Contenido

Introducción

Este documento aclara algo la confusión que acompaña a los diversos tipos de certificado, formatos y requisitos asociados a las diversas formas del Protocolo de Autenticación Ampliable (EAP). Los cinco tipos de certificado relacionados con EAP que se describen en este documento son Servidor, CA Raíz, CA Intermedia, Cliente y Máquina. Estos certificados se encuentran en diversos formatos y pueden tener requisitos diferentes según la implementación de EAP empleada.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Certificados de servidor

El certificado de servidor está instalado en el servidor de RADIUS y su propósito primario en el EAP es crear el túnel cifrado de Transport Layer Security (TLS) que protege la información de autenticación. Cuando usted utiliza el EAP MSCHAPv2, el certificado de servidor toma en rol secundario que es identificar al servidor de RADIUS como entidad confiable para la autenticación. Esto rol secundario es realizado con el uso del campo del Enhanced Key Usage (EKU). El campo del EKU identifica el certificado como certificado de servidor válido y lo verifica que raíz CA que publicó el certificado es una Raíz confiable CA. Esto requiere la presencia de certificado raíz CA. El Cisco Secure ACS requiere que el certificado sea formato binario codificado en base64 o DER-codificado del v3 X.509.

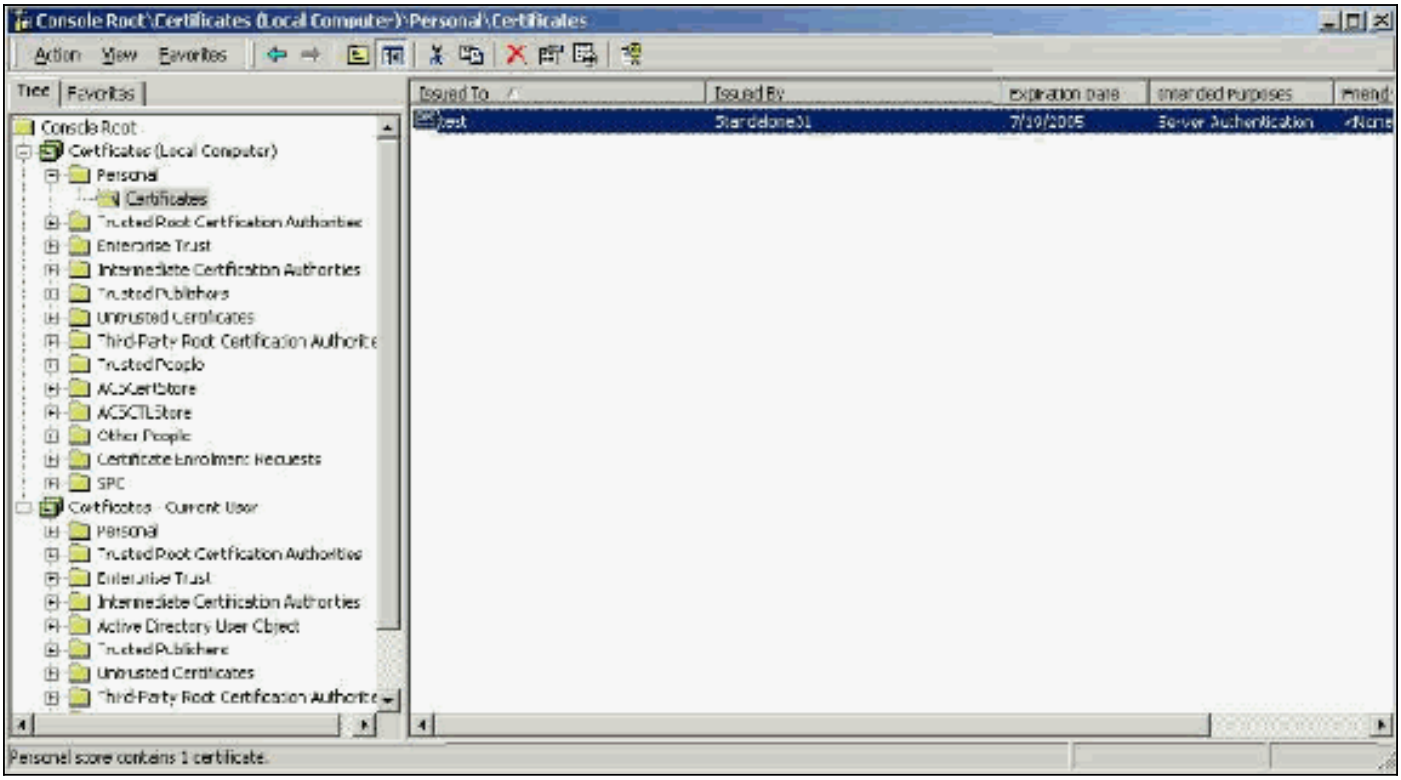
Usted puede crear este certificado con cualquiera el uso de un pedido de firma de certificado (CSR) en el ACS, que se somete a CA. O, usted puede también cortar el certificado con el uso de una forma interna de la creación del certificado de CA (como los servicios de certificados de Microsoft). Es importante observar que, mientras que usted puede crear el certificado de servidor con los tamaños de clave más grandes de 1024, ningún dominante más en gran parte de 1024 no trabaja con el PEAP. El cliente cuelga incluso si la autenticación pasa.

Si usted crea el certificado con el uso de un CSR, se crea con .cer, el .pem, o el formato de .txt. En las raras ocasiones, se crea sin la extensión. Asegúrese de que su certificado sea un archivo de sólo texto con una extensión que usted pueda cambiar según las necesidades (el dispositivo ACS utiliza la extensión de .cer o del .pem). Además, si usted utiliza un CSR, la clave privada del certificado se crea en la trayectoria que usted especifica como archivo distinto que pueda o no pueda tener una extensión y que tenga una contraseña asociada a él (la contraseña se requiera para la instalación en el ACS). Sin importar la extensión, asegúrese de que sea un archivo de sólo texto con una extensión que usted pueda cambiar según las necesidades (el dispositivo ACS utiliza la extensión .pvk o del .pem). Si no se especifica ninguna trayectoria para la clave privada, el ACS guarda la clave en el directorio de C:\Program Files \CiscoSecure ACS vx.x \ de CSAdmin \ de los registros y mira en este directorio si no se especifica ninguna trayectoria para el archivo de clave privado cuando usted instala el certificado.

Si el certificado se crea con el uso de los servicios de certificados de Microsoft certifique la forma del submittal, se aseguran de que usted marca las claves como exportable de modo que usted pueda instalar el certificado en el ACS. La creación de un certificado de este modo simplifica el proceso de instalación perceptiblemente. Usted puede instalarla directamente en el almacén apropiado de Windows de la interfaz Web de los servicios de certificados y después instalarla en el ACS del almacenamiento con el uso del CN como referencia. Un certificado instalado en el almacenaje informático de computadora local se puede también exportar del almacenamiento de Windows y instalar en otro ordenador fácilmente. Cuando exportan a este tipo de certificado, las claves necesitan ser marcadas como exportable y ser dadas una contraseña. El certificado

entonces aparece en el formato del .pfx que incluye la clave privada y el certificado de servidor.

Cuando está instalado correctamente en el almacén de certificados de Windows, el certificado de servidor necesita aparecer en los **Certificados (computadora local) > personal >** carpeta de los **Certificados** como se ve en esta ventana de muestra.



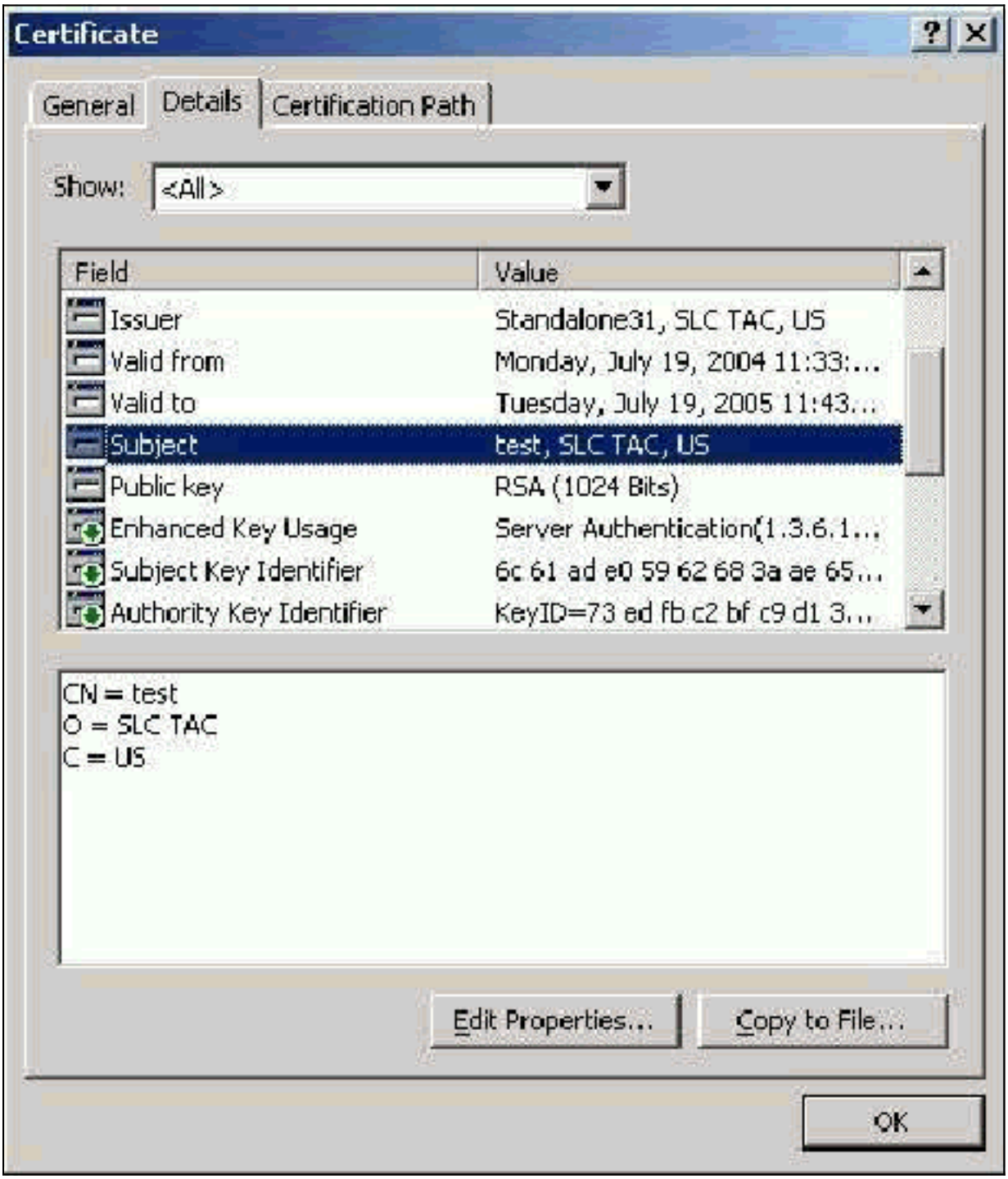
Los certificados autofirmados son le certifican crean sin una raíz o la participación intermediaria de CA. Tienen el mismo valor en los campos del tema y del emisor como a certificado raíz CA. La mayoría de los certificados autofirmados utilizan el formato del v1 X.509. Por lo tanto, no trabajan con el ACS. Sin embargo, a partir de la versión 3.3, el ACS tiene la capacidad de crear sus propios certificados autofirmados que usted pueda utilizar para el EAP-TLS y el PEAP. No utilice un tamaño de clave mayor de 1024 para la compatibilidad con el PEAP y el EAP-TLS. Si usted utiliza un certificado autofirmado, el certificado también actúa en calidad de certificado raíz CA y se debe instalar en los **Certificados (computadora local) >** carpeta de los **Trusted Root Certification Authority > de los Certificados del** cliente cuando usted utiliza al solicitante EAP de Microsoft. Instala automáticamente en el almacén de los Certificados de la Raíz confiable en el servidor. Sin embargo, debe todavía ser confiado en Certificate Trust List (Lista de confianza del certificado) adentro la configuración del certificado ACS. Vea raíz CA la sección de los Certificados para más información.

