ACA versión 2.0

Manual de OCSP Multiservicio

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: SACA-0200-0100-3-00

Contenido

CAPÍTULO 1

¿Cómo utilizar este manual?

1.1 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.

1.1.1 Recomendaciones y Advertencias

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

Importante

Este tipo de anotaciones contienen 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.

1.1.2 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 e

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

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*.

1.1.3 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.

1.2 Objetivo de este manual

OCSP Multiservicio es una aplicación que instala e inicia los servicios OCSP que sean necesarios para las autoridades certificadoras reconocidas dentro de la infraestructura ACA. Este manual está dirigido al personal que actuará como administrador de ACA, a cargo de labores de instalación y configuración de la misma.

Todas las especificaciones de la aplicación se encuentran en los siguientes capítulos de este manual.

CAPÍTULO 2

Introducción de la ACA

2.1 Introducción

ACA es una solución diseñada para proporcionar servicios de consulta en línea para las autoridades certificadoras que operan en un entorno de seguridad utilizando el protocolo estándar OCSP (RFC 2560).

En un entorno donde funcionan varias autoridades certificadoras, los usuarios tienen la necesidad de obtener información sobre el estado de revocación de los certificados emitidos por estas autoridades. La capacidad de obtener esta información usando mecanismos en línea es de gran valor en entornos críticos donde la información utilizada en el proceso de validación de certificados debe ser lo más reciente posible. Por ejemplo; en ambientes financieros y comerciales, como el caso de IDENTRUS en Norteamérica.

ACA es una solución que permite cumplir con esta demanda de manera flexible y permite integrar a un entorno crítico autoridades certificadoras que no cuentan con el servicio de consulta en línea como parte de su funcionalidad.

ACA permite crear servicios OCSP a través de un repositorio de información en donde se registra el status de revocación de los certificados emitidos por estas autoridades. El repositorio ACA cuenta con servicios de consulta, registro y administración que garantizan la disponibilidad, seguridad y control de la información crítica para el entorno de seguridad.

Los usuarios de infraestructuras de seguridad enfrentan el problema de la búsqueda de servicios de consulta. Las aplicaciones que manejan certificados digitales deben validar el status de revocación de los mismos y para tal fin deben obtener información que les permita localizar los servicios de consulta necesarios.

ACA permite simplificar este problema a través del intermediario OCSP que se encarga de recibir y dirigir las peticiones de consulta a los servicios designados y autorizados para responder a esas peticiones.

ACA incorpora distintas autoridades certificadoras a un entorno crítico, sin necesidad de someterlas a procesos de integración complicados y costosos, aprovechando productos e

infraestructuras existentes para extender al entorno de seguridad permitiendo responder a las necesidades de organizaciones de gran tamaño.

2.2 Arquitectura y componentes de ACA

ACA está formado de varios componentes que conforman una solución completa de acuerdo a las necesidades de los usuarios y a la infraestructura existente en una organización.

Los componentes de ACA se dividen en Internos y Externos.

Los componentes internos son los responsables de dar servicios y llevar a cabo las tareas de administración de la solución. Estos son:

1. OCSP Multiservicio

   El componente OCSP multiservicio es una aplicación que permite crear servidores OCSP capaces de generar respuestas a peticiones OCSP para autoridades que lo requieran. Estos servicios cuentan con la capacidad de realizar consultas en el repositorio ACA para obtener la información de revocación necesaria.

2. Servicio de registro de servidores OCSP
3. Repositorio de información ACA

   El repositorio ACA es una base de datos donde se almacena información de revocación, certificados digitales e información necesaria para la administración de la solución. Este repositorio cuenta con una interfaz de administración que sirve para controlar el uso del repositorio.

