SeguriServer versión 6.12

Manual de Agente

Revisión 1.0

SeguriData

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

Número de Parte: SeguriServer_Agente

Contenido

Capítulo 4. La Consola del Agente Certificador

Capítulo 5. El Módulo de Administración de Certificados

Capítulo 6. El Módulo de Ejecutivos de Registro

Capítulo 7. El Módulo de Requerimientos de Certificación

Capítulo 8. El Módulo de Administración Remota

Capítulo 9. Módulo de CRL

Capítulo 10. Módulo de Configuración

CAPÍTULO 1

¿Cómo utilizar este manual?

1.1 Organización de este manual

El Manual del Agente Administrador está orientado al personal que operará la Autoridad Certificadora de SeguriServer, a través de la aplicación del Agente Certificador 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.

1.2.2 Tipografía

Las convenciones tipográficas utilizadas a lo largo del manual indican tanto la fuente como el uso de los datos que aparecen bajo ese estilo.

El texto que aparezca con el tipo de letra *usuario*, deberá de introducirse tal cual aparece en el manual, en la interfaz que se esté utilizando en ese momento.

Los textos que se muestren como:

comando <*parámetro 1*>,[,<*parámetro 2*>] <parámetro 3>

denotarán la sintaxis de un comando. La palabra **comando**, se deberá escribir tal como aparece, en tanto que <*parámetro 1*> y <*parámetro 2*> se deberán de sustituir por valores que dependen del proceso que se realiza. El <parámetro 3> corresponde a un texto que se debe usar literalmente como aparece en la sintaxis.

Los símbolos < y > delimitarán el nombre del parámetro a que se haga referencia, requerida en el comando.

El uso de los paréntesis [y] se usarán para denotar la parte del comando que es opcional.

La sintaxis

[, <*parámetro 2*> …]

en un comando indica que se podrán agregar tantos parámetros como sea necesario

{ <*valor 1*> | <*valor 2*> | ... | <*valor n*> }

e indicará que se deberá usar solamente uno de los *n* valores listados entre las llaves.

Finalmente, para indicar los términos que se usan por primera vez o que están en otro idioma, se usará letra *cursiva*.

1.2.3 Acciones bajo la interfaz de usuario

Al interactuar con la interfaz de usuario, el acceso a los diversos menues se denotará como una secuencia de las opciones que se deben seleccionar, separadas por un símbolo triangular (») que indica el paso al siguiente nivel de submenú. Por ejemplo, para indicar que se debe seleccionar la opción Page Size … que se encuentra en el submenú Page Layout y éste a su vez se encuentra en el menú Format, se indicará como:

Format » Page Layout » Page Size …

El acceso a los menues se puede realizar con combinaciones de teclas y seleccionando la opción con la tecla [Return] o [Enter], o bien puede seleccionar con ayuda del puntero del ratón, en cuyo caso la selección se hará oprimiendo el botón izquierdo del ratón cuando el puntero se encuentre sobre la opción deseada.

A esta última forma de seleccionar una opción se le referirá como hacer *clic* sobre la opción.

CAPÍTULO 2

Documentos Digitales Seguros

2.1 Implicaciones del uso de documentos digitales

Las nuevas tecnologías han modificado radicalmente la manera en que se desarrollan algunas actividades cotidianas y con ello han agregado complejidad a todos los procesos, puesto que el intercambio de información se ha convertido en uno de los puntos críticos de esta nueva tendencia. Los conceptos de oficinas sin papel han surgido, basándose en el empleo de medios electrónicos, como una forma de sustituir documentación impresa o bien para agilizar trámites, simplificando los documentos impresos requeridos.

Este proceso no sería posible si no existieran medios confiables para transmitir volúmenes de información, lo cual se ha resuelto satisfactoriamente por medio de la tecnología disponible hoy en día, tal como se puede observar con las redes privadas o Internet.

Sin embargo, bajo este modelo surgen otros riesgos relacionados con el uso que se le puede dar a los medios, más que a los riesgos de corrupción de datos en la transmisión misma.

Cuando un grupo de usuarios comparte un canal de comunicación común y éste se usa para enviar información o documentos, hay escenarios adversos que se pueden presentar, por ejemplo:

- Es posible trasmitir información a alguno de los usuarios que comparten el canal y no hay certeza de que el destinatario esté presente al momento de recibirla, creando el riesgo de que una persona no autorizada obtenga información confidencial.
- Alguna persona distinta al destinatario puede interceptar la información que viaja en el canal de comunicación, permitiéndole modificar u ocultar la información antes de que llegue a su destinatario legítimo.
- Cuando una persona recibe información de otra, que tiene acceso al canal común, no cuenta con alguna forma de asegurar que el emisor es verdaderamente quien aparece como remitente de dicha información.

Ante este panorama, se hace indispensable contar con mecanismos que permitan garantizar el correcto aprovechamiento de los medios de enlace.

En los documentos impresos, existen ciertas características que nos permiten confiar en ellos, ya sea porque están sellados, firmados o porque presenciamos su elaboración y eso nos permite considerarlos como auténticos.

Estas características serían deseables en el caso de los documentos electrónicos, enfatizando principalmente cuatro aspectos:

- Confidencialidad. El documento debe ser visto solamente por el destinatario.
- Autenticidad. El documento debe ser emitido por un usuario legítimo del canal de comunicación.
- Integridad. El documento debe llegar a su destinatario sin alteraciones, tal como fue creado por el emisor.
- No repudio de la información. El documento debe contener testimonio de que fue realizado por el emisor ante terceros, sin posibilidad de que el emisor del documento niegue su responsabilidad.

Esta problemática se puede resolver mediante el uso de la *Criptografía*, que es una rama de las matemáticas que se puede aplicar a los documentos electrónicos, proporcionando las herramientas idóneas para solucionar la problemática descrita.

Al problema de la confidencialidad, se le relaciona comúnmente con las técnicas denominadas de *encripción* y al problema de la autenticidad se le resuelve mediante técnicas denominadas de firma digital, que en resumen se reducen a procedimientos criptográficos de encripción y *desencripción*.

2.2 Generación de llaves de encripción

Para llevar a cabo el proceso de *encripción* y *desencripción* de un documento digital, es necesario crear el medio para que las personas autorizadas puedan acceder la información contenida en él.

A mediados de la década de los setenta, se encontró la forma de transformar un bloque de información a través del uso de un código y revertir luego este proceso por medio de otro. Ambos códigos, no son otra cosa que un par de números muy grandes, relacionados entre sí y que comparten algunas propiedades matemáticas.

A este mecanismo se le llamó *Criptografía de Llave Pública*; dentro de las cuales, la más conocida se denomina *RSA*.

Para la aplicación de esta técnica, con ayuda de un programa de cómputo se calculan un par de números matemáticamente relacionados a los cuales se les denomina llaves. A estas llaves se les puede conceptualizar como un mensaje digital, un archivo o una secuencia de bits o bytes.

A uno de estos números se le denomina llave privada y al otro llave pública.

Por la forma en que se calculan, cuando estas llaves se generan en parejas, se relacionan de tal forma que para dos llaves públicas distintas, sus llaves privadas correspondientes serán diferentes.

Para el usuario, esto se traducirá en que su llave privada deberá mantenerse en secreto y su llave publica podrá darse a conocer sin mayor problema.

> **Importante**
>
> Puesto que la llave privada compromete a su propietario en el sentido de que lo hace responsable de ser el originador de un documento de manera ineludible, es de suma importancia que solamente el propietario tenga acceso a ella.

A partir del momento en que se cuenta con las llaves, es posible realizar varios procesos que nos permiten:

- Garantizar la autenticidad, integridad y el no repudio de la información, a través de las firmas digitales, y
- Garantizar la confidencialidad de los documentos digitales a través de la encripción de los documentos.

2.3 Firma digital de documentos digitales

La firma digital tendrá por objetivo generar un mensaje digital a partir del documento que se desea firmar y de la llave privada del emisor del documento. Al documento y a su firma, en conjunto se les llamará documento firmado.

> **Importante**
>
> A diferencia de la firma autógrafa, por la manera en que se genera la firma digital para dos documentos diferentes cualesquiera, las firmas digitales correspondientes serán distintas. Este hecho impide que la firma de un documento se trate de usar con un documento distinto. De la misma forma, si dos personas firman un mismo documento, las firmas digitales serán diferentes.

2.4 Autenticación de documentos

Al firmar los documentos digitales, se ha resuelto una parte de la problemática, puesto que existe una prueba de que el emisor del documento, realmente lo respalda al firmarlo con su llave privada.

La segunda parte del proceso tiene lugar cuando otra persona recibe el documento y necesita asegurarse de que el emisor es la persona que firma. A este proceso se le llama autenticación.

Para realizar la autenticación de un documento, se utiliza un programa de cómputo que se alimenta del documento firmado y la llave pública del supuesto firmante; con esta información, el programa indicará si es auténtico o no lo es.

En el caso de que el documento o la firma hayan sido alterados, por mínimo que sea el cambio, el resultado será que el documento no es auténtico.

De este último proceso, encontramos que para comprobar el origen del documento, así como su integridad, requerimos de la llave pública del emisor del documento. Esto tiene serias

implicaciones puesto que al crecer el número de personas con las que se intercambian documentos, resulta más difícil controlar las llaves en que se puede confiar.

Una solución para este problema se encuentra en los certificados digitales.

2.5 Certificados Digitales

El certificado digital es en sí un documento que está firmado por una persona o entidad llamada *Autoridad Certificadora* (AC). Este documento establece una liga entre una persona y su llave pública. En el certificado digital se encuentra la llave pública de la AC, la llave privada y el nombre de quien emite el documento.

La AC es quien garantiza que la llave pública recibida en el certificado, pertenece al sujeto que se menciona y por tanto cualquier persona que tenga el certificado de la AC puede autentificar cualquier documento emitido por el sujeto, siempre y cuando se confíe en la AC.

De la misma forma, la AC puede revocar un certificado, esto es que puede dejar de respaldar la identidad de un sujeto. La revocación puede darse por varias razones, por ejemplo:

- Si el certificado se pierde, puede revocaras y generar uno nuevo.
- Si el propietario deja de tener la responsabilidad que lo acreditaba para cierta actividad, puede restringirse, revocando el certificado.
- Si el propietario se ve involucrado en actividades que lo hagan no confiable, también puede revocarse.

Como medio de identificación, el certificado digital tiene varias características en su diseño, a saber:

- Tiene un período de vigencia que hace que se renueven las llaves, como una identificación que otorga alguna entidad a un sujeto, renovando la decisión de delegar responsabilidad a nombre de una empresa.
- Además de esta circunstancia, existe una razón técnica para que se renueven los certificados con cierta periodicidad. Con los avances tecnológicos, hay computadoras con mayores capacidades de cálculo y esto haría que el mecanismo de seguridad pudiera romperse, comprometiendo la información y responsabilidad del propietario de las llaves.
- Al generar un nuevo requerimiento, se puede aumentar gradualmente y según las necesidades del caso, el nivel de seguridad de las llaves.
- Las AC mantienen un control de los usuarios registrados certificados existentes. Cuando se autentica un documento, es posible confirmar si el certificado de el emisor del documento permanece.
- De igual manera, la AC mantiene actualizada una *Lista de Certificados Revocados* (CRL), la cual se puede consultar en cualquier momento a través de una red local o Internet.

Respecto a este último punto, la lista de certificados revocados, es firmada por la autoridad certificadora para garantizar su legitimidad y contiene información detallada sobre la fecha de revocación.

Dentro de este escenario, también puede suceder que el emisor de un documento envíe un mensaje y que quien recibe el mensaje argumente que la fecha no coincide, ya sea anterior o posterior, afectando al propósito del documento.

Esta problemática es resuelta mediante un tercero dentro del proceso, al cual se le llama *Autoridad de Oficialía de Partes* (AOP) y que tiene como función recibir mensajes, firmarlos estampando la hora y fecha y generando un recibo electrónico, que aclara cualquier disputa sobre el momento en el que se emite un documento.

2.6 Autoridades Registradoras

Cuando se crea una infraestructura de seguridad en la que existe una gran cantidad de posibles emisores de documentos digitales, el servicio de certificación de usuarios puede llegar a ser torpe debido a la demanda que tenga para la creación y revocación de certificados.

Para salvar este inconveniente, existe la figura de las *Autoridades Registradoras* (AR).

Para llevar a cabo el proceso de certificación de un usuario, el proceso inicia con la verificación de autenticidad de identidad de los usuarios.

A continuación se genera una llave privada y una llave pública a certificar, llamada requerimiento, el cual se certifica y se entrega al usuario, concluyendo el proceso de certificación.

El proceso de confirmar la identidad y recibir el requerimiento por parte del usuario, por lo general es realizado por la AR, la cual cuenta con la relación de confianza por parte de la AC y que certifica todos los requerimientos que recibe de la AR.

2.7 Encripción y desencripción de documentos

Hasta ahora, se ha detallado de que es posible asegurar la autenticidad, no repudio e integridad de documentos digitales, pero no se ha hablado acerca de la confidencialidad de los documentos digitales. Los mecanismos de firmado y generación de recibos electrónicos, cubren las necesidades para la gestión del documento en cuestión, pero es necesario asegurarnos de que los documentos sean vistos por las personas a quienes realmente se les autoriza el acceso a ellos.

