	TLS Web Cliente Auth.	Indica que el certificado se puede usar para autenticar a un cliente en una comunicación SSL ó TLS.
	Code Signing	Indica que el certificado se puede usar para firmar aplicaciones.
	Secure e-mail	Firma de e-mail.
	Time Stamping	Emisión de estampillas de tiempo.
	OCSP Signing	Firma de estatus de certificados en línea (OCSP).
	Microsoft Strong Encryption	Indica a las aplicaciones de Microsoft® que utilicen llaves y/ó algoritmos de exportación para encriptar información que tiene como destinatario el poseedor del certificado.
	Encrypting File System	Indica a los sistemas operativos de Microsoft® que el certificado se puede usar para encriptar archivos.
	Microsoft Smart Card Logon	Indica a las aplicaciones de Microsoft® que este certificado de puede usar para realizar un logon.
	Netscape Strong Encryption	Indica a los browsers de Netscape® que utilicen algoritmos y/o llaves de exportación para encriptar información que va destinada al poseedor de este certificado.
<i>Basic Constraints</i>		Limitantes básicas. Nos indica los límites (niveles de subordinación) que pueden depender del certificado de la AC.
	Usuario Final	Indica que el poseedor de este certificado no puede subordinar certificados.

4. Haga clic en la pestaña Nombre Alternos/Identificadores para especificar los datos de extensión Nombres Alternos del Sujeto y el tipo de codificación de la extensión Subject Key Identifier. (Figura 3.43).

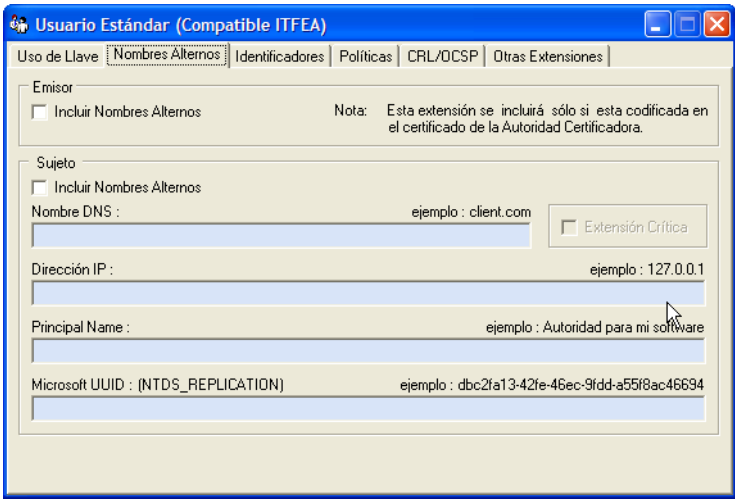


Figura 3.43 Nombres Alternos

Indique los parámetros correspondientes, como se indica en la Tabla 3.14.

Tabla 3.14 Parámetros de Nombres Alternos/Identificadores

Nombre de la Extensión	Atributos	Descripción
<i>Emisor</i>		Esta opción nos permite indicar si se incluirán los nombres alternos de la autoridad en el certificado del usuario.
	Incluir Nombres Alternos	Si se selecciona esta opción, los nombres alternos que tenga el certificado de la autoridad se replicarán en el certificado del usuario como nombres alternos de la autoridad.
<i>Sujeto</i>		Los nombres alternos del sujeto son "etiquetas" distintas del "nombre común" que se asignan al poseedor de un certificado. Recordemos que un certificado puede ser para un equipo ó un site.

Tabla 3.14 Parámetros de Nombres Alternos/Identificadores (Continuación)

Nombre de la Extensión	Atributos	Descripción
	Nombre DNS	Es el nombre del equipo por el que lo localiza un DNS.
	Dirección IP	Es la IP asignada al equipo.
	Principal Name	Indica el “nombre principal” como se define en Kerberos (RFC 1510)
	Microsoft UUID: (NTDS_REPLICATION)	Es el Identificador universal único (UUID) asignado a un proceso ó equipo.

5. Haga clic en la pestaña Identificadores para que se presente la siguiente ventana. (Figura 3.44).



Figura 3.44 Identificadores

Indique los parámetros correspondientes, como se indica en la Tabla 3.15.