Porque los certificados autofirmados se utilizan como certificado raíz CA para la validación del certificado de servidor cuando usted utiliza al solicitante EAP de Microsoft, y porque el período de validez no se puede aumentar del valor por defecto de un año, Cisco recomienda que usted lo utiliza solamente para el EAP como medida temporal hasta que usted pueda utilizar CA tradicional.

Campo Subject

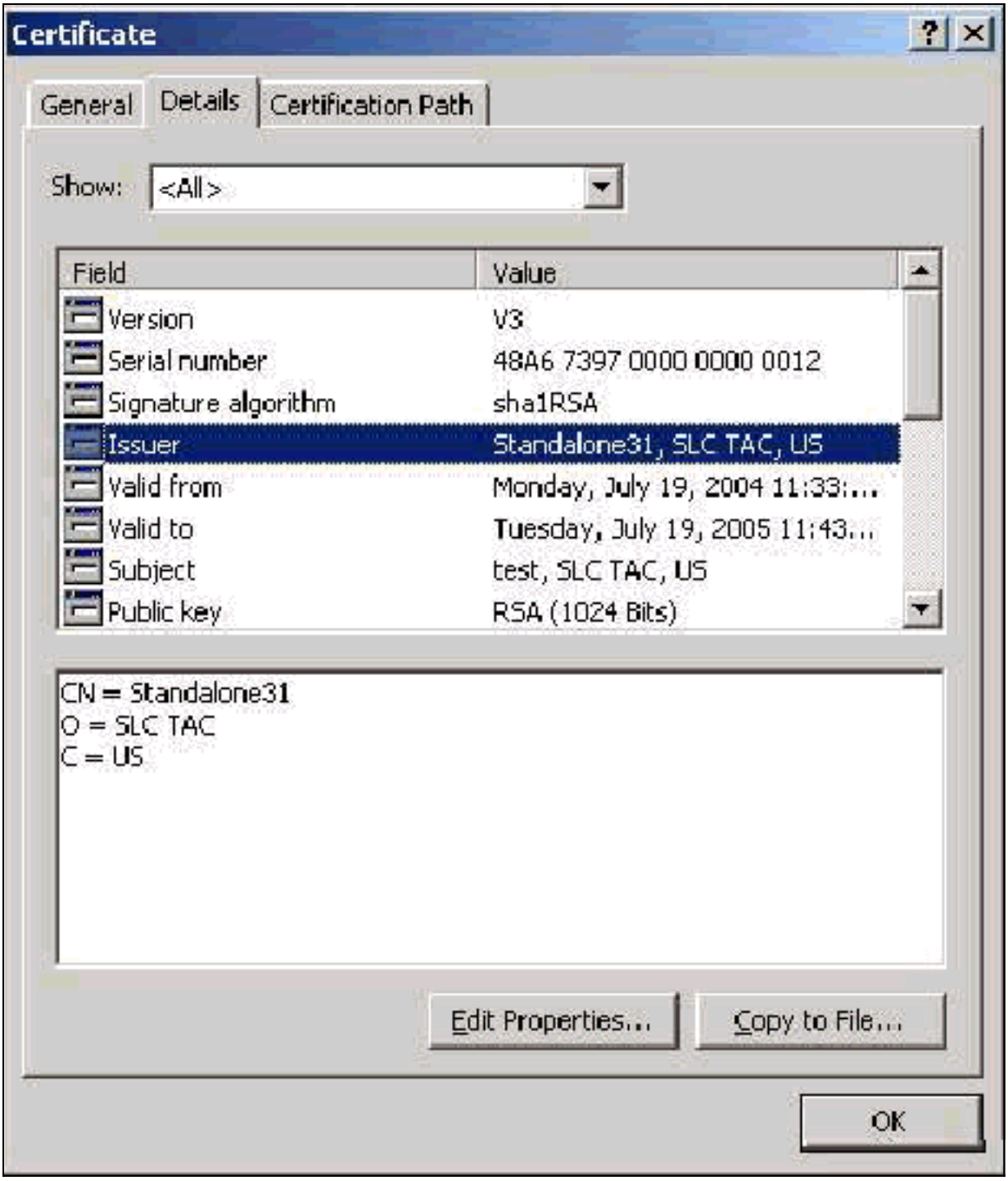
El campo Subject identifica el certificado. El valor CN se utiliza para determinar publicado para colocar en la ficha general del certificado y se puebla con la información que usted ingresa en el campo Subject del certificado en diálogo CSR ACS " o con la información del campo de nombre en los servicios de certificados de Microsoft. El valor CN se utiliza para decir a ACS qué

certificado necesita utilizar del almacén de certificados de la máquina local si la opción para instalar el certificado del almacenamiento se utiliza.



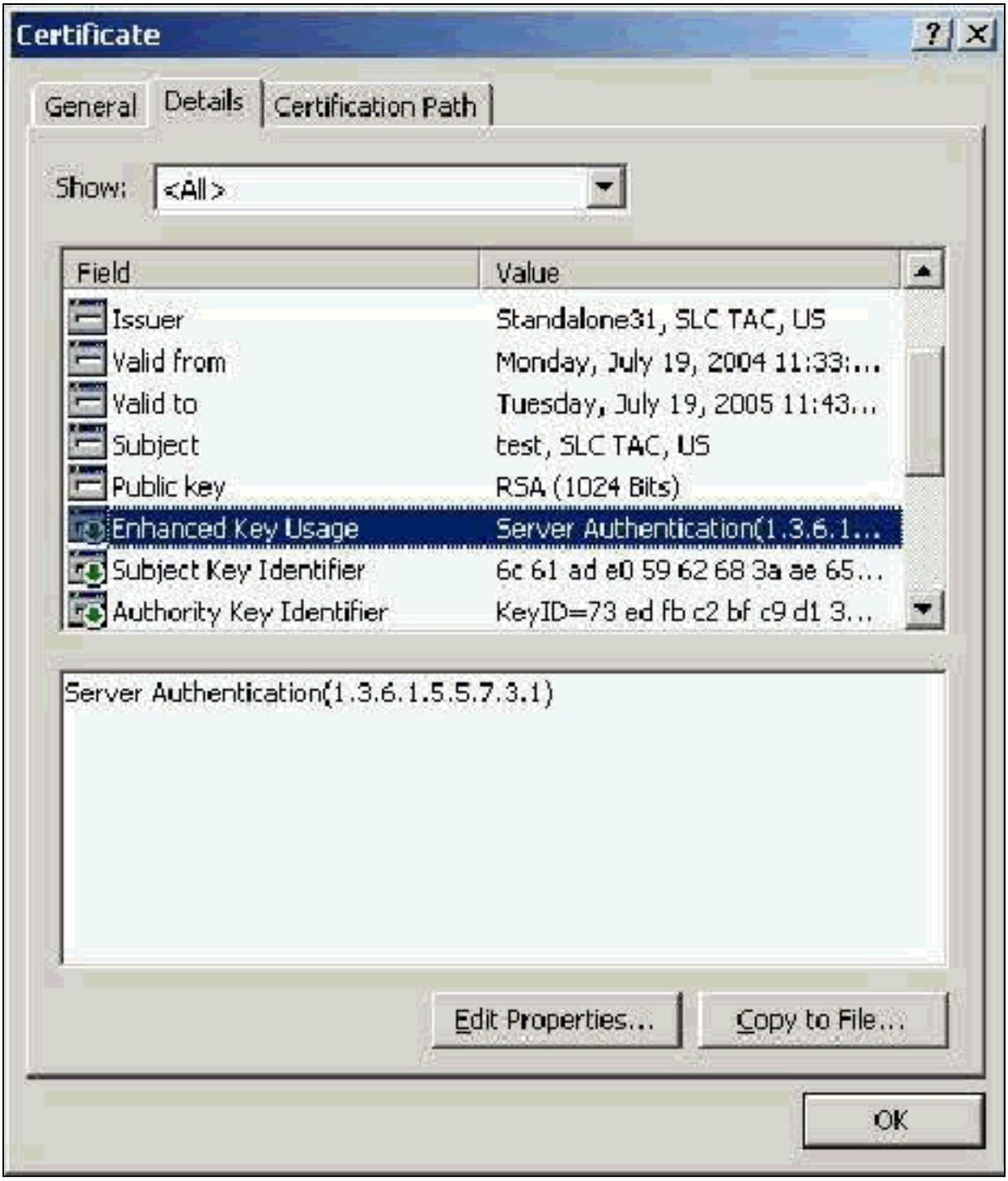
Campo del emisor

El campo del emisor identifica CA que corta el certificado. Utilice este valor para determinar el valor del publicado por el campo en la ficha general del certificado. Se puebla con el nombre de CA.