4. Administrador del repositorio ACA
5. Wizard de inicialización del repositorio ACA

Los componentes externos son los que interactuan directamente con los usuarios. Estos son:

1. Intermediario OCSP (OCSP Broker). Ver {2.3 Intermediario OCSP}

   El intermediario OCSP es un CGI que recibe las peticiones OCSP de las aplicaciones que requieren información sobre el status de revocación de certificados emitidos por autoridades certificadoras que no cuentan con OCSP. Este componente se encarga de dirigir las peticiones al servicio OCSP adecuado, utilizando la información que le proporciona el servicio de registro de servidores OCSP. En este servicio de registro se dan de alta los servidores OCSP reconocidos dentro del entorno y destinados a ofrecer la funcionalidad de consulta por OCSP para las autoridades que no cuentan con ella.

2. Servicios Web de registro. Ver {Ref a 2.4 Servicios Web ACA}

   Los servicios Web ACA son servicios que permiten realizar registro de certificados y actualizar su información de revocación. Estos servicios ofrecen seguridad en las operaciones de registro y revocación al requerir firma digital por parte de los agentes registradores.

La relación entre los componentes se ilustra en la Figura 2.1

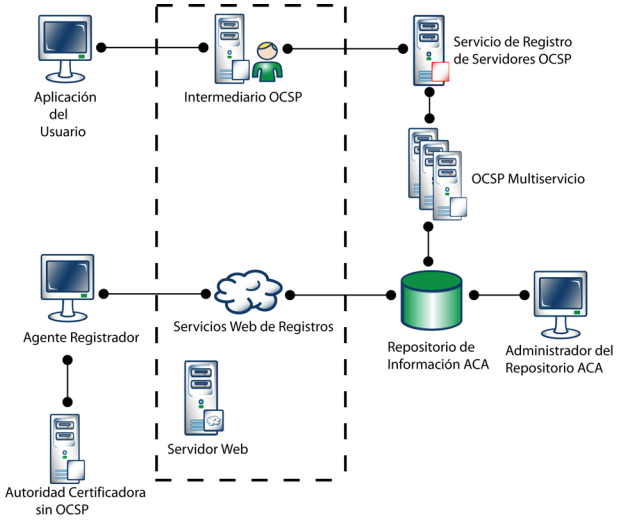


Figura 2.1 Componentes del Servicio de Validación de Certificados

CAPÍTULO 3

Instalación de OCSP Multiservicio

3.1 Requerimientos del sistema

Esta aplicación se encarga de instalar e iniciar los servicios OCSP que sean necesarios para las autoridades certificadoras reconocidas dentro de la infraestructura ACA. Los servicios OCSP deben configurarse usando esta aplicación de acuerdo a las necesidades de las autoridades certificadoras. En caso necesario, un servicio OCSP podrá accesar al repositorio ACA para obtener información de revocación. Además esta aplicación es utilizada para dar de alta servicios en el registro OCSP.

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 el ambiente Microsoft® Windows
- la instalación de aplicaciones de Microsoft® Windows y
- la configuración de servicios de red bajo Microsoft® Windows.

Los requerimientos mínimos para el equipo son:

- PC con procesador Pentium II @300MHz o superior.
- 64 Mb de memoria RAM
- 5 Mb libres en disco duro
- Unidad de CD-ROM
- Unidad de disco flexible o conexión a red
- Sistema operativo Microsoft® Windows 2000 Server® con ServicePack 2, o superior

- Un puerto serial habilitado y disponible, en caso de utilizar lector de Tarjeta Inteligente
- Cliente Oracle 8i ó superior

La aplicación se divide en dos etapas que deben ejecutarse en el siguiente orden:

1. Instalación de los componentes
2. Configuración de los servicios OCSP

Para iniciar la instalación deberá contar con el CD de la aplicación. Se recomienda leer el procedimiento de instalación para asegurarse de que se cuenta con todos los elementos necesarios para la instalación, así como tenerlo a la mano como referencia.

Finalmente, para el eventual caso de que requiera apoyo del Soporte Técnico de SeguriData, encontrará nuestros teléfonos en las primeras páginas de este manual.

