DISTRIBUCIÓN LIMITADA

SP Iberia

W2KDCMng: Certificación de Controladores de Dominio Windows 2008

DISTRIBUCIÓN LIMITADA

Certificación de Controladores de Dominio Windows 2008

Safelayer Secure Communications, S.A.

Teléfono: +34 93 508 80 90

Fax: +34 93 508 80 91

Web: www.safelayer.com

Email: support@safelayer.com

CONTENIDO

Introducción

El presente documento describe el uso de la aplicación **W2KDCMng**, cuyo cometido es facilitar la certificación de controladores de dominio Windows 2008 mediante autoridades de certificación de terceros.

La aplicación ofrece las siguientes utilidades:

- Borrado de los certificados de controlador de dominio existentes en la máquina. Esta funcionalidad es útil si se ha llegado a instalar una CA de Microsoft en el dominio, en cuyo caso el controlador de dominio se autocertifica sin pedir consentimiento al administrador de la máquina.
- Generación de la petición de certificación en formato PKCS#10, incluyendo las extensiones necesarias para su reconocimiento como certificado de controlador de dominio.
- Instalación del certificado una vez generado.

CAPÍTULO 1

Instalación

Ficheros de la aplicación

La aplicación se compone de tres ficheros:

- W2KDCMng.exe
- Interop.CAPICOM.dll
- Interop.CERTENROLLLib.dll

Dependencias de la aplicación

La aplicación depende de los siguientes componentes de Microsoft:

- **CAPICOM 2.1.0.2** Disponible en:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=860ee43a-a843-462f-abb5-ff88ea5896f6&DisplayLang=en

- **Microsoft .NET Framework**. Disponible en Windows Update, o también en:

  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=333325fd-ae52-4e35-b531-508d977d32a6

  NOTA: W2KDCMng ha sido probado sobre las siguientes versiones de .NET Framework:

  v 3.5

- **Windows 2008**

Instalación de la aplicación

La aplicación **W2KDCMng** no tiene programa de instalación. Para instalarla, deben seguirse los siguientes pasos:

1. Como requisito previo, la máquina donde se instale debe ser un Controlador de Dominio Windows 2008, y debe operarse con permisos de administración local.
2. Instalar el componente **Microsoft .NET Framework**.

3. Instalar **CAPICOM 2.1.0.2**. Este componente no tiene instalador, pero está encapsulado íntegramente en una DLL llamada `CAPICOM.DLL`. La instalación consiste en copiar el archivo a cualquier directorio del disco, por ejemplo `C:\Winnt\System32`, y ejecutar desde línea de comandos:

   ```
   regsvr32 capicom.dll
   ```

4. Copiar los archivos de la aplicación a cualquier directorio de la máquina.

Procedimiento alternativo

En el caso de que no sea posible o no se desee instalar el componente **Microsoft .NET Framework**, seguir los siguientes pasos.

1. Instalar **CAPICOM 2.1.0.2** en el Controlador de Dominio Windows 2008 siguiendo el mismo procedimiento anterior.

2. Instalar **Microsoft .NET Framework** en una máquina Windows 2008 distinta (en adelante **Máquina 2**).

3. Copiar el directorio `<WINNT>\Microsoft.NET\Framework` de la Máquina 2 a un directorio local cualquiera, por ejemplo `C:\DOTNET`, del Controlador de Dominio a certificar. En adelante, se hará referencia a este directorio como **<DOTNET>**.

4. Copiar el archivo `<WINNT>\mscoree.dll` de la Máquina 2 al directorio `<DOTNET>\v3.5` (Nótese que el nombre de este directorio coincide con el número de versión de Microsoft .NET Framework).

5. Copiar los archivos de la aplicación al mismo directorio (`<DOTNET>\v3.5`).

6. Editar el registro de Windows y realizar las siguientes operaciones:

   a. Crear la clave `HKLM/Software/Microsoft/.NETFramework`.

   b. Añadir un valor alfanumérico con las siguientes propiedades:

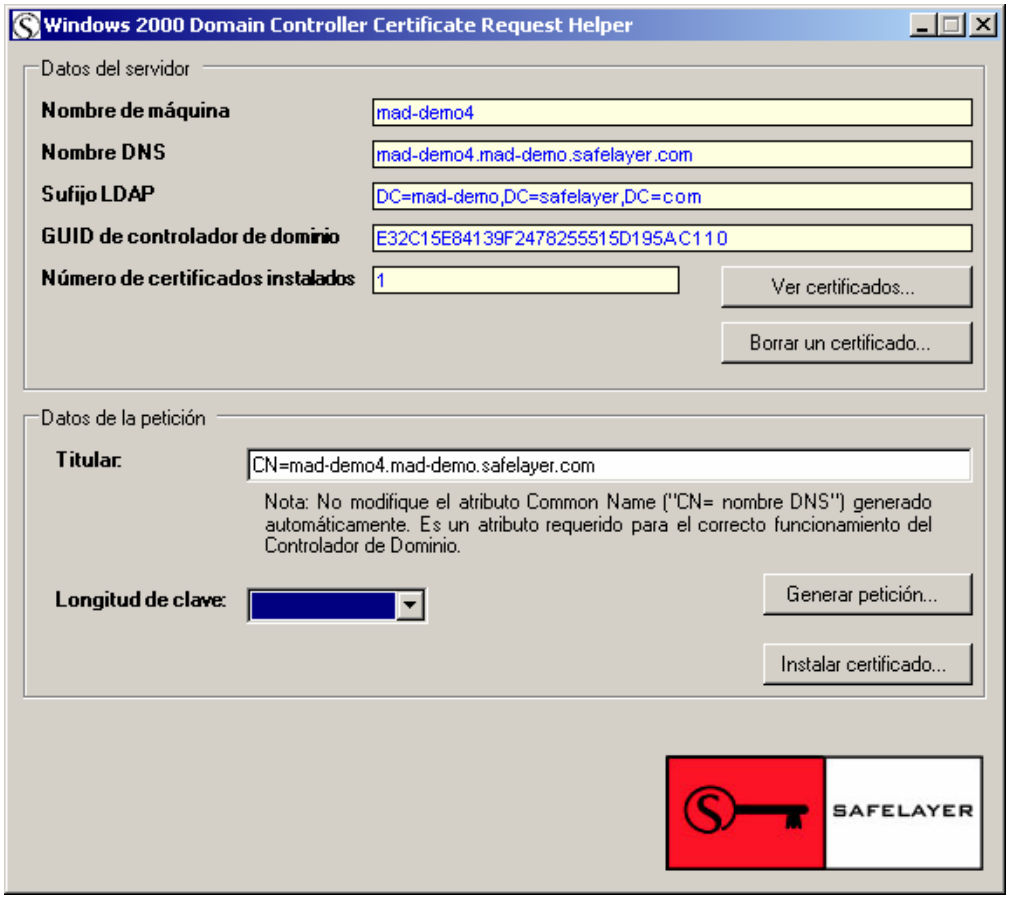
      Nombre: **InstallRoot**

      Valor**: <DOTNET>**

CAPÍTULO 2

Uso de W2KDCMng

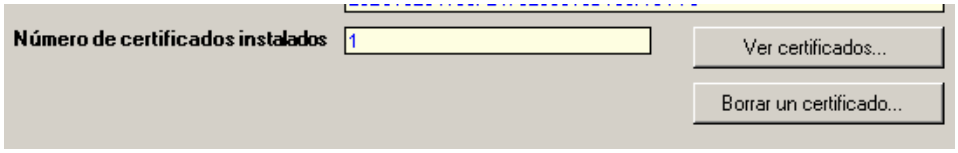
Para iniciar la aplicación, ejecute el archivo `W2KDCMng.exe`. La aplicación obtendrá los datos necesarios del dominio y, transcurridos unos segundos, mostrará la ventana principal:



En los siguientes apartados se describen las operaciones que permite realizar la aplicación.