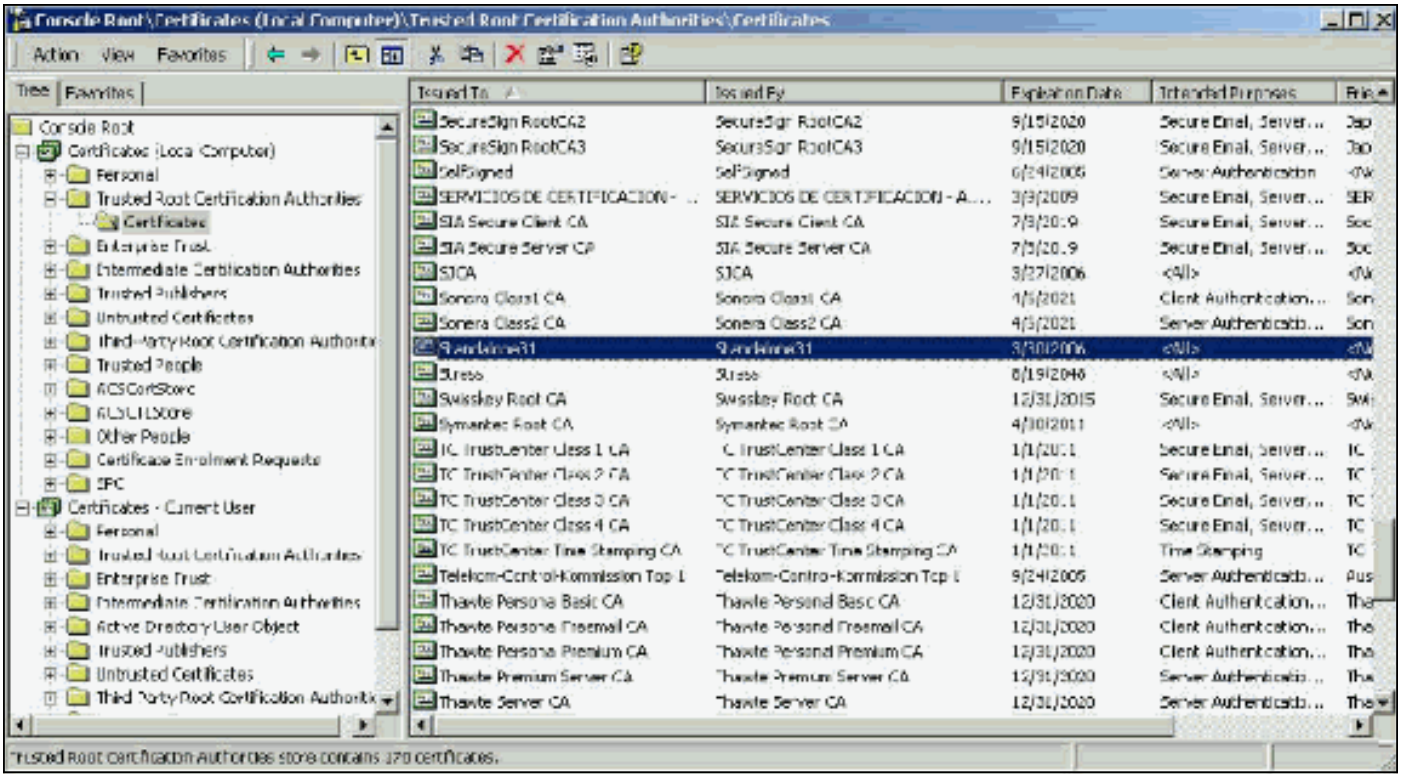
Campo del Enhanced Key Usage

El campo del Enhanced Key Usage identifica el propósito previsto del certificado y necesita ser enumerado como “autenticación de servidor”. Este campo es obligatorio cuando usted utiliza al solicitante de Microsoft para el PEAP y el EAP-TLS. Cuando usted utiliza los servicios de certificados de Microsoft, esto se configura en CA independiente con la selección de **Certificado de autenticación de servidor del** descenso-abajo previsto del propósito y en la empresa CA con la selección de **servidor Web del** descenso-abajo del Certificate Template plantilla de certificado. Si usted pide un certificado con el uso de un CSR con los servicios de certificados de Microsoft, usted no tiene la opción para especificar el propósito previsto con CA independiente. Por lo tanto, el campo del EKU está ausente. Con la empresa CA, usted tiene el descenso-abajo previsto del propósito. Algunos CA no crean los Certificados con un campo del EKU así que son inútiles cuando usted utiliza al solicitante EAP de Microsoft.



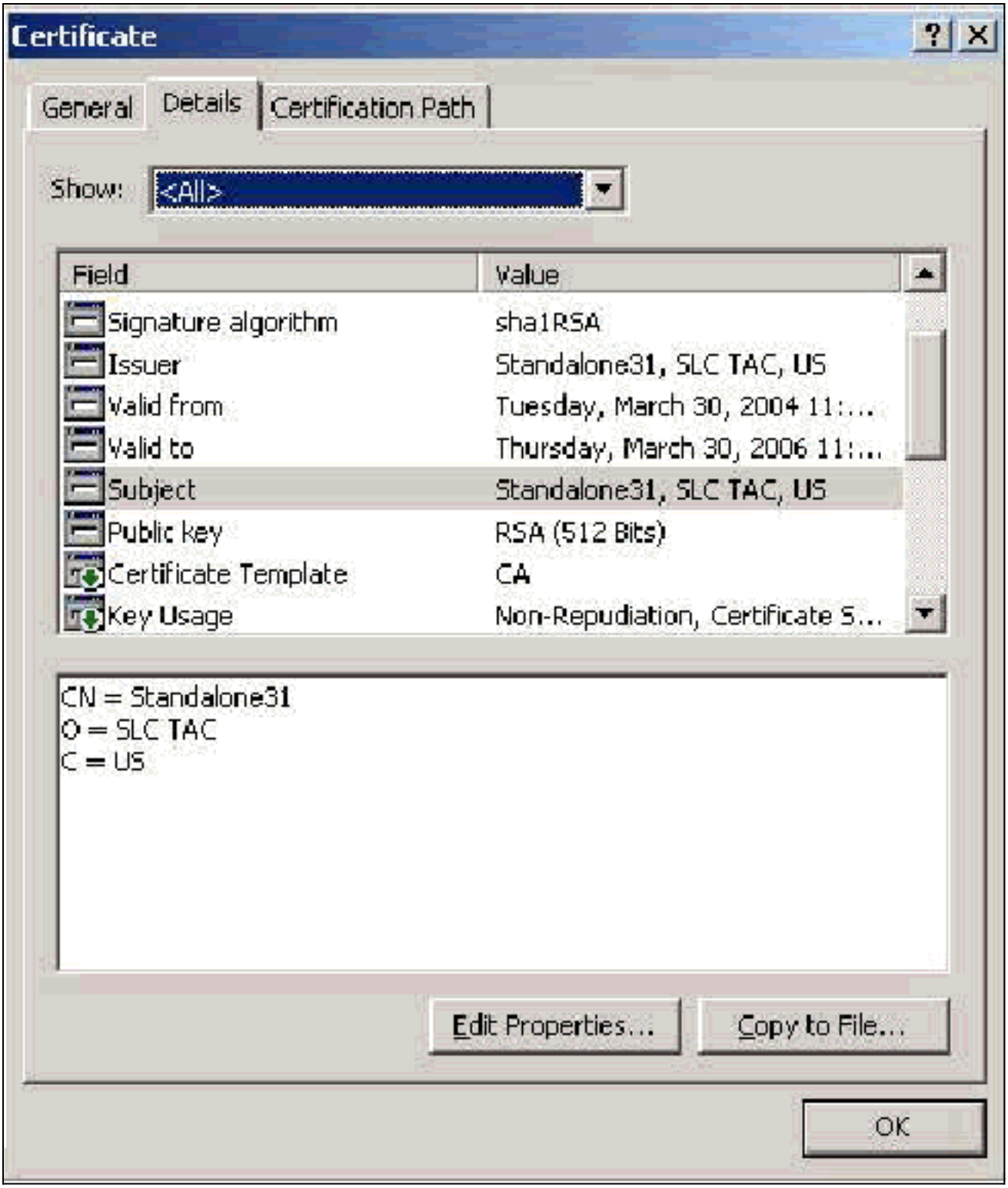
Raíz CA Certificados

El un propósito del certificado raíz CA es identificar el certificado de servidor (y el certificado de CA intermedio si procede) como certificado confiable al ACS y al supplicant del EAP MSCHAPv2 de Windows. Debe ser situado en el almacén de los Trusted Root Certification Authority en Windows en el servidor ACS y, en el caso del EAP MSCHAPv2, en la computadora cliente. La mayoría de los Certificados del otro vendedor raíz CA están instalados con Windows y hay poco esfuerzo implicado con esto. Si utilizan a los servicios de certificados de Microsoft y el servidor de certificados está en la misma máquina que el ACS, después certificado raíz CA está instalado automáticamente. Si certificado raíz CA no se encuentra en el almacén de los Trusted Root Certification Authority en Windows, después debe ser adquirido de su CA y ser instalado. Cuando está instalado correctamente en el almacén de certificados de Windows, certificado raíz CA necesita aparecer en los **Certificados (computadora local) >** carpeta de los **Trusted Root Certification Authority > de los Certificados** como se ve en esta ventana de muestra.