La tecnología *RSA* permite utilizar un par de llaves pública y privada para encriptar y desencriptar documentos digitales, bajo un esquema de encripción asimétrica, esto es que la llave que encripta el mensaje no es la misma que se requiere para desencriptar la información.

Desafortunadamente, el algoritmo *RSA* es extremadamente sofisticado y por tanto muy lento en los procesos de encripción y desencripción de bloques grandes de información.

Dado que el algoritmo *RSA* tiene un rendimiento aceptable para bloques pequeños de información, lo que se hace es encriptar el documento con una clave de acceso diferente a las llaves pública o privada, usando un algoritmo de encripción simétrica. A continuación se encripta la clave de acceso con la llave pública usando *RSA* en esta ocasión.

Al paquete formado por: la clave de acceso encriptada con *RSA* y al documento digital encriptado simétricamente se le llama sobre digital.

Una vez que se ha ensobretado el documento, éste se envía y al recibirlo el destinatario, desencripta la clave de acceso con su llave privada y procede a desencriptar el documento digital con la clave de acceso.

El concepto de sobre digital es muy flexible, lo cual se puede confirmar en el caso de que se desee enviar un documento a varias personas. El proceso sería el mismo, solamente que en el sobre digital se incluiría la clave de acceso encriptada con cada una de las llaves públicas correspondientes a los destinatarios.

Al utilizar la llave pública en el proceso de encripción, quedan implícitas todas las propiedades antes mencionadas respecto a la autenticidad, integridad y no repudio de la información.

2.8 La función de SeguriServer

Crear una infraestructura de seguridad es una tarea sumamente compleja si no se cuenta con los programas de cómputo apropiados que automaticen todos y cada uno de los procesos descritos de manera rápida y segura. SeguriServer es una herramienta indispensable para crear una Autoridad Certificadora completa que emite y administra certificados digitales de acuerdo a sus propias necesidades.

SeguriServer cuenta con los servicios de Autoridad Certificadora, Autoridad Registradora, generador de Requerimientos y Listas de Revocación de Certificados, así como las herramientas necesarias para dar mantenimiento a su infraestructura de seguridad.

La flexibilidad y solidez de SeguriServer le permite implementarse en arquitecturas redundantes tolerantes a fallas, que es un requisito indispensable en Autoridades Certificadoras institucionales, haciéndolo la mejor alternativa para su empresa.

CAPÍTULO 3

Instalación y Configuración del Agente Certificador

3.1 Requerimientos del Sistema

Se asume que la persona que realizará la instalación es el administrador de la red o cuenta con privilegios de acceso equivalentes y cuenta con conocimientos acerca de:

- el uso de programas bajo Microsoft® Windows,
- instalación de aplicaciones de Microsoft® Windows y
- configuración de servicios de red bajo Microsoft® Windows

Los requerimientos mínimos para el Agente Certificador de SeguriServer son:

- PC con procesador Pentium II @300MHz o superior.
- 32 Mb de memoria RAM
- 8 Mb libres en disco duro
- Unidad de CD-ROM
- Unidad de disco flexible o conexión a red
- Sistema operativo Microsoft® Windows 98 o superior.
- Un puerto serial habilitado y disponible, en caso de utilizar lector de Smart Cards (Opcional).
- Un certificado creado para Agente Certificador
- El certificado de la Autoridad Certificadora con que se conectará.

Los requerimientos para Windows Server 2008 a 32 bits son:

- Memoria de 2.0 GB de RAM
- 512 MB de espacio en Disco Duro

- Cliente en Base de Datos: SQL 2008, Oracle 11g ó 10g.

Para usar la aplicación del Agente Certificador será necesario instalarlo (Sección "3.2 Instalación del Agente Certificador") y configurarlo (Sección "3.3 Configuración del Agente Certificador"). Después de que se lleven a cabo los dos procedimientos, podrá comenzar la operación del Agente Certificador.

3.2 Instalación del Agente Certificador

Para instalar la aplicación del Agente Certificador de SeguriServer, inserte el CD de distribución de SeguriServer en el lector de CD-ROM y con ayuda del explorador de archivos localice el archivo *SetupAgente610.exe*. Ejecútelo haciendo doble clic en el nombre del archivo.

El asistente de instalación mostrará una nueva ventana con la identificación del producto (Figura 3.1).

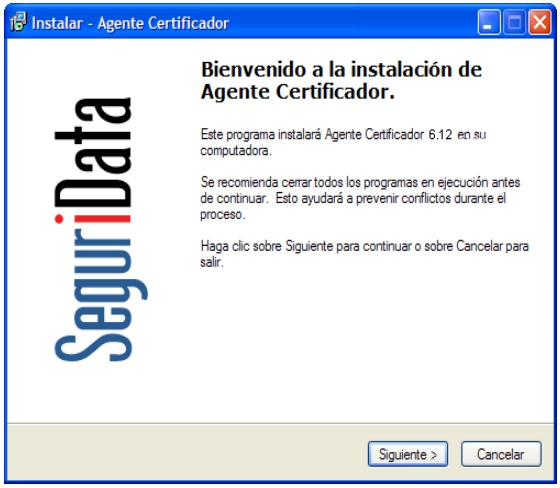

Figura 3.1 Ventana de Presentación

Para iniciar la instalación, haga clic en el botón Siguiente >.

A continuación, el asistente solicitará la ubicación en donde se instalará la aplicación del Agente Certificador. (Figura 3.2).

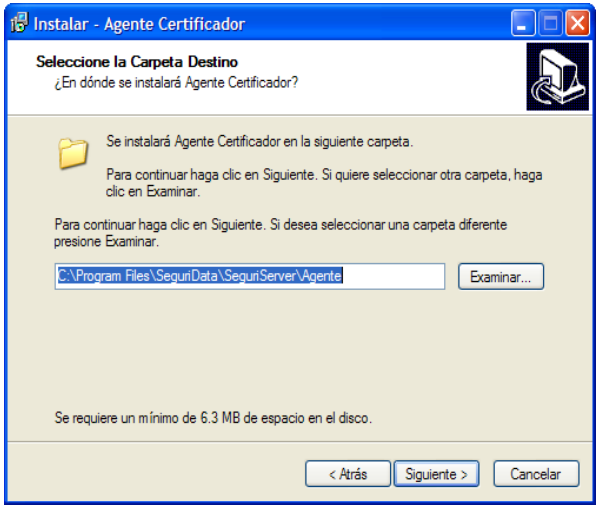

Figura 3.2 Selección de la Carpeta Destino

El valor predeterminado es el directorio:

C:\Program Files\SeguriData\SeguriServer\Agente

sin embargo puede cambiarse libremente la ubicación por otra ruta válida, sin que esto repercuta en el desempeño de la aplicación.

Para continuar con el proceso, haga clic en el botón Siguiente >.

Indique el grupo de programas bajo el que se creará el acceso a los componentes de SeguriServer bajo el menú de Microsoft® Windows. (Figura 3.3).

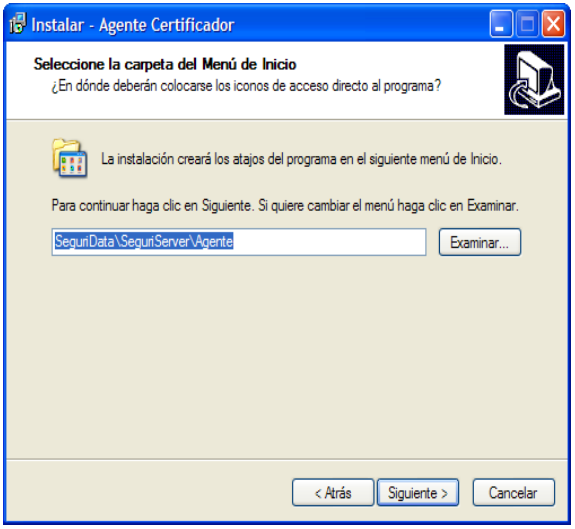

Figura 3.3 Selección de la Carpeta Menú de Inicio

Para continuar con el proceso, haga clic en el botón Siguiente >.

En el siguiente paso, se muestra un resumen de los valores seleccionados en las etapas anteriores. (Figura 3.4).

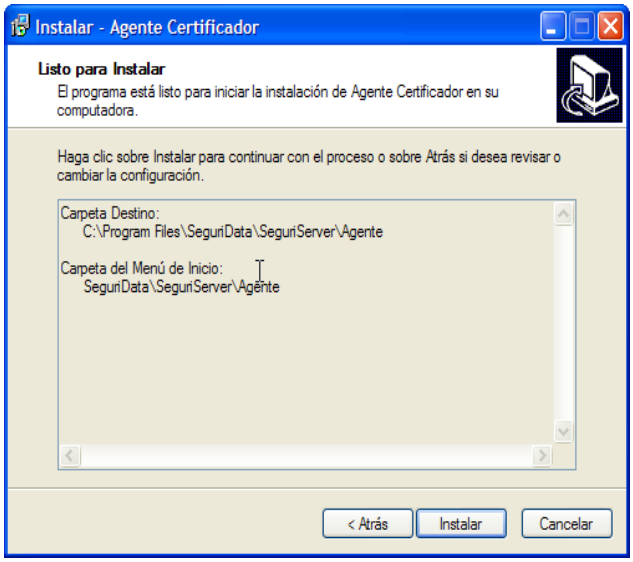

Figura 3.4 Ventana de Valores Seleccionados

Si son correctos, haga clic en el botón Instalar.

Importante

En caso de ser necesario, puede regresar a las pantallas anteriores por medio del botón < Atrás y modificar los parámetros de instalación.

El proceso de copia de archivos se iniciará y al terminar, el asistente mostrará un mensaje indicando el resultado de la instalación. (Figura 3.5).

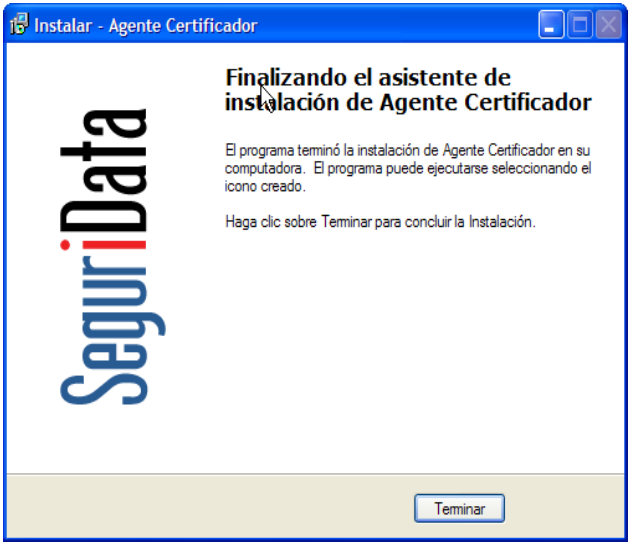

Figura 3.5 Resultado de la Instalación

El siguiente paso es configurar el Agente Certificador.

3.3 Configuración del Agente Certificador

Para acceder a la consola del Agente Certificador, deberá ejecutar la aplicación mediante:

Inicio @ Programas @ SeguriData @ SeguriServer @Agente @ Agente Certificador

En los siguientes capítulos se explicará la funcionalidad de cada opción de la consola de Administración de SeguriServer

La configuración del Agente Certificador establece la forma en que la aplicación accederá a la Autoridad Certificadora.

3.3.1 El Certificado del Agente Certificador

El Agente Certificador deberá tener un certificado emitido por la Autoridad Certificadora y registrado como Agente válido para la Autoridad.

Para este fin, es necesario crear un requerimiento de certificación con el editor de requerimientos que se instala junto con la aplicación del Agente Certificador.

3.4 Requerimiento de Certificación con ITFEA

Para crear el requerimiento deberá de ejecutar el editor de requerimientos por medio de:

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

Al iniciar, aparecerá una ventana solicitando la información que identifica al Agente, misma que tendrá que ser validada por la Autoridad Certificadora. (Figura 3.6).

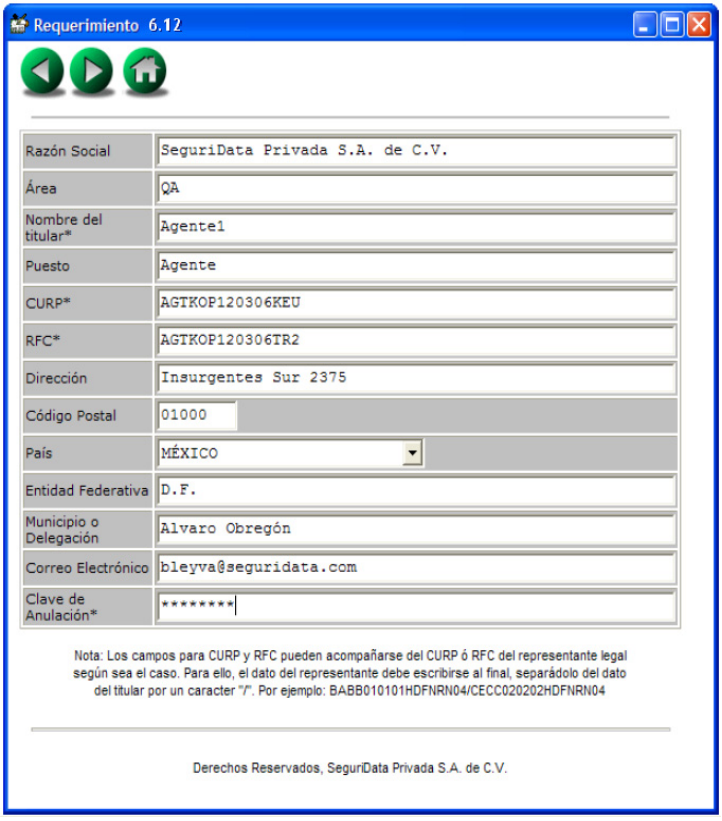

Figura 3.6 Requerimiento de Certificación

Importante

Los campos que tienen un asterisco, son obligatorios y no podrá avanzar en el proceso hasta proporcionar esa información.