Gestión de certificados de Windows 2008 DC

En la sección "Datos del servidor" dispone de las opciones de gestión de los certificados ya instalados en la máquina:

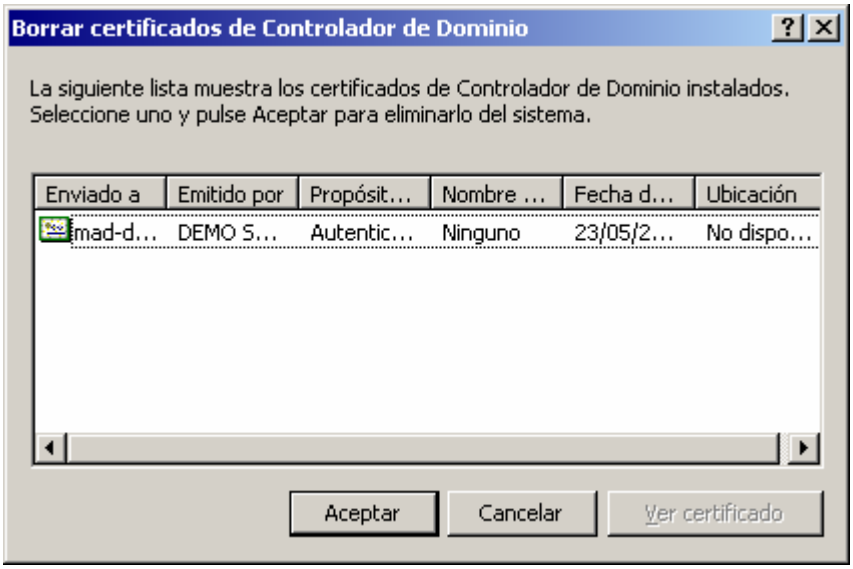


La etiqueta "Número de certificados instalados" muestra el número de certificados de controlador de dominio instalados en la máquina. Sólo muestra este tipo de certificados, ignorando cualquier otro tipo, como por ejemplo certificados personales o el certificado de la CA de Microsoft en caso de estar instalada. Además, muestra únicamente los certificados cuya cadena de certificación ha sido validada correctamente contra los almacenes de certificados de confianza de Windows. Si una vez instalado un certificado de controlador de dominio, no se añade a este contador, verifique que Windows valida correctamente el certificado recién instalado.

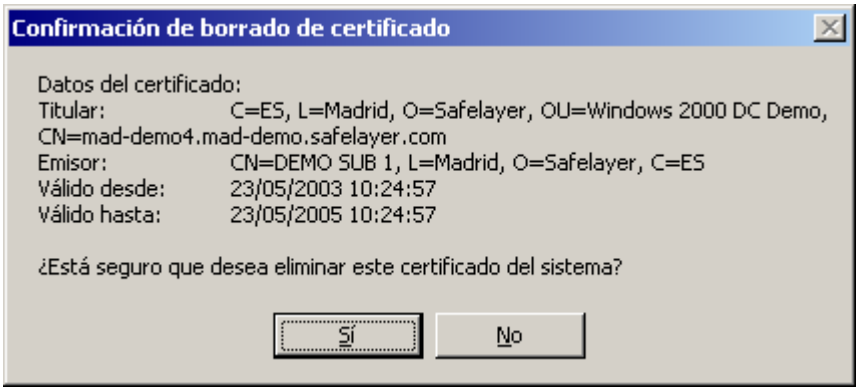
Si pulsa el botón "Ver certificados..." se mostrará la siguiente ventana:

Esta ventana le permite visualizar los detalles de los certificados de Controlador de Dominio instalados.