Tabla 3.15 Parámetros de Identificadores

Nombre de la Extensión	Atributo	Descripción
<i>Authority Key Identifier</i>		En ocasiones es útil incluir en los certificados de los usuarios información característica del certificado la autoridad que lo emitió, como por ejemplo: la digestión de la llave pública, los Nombres completos que la describen y/o el número de serie.
	Incluir Identificador de Llave	Si se selecciona esta opción, se incluye la digestión de la llave pública de la autoridad.
	Incluir NAMES	Si se quieren incluir los nombres de la autoridad en la extensión que identifica al emisor, se debe seleccionar esta opción.
	Incluir Número de Serie	Seleccionando esta opción se incluye el número de serie del certificado de la autoridad.
<i>Subject Key Identifier</i>		Es un identificador único de 20 bytes asignado a la llave pública contenida en el certificado. Los 20 bytes pueden ser calculados como lo indica el RFC3280 (incluyendo sólo los bits de la llave pública) ó como lo calcula Microsoft (incluyendo el algoritmo de la llave pública). Seleccione el correspondiente.

6. Haga clic en la pestaña Políticas para que se presente la siguiente ventana que permite indicar los datos de la extensión Certificate Policy Statement. (Figura 3.45).

Figura 3.45 Políticas

En caso de incluir la extensión CPS, el usuario debe proporcionar el identificador y al menos uno de los campos restantes.

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.16.

Tabla 3.16 Parámetros de Configuración de las Políticas

Nombre de la Extensión	Atributos	Descripción
<i>Políticas del Certificado</i>		Las políticas de un certificado se refieren a las políticas de emisión y uso a los que se debe apegar un certificado. Las políticas se pueden publicar en un site en internet y adicionalmente se puede poner un resumen de no más de 200 caracteres que sea incluido en el certificado.
	Incluir CPS	Si desea que el certificado contenga las políticas de certificación, seleccione esta opción.

Tabla 3.16 Parámetros de Configuración de las Políticas (Continuación)

Nombre de la Extensión	Atributos	Descripción
	Agregar a la extensión configurada en SeguriServer	Si en el servicio de SeguriServer se configuraron políticas de certificación y se selecciona esta opción, estas políticas se agregarán a las configuradas en SeguriServer.
	Reemplazar la Extensión	El seleccionar esta opción substituirá el URL y/o texto de la política que está configurada en SeguriServer por la que provea el administrador.
	URL	Es una URL donde se encuentra publicada la política de certificación. El objetivo es que sea legible para una persona que acepta el certificado
	Texto	Es un texto breve que resume la política de certificación. Su objetivo es que alguien que no tenga acceso a internet ó no quiera ir a ver la política completa en internet, tenga una idea básica de las políticas de certificación.

7. Haga clic en la pestaña CRL/OCSP para que se presente la siguiente ventana que permite indicar las extensiones CRL Distribution Point y Authority Info Access. (Figura 3.46).

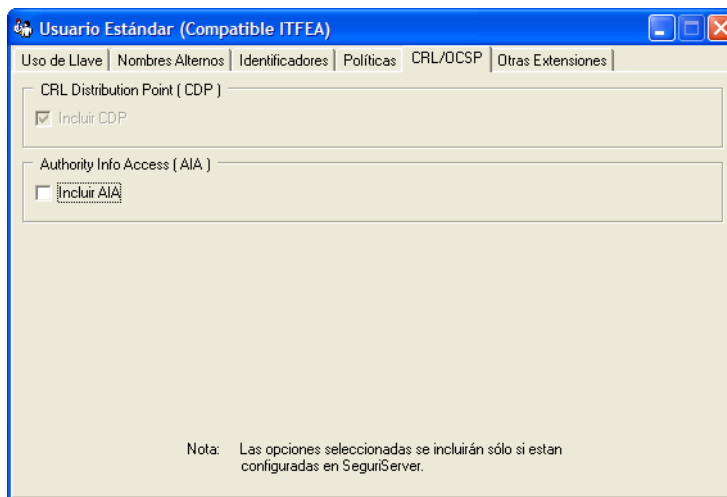


Figura 3.46 CRL/OCSP

En caso de incluir la extensión CDP, el usuario debe proporcionar al menos un campo de los que se solicitan.