Proporcione los datos que se solicitan, como se indica en la Tabla 3.1.

Tabla 3.1 Datos del Requerimiento de Certificación

Dato	Descripción
`Razón Social`	Indique el nombre de la empresa o razón social a la que pertenece el Agente.
`Area`	Indique el nombre del área a la que pertenece dentro de la empresa, el Agente.
`Nombre del Titular`	Indique el nombre del Agente.
`Puesto`	Indique el puesto que tiene el Agente en la empresa a la que pertenece.
`CURP`	Escriba el CURP del Agente. **Importante** Este campo puede ir acompañado con el CURP del representante legal, segun sea el caso. Éste deberá ir al final del CURP del Agente separado por el signo "/", por ejemplo: RETY850411HYUTES09/GTYU920622OFDERGH15
`RFC`	Escriba el RFC del Agente. **Importante** Este campo puede ir acompañado con el RFC del representante legal, segun sea el caso. Éste deberá ir al final del RFC del Agente separado por el signo "/", por ejemplo: RETY850411HYU9/GTYU920622OFDER5
`Dirección`	Indique la dirección de la empresa a la que pertenece el Agente.
`Código Postal`	Indique el código postal de la dirección anterior.
`País`	Seleccione el país a la que pertenece el Agente.
`Entidad`	Indique la entidad federativa a la que pertenece el Agente.
`Municipio o Delegación`	Indique el municipio o delegación a la que pertenece el Agente.
`Correo Electrónico`	Indique el correo electrónico del Agente.
`Clave de Anulación`	Indique la clave de anulación, la cual es requerida al momento de revocar su certificado. Ésta deberá estar conformada de al menos 8 caracteres combinados entre números y letras.

Para desplazarse en la interfaz deberá hacer clic en el botón para avanzar a la siguiente ventana, o bien si desea regresar a la anterior. Si desea salir de la interfaz sin concluir el proceso, utilice el botón con la figura .

Al terminar de introducir la información, deberá avanzar al siguiente paso.

En la siguiente ventana, se definirá el control de acceso y características de las llaves que se generarán. (Figura 3.7).

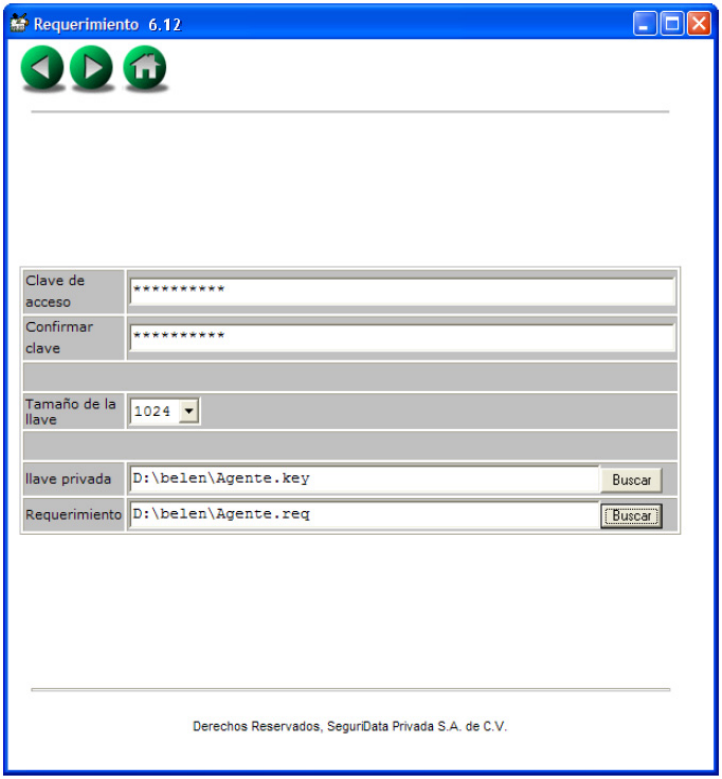

Figura 3.7 Características de la Llave Privada

Proporcione los datos que se solicitan, como se indica en la Tabla 3.2.

Tabla 3.2 Datos para Generar las Llaves

Dato	Descripción
`Clave de Acceso`	Escriba una Clave de Acceso que permitirá utilizar las llaves de encripción y el certificado una vez que éste sea generado. Ésta deberá contener una combinación de números, letras mayúsculas, letras minúsculas y espacios, con una longitud mínima de 8 caracteres y un máximo de 255.
`Confirmar Clave de Acceso`	Indique nuevamente su clave de acceso para confirmar que la escribió correctamente. **Importante** Es importante que el usuario recuerde esta clave, puesto que no existe forma de recuperarla.
`Tamaño de la LLave`	Seleccione el Tamaño de la Llave, que puede ser de 512, 1024 o 2048 bits de longitud. Entre más grande sea, mayor será el nivel de seguridad para sus llaves. Se recomienda que usen 1024 bits puesto que representa un buen nivel de seguridad, sin que los procesos de encripción, desencripción, autenticación, etc. requieran mucho tiempo.
`Llave Privada`	Haga clic en el botón Buscar para indicar la ruta y el nombre del archivo (.Key) donde se guardará la Llave Privada.
`Requerimiento`	Haga clic en el botón Buscar para indicar la ruta y el nombre del archivo donde se guardará el Requerimiento (.Req).

Una vez introducidos estos datos, deberá avanzar al siguiente paso, en el que aparecerá un mensaje indicando que el proceso de generación de números aleatorios requeridos para crear las llaves dará inicio. (Figura 3.8).

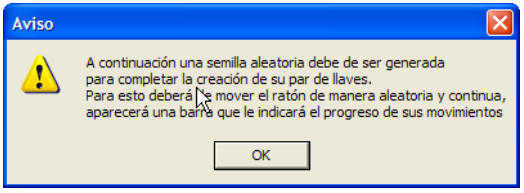

Figura 3.8 Aviso

Debido a la limitación de las computadoras para generar números verdaderamente aleatorios, se requerirá la intervención del usuario para introducir condiciones variables cada vez que se realice este proceso. Aparecerá una ventana alargada horizontalmente y al mover el ratón se

mostrará una barra de avance en color azul. Se deberá mover el ratón sin un patrón en particular hasta completar el proceso. (Figura 3.9).

Figura 3.9 Avance

Al terminar, se mostrará un mensaje indicando que el proceso ha finalizado. (Figura 3.10).

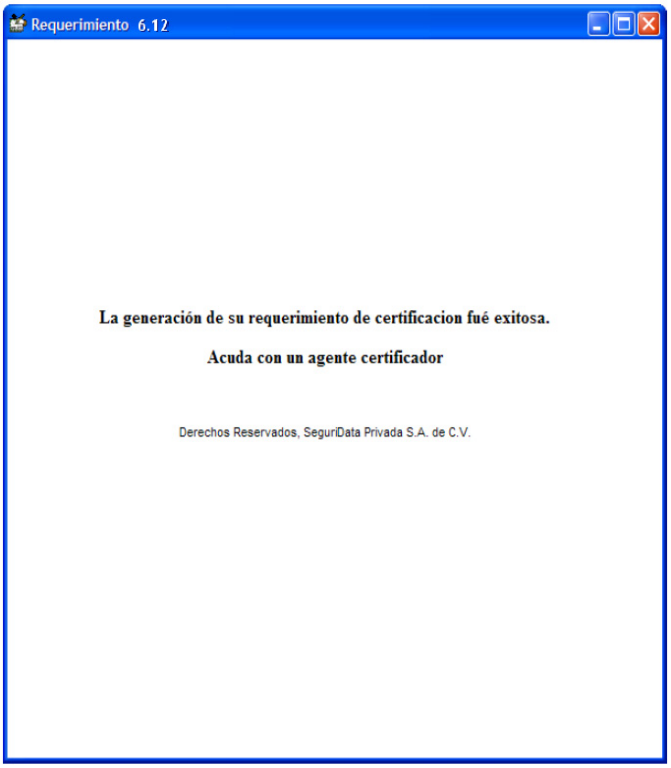

Figura 3.10 Resultado de la Generación del Requerimiento

Dependiendo de las políticas de cada autoridad, se hará llegar por el medio apropiado el archivo con extensión *.req* a la Autoridad Certificadora para que se genere el certificado correspondiente.

> **Importante**
>
> Es importante guardar la llave privada (*.key*) en un lugar seguro, puesto que sin ella no se podrá realizar ninguna operación.

Al recibir el certificado, podrá acceder a la aplicación del Agente Certificador.

3.5 Requerimiento de Certificación sin ITFEA

También existe otro tipo de requerimiento sin ITFEA, en el cual los campos obligatorios para la generación del requerimiento son los siguientes: (Figura 3.11).

- Razón Social
- Nombre del Titular
- Correo Electrónico

- Clave de Anulación

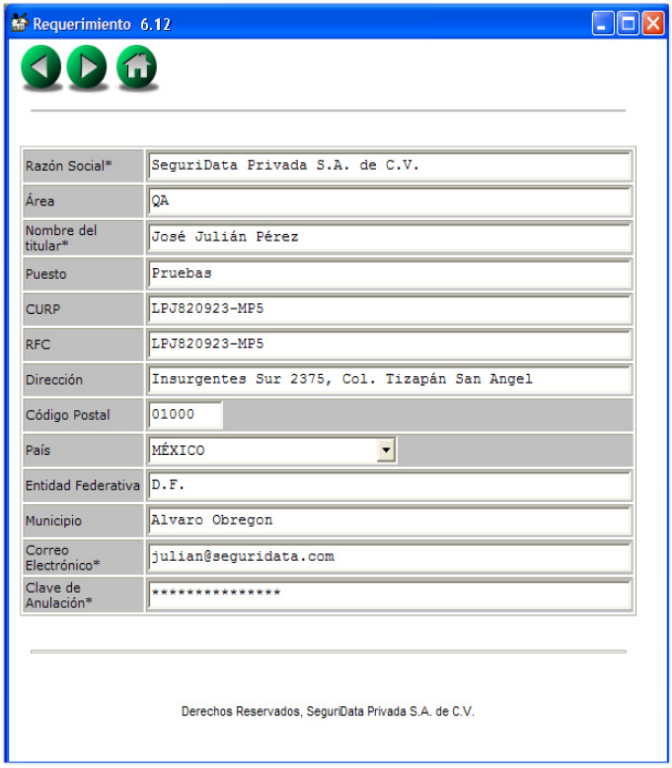

Figura 3.11 Requerimiento sin ITFEA

3.5.1 Parámetros del Agente Certificador

Cuando se ejecuta por primera vez la aplicación, se presentará la siguiente ventana de configuración. (Figura 3.12).

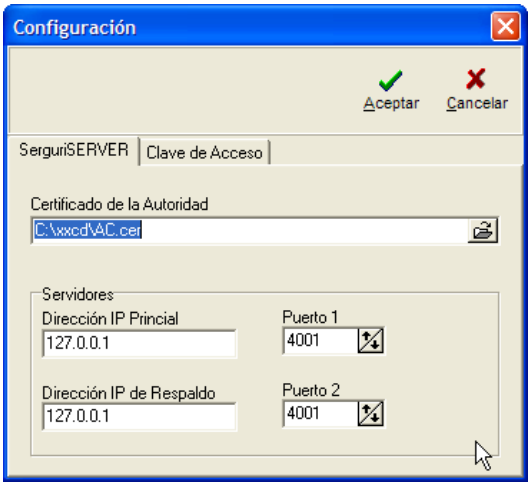

Figura 3.12 Ventana de Configuración

Estos parámetros se refieren a la ubicación del certificado de la AC y al enlace de comunicación con ella.

Los parámetros configurables se indican en la Tabla 3.3.

Tabla 3.3 Parámetros configurables del Agente Certificador

El parámetro …	es …
Certificado de la Autoridad	la ubicación del certificado de la Autoridad Certificadora.
Servidor Principal	la dirección IP a través de la cual se accede a la Autoridad Certificadora.
Puerto 1	el puerto de comunicaciones asociado a la IP del parámetro anterior.
Servidor de Respaldo	es la dirección IP del servidor alternativo, bajo un esquema de alta disponibilidad, en donde se encuentra la réplica de la Autoridad Certificadora que atenderá peticiones en caso de que el equipo del Servidor Principal 1 presente alguna falla. Si la Autoridad Certificadora no funciona en una infraestructura de este tipo, entonces se deberá asignar el mismo que el de Servidor Principal 1.

