



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 |
| 1.4 Nueva Funcionalidad               | 1 - 2 |

---

## Capítulo 2. Los componentes de SeguriServer

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

---

## Capítulo 3. Configuración de OCSP Responder

|  |       |
|--|-------|
| 3.1 Configuración del respondedor de OCSP        | 3 - 2 |
| 3.2 Parámetros del Servicio                      | 3 - 2 |
| 3.3 Administración de Autoridades Certificadoras | 3 - 3 |
| 3.3.1. Agregar Autoridades Certificadoras        | 3 - 4 |
| 3.3.2. Eliminar Autoridades Certificadoras       | 3 - 5 |
| 3.3.3. Ver el Detalle de un Certificado          | 3 - 6 |
| 3.4 Parámetros del Respondedor OCSP              | 3 - 7 |
| 3.5 Configuración de la Base de Datos            | 3 - 9 |



## 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.

---

**Q 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 | Describir el servicio de consulta Online Certificate Status Protocol (OCSP), que permite verificar el estado de revocación de un certificado y atender las peticiones de consulta. |
| 1.4 Nueva Funcionalidad | Adaptación de aplicación al protocolo IES del Banco de México por validación de unicidad de llaves. (Revisión de llave pública no duplicada en entidades del gobierno).            |

## 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).

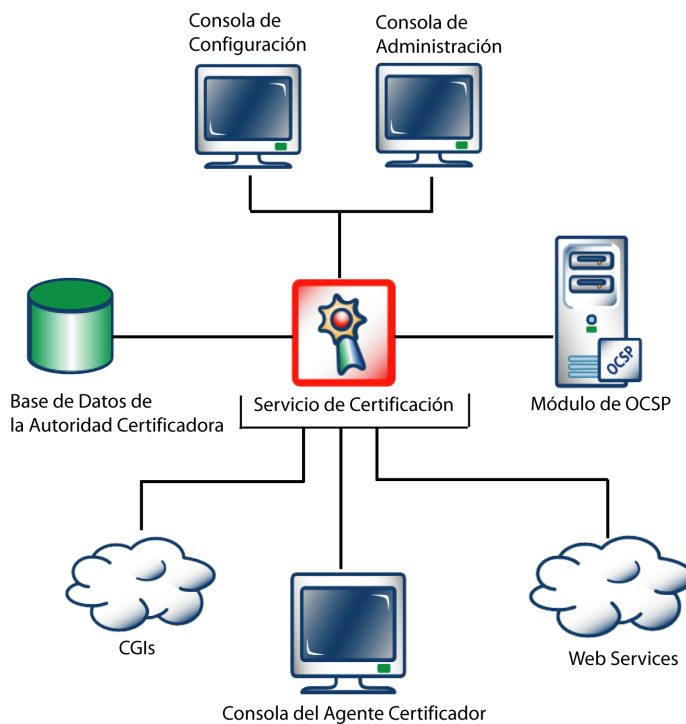


Figura 2.1 Diagrama de los Componentes de SeguriServer

### / 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

# Configuración de OCSP Responder

Uno de los puntos más sensibles en cuanto al uso de los certificados, es el de conocer el estado de revocación que tienen al momento de ser utilizados.

La primera alternativa es la de usar listas de certificados revocados (CRLs), sin embargo, éstas no proporcionan la información actualizada al momento de la consulta.

Una alternativa es la de usar un protocolo de consulta en línea como el Online Certificate Status Protocol (OCSP).

Dentro de los componentes de SeguriServer, se encuentra un servicio de consulta que permite a cualquier aplicación que use este protocolo para verificar el estado de revocación de un certificado, atender las peticiones de consulta y canalizarlas a un servicio de certificación de SeguriServer.

El respondedor automáticamente buscará la autoridad que emitió el certificado consultado y devolverá la respuesta.

Esta aplicación se encuentra en el directorio en que se instaló SeguriServer bajo el nombre *OCSP\_Responder.exe*.

Para utilizar esta aplicación es necesario copiarla y configurarla al equipo en que atenderá peticiones.