Campos del tema y del emisor

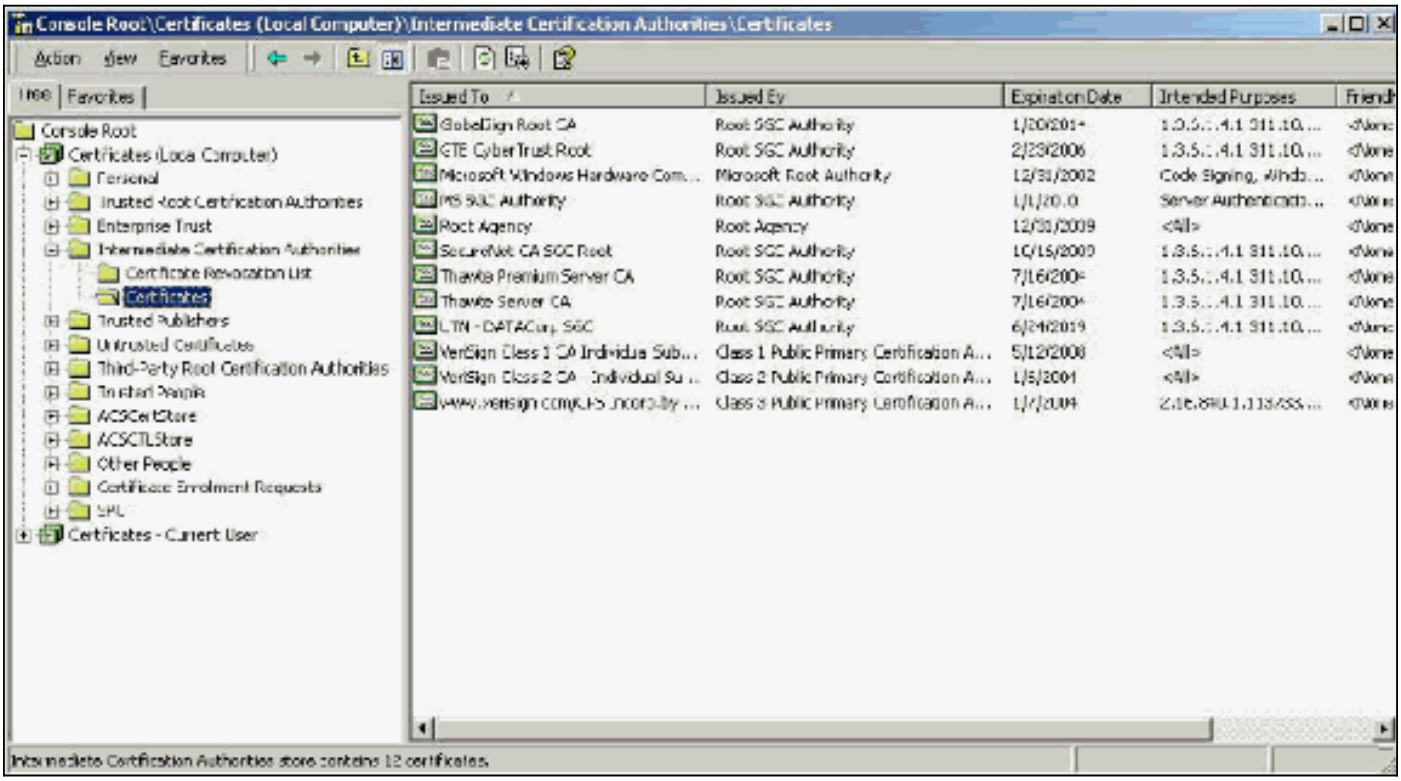
Los campos del tema y del emisor identifican CA y necesitan ser exactamente lo mismo. Utilice estos campos para poblar publicado a y publicado por los campos en la ficha general del certificado. Se pueblan con el nombre del raíz CA.



Certificados de CA intermedios

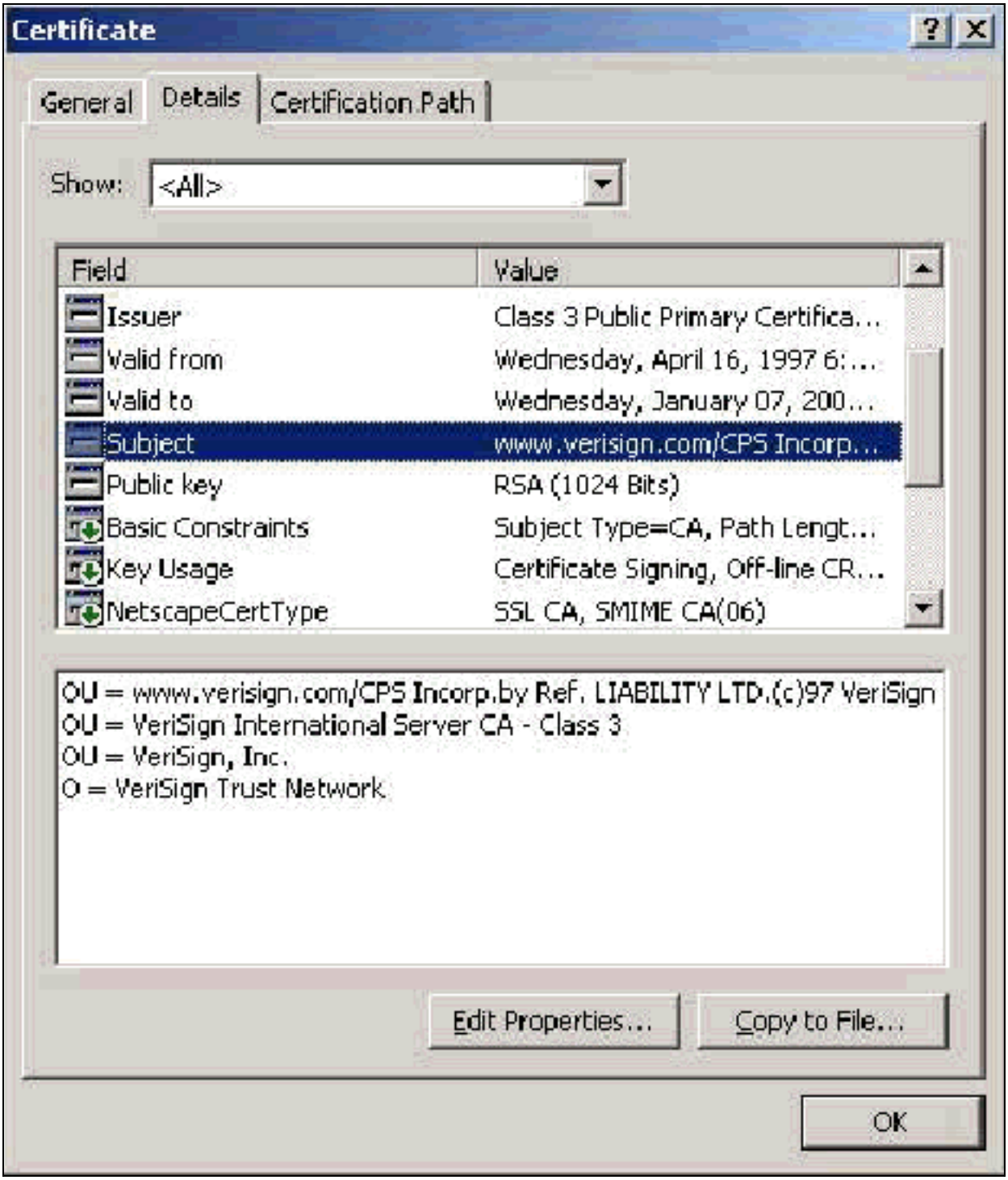
Los Certificados de CA intermedios son los Certificados que usted utiliza para identificar CA que es subordinado a raíz CA. Algunos certificados de servidor (los Certificados inalámbricos de Verisign) se crean con el uso de CA intermedio. Si se utiliza un certificado de servidor que es cortado por un intermedio CA, el certificado de CA intermedio se debe instalar en el área intermedia de las autoridades de certificación del almacenamiento de máquina local en el servidor ACS. También, si utilizan al solicitante EAP de Microsoft en el cliente, certificado raíz CA raíz CA que creó del certificado de CA intermedio debe también estar en el almacén apropiado en el servidor ACS y el cliente para poder establecer el encadenamiento de la confianza. Certificado raíz CA y el certificado de CA intermedio se debe marcar como de confianza en el ACS y en el

cliente. La mayoría de los Certificados de CA del intermedio no están instalados con Windows así que usted necesidad más probable de adquirirlo del vendedor. Cuando está instalado correctamente en el almacén de certificados de Windows, el certificado de CA intermedio aparece en los **Certificados (computadora local) >** carpeta **intermedia de las autoridades de certificación > de los Certificados** como se ve en esta ventana de muestra.