Tabla 3.3 Parámetros configurables del Agente Certificador

El parámetro ...	es ...
Puerto 2	Es el puerto de comunicaciones asociado a la IP del parámetro anterior.

Warning

Al terminar de realizar los cambios, haga clic en el botón Aceptar, de lo contrario los cambios realizados se perderán.

3.6 Cambio de Clave de Acceso

Como parte de las políticas de seguridad recomendadas en una infraestructura de seguridad, está la de cambiar frecuentemente las claves de acceso. La aplicación del Agente Certificador permite cambiar la llave de acceso de su certificado en el módulo de Configuración, haciendo clic en la carpeta Clave de Acceso. (Figura 3.13).

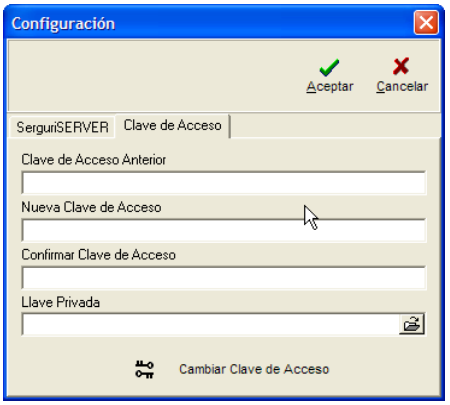

Figura 3.13 Configuración de la Clave de Acceso

El procedimiento para cambiar la Clave de Acceso se indica en la Tabla 3.4.

Tabla 3.4 Procedimiento para cambiar la Clave de Acceso

Paso	Acción
1	Indique la Clave de Acceso Anterior.
2	Escriba la nueva contraseña en el campo Nueva Clave de Acceso y confirmarla en Confirmar Clave de Acceso.
3	Si la Llave Privada del Agente Certificador cambió de ubicación, indicarla en el campo Llave Privada.
4	Hacer clic en el botón Cambiar Clave de Acceso.

CAPÍTULO 4

La Consola del Agente Certificador

La Consola del Agente Certificador es el medio para acceder a las funciones que ofrece la Autoridad Certificadora de SeguriServer.

4.1 Acceso a la Aplicación

Para acceder a la consola del Agente Certificador de SeguriServer, es necesario ejecutar la aplicación a través de:

Inicio < Programas < SeguriData < SeguriServer < Agente < Agente Certificador

Al iniciar la aplicación, aparecerá una ventana que controlará el acceso a la consola de administración. (Figura 4.1).

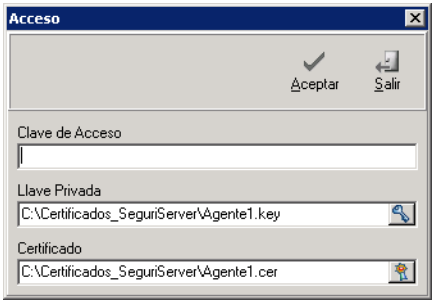

Figura 4.1 Ventana de Acceso

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 del Agente Certificador. (Figura 4.2).

Figura 4.2 Consola del Agente Certificador

4.2 Modos de Acceso a la Consola

Un Agente Certificador puede tener distintos permisos al interactuar con la Autoridad Certificadora, mismos que se definen al momento de crear el certificado del Agente.

Existen tres variantes y en términos de estas capacidades, la Consola del Agente Certificador deshabilitará aquellos módulos a los que no tiene acceso.

Cada uno de los módulos mantiene su funcionalidad independientemente del tipo de Agente que los accede, por ejemplo, el módulo de Administración Remota será siempre el mismo pero para algunos perfiles no estará disponible.

4.2.1 Agente Certificador de Revocación Local

Este perfil solamente permite revocar certificados, independientemente de que hayan sido solicitados por él o por otro Agente Certificador.

La Consola del Agente certificador sólo presentará las opciones:

- *Administración Remota*
- *CRL*
- *Configuración*

4.2.2 Agente Certificador para Certificación

En este caso, el Agente puede gestionar certificados y revocar los que hayan sido solicitados por él. En ningún caso podrá revocar certificados gestionados por otro Agente Certificador.

También se le permite definir los Ejecutivos de Registro de quienes recibirá requerimientos de usuario final.

La Consola del Agente certificador sólo presentará las opciones:

- *Certificados*
- *Ejecutivos de Registro*
- *Requerimientos de Certificación*
- *CRL*

- *Configuración*

4.2.3 Agente Certificador para Certificación y Revocación

Este perfil permite realizar todas las operaciones posibles para un Agente Certificador: gestión de certificados, revocación de certificados emitidos por cualquier Agente y definición de Ejecutivos de Registro.

La Consola del Agente certificador presentará todas las opciones, como se muestra en la Figura 4.3.

Figura 4.3 Opciones del Agente Certificador para Certificación y Revocación

Las opciones son:

- *Certificados*. Ver Capítulo 5 ” El Módulo de Administración de Certificados” en la página 5-1
- *Ejecutivos de Registro*. Ver Capítulo 6 ” El Módulo de Ejecutivos de Registro” en la página 6-1
- *Requerimiento de Certificación*. Ver Capítulo 7 ” El Módulo de Requerimientos de Certificación” en la página 7-1
- *Administración Remota*. Ver Capítulo 8 ” El Módulo de Administración Remota” en la página 8-1
- *CRL*. Ver Capítulo 9 ” Módulo de CRL” en la página 9-1
- *Configuración*. Ver Capítulo 10 ” Módulo de Configuración” en la página 10-1

CAPÍTULO 5

El Módulo de Administración de Certificados

Este módulo de la consola permite realizar consultas o revocaciones de certificados gestionados por el Agente Certificador.

Para acceder a estas funciones, deberá seleccionar *Certificados* en la Consola del Agente Certificador. (Figura 5.1).

Figura 5.1 Opción Certificados

En la ventana que aparecerá, se desplegarán los certificados que hayan sido emitidos a través de este Agente Certificador. (Figura 5.2).

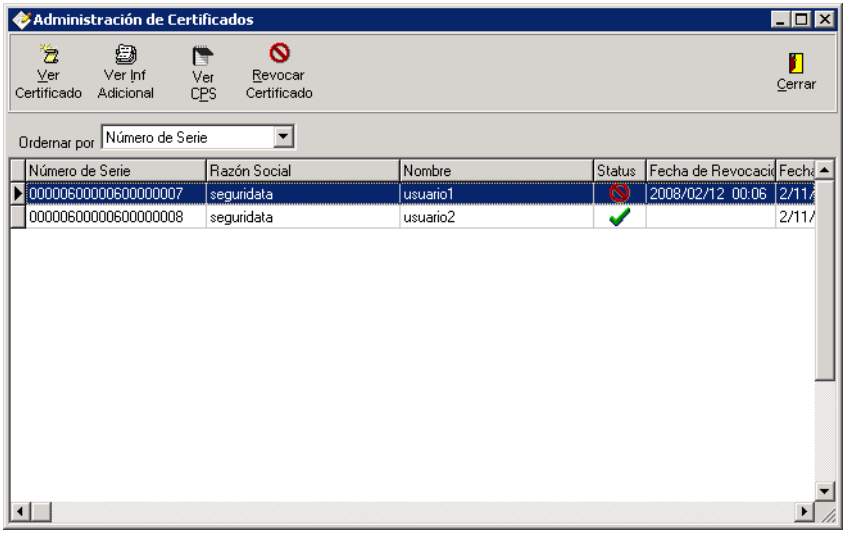

Figura 5.2 Certificados emitidos por el Agente Certificador

En este módulo es posible realizar los siguientes procedimientos:

- Ver información de Certificados
- Ver Información Adicional del Certificado
- Ver CSP
- Revocar Certificados

Para cerrar la ventana de éste módulo, deberá hacer clic en el botón *Cerrar*.

Importante

Estos procedimientos solamente actuarán sobre los certificados gestionados a través de este Agente Certificador. Los certificados gestionados por otro medio (Agente, Administrador, etc.), no aparecerán en este módulo, aún cuando existan en la base de datos de SeguriServer.

5.1 Ver Información de Certificados

Si se desea consultar información detallada de alguno de los certificados que ha gestionado el Agente Certificador, deberá de acceder a la ventana del módulo de Administración de Certificados y seleccionar el renglón correspondiente al certificado que se desea consultar, seguido de un clic en el botón *Ver Certificado*. (Figura 5.3).

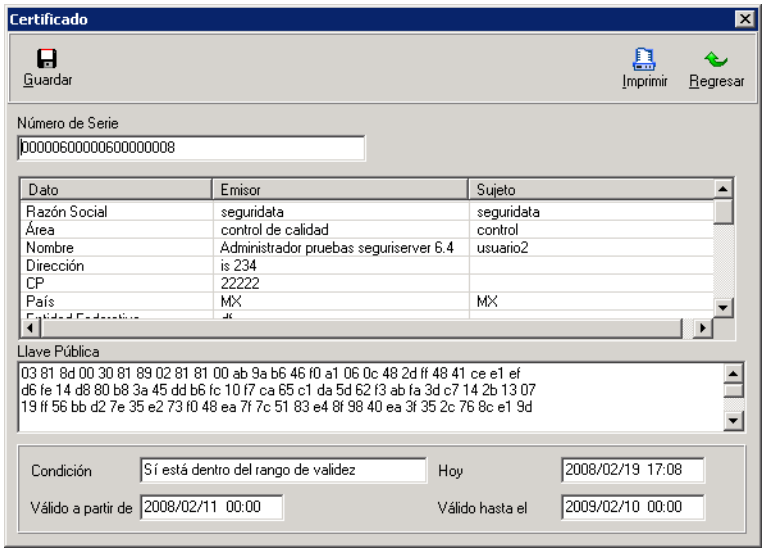

Figura 5.3 Detalle del Certificado seleccionado

En esta ventana, se presentan todos los datos que contiene el certificado.

En caso de ser necesario se puede descargar este certificado a un archivo, haciendo clic en el botón *Guardar*, o bien es posible imprimir la información haciendo clic en el botón *Imprimir*.

Al terminar la consulta del certificado, deberá de cerrar la ventana haciendo clic en el botón *Regresar*.

Importante

Si en su configuración apareció en TRUE, la impresión de los certificados le aparecerá

5.2 Consultar Información Adicional

Al generar el requerimiento de un usuario, es posible capturar información adicional, que si bien no estará almacenada dentro del certificado, se puede mantener registrada y asociada a él, en la base de datos de SeguriServer.

> **Importante**
>
> El almacenamiento de la información adicional responde a las necesidades particulares de cada infraestructura de seguridad y requerirá la personalización de la interfaz de la aplicación para crear requerimientos, tal como se indica en el manual de "Instalación y Configuración de SeguriServer".

Si existe esa información en la base de datos, podrá ser consultada seleccionando el renglón correspondiente al certificado que se desea consultar, en la ventana del módulo de Administración de Certificados seguido de un clic en el botón *Ver Inf Adicional*.

5.3 Ver CSP

Esta opción presenta una ventana con información de las obligaciones y facultades que tiene el certificado seleccionado. Para ver esta información haga clic en la opción *Ver CPS* del menú. (Figura 5.4).

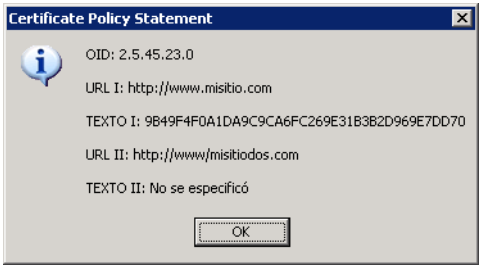

Figura 5.4 Información Certificate Policy Statement

Haga clic en el botón *OK* para cerrar la ventana.

5.4 Revocar Certificados

Cuando se desee revocar un certificado, deberá de acceder a la ventana del módulo de Administración de Certificados y seleccionar el renglón correspondiente al certificado que se desea revocar, seguido de un clic en el botón *Revocar Certificado*.(Figura 5.5).

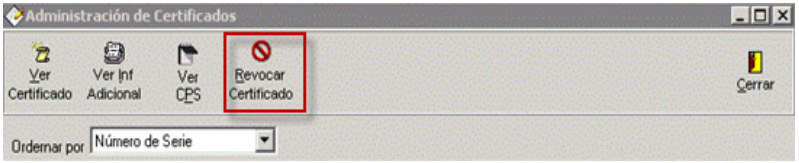

Figura 5.5 Revocar Certificado

Aparecerá una ventana de diálogo solicitando que se confirme la intención de revocar el certificado.(Figura 5.6).

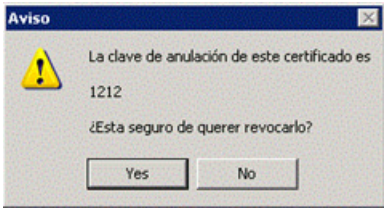

Figura 5.6 Aviso de Revocación

Importante

Si en su configuración apareció en TRUE, el mensaje de confirmación de revocación le aparecerá

Después de revocarlo o de no proseguir con ello, regresará a la ventana del módulo de Administración de Certificados.

Importante

Si un usuario solicita la revocación de su certificado, es recomendable que proporcione la clave de anulación definida al momento de llenar el requerimiento del certificado para asegurar la identidad del mismo. Para apoyar esta práctica, la clave de anulación también aparece en la ventana de diálogo en que se confirma la revocación.