---

### / Importante

Es posible que el respondedor OCSP se encuentre en el mismo equipo del servicio de certificación, sin embargo, esto puede impactar en el rendimiento del equipo al atender consultas y operaciones de certificación al mismo tiempo.

---

Los requerimientos de esta aplicación se reducen a contar con un certificado con el atributo OCSP Responder habilitado, los certificados de los servicios de certificación contra los que se realizarán las consultas y acceso a través de la red al equipo en que se encuentran estos servicios.

### 3.1 Configuración del respondedor de OCSP

La configuración de la aplicación, se divide en cuatro partes:

- Parámetros del Servicio
- Administración de Autoridades Certificadoras
- Acceso Automático del respondedor OCSP
- Parámetros de la Base de Datos

Estas operaciones requieren que el archivo *OCSP\_Responder.exe* se encuentre en el equipo que actuará como respondedor OCSP y deberá de ejecutarlo mediante una sesión de línea de comandos.

### 3.2 Parámetros del Servicio

Para que el servicio se pueda controlar fácilmente, haga clic en la carpeta Servicio. (Figura 3.1).



Figura 3.1 Configuración del Servicio

Antes de instalar el servicio, indique el Puerto en el que se atenderán las solicitudes de verificación de estado de revocación, y el archivo en el que residirá la Bitácora de operaciones del respondedor OCSP.

Una vez especificados estos valores, podrá proceder a operar el servicio.

Las operaciones que se pueden realizar son:

- **Instalar**  
El servicio del respondedor OCSP se instalará como servicio del sistema. Se desinstalará estando detenido por medio de Borrar.
- **Remover**  
El servicio del respondedor OCSP se desinstalará de los servicios del sistema. Se podrá borrar siempre que esté detenido.
- **Iniciar**  
El servicio del respondedor OCSP comenzará a atender peticiones. Se podrá ejecutar siempre que se encuentre instalado.
- **Detener**  
El servicio del respondedor OCSP dejará de atender peticiones. Se podrá detener si se encuentra en ejecución.

---

### / Importante

---

Siempre que realice un cambio en algún parámetro de esta ventana, es importante que haga clic en el botón Guardar, para que se mantengan los cambios realizados.

---

## 3.3 Administración de Autoridades Certificadoras

El servicio de OCSP requiere conocer las autoridades con las que consultará el estado de los certificados.

Para esto, se deberá de proporcionar la identificación de la autoridad mediante el certificado del servicio de certificación correspondiente.

Haga clic en la pestaña Autoridades para administrarlas convenientemente.

Las operaciones posibles son agregar, eliminar y modificar autoridades certificadoras. (Figura 3.2).

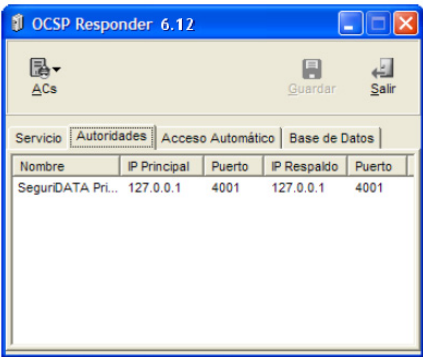


Figura 3.2 Configuración de las Autoridades

3.3.1 Agregar Autoridades Certificadoras

Para agregar el certificado de la Autoridad Certificadora, haga clic en el botón ACs y seleccione Agregar del menú. (Figura 3.3).

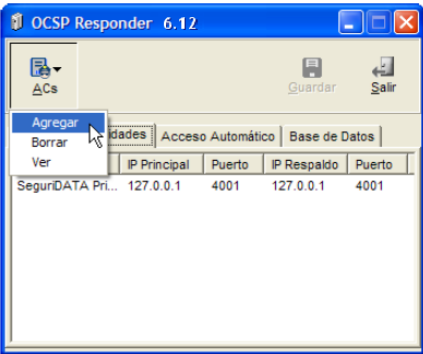


Figura 3.3 Agregar Autoridad

Se presentará el selector de archivos para localizar el certificado de la Autoridad Certificadora correspondiente.