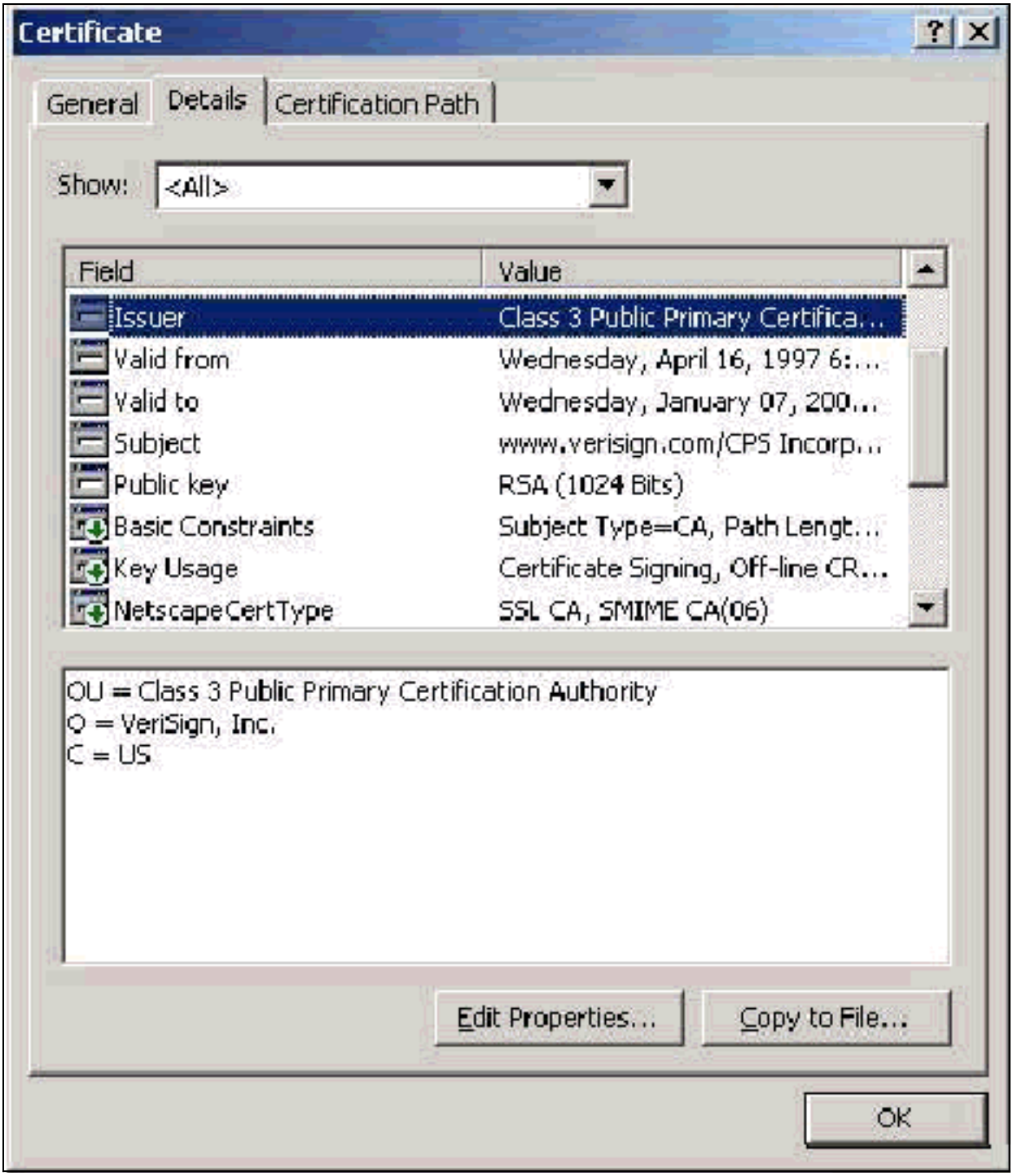
Campo Subject

El campo Subject identifica CA intermedio. Este valor se utiliza para determinar publicado para colocar en la ficha general del certificado.



Campo del emisor

El campo del emisor identifica CA que corta el certificado. Utilice este valor para determinar el valor del publicado por el campo en la ficha general del certificado. Se puebla con el nombre de CA.



Certificados del cliente

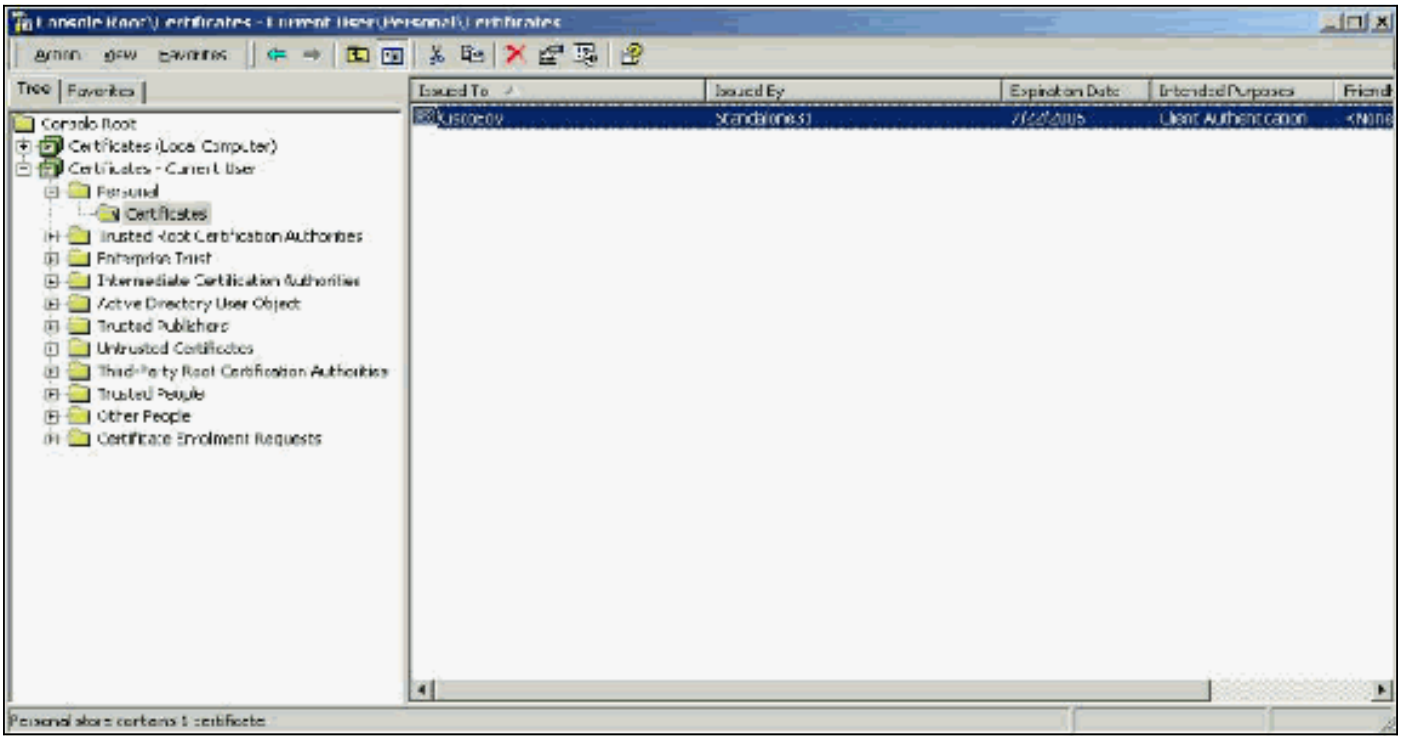
Los certificados del cliente se utilizan para identificar positivamente al usuario en el EAP-TLS. No tienen ningún papel en la construcción del túnel de TLS y no se utilizan para el cifrado. La identificación positiva es lograda por uno de tres significa:

- ¿**Comparación CN (o nombre)**? Compara el CN en el certificado con el nombre de usuario en la base de datos. Más información sobre este tipo de la comparación se incluye en la descripción del campo Subject del certificado.
- ¿**Comparación SAN**? Compara el SAN en el certificado con el nombre de usuario en la base de datos. Esto se soporta solamente a partir de ACS 3.2. Más información sobre este tipo de la comparación se incluye en la descripción del campo de nombre alternativo sujeto del certificado.

- ¿**Comparación binaria**? Compara el certificado con una copia binaria del certificado salvado en la base de datos (solamente el AD y el LDAP pueden hacer esto). Si usted utiliza la comparación binaria del certificado, usted debe salvar el Certificado de usuario en un formato binario. También, para el LDAP genérico y el Active Directory, el atributo que salva el certificado debe ser el atributo estándar LDAP nombrado “usercertificate”.

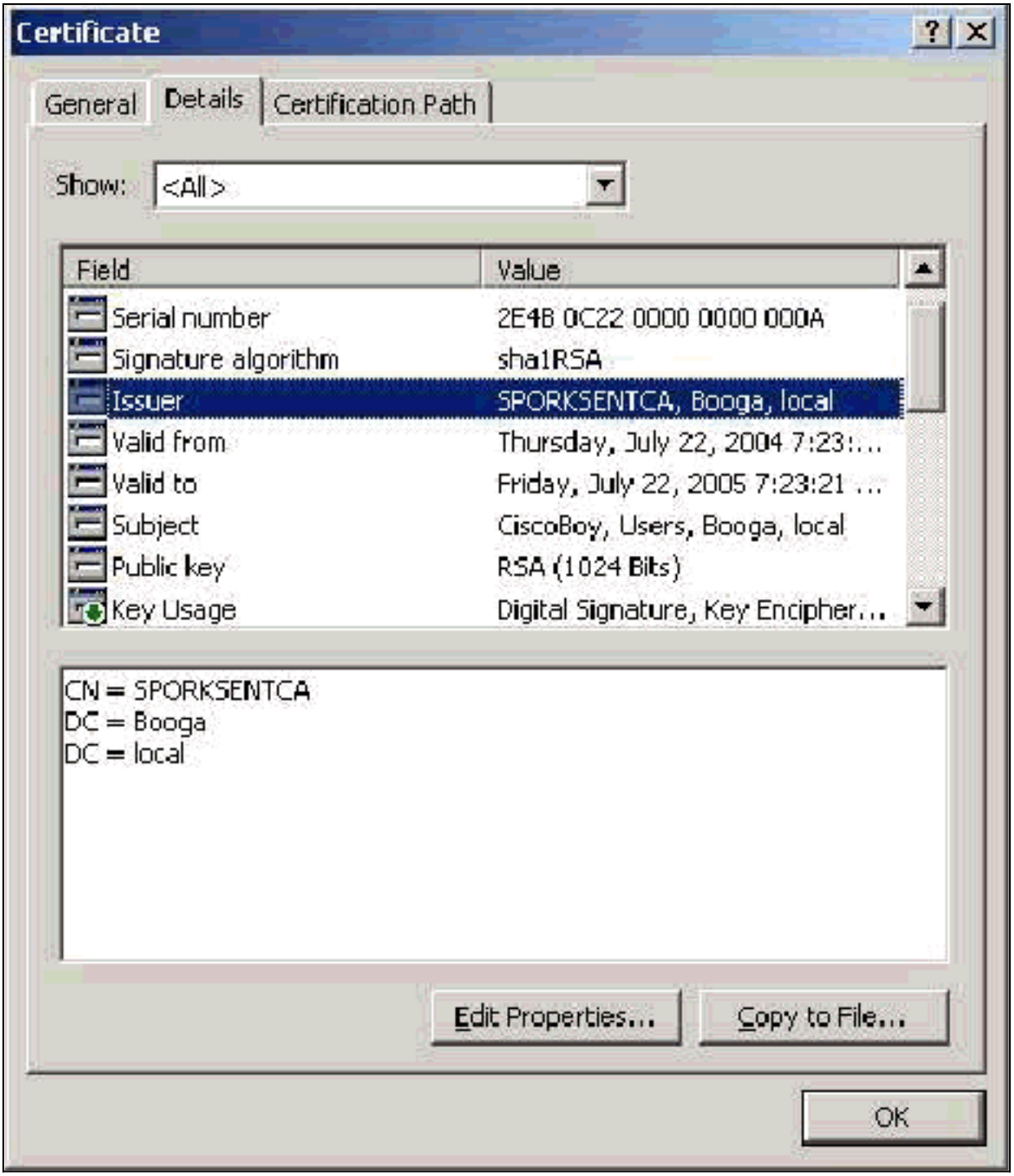
Se utiliza cualquier método de comparación, la información en el campo adecuado (CN o SAN) debe hacer juego el nombre que su base de datos utiliza para la autenticación. El AD utiliza el nombre de NETBIOS para la autenticación en el modo mezclado y el UPN en el modo nativo.