Warning

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

CAPÍTULO 6

El Módulo de Ejecutivos de Registro

Dentro de una infraestructura de seguridad, la raíz de la confianza recae en la AC. Esta a su vez, delega la responsabilidad de garantizar la identidad del usuario solicitante a un Agente Certificador y una vez aceptado, procede a registrarlo ante la AC.

Sin embargo, debido a la cantidad de certificados que se tienen que gestionar o por necesidades operativas de la entidad que usa la AC, puede no ser suficiente el delegar la responsabilidad del cumplimiento de requisitos a un Agente Certificador, creando la necesidad de un nivel subordinado menor.

Este papel lo desempeña el Ejecutivo de Registro, quien se encarga de aceptar un requerimiento sujeto al cumplimiento de ciertos requisitos.

Si es aceptado, entonces el Ejecutivo de Registro procede a firmar digitalmente el Requerimiento del usuario y lo transmite al Agente Certificador.

Dada la relación de confianza entre ejecutivos y agentes, los requerimientos recibidos de los Ejecutivos de Registro autorizados, son procesados de manera inmediata hacia la AC, gestionando el certificado correspondiente.

Una vez que el Agente Certificador recibe el certificado, lo retransmite a su vez al Ejecutivo de Registro quien lo entregará al usuario final. (Figura 6.1).

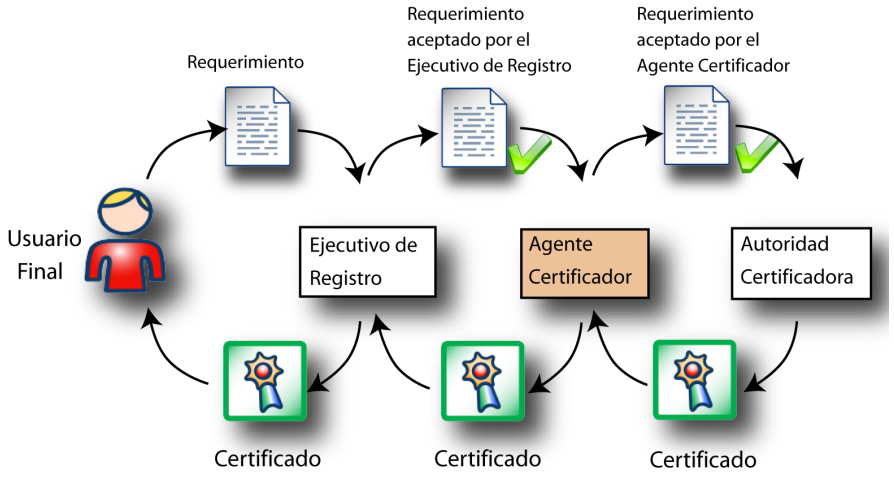

Figura 6.1 Gestión de un Certificado a través de un Ejecutivo de Registro

Para asegurar la identidad del ejecutivo que envía el requerimiento, se deberá crear un certificado especial de Ejecutivo de Registro, que se registrará en el Agente Certificador y de esa manera pueda identificar y procesar automáticamente los Requerimientos que reciba de él.

La administración de los ejecutivos de registro se realiza en este módulo.

Los procedimientos disponibles para este efecto son:

- Ver el Certificado de un Ejecutivo de Registro
- Agregar Ejecutivos de Registro
- Borrar Ejecutivos de Registro

Para acceder a estas funciones, haga clic en la opción *`Ejecutivos de Registro`* en la Consola del Agente Certificador. (Figura 6.2).

Figura 6.2 Opción Ejecutivos de Registro

A continuación se mostrará la ventana de Ejecutivos de Registro. (Figura 6.3).

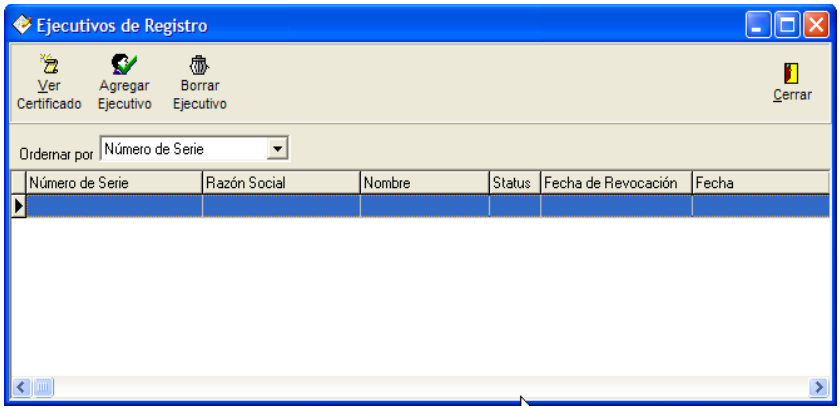

Figura 6.3 Ventana de Ejecutivos de Registro

En la parte inferior aparecerán todos los Ejecutivos de Registro reconocidos.

Para facilitar su consulta, pueden ordenarse por:

- Número de Serie
- Razón Social
- Nombre
- Revocados

Para ordenar los Ejecutivos por alguno de estos criterios, deberá usar el control *Ordenar por* y seleccionar el campo deseado en la lista que se mostrará. (Figura 6.4).

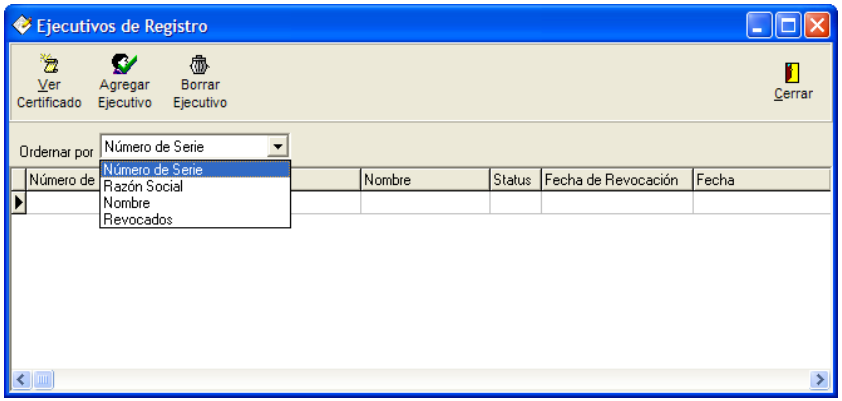

Figura 6.4 Ordenar a los Ejecutivos de Registro

Al terminar, haga clic en el botón *Cerrar* para cerrar la ventana de este módulo.

6.1 Consulta de Certificados de Ejecutivo de Registro

Si se desea consultar información detallada del certificado de un Ejecutivo de Registro, deberá seleccionar el renglón correspondiente al certificado que se desea consultar, y haga clic en el botón *Ver Certificado*.

En la ventana que aparecerá, están todos los datos que contiene el certificado. (Figura 6.5).

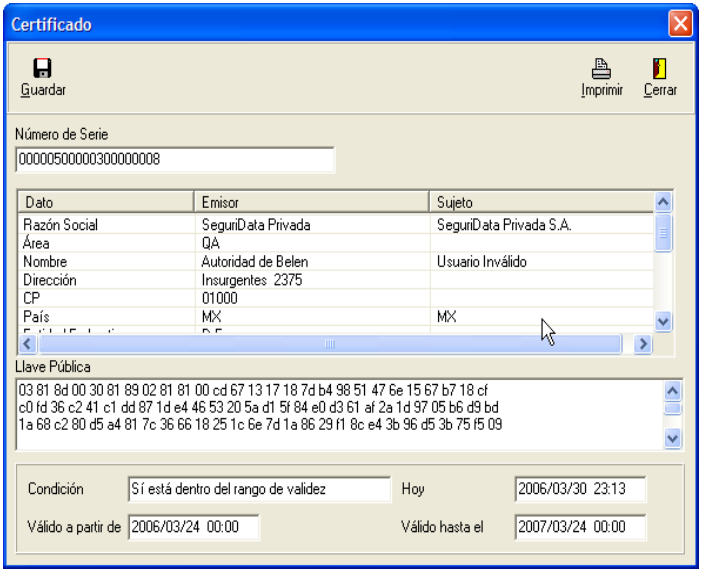

Figura 6.5 Datos del Certificado de un Ejecutivo de Registro

En caso de ser necesario, podrá almacenar este certificado en un archivo para su distribución, haciendo clic en el botón *Guardar* o bien es posible imprimir la información haciendo clic en el botón *Imprimir*.

Al terminar, deberá de cerrar la ventana haciendo clic en el botón *Terminar*.

6.2 Agregar Ejecutivos de Registro

Cuando sea necesario incorporar a un Ejecutivo de Registro dentro del proceso de certificación de usuarios, deberá usar esta opción.

Una vez incorporado, cuando el Agente Certificador reciba los requerimientos aceptados por el Ejecutivo de Registro, los transmitirá de inmediato a la AC para crear el certificado correspondiente.

Para esto, haga clic en el botón *Agregar Ejecutivo*. Aparecerá el selector de archivos y deberá indicar la ubicación completa del certificado del Ejecutivo que se desea agregar.

> **Importante**
>
> El certificado que se puede utilizar para registrar a un Ejecutivo de Registro, no tiene alguna característica en particular y podrá ser generado como cualquier otro requerimiento de usuario.

Una vez que se haya seleccionado el certificado, aparecerá una ventana mostrando los datos que contiene el certificado, de la misma manera y con las mismas alternativas que cuando se consulta un certificado de Ejecutivo de Registro. "6.1 Consulta de Certificados de Ejecutivo de Registro" en la página 6-4.

Al terminar de revisar la información deberá de cerrar la ventana haciendo clic en el botón *Cerrar*, regresando a la ventana del módulo de Ejecutivos de Registro.

6.3 Borrar un Ejecutivo

Cuando se desee eliminar un Ejecutivo de Registro, es porque no se aceptarán directamente los requerimientos que vengan firmados por un cierto Ejecutivo, por tal motivo se deberá de borrar de la lista.

> **Importante**
>
> Este procedimiento no es definitivo, ya que puede revertirse. Es posible volver a dar de alta como Ejecutivo a un usuario, usando el mismo certificado que alguna vez ya haya sido usado. Ver "6.2 Agregar Ejecutivos de Registro".

> **Warning**
>
> Para esto, deberá seleccionar el renglón correspondiente al certificado que se desee eliminar, y hacer clic en el botón *Borrar Ejecutivo*.

Aparecerá una ventana solicitando la confirmación de que se desea eliminar al Ejecutivo y al responder a este diálogo, se realizará la acción seleccionada, para regresar posteriormente a la ventana del módulo de Ejecutivos de Registro.

CAPÍTULO 7

El Módulo de Requerimientos de Certificación

El Agente Certificador tiene como función el gestionar los requerimientos para generar los certificados, interactuando con la AC de SeguriServer.

Para utilizar esta función haga clic en la opción *Requerimientos de Certificación* de la consola del Agente Certificador. (Figura 7.1).

Figura 7.1 Requerimientos de Certificación

Aparecerá la ventana desde la cual se generan los certificados. (Figura 7.2).

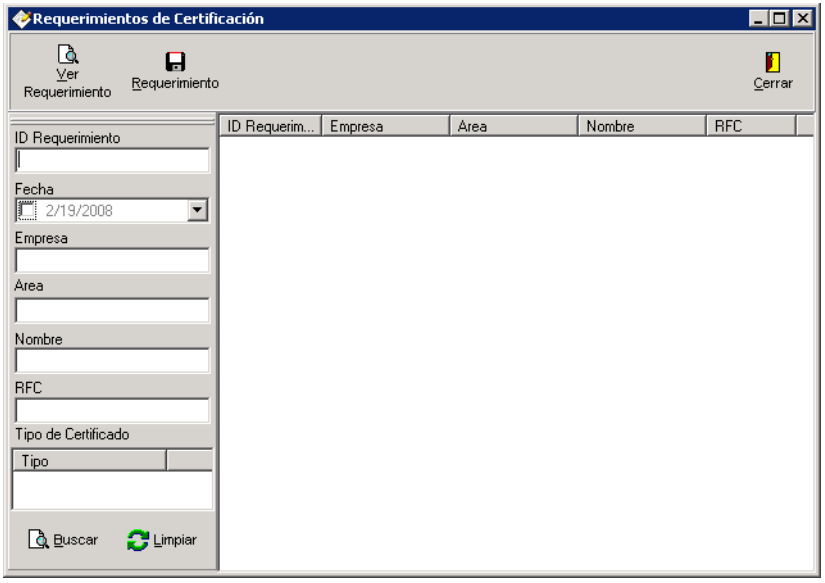

Figura 7.2 Generación de Certificados

El proceso de certificación de requerimientos, se puede llevar a cabo de dos maneras distintas:

- Recibiendo los requerimientos a través de un archivo que contenga el requerimiento por distintos medios, o
- Usando los requerimientos que se encuentra en el repositorio de la Autoridad Certificadora de SeguriServer, dado que fueron elaborados a través de una página Web.

7.1 Certificación de Requerimientos en Archivo

En este caso, el usuario o el Ejecutivo de Registro hace llegar al Agente Certificador, el archivo con el requerimiento a través de cualquier medio (disquete, CD, e-mail, etc.).