Se desplegará una ventana en la que se deberá indicar la ubicación del archivo que contiene el Certificado, además de las Dirección IP y Puerto en que atienden las peticiones, tanto la principal como la de respaldo. (Figura 3.4).



Figura 3.4 Datos de la Nueva Autoridad

Al terminar de proporcionar los parámetros haga clic en el ícono verde (aceptar). Este procedimiento se deberá repetir para cada autoridad que se desee consultar.

### 3.3.2 Eliminar Autoridades Certificadoras

Si desea eliminar una Autoridad Certificadora, selecciónela y haga clic en el botón ACs y elija Borrar del menú. (Figura 3.5).

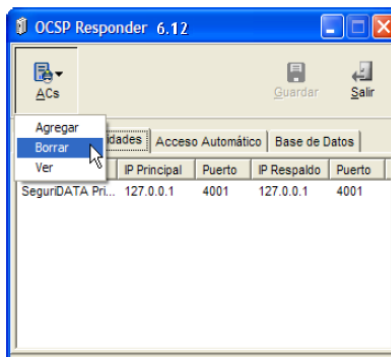


Figura 3.5 Borrar Autoridad

**Warning**

La autoridad seleccionada será borrada y no será consultada en lo sucesivo.

**Importante**

Siempre que realice un cambio en algún parámetro de esta ventana, es importante que haga clic en el botón Guardar, para que se mantengan los cambios realizados.

3.3.3 Ver el Detalle de un Certificado

Si desea ver el detalle del certificado de una autoridad certificadora, selecciónela y haga clic en el botón ACs y elija Ver del menú, como se muestra en la Figura 3.6.



Figura 3.6 Ver Detalle de un Certificado



A continuación se presentará la siguiente ventana con el detalle del certificado de la autoridad certificadora seleccionada. (Figura 3.7).

Certificado

Guardar

Regresar

Número de Serie

01

| Dato         | Emisor                            | Sujeto                            |
|--------------|-----------------------------------|-----------------------------------|
| Razón Social | SeguriDATA Privada, S.A.          | SeguriDATA Privada, S.A.          |
| Area         | QA                                | QA                                |
| Nombre       | Autoridad Certificadora Belencita | Autoridad Certificadora Belencita |
| Dirección    | Panzacola #62, 1er. Piso          | Panzacola #62, 1er. Piso          |
| CP           | 04000                             | 04000                             |
| País         | MX                                | MX                                |

Llave Pública

03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 b6 07 cf 95 a6 cf 3e 12 ab a6 5e 79 f0  
b2 3c 77 38 18 60 60 55 5e 79 81 24 75 c5 72 f9 da 3b 97 f0 53 4a 87 51 78 e7 31 75  
db 92 f4 13 a5 45 e6 a6 53 bc df 1b 92 de 80 61 d2 68 e3 f4 0c 81 1d 67 b6 0d 94 20

Condición

Sí está dentro del rango de validez

Hoy

2007/12/13 19:33

Válido a partir de

2004/11/10 00:00

Válido hasta el

2014/11/08 00:00

Figura 3.7 Detalle del Certificado

3.4 Parámetros del Respondedor OCSP

Las respuestas que devuelve el respondedor OCSP son firmadas con el certificado que se asocia a este servicio. Este certificado deberá tener el atributo de OCSP Responder habilitado.

Haga clic en la carpeta Acceso Automático que presenta la siguiente ventana. (Figura 3.8).



Figura 3.8 Configuración del Acceso Automático

Seleccione la casilla Utilizar Login Automático si desea utilizar esta opción, e indique los nombres de los archivos que contienen el Certificado y Llave Privada, incluyendo su ubicación completa.

Es posible hacer clic en el ícono a la derecha de cada campo para usar el selector de archivos y localizarlos fácilmente.

Finalmente, deberá escribir su Clave de Acceso para usar esta funcionalidad.

### / Importante

Siempre que realice un cambio en un parámetro de esta ventana, es importante que haga clic en el botón Guardar, para que se mantengan los cambios realizados.

### 3.5 Configuración de la Base de Datos


Parámetros que permiten configurar la base de datos de SeguriServer, con el fin de que OSCP Responder se comuniquen directamente a esta base y consulte el estatus de los certificados más rápido. (Figura 3.9).