3.2 Instalación de los componentes

Inserte el CD de la aplicación en el lector de CD-ROM y con ayuda del explorador de archivos localice el archivo `OCSPMultiservicioACA21.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 Inicio de la Instalación

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

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

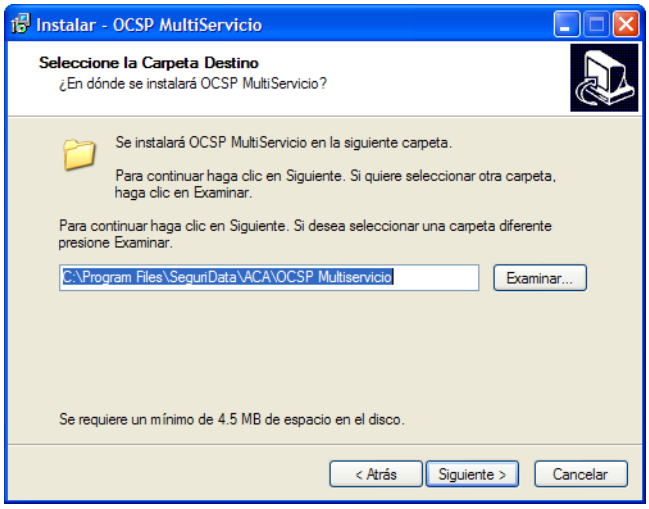


Figura 3.2 Selección de la Carpeta Destino

El valor predeterminado es el directorio

```
c:\Program Files\SeguriData\ACA\OCSP Multiservicio
```

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, deberá de hacer clic en el botón Siguiente >.

Como siguiente paso se deberá indicar el grupo de programas bajo el que se creará el acceso a los componentes de la aplicación bajo el menú de Microsoft® Windows. (Figura 3.3).

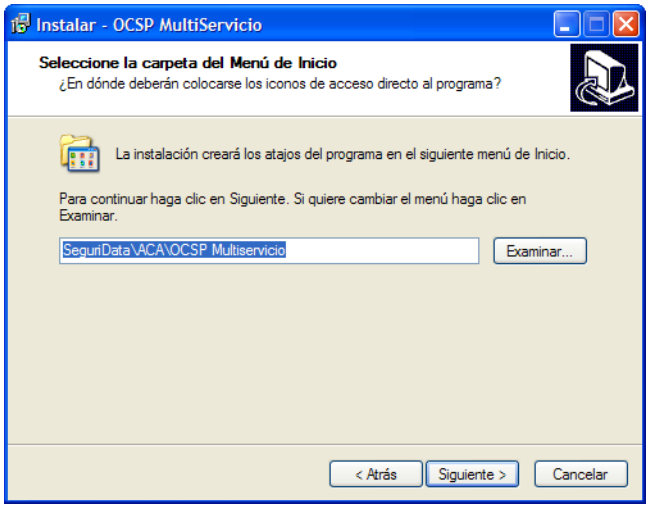


Figura 3.3 Selección de la Carpeta Menú de Inicio

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).

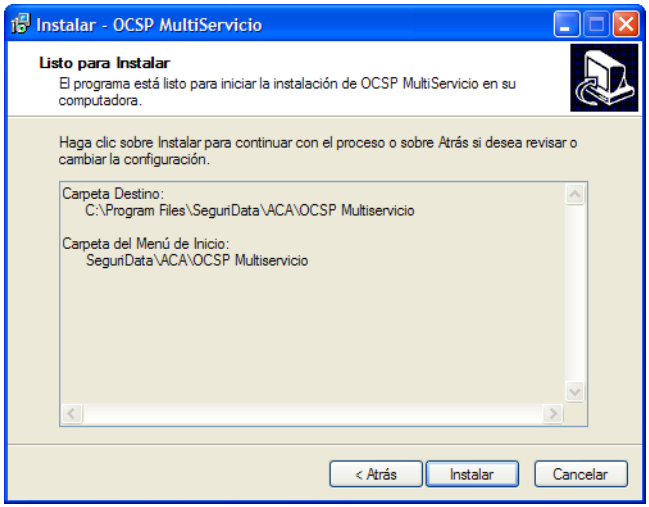


Figura 3.4 Resumen de Valores Seleccionados

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

Haga clic en el botón Terminar.

CAPÍTULO 4

Configuración de OCSP Multiservicio

Este módulo permite definir varios servicios OCSP en un mismo equipo, a través de la siguiente consola. (Figura 4.1).

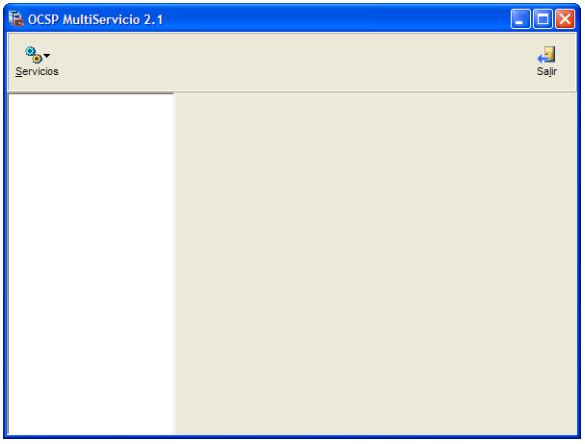


Figura 4.1 Consola de Configuración

4.1 Administración de Servicios OCSP

4.1.1 Nuevo Servicio

Como primer paso será la creación de un nuevo servicio OCSP. Haga clic en botón Servicios que presenta el siguiente menú. (Figura 4.2).

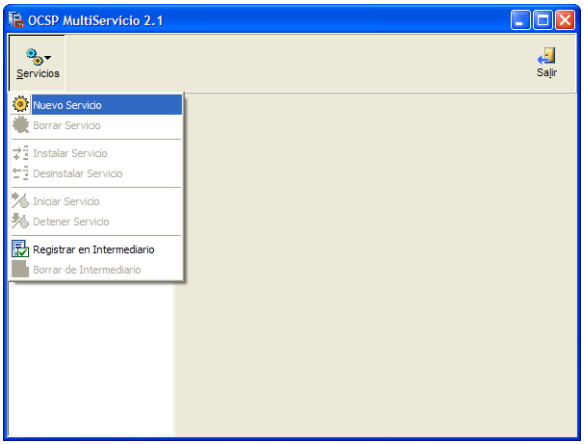


Figura 4.2 Nuevo Servicio

Seleccione la opción Nuevo Servicio del menú.

A continuación se presentará el nombre del nuevo servicio que por omisión de la aplicación se le asigna un nombre, si desea puede cambiarlo haciendo clic sobre éste. (Figura 4.3).

Figura 4.3 Nombre del Nuevo Servicio OCSP

En el campo Bitácora indique la ruta y escriba el nombre del archivo donde se guardaran los registros de errores de la aplicación.

En el campo Puerto seleccione el número de puerto por donde escuchará las peticiones el nuevo servicio OCSP.

Importante

Para identificar que un servicio ha sido creado, éste se marcará con una esfera de color azul.

Haga clic en el icono [+] para desplegar las carpetas de configuración del nuevo servicio OCSP, como se muestra en la Figura 4.4.

Figura 4.4 Carpetas de Configuración

4.2 Acceso Automático

Se utiliza para que el Servicio OCSP inicie automáticamente sin intervención del administrador. (Figura 4.5).

Figura 4.5 Configuración del Acceso Automático

Para activar el modo automático, marque la casilla Utilizar Acceso Automático e indique los parámetros de acuerdo a la Tabla 4.1

Tabla 4.1 Parámetros de Acceso

Parámetro	Descripción
Clave de Acceso	Indique la clave de acceso para la llave privada del servicio OCSP.
Llave Privada OCSP	Indique la ruta y el nombre de la llave privada del servicio OCSP.
Certificado OCSP	Indique la ruta y el nombre del certificado del servicio OCSP.

4.3 Autoridad Certificadora

Esta consola permite dar de alta el certificado de la autoridad certificadora del servicio OCSP. (Figura 4.6).

Figura 4.6 Configuración de la Autoridad Certificadora del Servicio OCSP

Indique la ruta y el nombre del Certificado de Autoridad Certificadora del servicio OCSP. Una vez indicado el certificado, se presentaran los datos generales de éste en el campo Datos de Autoridad Certificadora.

4.4 Información de Revocación

Permite obtener el detalle de una revocación de un certificado por medio de SeguriServer o de un repositorio central. (Figura 4.7).

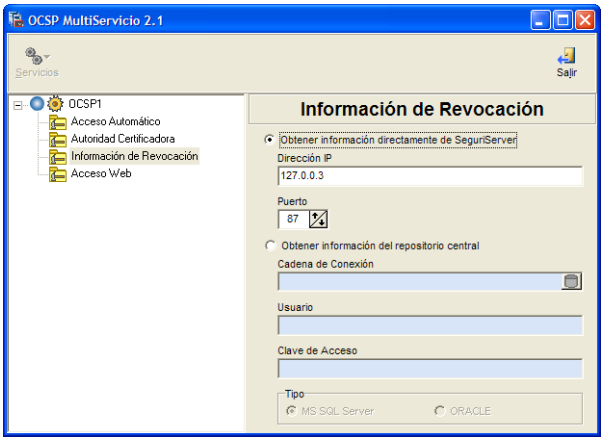


Figura 4.7 Información de Revocación

Marque la opción del modo de operación correspondiente y llene los parámetros necesarios.

Los parámetros requeridos para SeguriServer se explican en la Tabla 4.2.

Tabla 4.2 Parámetros de SeguriServer

Parámetro	Descripción
Dirección IP	Indique la dirección IP de SeguriServer.
Puerto	Indique el puerto por donde escucha las peticiones SeguriServer.

Marque el tipo de base de datos e indique parámetros requeridos para el Repositorio Central que se explican en la Tabla 4.3.

Tabla 4.3 Parámetros para repositorio central

Parámetro	Descripción
Cadena de Conexión	Haga clic en el botón a la derecha del campo. Se desplegará una ventana en la que deberá seleccionar el manejador de base de datos: Provider for SQL Server o Provider for Oracle.

Tabla 4.3 Parámetros para repositorio central (Continuación)

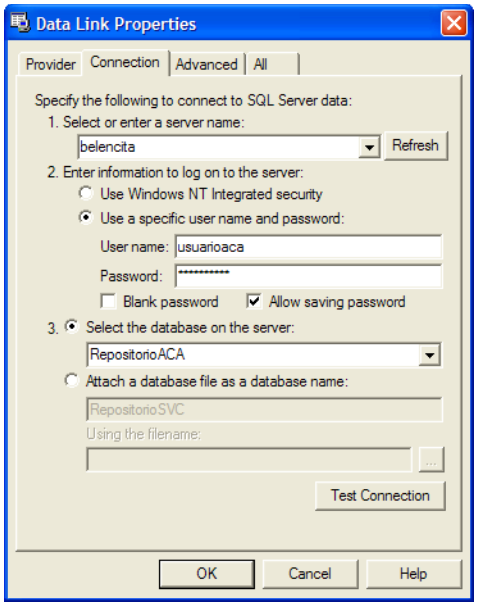
Parámetro	Descripción
	Haga clic en la carpeta Connection.  En la siguiente ventana especifique los parámetros de acceso. 1.- Select or enter a server name: a) Haga clic sobre la lista de servidores. A continuación se desplegarán los nombres de aquellos que están disponibles. Seleccione el nombre del 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 como usuario, clave de acceso, etc.

Tabla 4.3 Parámetros para repositorio central (Continuación)

Parámetro	Descripción
	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.
Usuario y Clave	El usuario y clave de acceso son definidos en el campo Cadena de Conexión y se reflejan en estos campos.

4.5 Acceso Web para Intermediario OCSP

Permite aportar la información necesaria para registrar este servicio con el intermediario. (Figura 4.8).

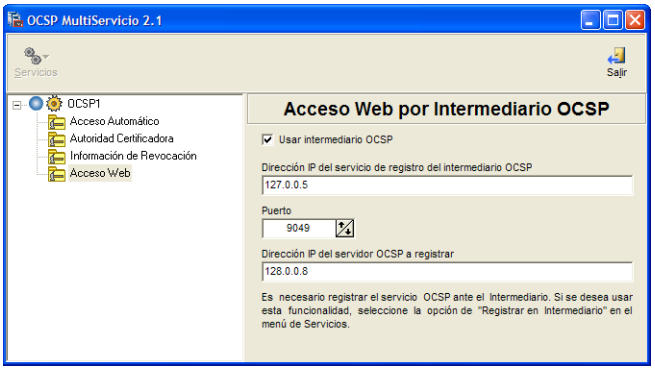


Figura 4.8 Configuración del Acceso Web por Intermediario OCSP

Para Usar intermediario OCSP marque la casilla y proporcione los parámetros solicitados como se muestra en la Tabla 4.4.

Tabla 4.4 Parámetros de Intermediario OCSP

Parámetro	Descripción
Dirección IP del servicio de registro del Intermediario OCSP	Indique la dirección IP del servicio de registro de intermediario OCSP.
Puerto	Indique el número de puerto del servicio de registro del intermediario OCSP.
Dirección IP del servidor OCSP a registrar.	Indique la dirección IP del servidor OCSP que se va a registrar.

Precaución

Registre el servicio OCSP ante el intermediario que corresponde, seleccionando el botón Servicios y elija la opción Registrar en Intermediario, para crear el intermediario en la lista de clientes de un servicio OCSP. (Figura 4.9).

Figura 4.9 Registrar en Intermediario

Y para eliminar el Intermediario de la lista de clientes de un servicio OCSP, haga clic en el botón Servicios y seleccione la opción Borrar Intermediario.

4.6 Instalación del Nuevo Servicio

Una vez que se hayan configurado todos los parámetros del servicio OCSP, éste deberá ser instalado para que aparezca como servicio en Windows y el sistema operativo lo

registre. Haga clic en el botón Servicios y seleccione la opción Instalar Servicio como se muestra en la Figura 4.10.

Figura 4.10 Instalar Servicio

Importante

La esfera de color azul cambiará a color rojo indicando que el servicio ha sido instalado, como se muestra en la Figura 4.11.

Figura 4.11 Servicio Instalado

4.7 Iniciar el Nuevo Servicio

A continuación se deberá iniciar el servicio OCSP. Haga clic en el botón Servicios y seleccione la opción Iniciar Servicio del menú, como se muestra en la Figura 4.12.

Figura 4.12 Iniciar Servicio

Importante

La esfera de color rojo cambiará a color verde indicando que el servicio ha sido ejecutado, como se muestra en la Figura 4.13.

Figura 4.13 Servicio Iniciado

4.8 Borrar Servicio

Para eliminar un servicio, es necesario que éste haya sido detenido. Haga clic en el botón Servicios y seleccione la opción Detener Servicio, como se muestra en la Figura 4.14.

Figura 4.14 Detener Servicio

Importante

La esfera de color verde cambiará a color rojo indicando que el servicio ha sido detenido.

A continuación haga clic en el botón Servicios y seleccione la opción Borrar Servicio, como se muestra en la Figura 4.15.

Figura 4.15 Borrar Servicio

Importante

Al finalizar la configuración, deberá terminar la sesión, haciendo clic en el botón Salir.