En cuanto el Agente Certificador tiene la certeza de que el usuario cumple todos los requisitos impuestos para este fin, o bien que el requerimiento fue enviado por un Ejecutivo de Registro, genera el certificado, cargando el archivo que contiene el requerimiento y gestionando el certificado ante la Autoridad Certificadora.

Para realizar este proceso, haga clic en el botón *Requerimiento*, que presenta el selector de archivos para indicar la ubicación del archivo que contiene el requerimiento.

7.1.1 Requerimiento

Al terminar la selección, aparecerá una ventana que muestra los datos que contiene el requerimiento. (Figura 7.3).

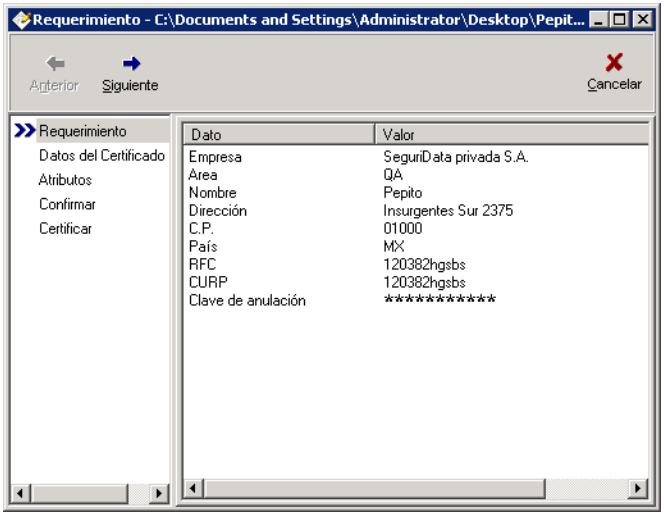

Figura 7.3 Datos del Requerimiento

Si el requerimiento es el correcto para certificar, haga clic en el botón *Siguiente*, en caso contrario haga clic en el botón *Cancelar*.

7.1.2 Datos del Certificado

A continuación, seleccione las características del certificado que se generará. (Figura 7.4).

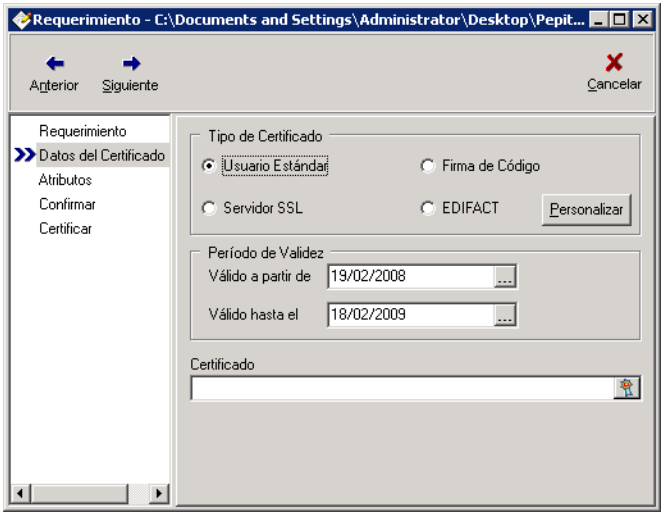

Figura 7.4 Tipo de Certificado

Con ayuda de las casillas de selección, deberá indicar:

- si se desea solicitar un certificado *Usuario Estándar*
- si se desea solicitar un certificado del *Servidor SSL*
- si se desea solicitar un certificado de *Firma de Código*
- si se desea solicitar un certificado *EDIFACT*
- *Fechas de Validez* del certificado, y
- el nombre del archivo para el *Certificado*

Haga clic en el botón *Siguiente*.

Si desea personalizar las extensiones del certificado en cuestión, haga clic en el botón *Personalizar* que presenta las siguientes ventanas.

En la siguiente ventana deberá habilitar/deshabilitar las banderas de las extensiones según lo requiera. (Figura 7.5).

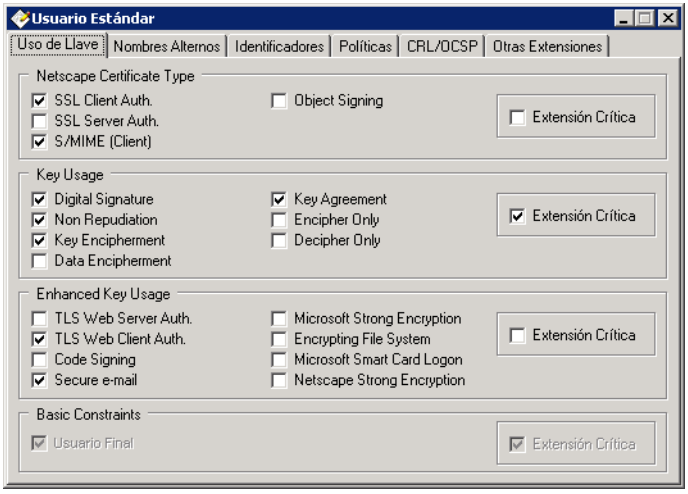

Figura 7.5 Uso de Llaves

A continuación indique los parámetros que se solicitan como se muestra en la Tabla 7.1.

Tabla 7.1 Parámetros de Uso de Llave

Nombre de la Extensión	Atributos	Descripción
Netscape Certificate Type		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 CA`	Indica que el certificado pertenece a una AC que emitirá certificados de sitios web.
	`S/MIME CA`	Indica que la AC podrá emitir certificados que sirvan para firma de documentos.
	`Object Signing CA`	Indica que la AC podrá emitir certificados que sirvan para firmar software ejecutable.

Tabla 7.1 Parámetros de Uso de Llave (Continuación)

Nombre de la Extensión	Atributos	Descripción
Key Usage		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.
Enhanced Key Usage		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.
	`Secure e-mail`	Firma de e-mail.
	`Time Stamping`	Emisión de estampillas de tiempo.
	`OCSP Signing`	Firma de estatus de certificados en línea (OCSP).
Basic Contraints		Limitantes básicas. Nos indica los límites (niveles de subordinación) que pueden depender del certificado de la AC.

Haga clic en la pestaña *Nombre Alternos* para especificar los datos de extensión *Nombres Alternos del Sujeto* y *Nombres Alternos del Emisor*. (Figura 7.6).

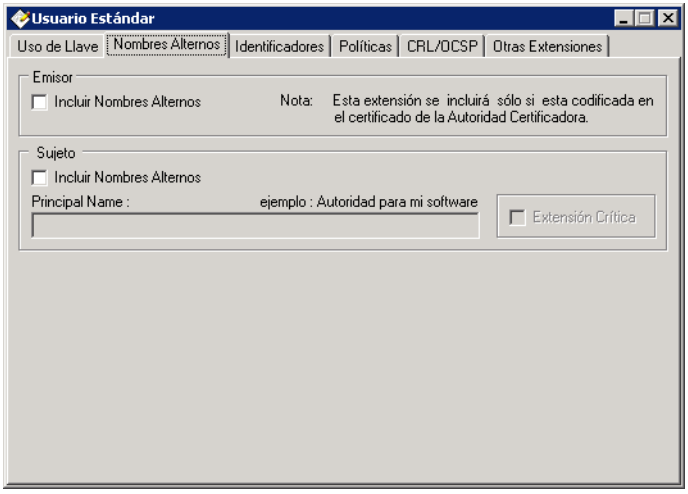

Figura 7.6 Nombres Alternos

A continuación proporcione los datos que se solicitan, como se indica en la Tabla 7.2.

Tabla 7.2 Parámetros de Configuración de los Nombres Alternos

Nombre de la Extensión	Descripción
`Emisor`	Si se selecciona esta opción, los nombres alternos de la autoridad (si es que existen), serán incluidos en el certificado del Agente.
`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. Marque esta casilla si desea utilizar esta extensión.
`Principal Name`	Indica el "nombre principal" como se define en *Kerberos* (RFC 1510).

Haga clic en la pestaña *Identificadores* para configurar que se incluyan en el certificado del Agente, las extensiones que identifican de manera única a la autoridad y al Agente. (Figura 7.7).

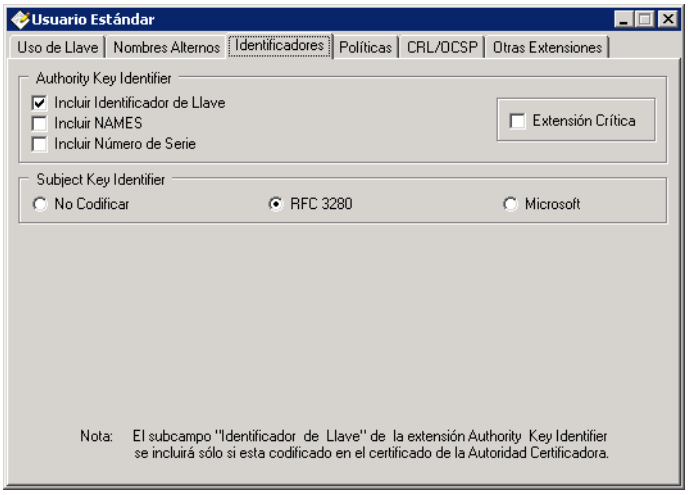

Figura 7.7 Identificadores

A continuación proporcione los datos que se solicitan, como se indica en la Tabla 7.3.

Tabla 7.3 Parámetros de Configuración de los Identificadores

Nombre de la Extensión	Descripción
`Incluir Identificador de Llave`	Se debe seleccionar esta opción si se desea que el identificador de la llave de la AC, aparezca en el certificado del Agente para poder identificar con qué certificado se firmó.
`Incluir NAMES`	Si se desea que los NAMES del emisor de la autoridad aparezcan como identificador de la entidad que generó el certificado del agente, se debe seleccionar esta opción. (Véase además la nota siguiente respecto al número de serie).
`Incluir Número de Serie`	Si se desea que el número de serie de la AC aparezca como identificador del certificado que emitió al Agente, seleccione esta opción. Es de uso generalizado el identificar a un certificado con los NAMES de su autoridad y además su número de serie. Si se desea utilizar ese método de identificación par el emisor del agente se recomienda usar en combinación el campo NAMES y Número de serie. Como opción alterna (ó complementaria), si la autoridad cuenta con Identificador de llave en sus atributos, se puede utilizar también dicho campo.

Tabla 7.3 Parámetros de Configuración de los Identificadores (Continuación)

Nombre de la Extensión	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 7.8).

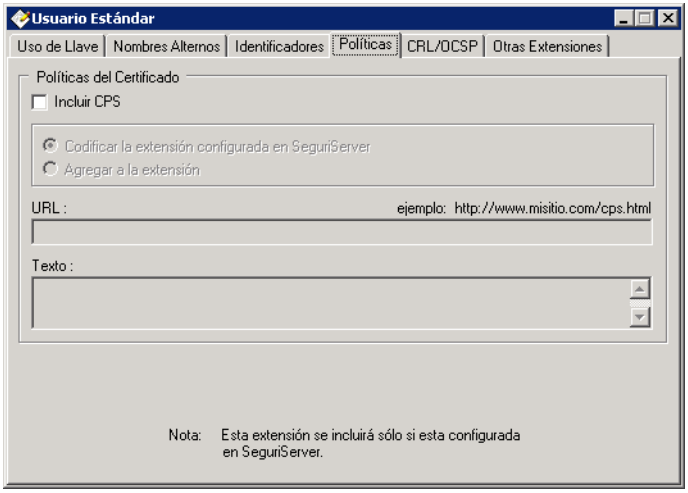

Figura 7.8 Políticas

Si desea incluir CSP, proporcione los parámetros que se solicitan, como se indica en la Tabla 7.4.

Tabla 7.4 Parámetros de Configuración de las Políticas

Nombre de la Extensión	Descripción
`Codificar la extensión configurada en SeguriServer`	Si se decide incluir la extensión CPS, ésta puede ser exactamente la misma que la que se configuró en SeguriServer. Si se desea que ésta se incluya en el certificado del Agente, debe seleccionar esta opción.

Tabla 7.4 Parámetros de Configuración de las Políticas (Continuación)

Nombre de la Extensión	Descripción
Agregar a la Extensión	Si además de la extensión CPS configurada en SeguriServer se desea incluir otra CPS, debe seleccionar esta opción y configurar una URL y/o un texto en los campos siguientes.
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 7.9).

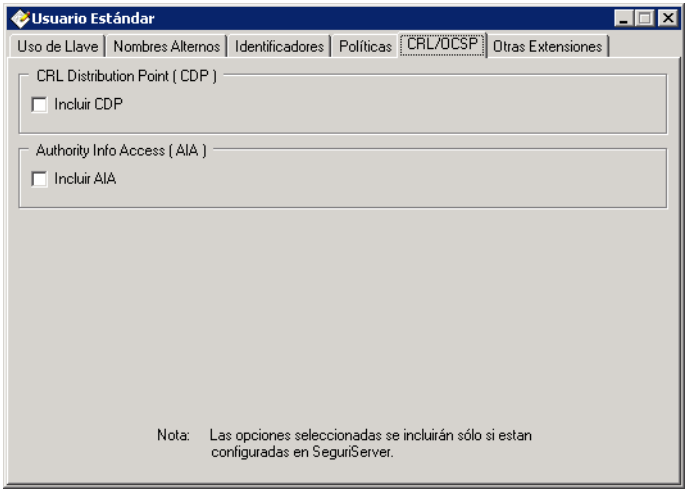

Figura 7.9 CRL/OCSP

Marque las siguientes casillas, como se indica en la Tabla 7.5.