En caso de incluir AIA, el usuario debe proporcionar al menos un campo de los que se solicitan.

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.17.

Tabla 3.17 Parámetros de Configuración del CRL/OCSP

Nombre de la Extensión	Atributos	Descripción
<i>CRL Distribution Point (CDP)</i>	Incluir CDP	Esta extensión indica a las personas y aplicaciones que acepten el certificado dónde pueden consultar un CRL donde eventualmente aparecería si el certificado está revocado o no. Marque esta casilla si desea incluir CDP en el certificado.
<i>Authority Info Access (AIA)</i>		Esta extensión indica URLs donde se encuentran servicios que puede dar la Autoridad emisora del certificado.

Tabla 3.17 Parámetros de Configuración del CRL/OCSP (Continuación)

Nombre de la Extensión	Atributos	Descripción
	Incluir AIA	Marque esta opción si desea incluir AIA en el certificado.

8. Haga clic en la pestaña Otras Extensiones que presenta la siguiente ventana que permite indicar los datos de las extensiones Autoridad EDIFACT, Comentario Netscape, URL Netscape y Microsoft Enroll Certificate Template Name. (Figura 3.47).

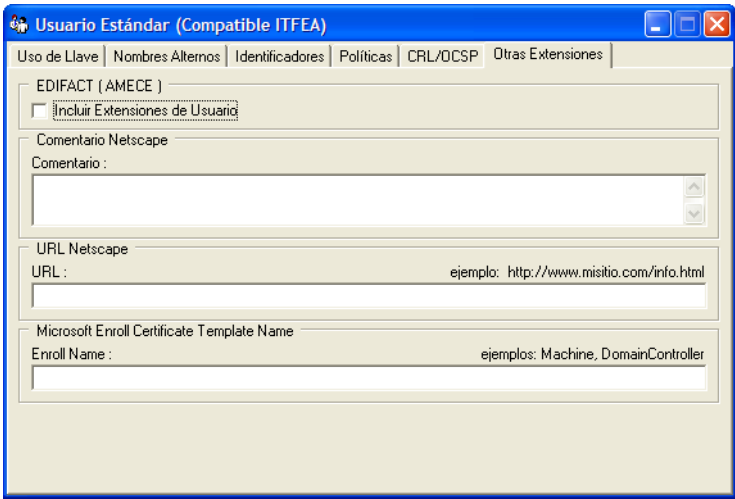


Figura 3.47 Otras Extensiones

Seleccione los parámetros correspondientes, como se indica en la Tabla 3.18.

Tabla 3.18 Parámetros de Configuración de Otras Extensiones

Nombre de la Extensión	Atributos	Descripción
EDIFACT (AMECE)		Este campo solicita que se generen las distintas extensiones (definidas por el comité de seguridad de AMECE) para señalar que el certificado que se está generando será una AC ó un usuario final y que incluya a su vez las extensiones necesarias para poder convertir el certificado X.509 a un certificado EDIFACT.

Tabla 3.18 Parámetros de Configuración de Otras Extensiones (Continuación)

Nombre de la Extensión	Atributos	Descripción
<i>Comentario/URL Netscape</i>	Incluir Extensiones de Usuarios	Indica que se incluyan las extensiones necesarias para poder hacer convertible el certificado X.509 a un certificado de EDIFACT (certificado de autoridad).
	Comentario	Estas extensiones, definida por Netscape® indican a un browser de netscape que si es solicitada información adicional del certificado muestren un comentario ó lo lleven a un url donde está publicada información al respecto del certificado.
	URL	Texto a desplegar si se solicita información del certificado.
<i>Microsoft Enroll Certificate Template Name</i>		URL a direccionar si se solicita más información del certificado.
	Enroll Name	En aplicaciones de Microsoft®, en ocasiones es necesario indicar un rol que tendrá el certificado emitido.
		El nombre del rol se debe indicar en este campo.

9. Haga clic en la pestaña Permisos del Agente, para definir las capacidades de operación del Agente. (Figura 3.48).

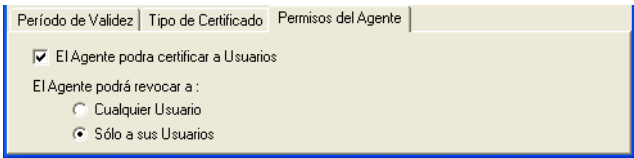


Figura 3.48 Permisos del Agente

Existen tres perfiles posibles, los cuales se describen en la Tabla 3.19.

Tabla 3.19 Permisos del Agente

El permiso ...	permite ...	y se selecciona con ...
No Certificar y Revocar a cualquier usuario	únicamente transmitir peticiones de revocación a la autoridad certificadora, sin importar el agente que lo haya solicitado originalmente.	<input type="checkbox"/> El Agente podrá certificar a Usuarios <input checked="" type="radio"/> Cualquier Usuario

Tabla 3.19 Permisos del Agente (Continuación)

El permiso ...	permite ...	y se selecciona con ...
Certificar y Revocar a cualquier usuario	solicitar certificados a la autoridad certificadora y transmitir peticiones de revocación a la autoridad, sin importar el agente que lo haya solicitado originalmente.	<input checked="" type="checkbox"/> El Agente podrá certificar a Usuarios <input checked="" type="radio"/> Cualquier Usuario
Certificar y Revocar solo a sus usuarios	solicitar certificados a la autoridad certificadora y transmitir peticiones de revocación de certificados que él haya solicitado originalmente.	<input checked="" type="checkbox"/> El Agente podrá certificar a Usuarios <input checked="" type="radio"/> Sólo a sus Usuarios

Una vez que se han definido todos los parámetros, haga clic en el botón Generar Certificado.

/ Importante

En la ventana Administración de Agentes, siempre se mostrarán los Agentes registrados en la autoridad certificadora, mostrando su situación y atributos.

3.6.2 Eliminar Agentes Certificadores

La eliminación de un agente para impedir que siga interactuando con la autoridad certificadora, consiste en la revocación de su certificado. Una vez que se ha revocado el certificado de un Agente Certificador, las peticiones subsecuentes de ese agente serán ignoradas por la autoridad certificadora de SeguriServer.

Para llevar a cabo este proceso, seleccione el certificado del Agente a revocar y haga clic en la opción Revocar Agente del menú. (Figura 3.49).

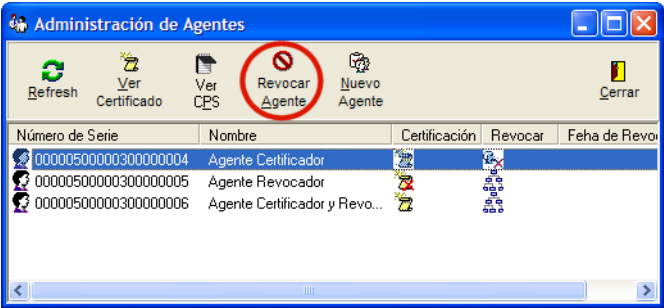


Figura 3.49 Revocar Agente

Warning

El proceso de revocación de un certificado de agente **NO** es reversible. Para reactivarlo, será necesario crear un nuevo requerimiento y agregarlo como un nuevo agente certificador.

Se presentará la siguiente ventana solicitando la confirmación de la revocación. (Figura 3.50).

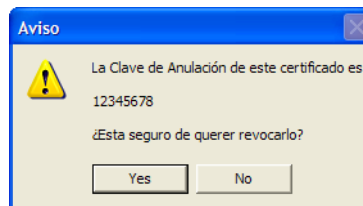


Figura 3.50 Confirmación de Revocación

3.6.3 Consulta de Certificados de Agentes Certificadores

Para consultar el detalle de un certificado de un agente, selecciónelo y haga clic en la opción Ver Certificado del menú. (Figura 3.51).

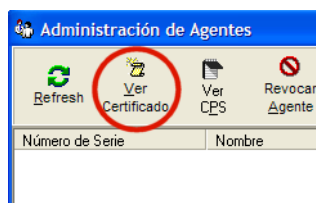


Figura 3.51 Ver Certificado

La información aparecerá en una nueva ventana en donde se podrá Guardar la información en un archivo o Imprimir los datos mostrados. Una vez que se haya consultado, deberá de hacer clic en el botón Cerrar para regresar a la ventana anterior.

Importante

Si consulta el certificado de un Agente que ha sido revocado, sólo aparecerá un cuadro de diálogo con la fecha y hora en que fue revocado.

3.7 Obtención de CRLs

Los CRLs son listas de certificados revocados de usuarios. Las listas son generadas por la autoridad certificadora y se descargan a un archivo a petición del administrador.

Para realizar estas operaciones, haga clic en el botón CRL de la consola de Administración. (Figura 3.52).



Figura 3.52 Opción CRL

A continuación se presentará la siguiente ventana. (Figura 3.53).

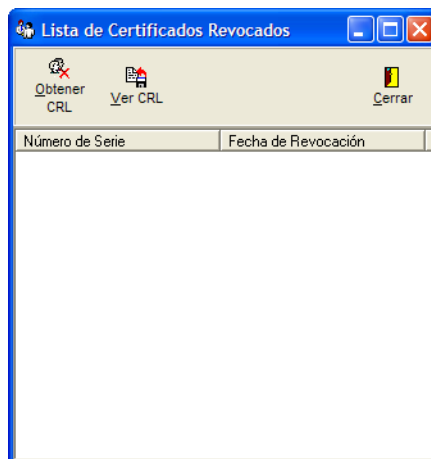


Figura 3.53 Obtener CRL

Para descargar una CRL, haga clic en la opción Obtener CRL del menú. Se presentará un mensaje indicando que se está generando la CRL y después se mostrará el selector de archivos para indicar el nombre y ruta del archivo donde se guardará la lista. Haga clic en el botón Save.

Al terminar, se presentará el contenido de la lista de certificados revocados con su número de serie y fecha de revocación.

3.7.1 Consulta de CRLs

La CRL que se ha descargado y guardado en archivo, puede ser consultada en cualquier momento, sin necesidad de acceder a la autoridad certificadora nuevamente, desde la ventana de manipulación de CRLs.

Para ver el detalle de una CRL, haga clic en el botón Ver CRL del menú. (Figura 3.54).

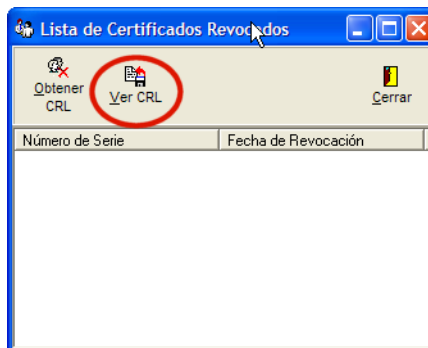


Figura 3.54 Ver CRL

Se presentará el selector de archivos que permite localizar el archivo que contiene la CRL.

Importante

Es recomendable que el proceso de generación se realice justo después de haber revocado certificados, con la finalidad de contar con la relación más actualizada en todo momento.

3.8 Configuración

Los parámetros de acceso a la consola y comunicaciones con la autoridad certificadora se pueden modificar accediendo a la opción de Configuración, de la consola de administración de SeguriServer. (Figura 3.55).



Figura 3.55 Configuración

3.8.1 Parámetros de Acceso a la Autoridad Certificadora

Para modificar los parámetros de SeguriServer, seleccione la carpeta SeguriSERVER. (Figura 3.56).

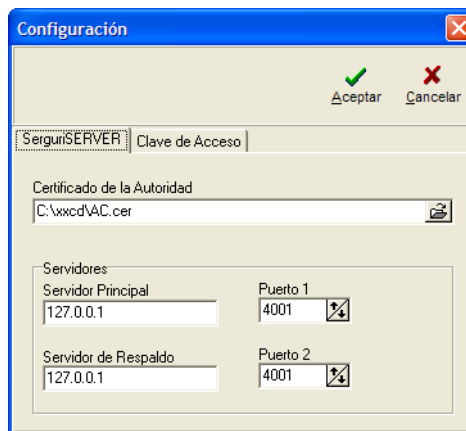


Figura 3.56 Configuración de SeguriServer

Los parámetros que se pueden modificar son:

1. Certificado de la Autoridad. Es el archivo que contiene el certificado de la autoridad certificadora. Indique la ruta y el nombre del archivo que contiene el certificado de la autoridad.
2. Servidor Principal. Es la dirección IP a través de la cual se accede a la autoridad certificadora.
3. Puerto 1. Es el puerto de comunicaciones habilitado para conectarse con la autoridad certificadora.
4. Servidor de Respaldo. Bajo un esquema de alta disponibilidad, es la dirección del servidor alternativo en donde se encuentra la autoridad certificadora en caso de que el equipo del Servidor Principal falle. Si la autoridad certificadora no funciona en una infraestructura de este tipo, entonces su valor deberá ser el mismo que el de Servidor Principal.
5. Puerto 2. Es el puerto de comunicaciones habilitado para conectarse con el Servidor de Respaldo de la autoridad certificadora.

Al terminar de realizar los cambios, haga clic en el botón Aceptar.

3.8.2 Parámetros de Acceso a la Consola de Administración

Para cambiar la clave de acceso con la cual se ingreso a la aplicación, seleccione la carpeta Clave de Acceso. (Figura 3.57).



Figura 3.57 Cambio de Clave de Acceso

Los parámetros que se pueden modificar son:

1. Clave de Acceso Anterior. Es la clave con que se accedió a la consola de administración.
2. Nueva Clave de Acceso. Es la nueva clave que se desea asignar para controlar el acceso a la consola de administración.
3. Confirmar Clave de Acceso. Es la misma clave del campo anterior y sirve de confirmación para la nueva clave de acceso.
4. Llave Privada. Es el archivo que contiene la llave privada del administrador de la autoridad certificadora. Debe especificarse su ubicación completa (directorio y nombre).

Una vez que haya modificado estos campos, haga clic en el botón Cambiar Clave de Acceso para guardar los cambios realizados.

Al terminar de realizar los cambios, haga clic en el botón Aceptar, para regresar a la consola de administración.

APÉNDICE A

Uso de PKCS12

PKCS12 es una aplicación que permite agrupar la clave de acceso, el certificado, la llave privada y el certificado de la autoridad certificadora (opcional), en un solo archivo.

Para acceder a esta aplicación seleccione el menú:

Start > Programs > SeguriData > SeguriServer > PKCS12

A continuación se presentará la siguiente ventana. (Figura A.1).

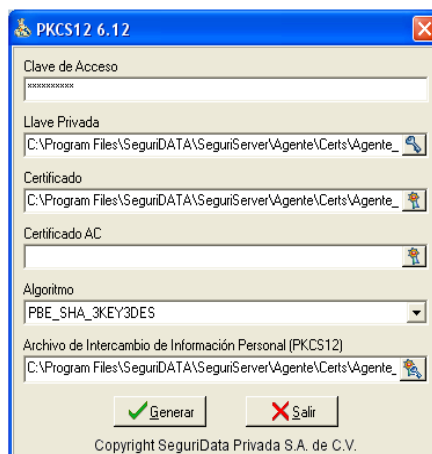






Figura A.1 Datos Solicitados

Indique los datos que se solicitan, como se muestra en la Tabla A.1

Tabla A.1 Datos del Certificado

Campo	Descripción
Clave de Acceso	Indique la clave de acceso a la llave privada.

Tabla A.1 Datos del Certificado

Campo	Descripción
Llave Privada	Haga clic en el icono  para localizar la llave privada con extensión .key.
Certificado	Haga clic en el icono  para localizar el certificado con extensión .cer.
Certificado AC	Haga clic en el icono  para localizar el certificado de la Autoridad Certificadora que generó el certificado del campo anterior.
Algoritmo	Seleccione el algoritmo correspondiente: PBE_SHA_3KEY3DES: PBE_SHA_40BIT_RC2_CBC PBE_SHA_128_BIT_RC2_CBC
Archivo de Intercambio de Información Personal (PKCS12)	Haga clic en el icono  para indicar la ruta y el nombre del archivo PKCS12 a generar.

A continuación, haga clic en el botón *Generar*.

Por último se presentará un mensaje con el resultado del proceso. (Figura A.2).

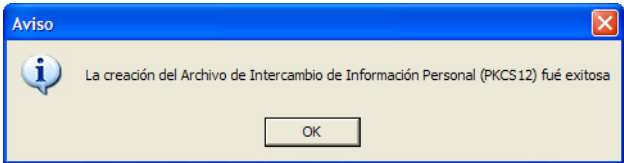


Figura A.2 Mensaje