Esta sección discute la generación del certificado del cliente con el uso de los servicios de certificados de Microsoft. El EAP-TLS requiere un certificado del cliente único para que cada usuario sea autenticado. El certificado se debe instalar en cada ordenador para cada usuario. Cuando está instalado correctamente, el certificado está situado en los **Certificados - Usuario usuario actual > personal >** carpeta de los **Certificados** como se ve en esta ventana de muestra.



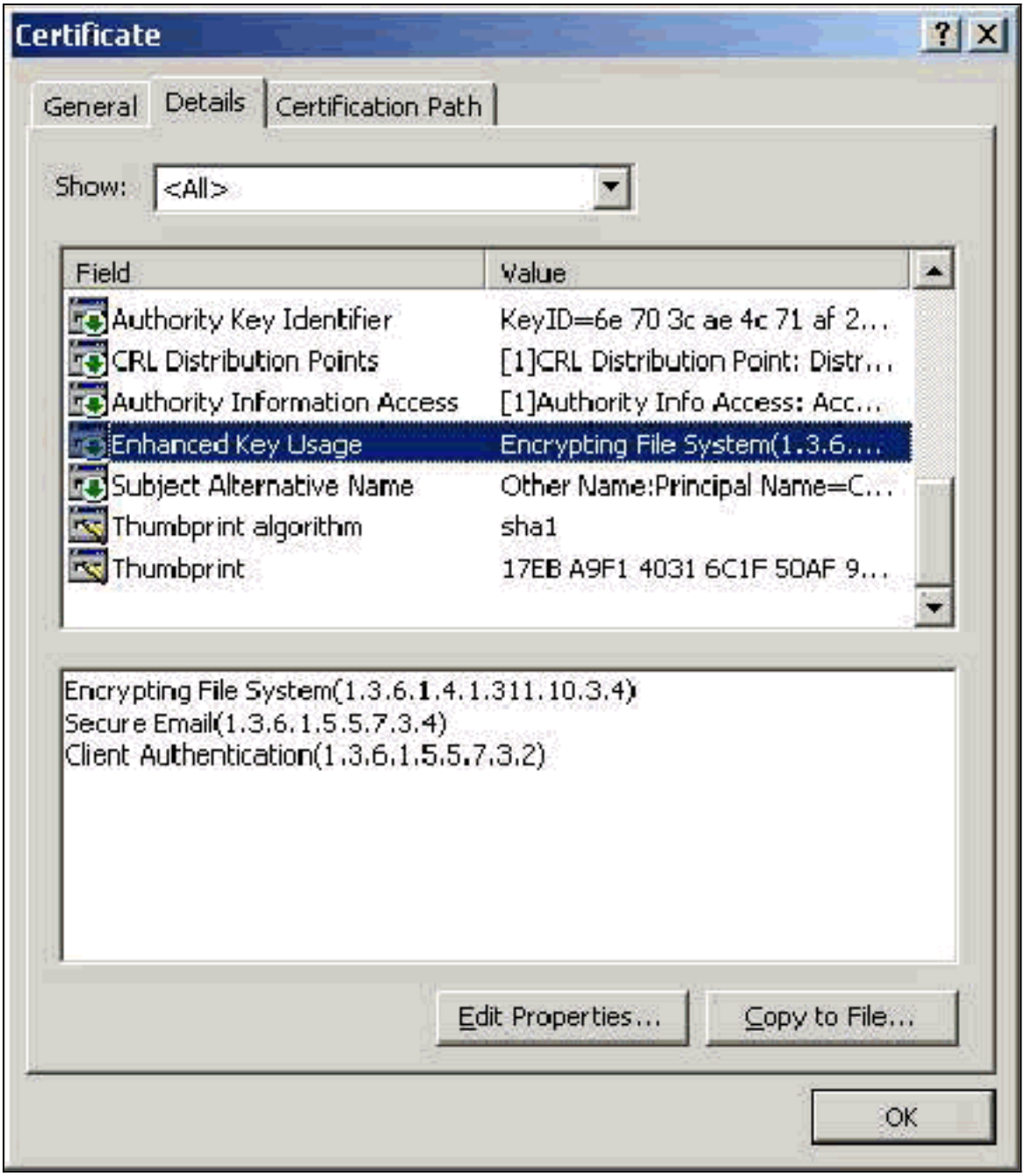
Campo del emisor

El campo del emisor identifica CA que corta el certificado. Utilice este valor para determinar el valor del publicado por el campo en la ficha general del certificado. Esto se puebla con el nombre de CA.



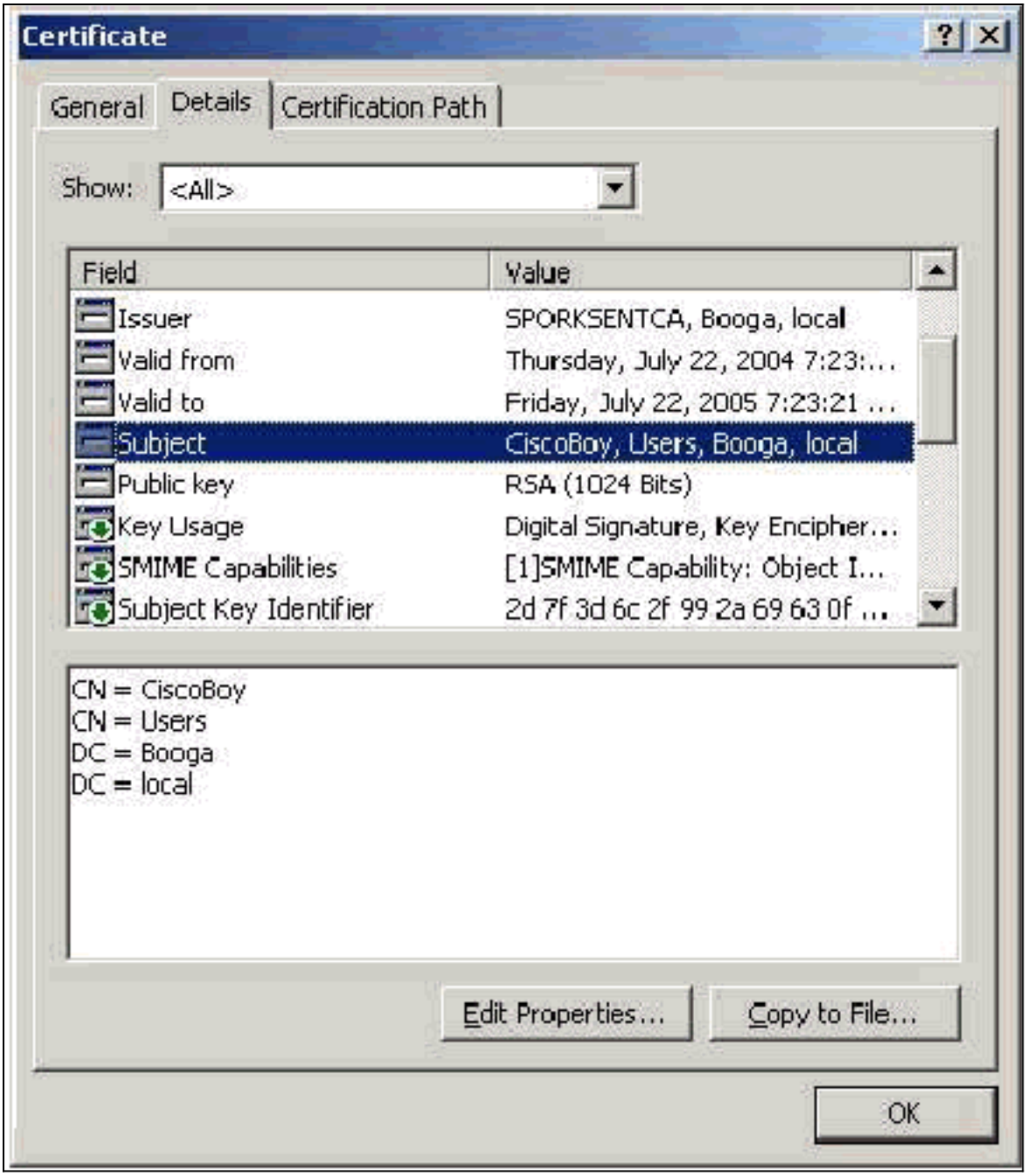
Campo del Enhanced Key Usage

El campo del Enhanced Key Usage identifica el propósito previsto del certificado y necesita contener la autenticación de cliente. Este campo es obligatorio cuando usted utiliza al solicitante de Microsoft para el PEAP y el EAP-TLS. Cuando usted utiliza los servicios de certificados de Microsoft, esto se configura en CA independiente cuando usted selecciona el **Certificado de autenticación del cliente del** descenso-abajo previsto del propósito y en la empresa CA cuando usted selecciona al **usuario del** descenso-abajo del Certificate Template plantilla de certificado. Si usted pide un certificado con el uso de un CSR con los servicios de certificados de Microsoft, usted no tiene la opción para especificar el propósito previsto con CA independiente. Por lo tanto, el campo del EKU está ausente. Con la empresa CA, usted tiene el descenso-abajo previsto del propósito. Algunos CA no crean los Certificados con un campo del EKU. Son inútiles cuando usted utiliza al solicitante EAP de Microsoft.