Tabla 7.5 Parámetros de Configuración del CRL/OCSP

Nombre de la Extensión	Descripción
CRL Distribution Point (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.
Authority Info Access (AIA)	Esta extensión indica URLs donde se encuentran servicios que puede dar la Autoridad emisora del 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*, *Microsoft Enroll Certificate Template Name* y *Microsoft CA Key Index Pair*. (Figura 7.10).

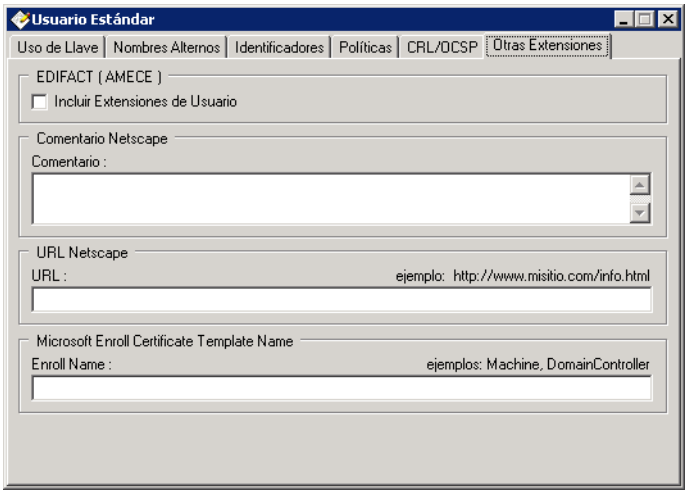

Figura 7.10 Otras Extensiones

Proporcione los parámetros que se solicitan, como se indica en la Tabla 7.6.

Tabla 7.6 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.
Comentario/URL Netscape		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.
Microsoft Enroll Certificate Template Name		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.

A continuación haga clic en el botón *`Continuar`*.

7.1.3 Atributos

En seguida, se desplegarán los atributos extendidos del certificado, en caso de que existan. (Figura 7.11).

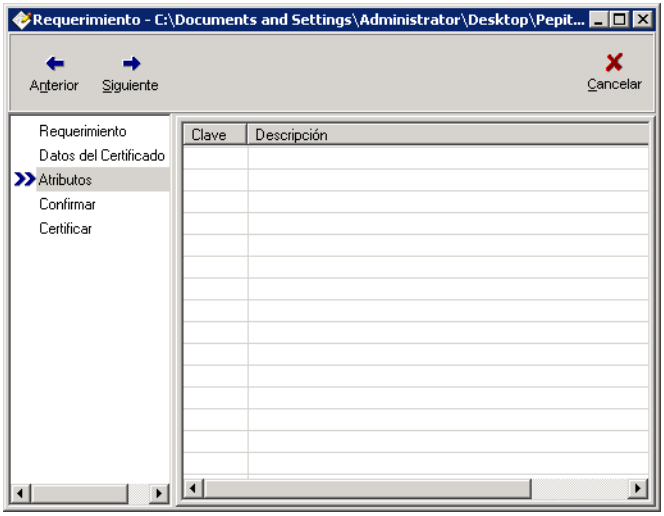

Figura 7.11 Atributos

Se presentará una ventana que muestra los datos que contiene el certificado. Haga clic en el botón *Siguiente*.

7.1.4 Confirmar

Finalmente, se desplegará un resumen de las características del certificado que se generará. (Figura 7.12).

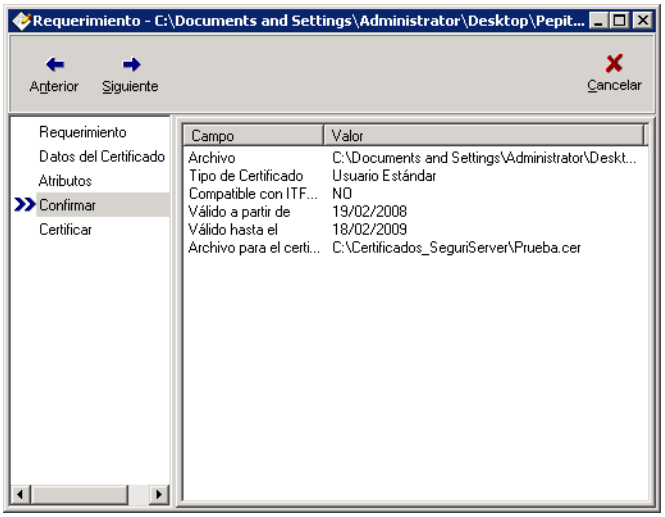

Figura 7.12 Confirmar

Si la información es correcta, haga clic en el botón *Siguiente* para iniciar la certificación del requerimiento.

Importante

Los valores válidos para el archivo cfgagente.ini son 0 (False) y 1 (True). Este archivo se encontrará en la ruta en donde se instale la aplicación de Agente. Por default todos los parámetros están en 0.

Se mostrará un mensaje indicando que este proceso puede durar varios minutos y al terminar, regresará al módulo de Certificación de Requerimientos. (Figura 7.13).

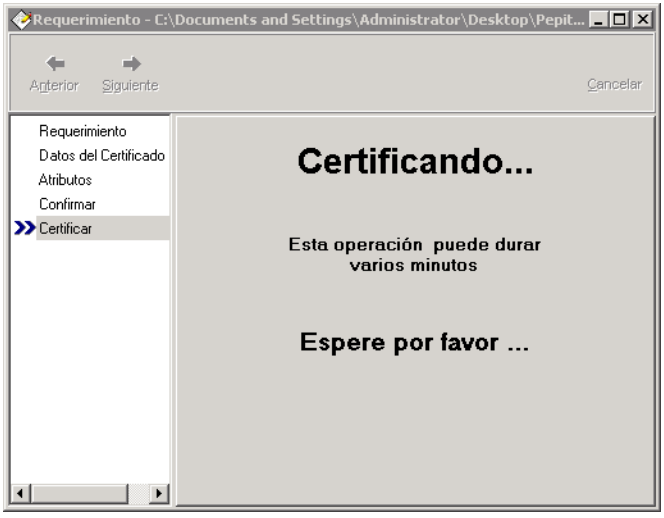

Figura 7.13 Proceso de Certificación

Si en su configuración apareció en TRUE, la impresión de reportes le aparecerá (Figura 7.14).

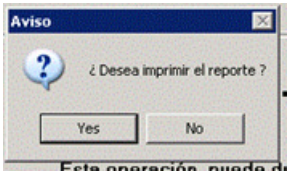

Figura 7.14 Aviso

La siguiente pantalla el reporte del certificado generado (Figura 7.15).

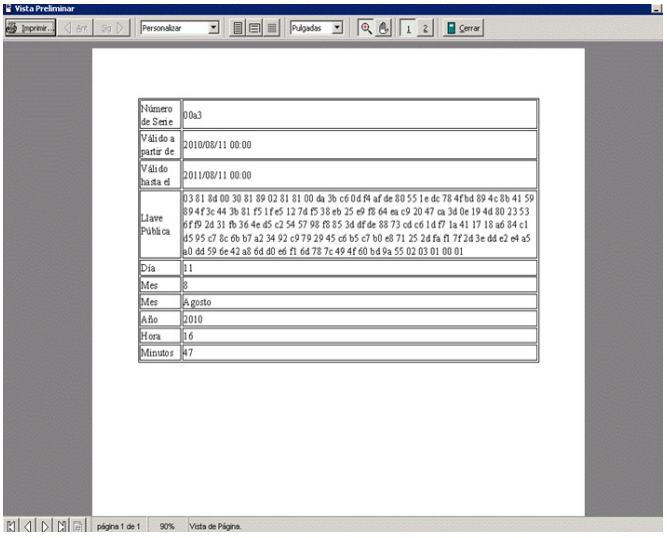

Figura 7.15 Vista Previa del Reporte

7.2 Certificación de requerimientos llenados en página Web

En este caso, el usuario llena un formato de requerimiento en una página Web y a través de un CGI se envía a un repositorio de requerimientos pendientes de certificación en la base de datos de la Autoridad Certificadora.

Cuando el usuario se presenta ante el Agente Certificador para dar cumplimiento con todos los requisitos para obtener un certificado, el Agente accede a la base de datos de la Autoridad Certificadora y busca el requerimiento.

Una vez localizado, puede indicar a la Autoridad Certificadora que genere el certificado correspondiente y devuelva el número de serie para que el usuario obtenga su certificado a través de una página Web. (Figura 7.16).

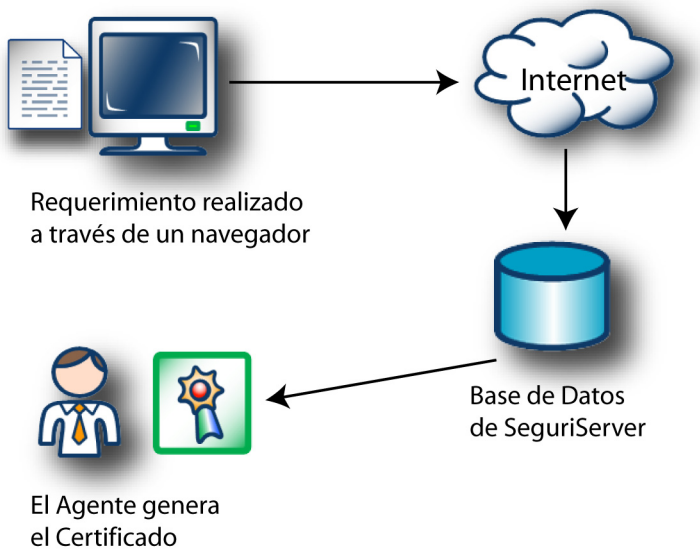

Figura 7.16 Proceso de Obtención de un Certificado a través de un Navegador

Para realizar este proceso, el usuario se deberá presentar ante el Agente Certificador y comprobar que cumple con los requisitos para obtener un certificado.

Para iniciar el procedimiento de certificación, el usuario deberá proporcionar el número de serie que le fue proporcionado a través de la página Web al concluir el llenado de su requerimiento.

El Agente deberá de usar este número de serie o en su defecto algunos otros datos que permitan recuperar el requerimiento buscado, introduciendo los datos en los campos correspondientes. (Figura 7.17).

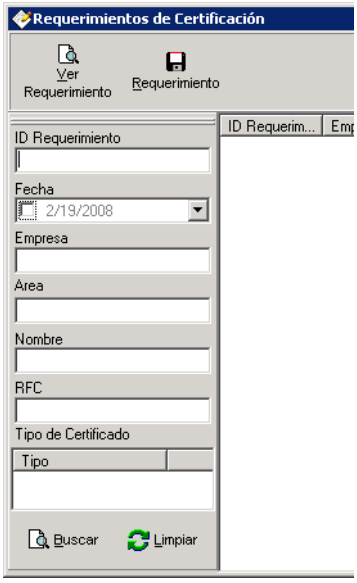

Figura 7.17 Buscar Requerimiento

Haga clic en el botón *Buscar*.

Los requerimientos que satisfagan los criterios, se desplegarán del lado derecho de la ventana, de donde se deberá seleccionar el renglón del requerimiento buscado y hacer clic en el botón *Requerimiento*.

Importante

Si se desea revisar los datos contenidos en el requerimiento sin generar el certificado, deberá seleccionar el renglón del requerimiento buscado y hacer clic en el botón *Ver Requerimiento*.

Importante

Si desea iniciar una nueva búsqueda haga clic en el botón *Limpiar* para vaciar todos los campos con criterios de búsqueda.

Una vez localizado el requerimiento, se presentará la siguiente ventana con los datos del Requerimiento. (Figura 7.18).

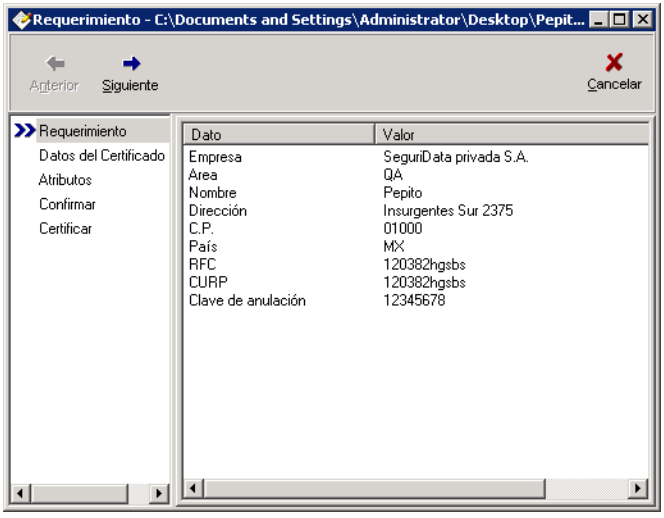

Figura 7.18 Datos del Requerimiento

Para iniciar la certificación, haga clic en el botón *Siguiente* y siga los pasos de la Sección "7.1 Certificación de Requerimientos en Archivo" en la página 7-2.

CAPÍTULO 8

El Módulo de Administración Remota

En este módulo se realizan operaciones de consulta y revocación de certificados que se encuentren registrados en la Autoridad Certificadora, independientemente del Agente Certificador que los haya gestionado.

Para acceder a estas funciones, haga clic en la opción *Administración Remota* de la Consola del Agente Certificador. (Figura 8.1).

Figura 8.1 Administración Remota

Importante

Este módulo estará disponible solamente si al certificado del Agente Certificador se le habilitaron esos permisos al momento de ser generado.

A continuación se presentará la siguiente ventana. (Figura 8.2).

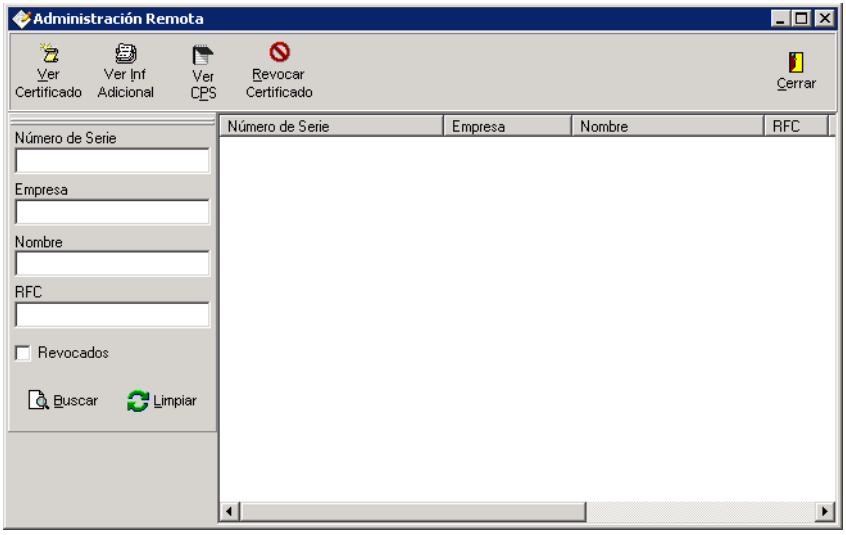

Figura 8.2 Ventana de Búsqueda y Consulta

En este módulo es posible realizar dos procedimientos:

- Ver Información de Certificados
- Revocar Certificados

Para cerrar la ventana de éste módulo, deberá hacer clic en el botón *Cerrar*.

8.1 Ver información de Certificados

Si desea consultar los certificados que ha gestionado el Agente Certificador, indique algún criterio de búsqueda en la parte izquierda de la ventana y haga clic en el botón *Buscar*. (Figura 8.3).

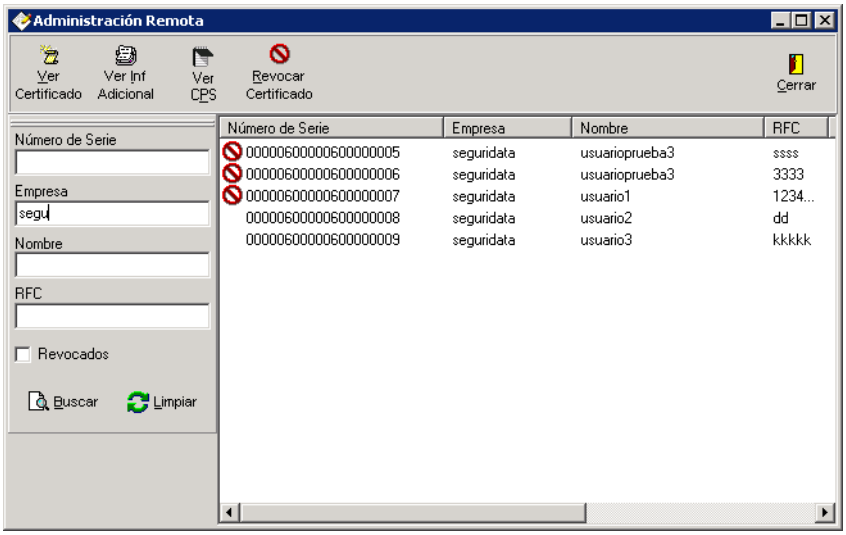

Figura 8.3 Resultado de la Búsqueda

Se presentaran los certificados con el criterio de búsqueda indicado.

Si desea ver el detalle de un certificado, selecciónelo y haga clic en el botón *Ver Certificado*. (Figura 8.4).

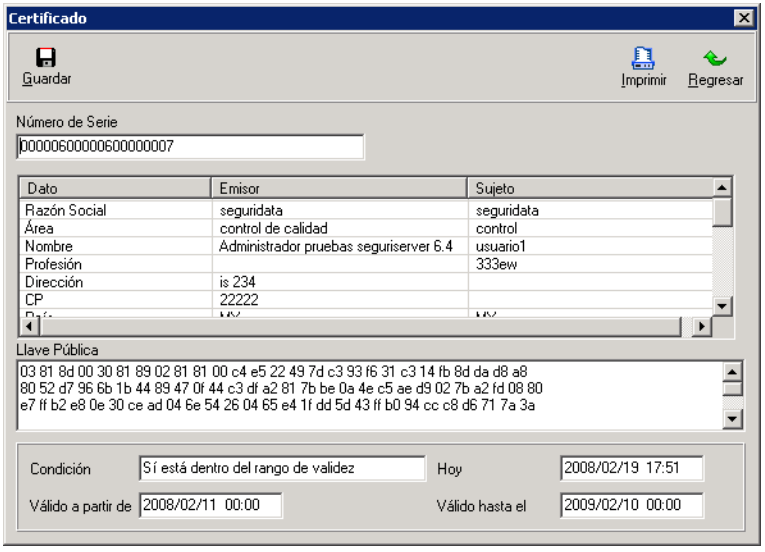

Figura 8.4 Detalle de un Certificado

En caso de ser necesario se puede almacenar este certificado en un archivo, para su distribución, haciendo clic en el botón *Guardar*, o bien es posible enviar a la impresora toda la información haciendo clic en el botón *Imprimir*.

Para salir de esta ventana, haga clic en el botón *Regresar*.

8.2 Consultar información adicional

Al generar el requerimiento de un usuario, es posible capturar información adicional a la necesaria para crear un certificado para fines específicos del usuario de la Autoridad Certificadora. SeguriServer permite capturar esta información y almacenarla asociada al certificado correspondiente.

Importante

El almacenamiento de la información adicional responde a las necesidades particulares de cada infraestructura de seguridad y requerirá la personalización de la interfaz de la aplicación para crear requerimientos, tal como se indica en el manual de Instalación y Configuración de SeguriServer.

La información adicional que se registre en la base de datos de SeguriServer, podrá ser consultada en la ventana del módulo de Administración Remota, seleccionando el renglón correspondiente al certificado que se desea consultar, seguido de un clic en el botón *Ver Inf Adicional*.

8.3 Revocar Certificados

Cuando se desee revocar un certificado, seleccione el renglón correspondiente al certificado que se revocará, seguido de un clic en el botón *Revocar Certificado*.

Aparecerá una ventana de diálogo solicitando que se confirme el proceso.

Importante

Si un usuario solicita la revocación de su certificado, es recomendable que proporcione la clave de anulación definida al momento de llenar el requerimiento del certificado para asegurar que quien solicita la revocación sea la misma persona que lo elaboró.
En la ventana de diálogo que confirma la revocación de un certificado, se mostrará la clave de anulación.

Warning

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

Warning

Si utiliza la CRL emitida por la Autoridad Certificadora para consultar la situación de certificados, se recomienda su actualización después de realizar revocaciones.

CAPÍTULO 9

Módulo de CRL

En este módulo se obtienen las CRLs actualizadas, directamente de la AC.

Para acceder a estas funciones, haga clic en la opción CRL de la consola del agente certificador. (Figura 9.1).

Figura 9.1 CRL

A continuación se presentará una ventana la cual permite actualizar la CRL del Agente Certificador y consultar una CRL almacenada en disco. (Figura 9.2).

Figura 9.2 Lista de Certificados Revocados

Las CRLs se ven afectadas por la revocación de certificados, por lo que es importante actualizarlas constantemente antes de realizar consultas de certificado.

Importante

Si el Agente Certificador está habilitado para revocar certificados en el módulo Administración Remota, es importante que después de realizar revocaciones se actualice la CRL, o de lo contrario los cambios no se reflejarán al consultar certificados en el módulo de Certificados.

9.1 Actualizar la CRL del Agente Certificador

Para realizar este procedimiento haga clic en el botón *Obtener CRL*.

A continuación se presentará el selector de archivos para que indique el archivo donde se guardará la CRL. Enseguida se solicitará la lista de certificados revocados a la Autoridad Certificadora correspondiente y ésta se presentará en la ventana con los certificados revocados.

9.2 Consulta de otras CRLs

Cada vez que se solicita una CRL, ésta se deposita en un archivo y eso permite crear un historial de revocación de certificados.

Si desea consultar una CRL anterior, haga clic en el botón *Ver CRL* que presenta el selector de archivos para que seleccione la CRL almacenada en disco para su consulta.

CAPÍTULO 10

Módulo de Configuración

Para acceder a este módulo haga clic en la opción *Configuración* de la consola del Agente Certificador. (Figura 10.1).

Figura 10.1 Configuración

A continuación se presenta la siguiente ventana con los parámetros configurables de SeguriServer. (Figura 10.2).

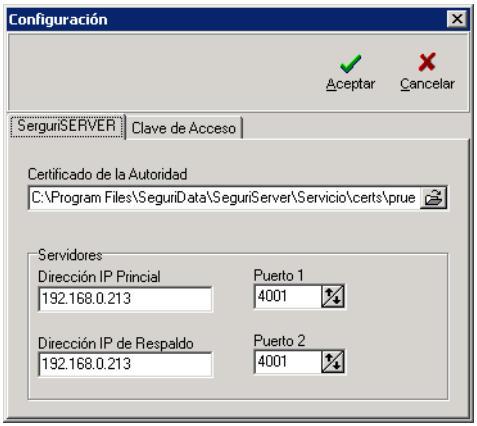

Figura 10.2 Ventana de Configuración de SeguriServer

Estos parámetros se refieren a la ubicación del certificado de la AC y al enlace de comunicación con ella.

Los parámetros configurables se indican en la Tabla 10.1.

Tabla 10.1 Parámetros de Configuración

El parámetro …	es …
Certificado de la Autoridad	la ubicación del certificado de la Autoridad Certificadora.
Servidor Principal	la dirección IP a través de la cual se accede a la Autoridad Certificadora.
Puerto 1	el puerto de comunicaciones asociado a la IP del parámetro anterior.
Servidor de Respaldo	es la dirección IP del servidor alternativo, bajo un esquema de alta disponibilidad, en donde se encuentra la réplica de la Autoridad Certificadora que atenderá peticiones en caso de que el equipo del *Servidor Principal 1* presente alguna falla. Si la Autoridad Certificadora no funciona en una infraestructura de este tipo, entonces se deberá asignar el mismo que el de *Servidor Principal 1.*
Puerto 2	Es el puerto de comunicaciones asociado a la IP del parámetro anterior.

Warning

Al terminar de realizar los cambios, haga clic en el botón *Aceptar*, de lo contrario los cambios realizados se perderán.

10.0.1Cambio de Clave de Acceso

Como parte de las políticas de seguridad recomendadas en una infraestructura de seguridad, está la de cambiar frecuentemente las claves de acceso. La aplicación del Agente Certificador permite cambiar la llave de acceso de su certificado en el módulo de *Configuración*, haciendo clic en la carpeta *Clave de Acceso*. (Figura 10.3).

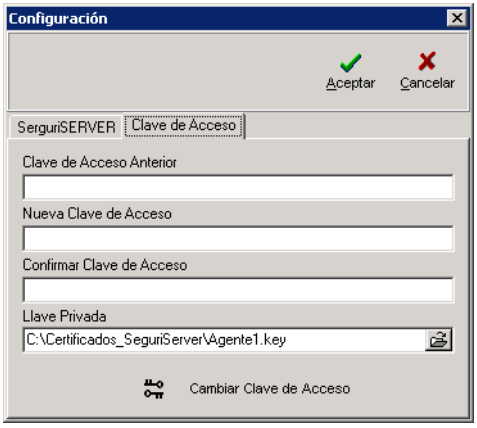

Figura 10.3 Configuración de la Clave de Acceso

El procedimiento para cambiar la *Clave de Acceso* se indica en la Tabla 10.2.

Tabla 10.2 Procedimiento para cambiar la Clave de Acceso

Paso	Acción
1	Indique la *Clave de Acceso Anterior*.
2	Escriba la nueva contraseña en el campo *Nueva Clave de Acceso*.
3	Confirme la nueva clave de acceso en el campo *Confirmar Clave de Acceso*.
4	Si la *Llave Privada* del Agente Certificador cambió de ubicación, indicarla en el campo *Llave Privada*.

Por último haga clic en el botón *Cambiar Clave de Acceso* para que se realice el cambio.

Importante

Al terminar de realizar los cambios es importante que haga clic en el botón *Aceptar*, de lo contrario todos los cambios se perderán.