Si desea eliminar alguno de los certificados existentes, pulse el botón "Borrar un certificado...". Se mostrará una ventana muy similar a la anterior:

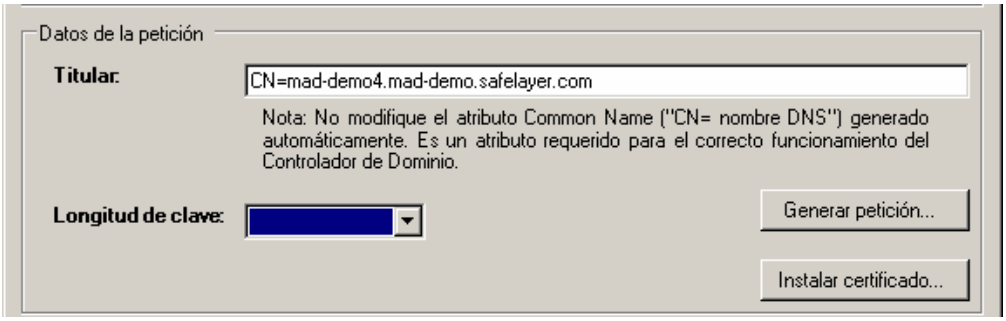


Seleccione el certificado que desee eliminar, y pulse **Aceptar**. Se mostrará un mensaje de confirmación:



Generación de la petición de certificación

En la sección "Datos de la petición" dispone de las opciones para generar la petición de certificación:



Para generar la petición siga los siguientes pasos:

1. Defina la longitud de clave. Se soportan longitudes de clave de 1024 y 2048 bits.

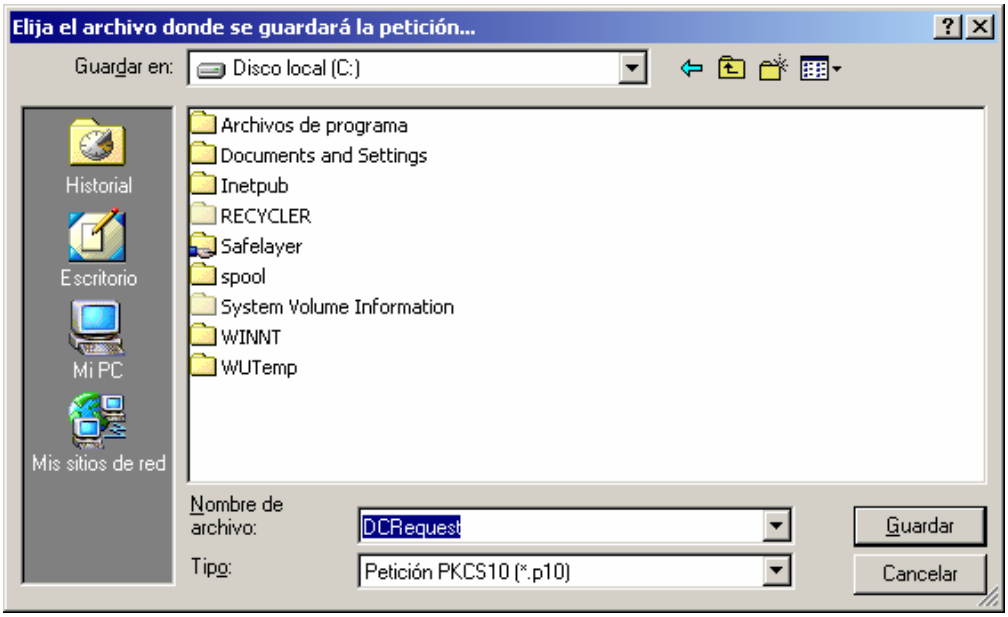
2. Defina el Subject (Titular) que tendrá el certificado. Para ello, edite el cuadro de texto "Titular" para añadir los atributos que desee, sin eliminar el atributo Common Name (CN), que es obligatorio. Tenga en cuenta que en este cuadro de texto el orden de los atributos es el contrario al habitual. Por ejemplo, si desea definir el Subject como

   ```
   CN=mad-demo4.mad-demo.safelayer.com, OU=Pruebas, O=Safelayer, C=ES
   ```

   deberá escribirlo como

   ```
   C=ES, O=Safelayer, OU=Pruebas, CN= mad-demo4.mad-demo.safelayer.com
   ```

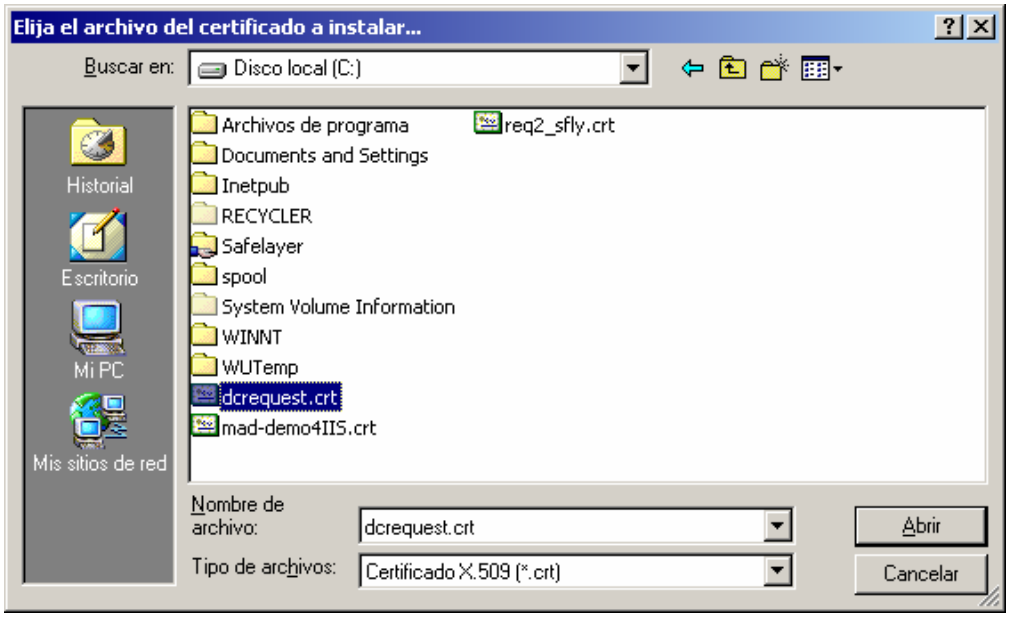
3. Pulse el botón "Generar petición...". Se mostrará una ventana preguntándole por el fichero en el que se guardará la petición:



4. Una vez escogido el fichero, pulse **Guardar**. Dependiendo de la longitud de clave y de la velocidad del sistema, este proceso podrá durar unos segundos, tras los cuales verá un mensaje de finalización:

Instalación del certificado

Una vez generado el certificado del Controlador de Dominio, pulse el botón "Instalar certificado...". El programa le pedirá el fichero del certificado:



Una vez seleccionado el archivo, recibirá un mensaje de finalización:

APÉNDICE A

Plantilla de certificación

Para completar la certificación de un controlador de dominio Windows 2008 mediante KeyOne® CA, es necesario configurar una plantilla de certificación que incorpore las extensiones necesarias. La siguiente plantilla sirve de ejemplo para estos propósitos:

```
version = v3
serialNumber = sequential
signingAlgorithms = :set *sha1WithRsaSignature
validityPeriod = :timeoffset 2 year
publicKey = :record algorithm, parameters, minBits, maxBits
publicKey.algorithm = rsaEncryption
publicKey.parameters = :text ""
publicKey.minBits = :number 1024
publicKey.maxBits = :number any
subjectAltName = present any
keyUsage = present :set *digitalSignature, *keyEncipherment
extKeyUsage = present :set *serverAuth, *clientAuth
subjectKeyIdentifier = present any
authorityKeyIdentifier = present any
cRLDistributionPoints = present any
OID.1.3.6.1.4.1.311.20.2 = present :asn1encoding
'HiAARABvAG0AYQBpAG4AQwBvAG4AdABByAG8AbABsAGUAcg=='
```

SAFELAYER SECURE COMMUNICATIONS, S.A.

Edificio Valrealty C/ Basauri, 17 Edifico B Pl. Baja Izq. Of. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652
Edif. World Trade Center (S-4), Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091

WWW.SAFELAYER.COM