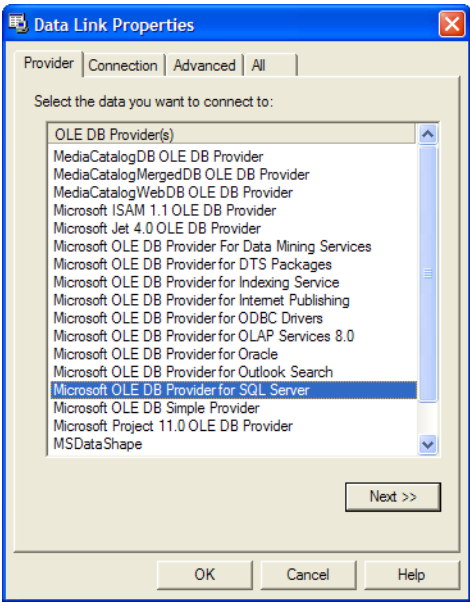


Figura 3.9 Configuración de la Base de Datos

Si desea utilizar esta función, marque la casilla Hacer consulta en base de datos y proporcione los datos solicitados como se indica en la Tabla 3.1.

Tabla 3.1 Parámetros de Configuración de la base de datos de SeguriServer

| Parámetro          | Descripción  |
|--------------------|--|
| Cadena de Conexión | Haga clic en el botón  que presenta la siguiente ventana. |

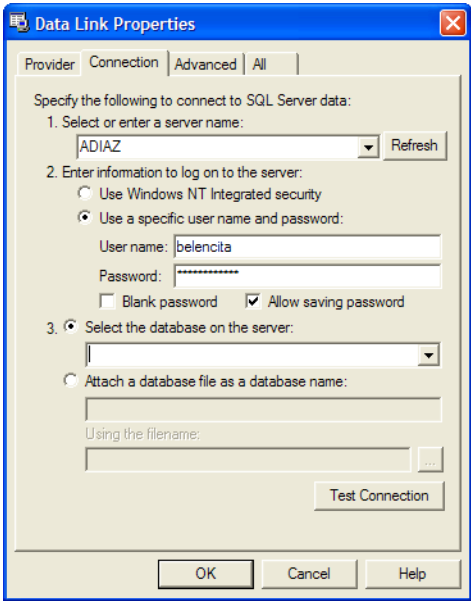


Seleccione el tipo de base de datos para la conexión a la misma. Haga clic en el botón Next >>.

Tabla 3.1 Parámetros de Configuración de la base de datos de SeguriServer (Continuación)

| Parámetro | Descripción |
|-----------|-------------|
|-----------|-------------|

Haga clic en la carpeta Connection.



Indique los datos solicitados:

- 1.- Select or enter a server name:
  - a) Haga clic sobre la lista de servidores. A continuación se desplegarán los nombres de aquellos que están disponibles. Seleccione el nombre del servidor donde fue creada la base de datos.
- 2.- Enter information to log on to the server
  - a) Para especificar un usuario SQL, seleccione la opción Use a specific user name and password
  - b) En el campo User name especifique el nombre del usuario de base de datos.
  - c) En el campo Password especifique la contraseña para el usuario indicado anteriormente.
  - d) Marque la casilla Allow saving password
- 3.- Select the database on the server
  - a) Haga clic sobre la lista de bases de datos disponibles en el servidor configurado.
  - b) Haga clic en le botón Test Connection para verificar la conexión.

Haga clic en el botón OK.

Tabla 3.1 Parámetros de Configuración de la base de datos de SeguriServer (Continuación)

| Parámetro                 | Descripción  |
|---------------------------|--|
| Usuario                   | Indique el nombre del usuario de la base de datos.             |
| Clave de acceso           | Escriba la clave de acceso a la base de datos de SeguriServer. |
| Servidor de Base de Datos | Seleccione el tipo de base de datos que utiliza SeguriServer.  |

/ Importante

Siempre que realice un cambio en algún parámetro de esta ventana, es importante que haga clic en el botón Guardar, para que se mantengan los cambios realizados.