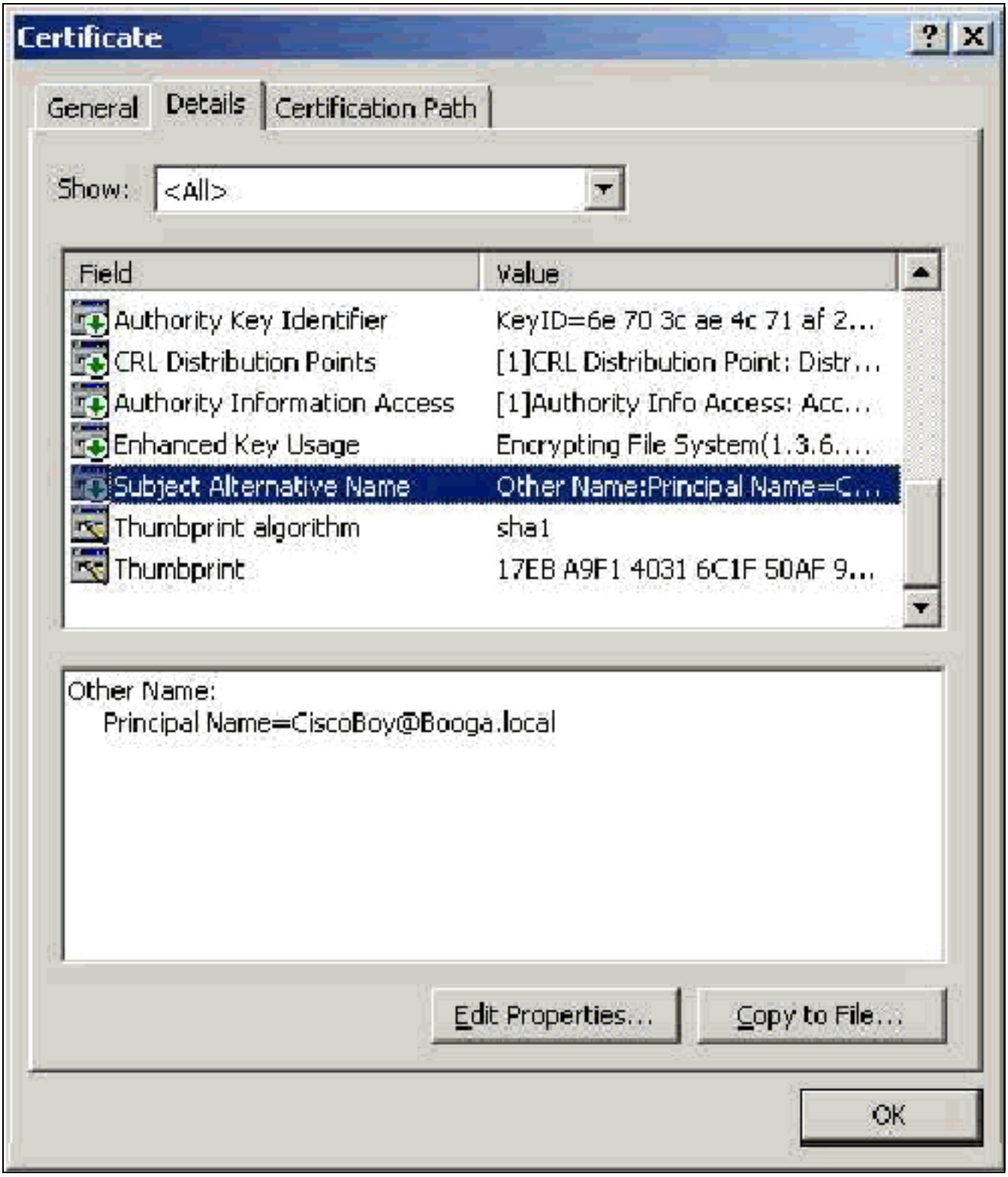
Campo Subject

Este campo se utiliza en la comparación CN. El primer CN enumerado se compara contra la base de datos para encontrar una coincidencia. Si se encuentra una coincidencia, la autenticación tiene éxito. Si usted utiliza CA independiente, el CN se puebla con sea cual sea usted pone en el campo de nombre en la forma del submittal del certificado. Si usted utiliza la empresa CA, el CN se puebla automáticamente con el nombre de la cuenta como se lista en la consola de los usuarios de directorio activo y computadora (éste no hace juego necesariamente el UPN o el nombre de NETBIOS).



Campo de nombre alternativo sujeto

El campo de nombre alternativo sujeto se utiliza en la comparación SAN. El SAN enumerado se compara contra la base de datos para encontrar una coincidencia. Si se encuentra una coincidencia, la autenticación tiene éxito. Si usted utiliza la empresa CA, el SAN se puebla automáticamente con el @domain del nombre de inicio del Active Directory (UPN). CA independiente no incluye un campo SAN así que usted no puede utilizar la comparación SAN.



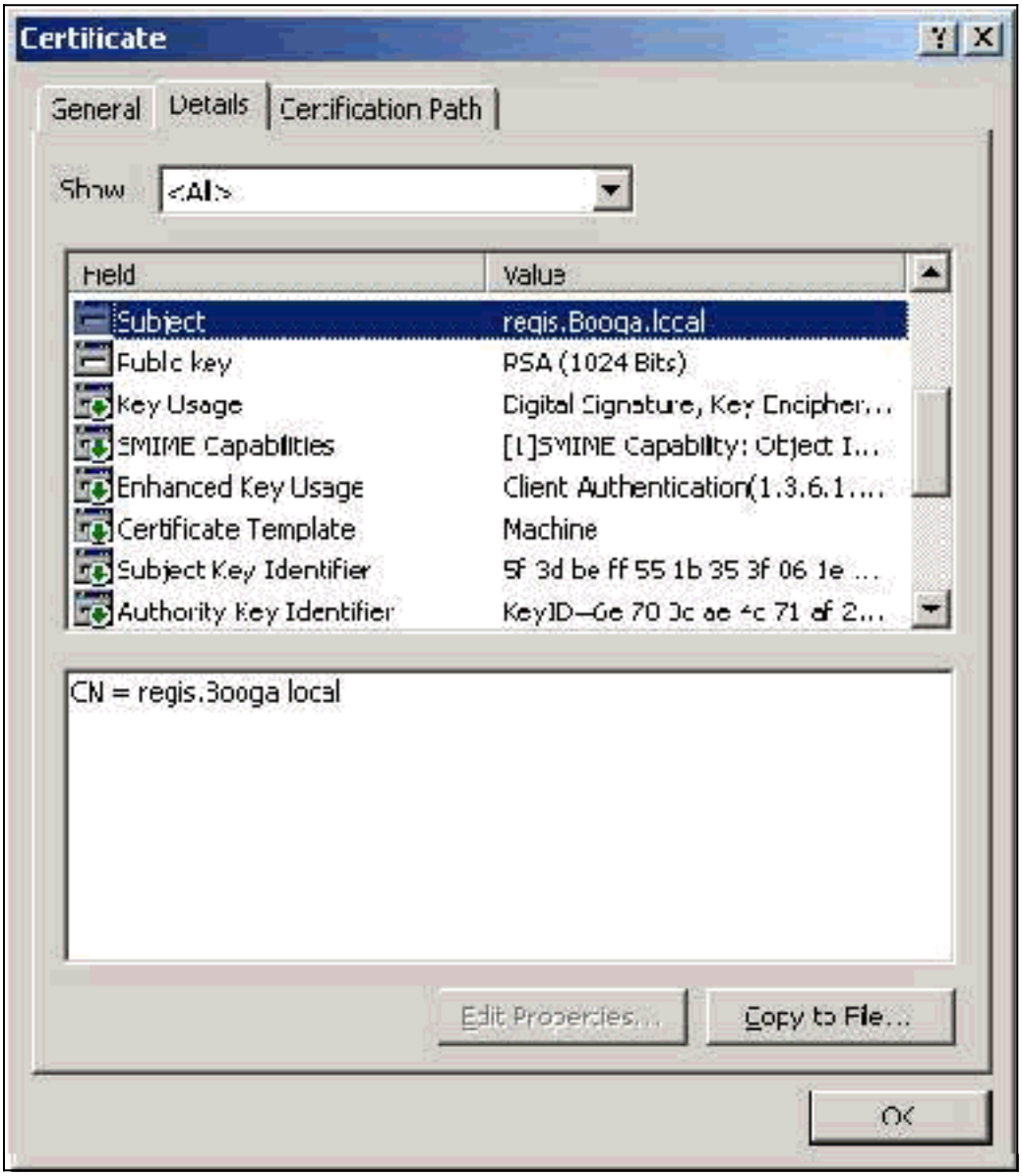
Certificados de la máquina

Los certificados de la máquina se utilizan en el EAP-TLS para identificar positivamente el ordenador cuando usted utiliza la autenticación de la máquina. Usted puede acceder solamente estos Certificados cuando usted configura su empresa CA de Microsoft para el Autoregistro del certificado y se une al ordenador al dominio. El certificado se crea automáticamente cuando usted utiliza las credenciales del Active Directory del ordenador y las instala en el almacenaje informático de computadora local. Las Computadoras que son ya miembros del dominio antes de que usted configure el Autoregistro reciben un certificado la próxima vez los reinicios de ese Windows. El certificado de la máquina está instalado en los **Certificados (computadora local) > personal >** carpeta de los **Certificados de los** Certificados (computadora local) MMC broche-en

apenas los certificados de servidor similares. Usted no puede instalar estos Certificados en ninguna otra máquina puesto que usted no puede exportar la clave privada.

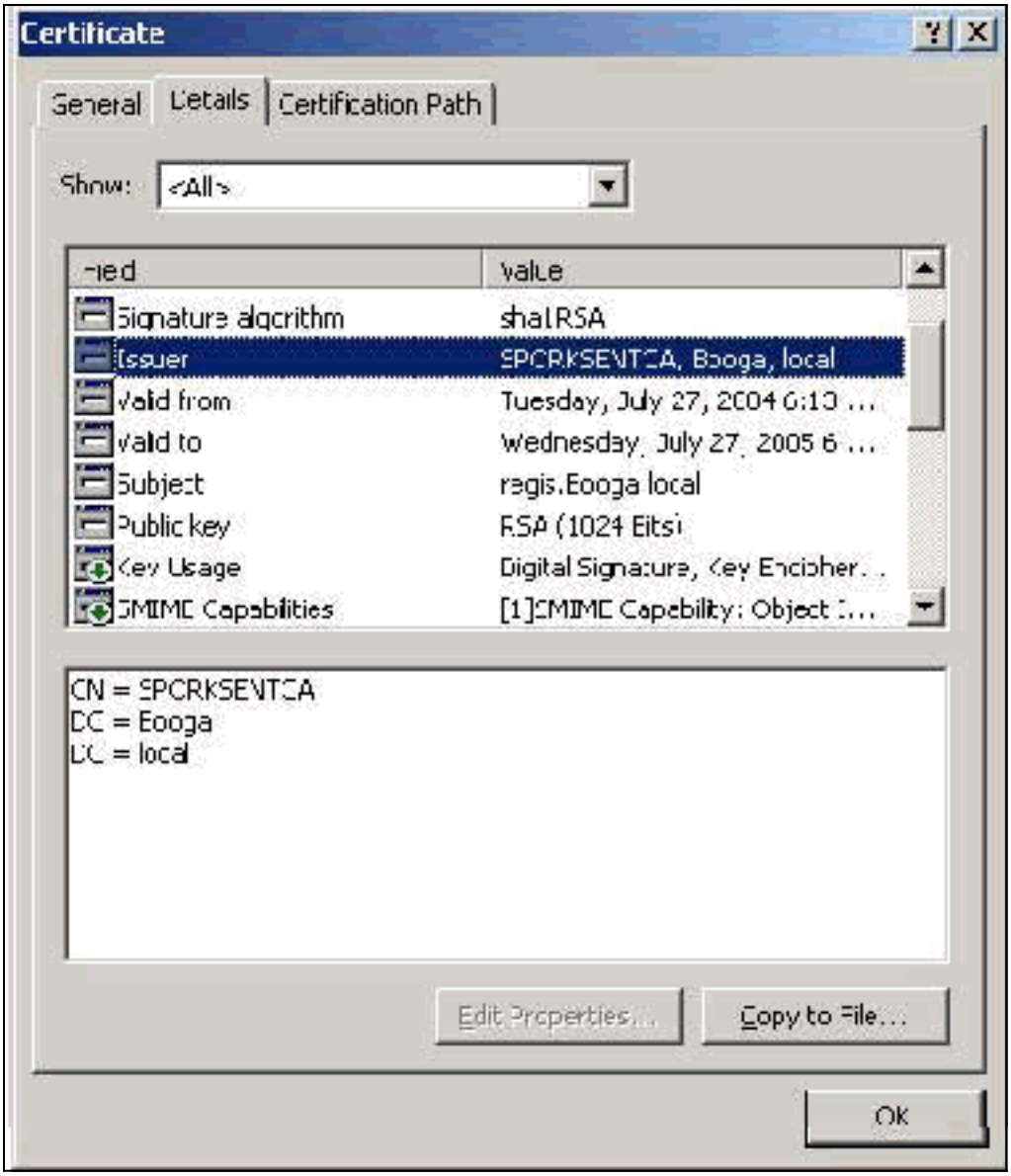
Tema y campos SAN

El tema y los campos SAN identifican el ordenador. El valor es poblado por el nombre calificado completamente del ordenador y utilizado para determinar publicado para colocar en la ficha general del certificado y es lo mismo para el tema y los campos SAN.



Campo del emisor

El campo del emisor identifica CA que corta el certificado. Utilice este valor para determinar el valor del publicado por el campo en la ficha general del certificado. Se puebla con el nombre de CA.



Apéndice A - Extensiones del certificado comunes

¿**.csr**? Esto no es realmente un certificado sino bastante un pedido de firma de certificado. Es un archivo de sólo texto con este formato:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtDCCAR0CAQIwDzENMAsGA1UEAxMETW9yazCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAu3duNPToM71ljadL1hMWTMTl2yzDn2btVQsWHjdS9FARBOpVIuQe
BAMCBkAwDQYJKoZIhvcNAQEFBQADgYEAkvHoMkTY0mhHwavsDey8IN7DsN0Io6vP
tyjWnoKzHycO6NHt3k7f55Ch/nQ6ONSGBs02uYpjUUPJPqlhGBY4VEcV39zdPNs8
uPCuex/LZ4sOqgmd6WOxup3rEI01fJnqjpd7fwbX9Jr3Awc1gFsXS0Kg3WnjJD4i
ILII9Vhw89s=
-----END CERTIFICATE REQUEST-----
```

¿**.pvk**? Esta extensión denota una clave privada aunque la extensión no garantiza que el contenido es realmente una clave privada. La necesidad contenta de ser sólo texto con este formato:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,751DA1C8E250B96B

YyLE3zsDTY1+Kq+6gAUF+YCO452KHmQJQn7AKxMnDqHeQrAePReL/zuxHiKsBjrN
h2FGzV17bBVnBQZ/Ci/j92HYeQ2VZD8wB6lYFsWV/30kYeyPYRctweteKFfgpFHi
/ES9B0bWzrpFS1El+I2L6o1dwnUkmMBIC1j1WNV3Xo+/5NFei1mdlgRMRtzR85Ub
4hUWzWCsRSFEcHEcNcsfxkach9stzkIMWB6d7RyvWyqNfb627O2MhMhA9T01LYri
NdM/Tsdz3Kfc7AXiNMvti5R0mSV89d6epLLE69PTWZLNxasCsCybhNt/ya/z7y1S
bE4iBAwdZ9jCyuBB9viLBqps39zfiYrRTDkDXiVH3oIWKBbM3OEw3apgLFZiVRqZ
07xaX7oQyy4tQfo4UNnhPTX3kiMBA6t6UJvs6VIHsIIXYEYlHbL6bA==
-----END RSA PRIVATE KEY-----
```

¿**.cer**? Ésta es una extensión genérica que denota un certificado. El servidor, raíz CA, y los Certificados de CA intermedios pueden estar en este formato. Es comúnmente un archivo de sólo texto con una extensión que usted pueda cambiar mientras que usted necesita y puede ser DER o formato del base 64. Usted puede importar este formato en el almacén de certificados de Windows.

¿**.pem**? Significa Privacy Enhanced Mail de esta extensión. Esta extensión es de uso general con UNIX, Linux, BSD, y así sucesivamente. Se utiliza generalmente para los certificados de servidor y las claves privadas, y es comúnmente un archivo de sólo texto con una extensión que usted pueda cambiar mientras que usted necesita del .pem a .cer de modo que usted pueda importarlo al almacén de certificados de Windows.

El contenido interno de .cer y de los archivos del .pem parece generalmente esta salida:

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAy+gAwIBAgIKSKZzlwAAAAAAEjANBgkqhkiG9w0BAQUFADA2MQswCQYD
VQQGEwJVUzEQMA4GA1UEChMHU0xDIFRBQzEVMBMGA1UEAxMMU3RhbmRhbG9uZTMx
MB4XDTA0MDcxOTE3MzMyNVoXDTA1MDcxOTE3NDMyNVowLjELMAkGA1UEBhMCVVMx
AAQAGBvkDy7BaMBJgFRuS+QU8o2XfH5aAQiCcyKu/jK6mMt64QyCy9k=
-----END CERTIFICATE-----
```

¿**.pfx**? Este intercambio de la información personal de la significa de la extensión. Este formato es un método que usted puede utilizar para liar los Certificados en un archivo único. Por ejemplo, usted puede liar un certificado de servidor y su clave privada asociada y certificado raíz CA en un archivo e importar fácilmente el archivo en el almacén de certificados apropiado de Windows. Es el más de uso general para el servidor y los certificados del cliente. Desafortunadamente, si a certificado raíz CA es incluida, certificado raíz CA está instalado siempre en el almacén del Usuario usuario actual en vez del almacenaje informático de computadora local incluso si el almacenaje informático de computadora local se especifica para la instalación.

el formato **.p12?This** generalmente se considera solamente con un certificado del cliente. Usted puede importar este formato en el almacén de certificados de Windows.

.p7b?This es otro formato que salva los certificados múltiples en un archivo. Usted puede importar este formato en el almacén de certificados de Windows.

Apéndice B - Conversión del formato del certificado

En la mayoría de los casos, la conversión del certificado ocurre cuando usted cambia la extensión (por ejemplo, del .pem a .cer) puesto que los Certificados están comúnmente en el formato de

texto sin formato. A veces, un certificado no está en el formato del texto simple y usted debe convertirlo con el uso de una herramienta tal como OpenSSL . Por ejemplo, el motor de solución ACS no puede instalar los Certificados en el formato del .pfx. Por lo tanto, usted debe convertir el certificado y la clave privada en un formato usable. Éste es el sintaxis del comando básico para el OpenSSL:

```
openssl pkcs12 -in c:\certs \test.pfx -out c:\certs \test.pem
```

Le indican para la contraseña de la importación y la palabra clave PEM. Estas contraseñas necesitan ser lo mismo y son la contraseña de la clave privada se especifica que cuando se exporta el .pfx. La salida es un solo archivo del .pem que incluye todos los Certificados y claves privadas en el .pfx. Este archivo se puede referir en el ACS como el certificado y el archivo de clave privado y él instala sin los problemas.

C del apéndice - Período de la validez del certificado

Un certificado es solamente usable durante su período de validez. El período de validez para a certificado raíz CA se determina cuando raíz CA se establece y puede variar. El período de validez para un certificado de CA intermedio se determina cuando el CA se establece y no puede exceder el período de validez de raíz CA a cuál es subordinado. El período de validez para el servidor, fijan al cliente, y los certificados de la máquina automáticamente a un año con los servicios de certificados de Microsoft. Esto se puede cambiar solamente cuando usted corta el registro de Windows según el artículo de la base de conocimiento de Microsoft 254632 y no puede exceder el período de validez de raíz CA. El período de validez de los certificados autofirmados que el ACS genera es siempre un año y no se puede cambiar en las versiones actuales.

Información Relacionada

- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems