Guía de Certificados de EAP Versión 1.01

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.

Prerequisites

Requirements

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 se instala en el servidor RADIUS y su propósito principal en EAP es crear el túnel de seguridad de capa de transporte (TLS) cifrado que protege la información de autenticación. Cuando utiliza EAP-MSCHAPv2, el certificado de servidor asume una función secundaria que consiste en identificar el servidor RADIUS como una entidad de confianza para la autenticación. Esta función secundaria se realiza mediante el uso del campo Enhanced Key Usage (EKU) (Uso mejorado de claves)). El campo EKU identifica el certificado como un certificado de servidor válido y verifica que la CA raíz que emitió el certificado sea una CA raíz de confianza. Esto requiere la presencia del certificado de CA raíz. Cisco Secure ACS requiere que el certificado sea el formato X.509 v3 binario codificado en Base64 o DER-codificado.

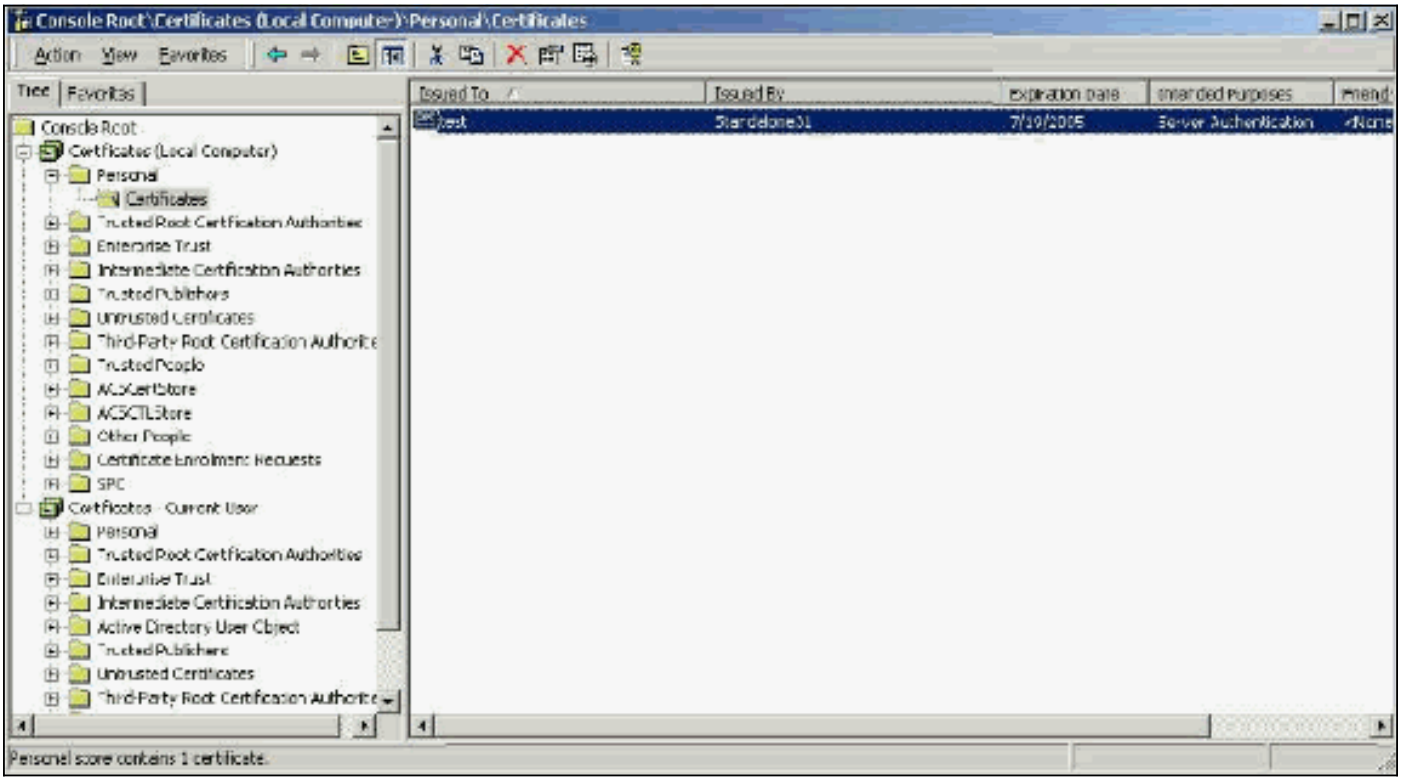
Puede crear este certificado con el uso de una solicitud de firma de certificado (CSR) en ACS, que se envía a una CA. También puede cortar el certificado mediante un formulario de creación de certificados de CA (como Microsoft Certificate Services) interno. Es importante tener en cuenta que, aunque puede crear el certificado de servidor con tamaños de clave mayores a 1024, cualquier clave mayor a 1024 no funciona con PEAP. El cliente se cuelga incluso si la autenticación pasa.

Si crea el certificado con el uso de un CSR, se crea con un formato .cer, .pem o .txt. En raras ocasiones, se crea sin extensión. Asegúrese de que el certificado es un archivo de texto sin formato con una extensión que puede cambiar según sea necesario (el dispositivo ACS utiliza la extensión .cer o .pem). Además, si utiliza un CSR, la clave privada del certificado se crea en la trayectoria que especifique como un archivo independiente que puede o no tener una extensión y que tiene asociada una contraseña (la contraseña es necesaria para la instalación en ACS). Independientemente de la extensión, asegúrese de que es un archivo de texto sin formato con una extensión que puede cambiar según sea necesario (el dispositivo ACS utiliza la extensión .pvk o .pem). Si no se especifica ninguna ruta de acceso para la clave privada, ACS guarda la clave en el directorio C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs y busca en este directorio si no se especifica ninguna ruta para el archivo de clave privada cuando instala el certificado.

Si el certificado se crea con el uso del formulario de envío de certificado de Servicios de Certificate Server de Microsoft, asegúrese de marcar las claves como exportables para que pueda instalar el certificado en ACS. La creación de un certificado de esta manera simplifica significativamente el proceso de instalación. Puede instalarlo directamente en el almacén de Windows adecuado desde la interfaz web de Servicios de Certificados y luego instalarlo en ACS

desde el almacenamiento con el uso de CN como referencia. Un certificado instalado en el almacén de equipos local también se puede exportar desde el almacenamiento de Windows e instalar en otro equipo con facilidad. Cuando se exporta este tipo de certificado, las claves deben marcarse como exportables y se les debe dar una contraseña. A continuación, el certificado aparece en formato .pfx que incluye la clave privada y el certificado del servidor.

Cuando se instala correctamente en el almacén de certificados de Windows, el certificado de servidor debe aparecer en la carpeta **Certificados (equipo local) > Personal > Certificados** como se ve en esta ventana de ejemplo.

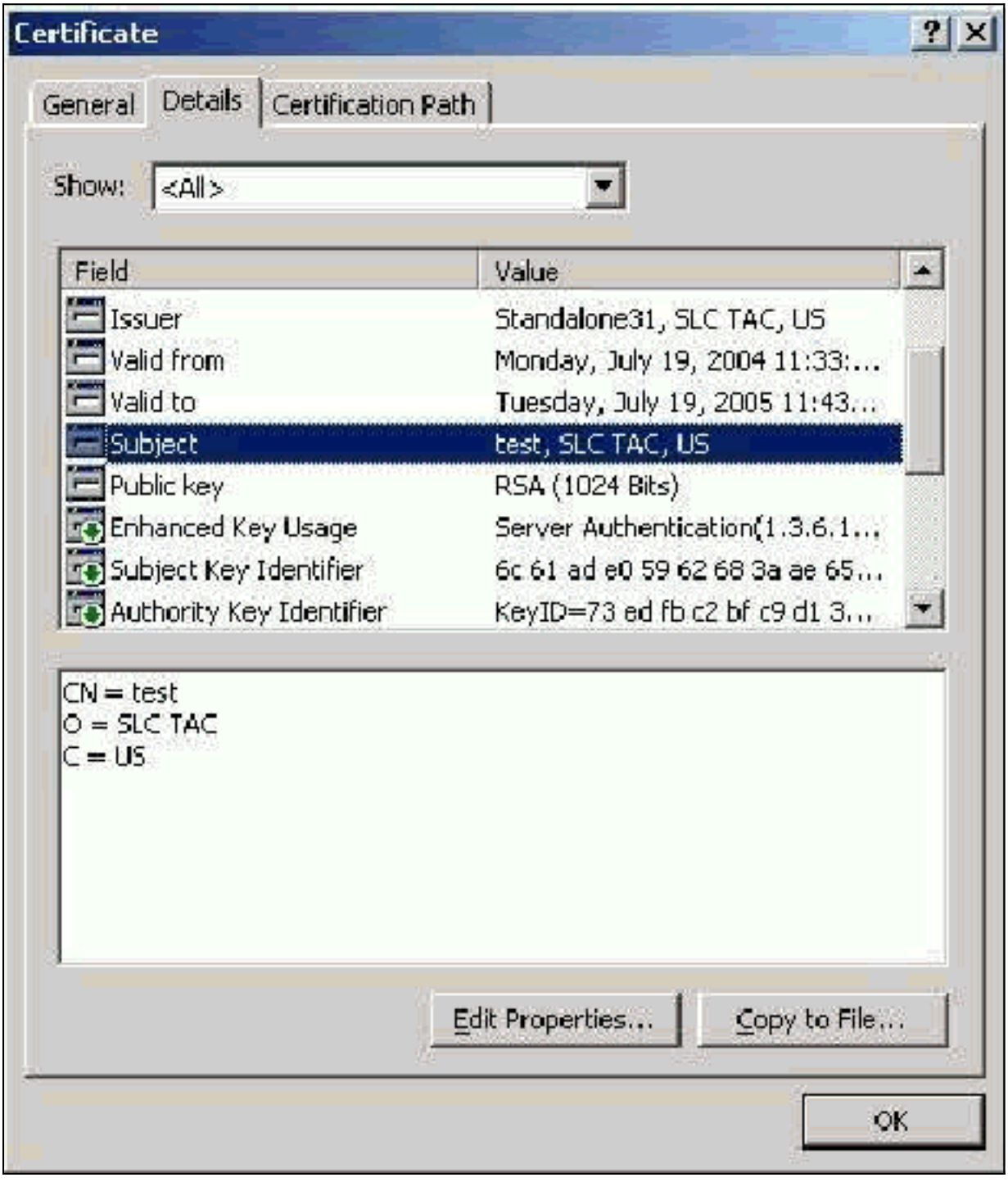


Los certificados autofirmados son certificados que se crean sin una raíz o la participación intermedia de la CA. Tienen el mismo valor tanto en el campo de asunto como en el de emisor, como un certificado de CA raíz. La mayoría de los certificados autofirmados utilizan el formato X.509 v1. Por lo tanto, no funcionan con ACS. Sin embargo, a partir de la versión 3.3, ACS tiene la capacidad de crear sus propios certificados autofirmados que puede utilizar para EAP-TLS y PEAP. No utilice un tamaño de clave mayor que 1024 para la compatibilidad con PEAP y EAP-TLS. Si utiliza un certificado autofirmado, el certificado también actúa en la capacidad del certificado de CA raíz y debe estar instalado en la carpeta **Certificados (equipo local) > Autoridades de certificación raíz de confianza > Certificados** del cliente cuando utiliza el suplicante EAP de Microsoft. Se instala automáticamente en el almacén de certificados raíz de confianza del servidor. Sin embargo, aún debe ser confiable en la Lista de Confianza de Certificados en la Configuración de Certificados ACS. Vea la sección Certificados de CA raíz para obtener más información.

Debido a que los certificados autofirmados se utilizan como el certificado CA raíz para la validación del certificado de servidor cuando se utiliza el suplicante EAP de Microsoft y debido a que el período de validez no puede aumentarse del valor predeterminado de un año, Cisco recomienda que sólo se utilicen para EAP como medida temporal hasta que se pueda utilizar una CA tradicional.

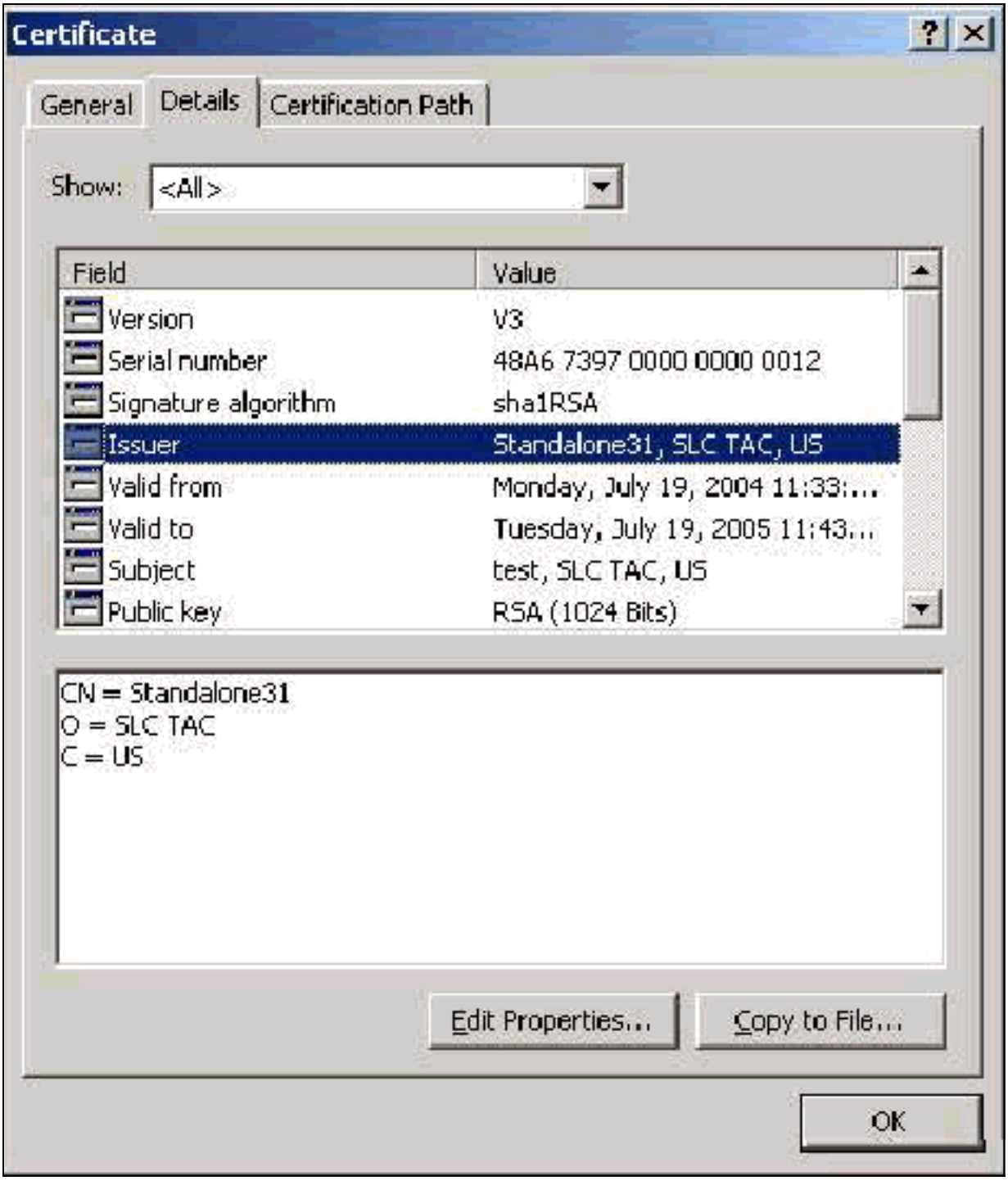
Campo Asunto

El campo Asunto identifica el certificado. El valor CN se utiliza para determinar el campo Emitido para en la ficha General del certificado y se rellena con la información que ingresa en el campo Asunto del certificado en el diálogo CSR de ACS o con la información del campo Nombre en Servicios de Certificados de Microsoft. El valor CN se utiliza para indicar al ACS qué certificado necesita utilizar del almacén de certificados del equipo local si se utiliza la opción de instalar el certificado desde el almacenamiento.



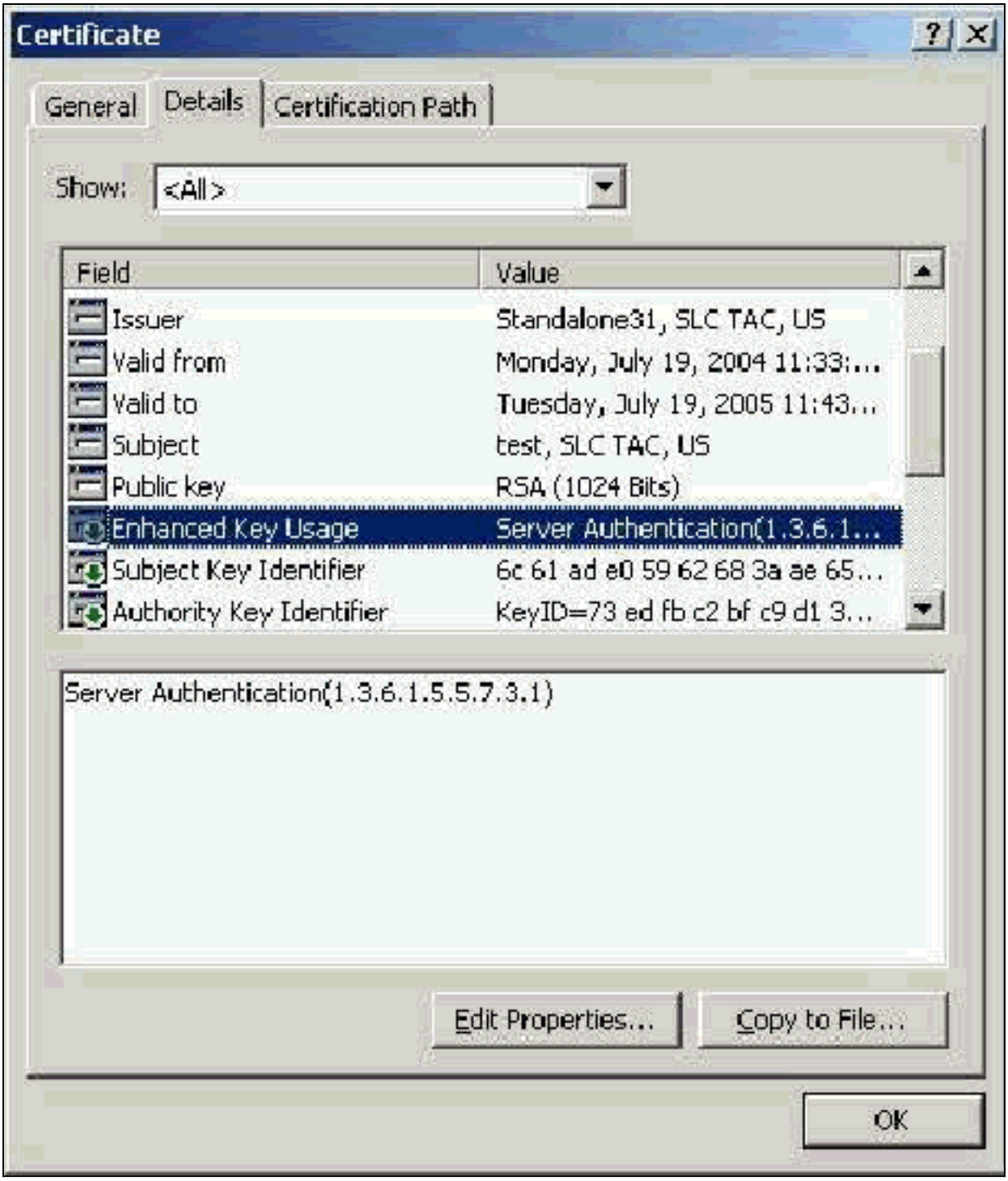
Campo del emisor

El campo Emisor identifica la CA que cortó el certificado. Utilice este valor para determinar el valor del campo Emitido por en la ficha General del certificado. Se rellena con el nombre de la CA.



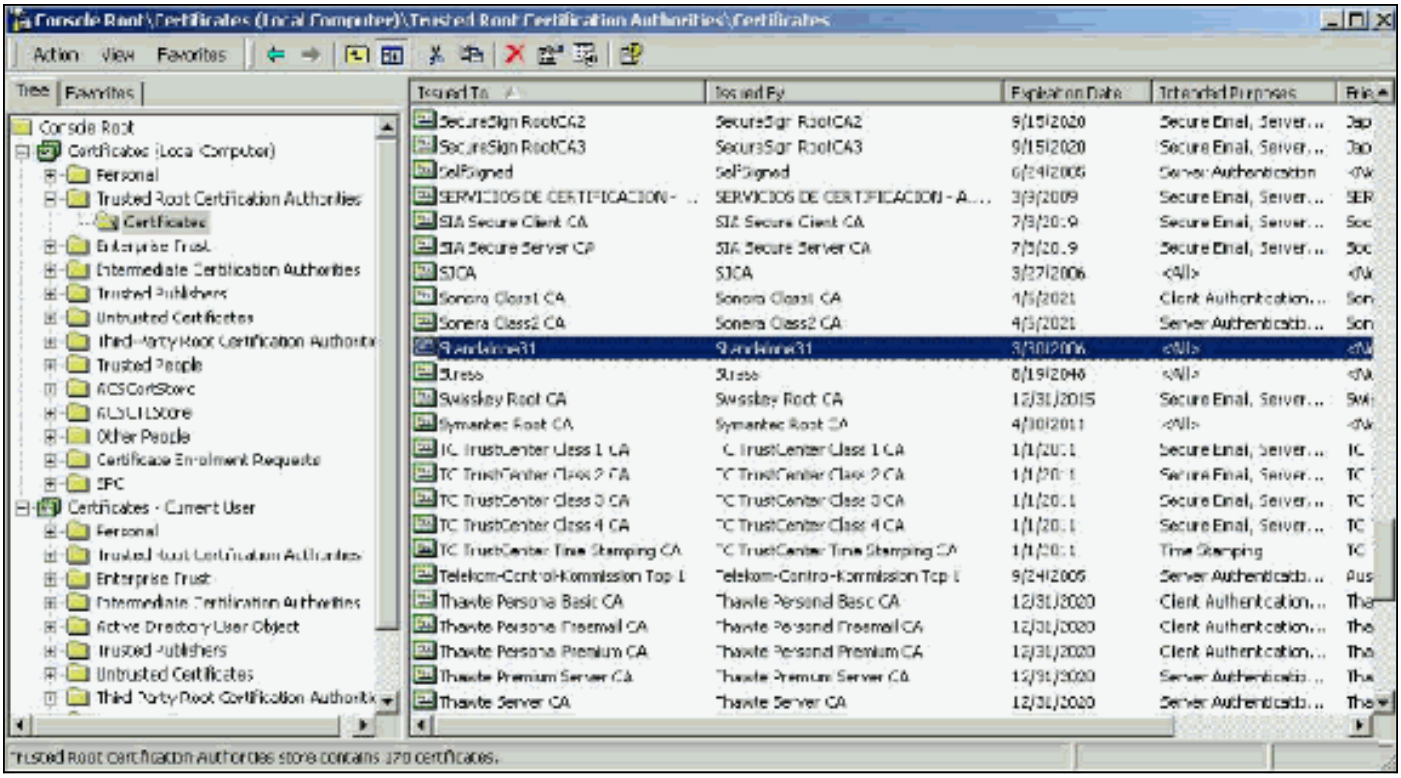
Campo de uso de clave mejorado

El campo Enhanced Key Usage (Uso mejorado de claves) identifica el propósito deseado del certificado y debe aparecer como "Server Authentication" (Autenticación del servidor). Este campo es obligatorio cuando utiliza el suplicante de Microsoft para PEAP y EAP-TLS. Cuando utiliza Microsoft Certificate Services, esto se configura en la CA independiente con la selección de **Server Authentication Certificate** en la lista desplegable Depósito esperado y en la CA empresarial con la selección de **Web Server** en la lista desplegable Plantilla de certificado. Si solicita un certificado con el uso de un CSR con Microsoft Certificate Services, no tiene la opción de especificar el propósito esperado con la CA independiente. Por lo tanto, el campo EKU está ausente. Con la CA empresarial, tiene el menú desplegable Objetivo esperado. Algunas CA no crean certificados con un campo EKU, por lo que no sirven cuando se utiliza el suplicante EAP de Microsoft.



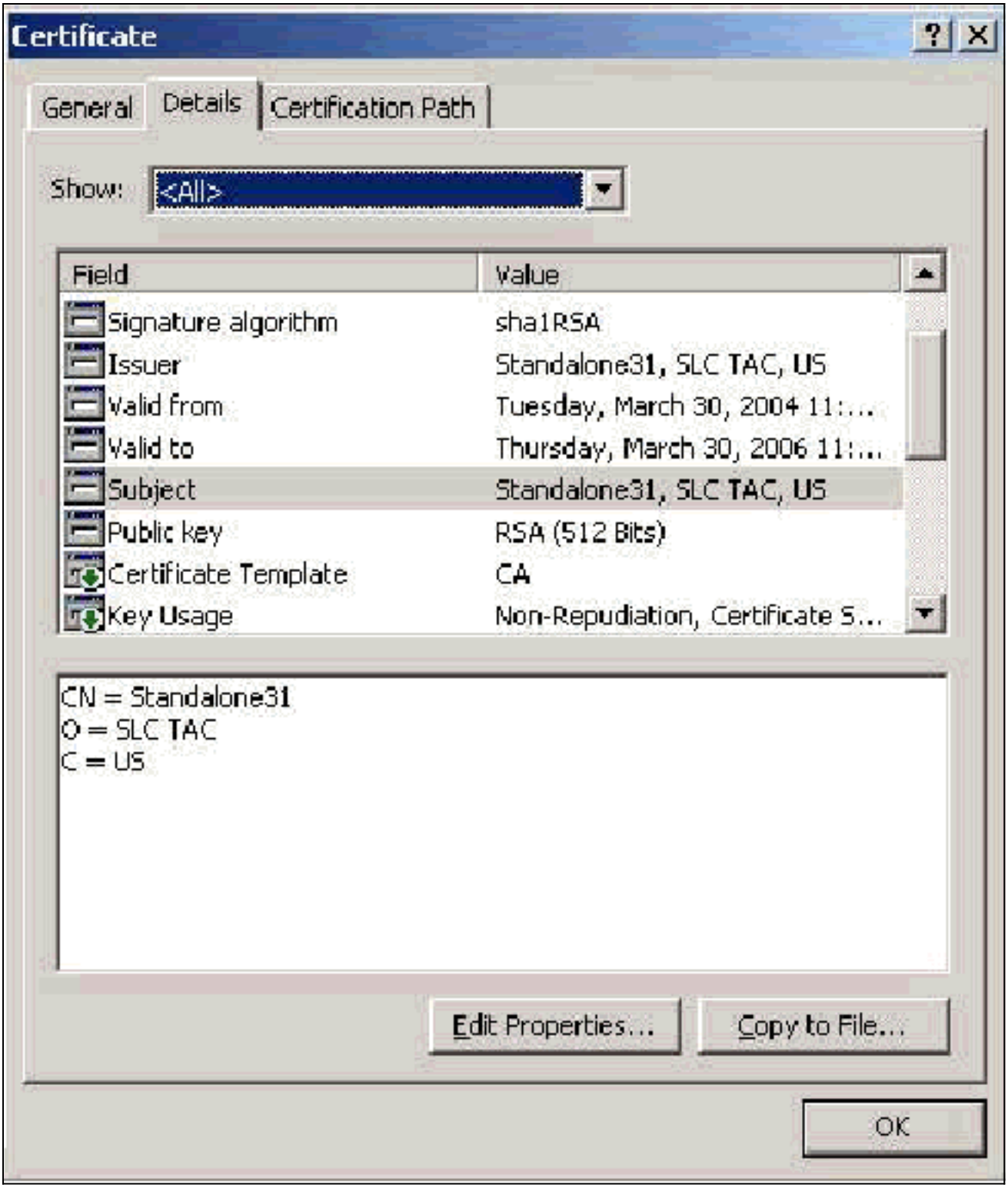
Certificados de CA raíz

El único propósito del certificado de CA raíz es identificar el certificado del servidor (y el certificado de CA intermedio, si corresponde) como un certificado de confianza para ACS y para el suplicante EAP-MSCHAPv2 de Windows. Debe estar ubicado en el almacén de Autoridades de certificación raíz de confianza en Windows tanto en el servidor ACS como, en el caso de EAP-MSCHAPv2, en el equipo cliente. La mayoría de los certificados de CA raíz de terceros se instalan con Windows y no se hace mucho esfuerzo al respecto. Si se utiliza Microsoft Certificate Services y el servidor de certificados está en la misma máquina que ACS, el certificado de CA raíz se instala automáticamente. Si el certificado de CA raíz no se encuentra en el almacén de Autoridades de certificación raíz de confianza en Windows, debe adquirirse de su CA e instalarse. Cuando se instala correctamente en el almacén de certificados de Windows, el certificado de CA raíz debe aparecer en la carpeta **Certificados (equipo local) > Autoridades de certificación raíz de confianza > Certificados** como se ve en esta ventana de ejemplo.



Campos de asunto y de emisor

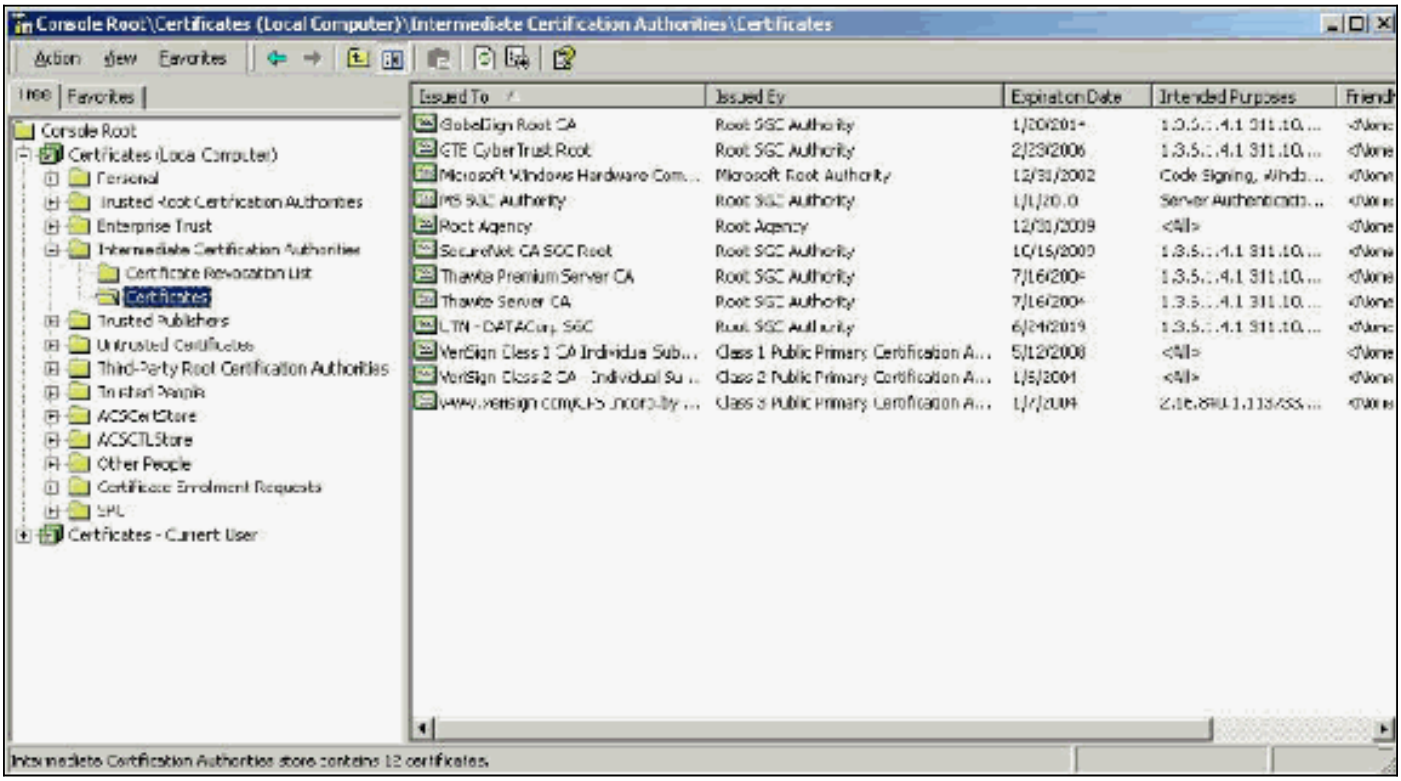
Los campos Asunto y Emisor identifican la CA y deben ser exactamente iguales. Utilice estos campos para rellenar los campos Emitido a y Emitido por en la ficha General del certificado. Se rellenan con el nombre de la CA raíz.



Certificados CA intermedios

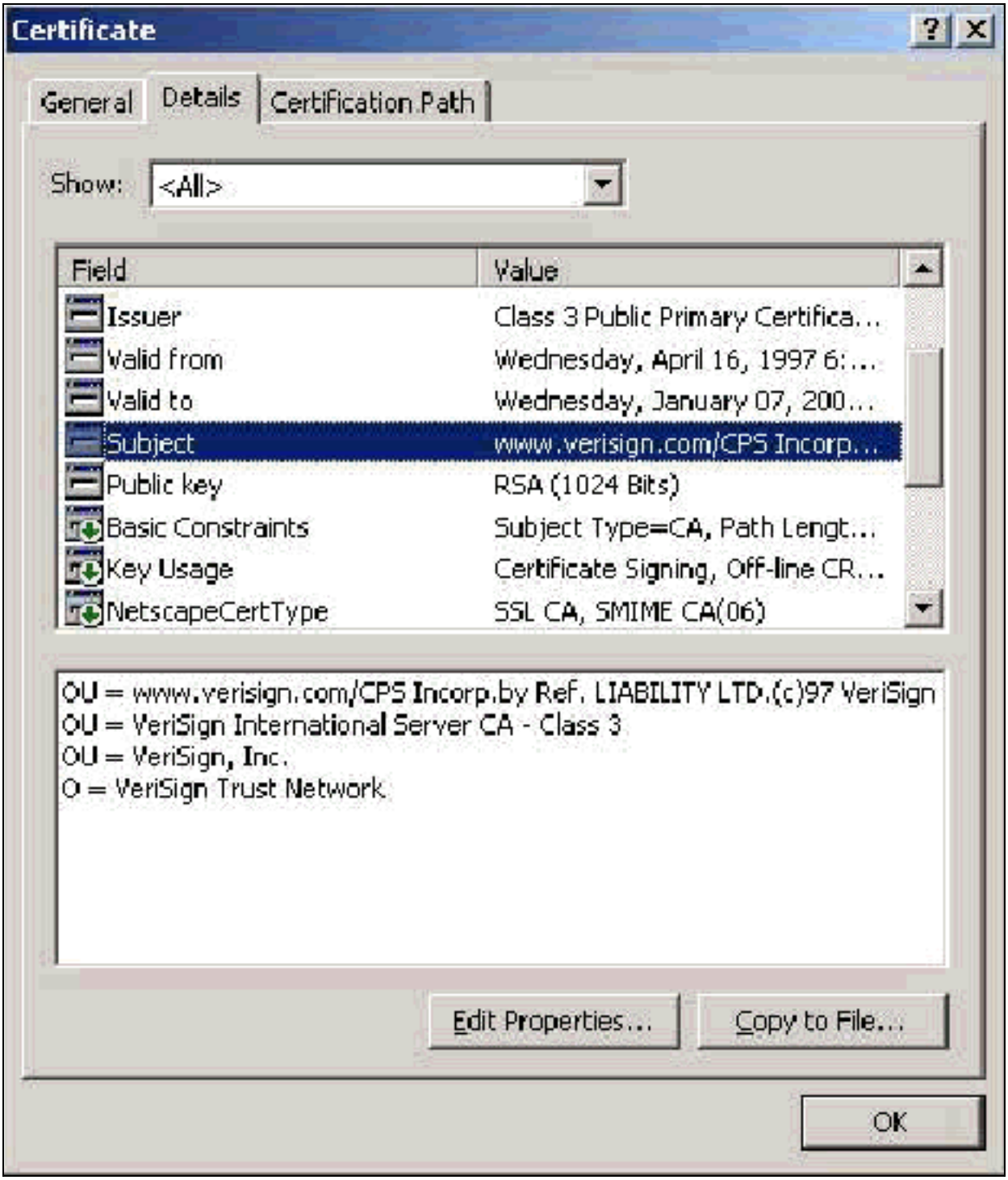
Los certificados CA intermedios son certificados que se utilizan para identificar una CA que está subordinada a una CA raíz. Algunos certificados de servidor (certificados inalámbricos de Verisign) se crean con el uso de una CA intermedia. Si se utiliza un certificado de servidor cortado por una CA intermedia, el certificado de CA intermedia debe instalarse en el área Autoridades de certificación intermedias del almacén de máquinas local en el servidor ACS. Además, si se utiliza el suplicante EAP de Microsoft en el cliente, el certificado CA raíz de la CA raíz que creó el certificado CA intermedio también debe estar en el almacén apropiado en el servidor ACS y el cliente para que se pueda establecer la cadena de confianza. Tanto el certificado de CA raíz como el certificado de CA intermedio deben marcarse como de confianza en ACS y en el cliente.

La mayoría de los certificados de la CA intermedia no están instalados con Windows, por lo que es muy probable que deba adquirirlos del proveedor. Cuando se instala correctamente en el almacén de certificados de Windows, el certificado de CA intermedio aparece en la carpeta **Certificados (equipo local) > Autoridades de certificación intermedias > Certificados** como se ve en esta ventana de ejemplo.



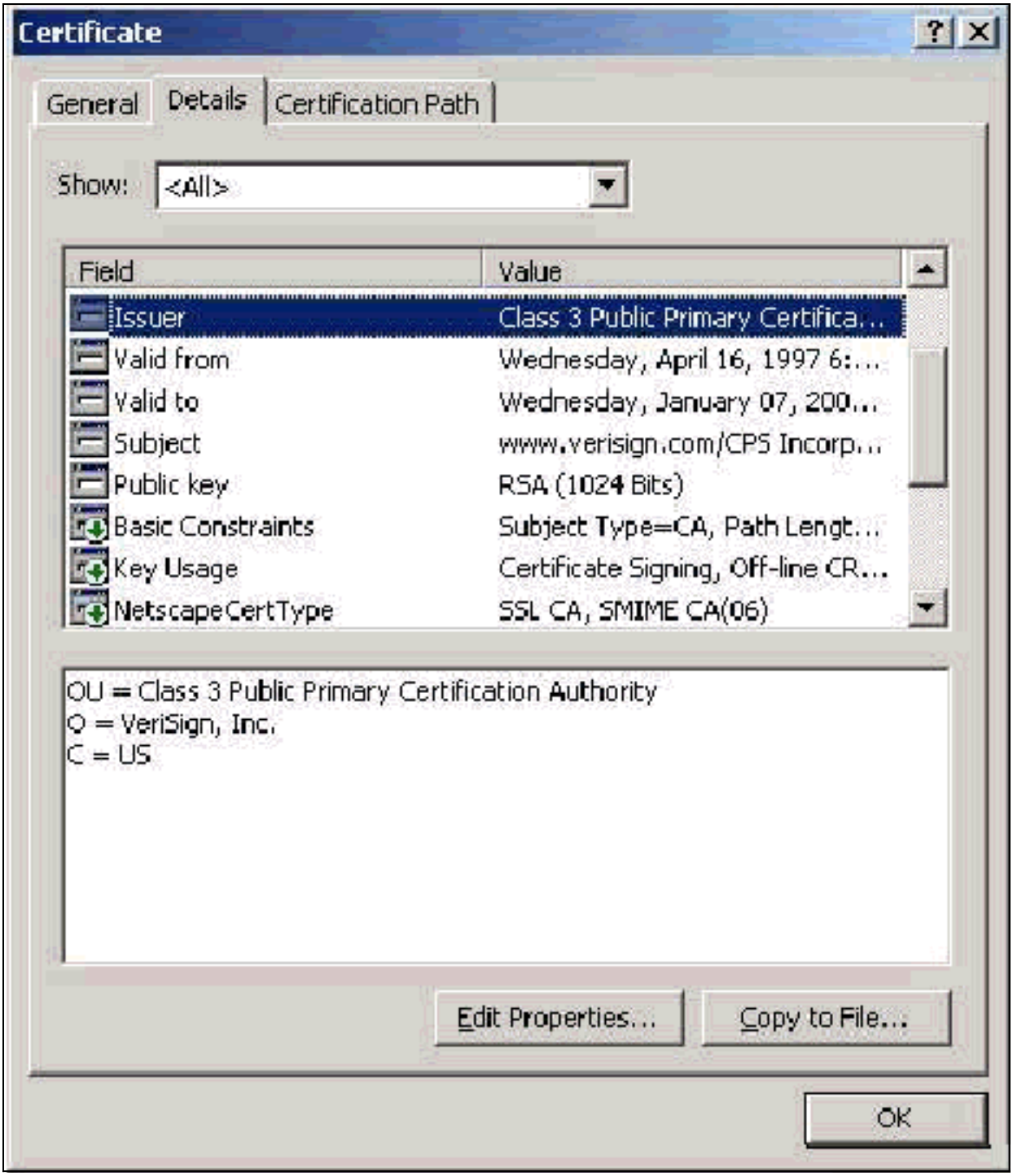
Campo Asunto

El campo Asunto identifica la CA intermedia. Este valor se utiliza para determinar el campo Emitido para en la ficha General del certificado.



Campo del emisor

El campo Emisor identifica la CA que cortó el certificado. Utilice este valor para determinar el valor del campo Emitido por en la ficha General del certificado. Se rellena con el nombre de la CA.



Certificados de cliente

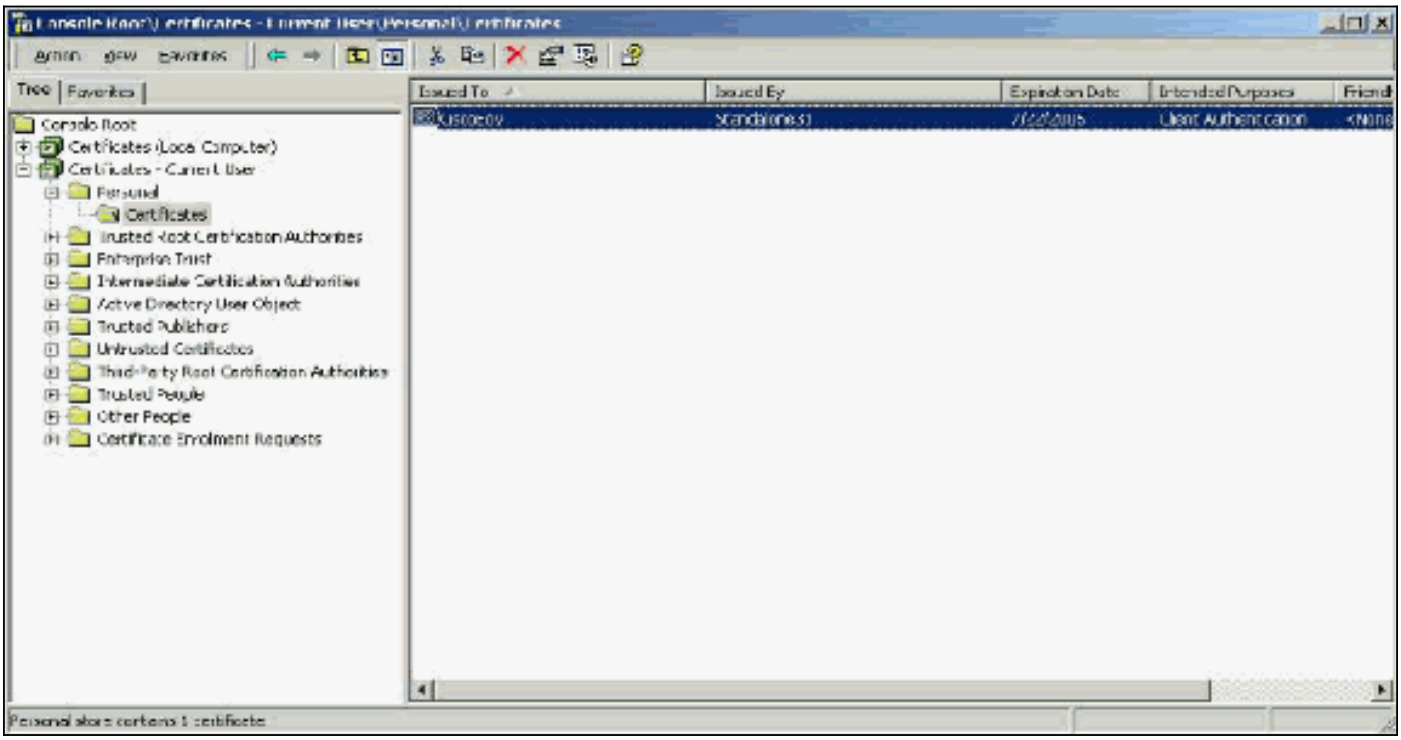
Los certificados de cliente se utilizan para identificar positivamente al usuario en EAP-TLS. No tienen ningún rol en la construcción del túnel TLS y no se utilizan para el cifrado. La identificación positiva se logra por uno de los tres medios siguientes:

- **Comparación CN (o Name)**: compara el CN del certificado con el nombre de usuario de la base de datos. Se incluye más información sobre este tipo de comparación en la descripción del campo Asunto del certificado.
- **Comparación SAN**: compara la SAN en el certificado con el nombre de usuario en la base de datos. Esto sólo se soporta a partir de ACS 3.2. Se incluye más información sobre este tipo de comparación en la descripción del campo Nombre alternativo del sujeto del certificado.
- **Comparación binaria**: compara el certificado con una copia binaria del certificado almacenado

en la base de datos (sólo AD y LDAP pueden hacerlo). Si utiliza la comparación binaria de certificados, debe almacenar el certificado de usuario en un formato binario. Además, para LDAP genérico y Active Directory, el atributo que almacena el certificado debe ser el atributo LDAP estándar denominado "usercertificate".

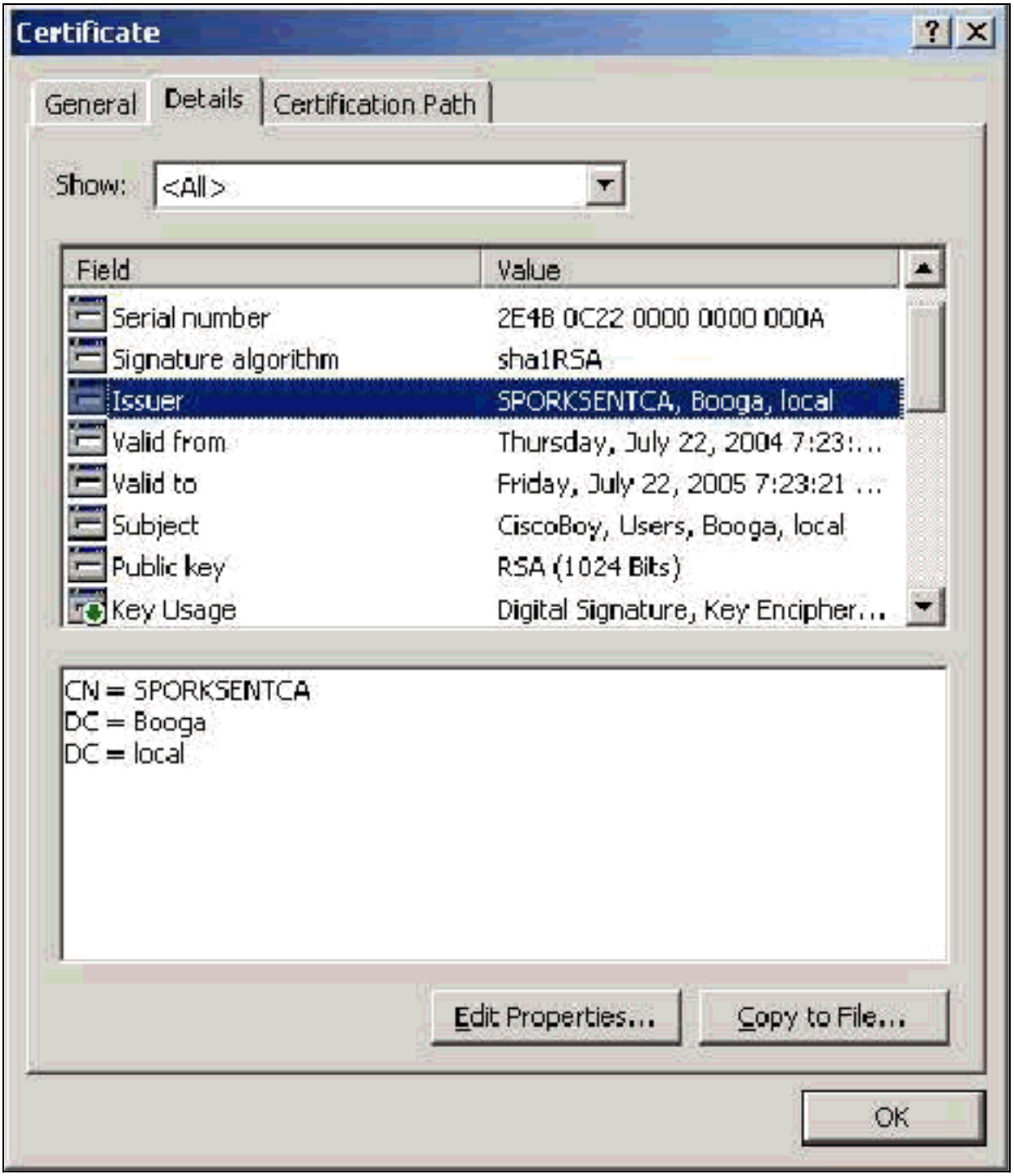
Independientemente del método de comparación que se utilice, la información del campo correspondiente (CN o SAN) debe coincidir con el nombre que utiliza la base de datos para la autenticación. AD utiliza el nombre de NetBios para la autenticación en modo mixto y UPN en modo nativo.

Esta sección trata la generación de certificados de cliente con el uso de Servicios de certificado de Microsoft. EAP-TLS requiere un certificado de cliente único para que cada usuario se autentique. El certificado debe estar instalado en cada equipo para cada usuario. Cuando se instala correctamente, el certificado se encuentra en la carpeta **Certificates -Current User > Personal > Certificates** como se ve en esta ventana de ejemplo.



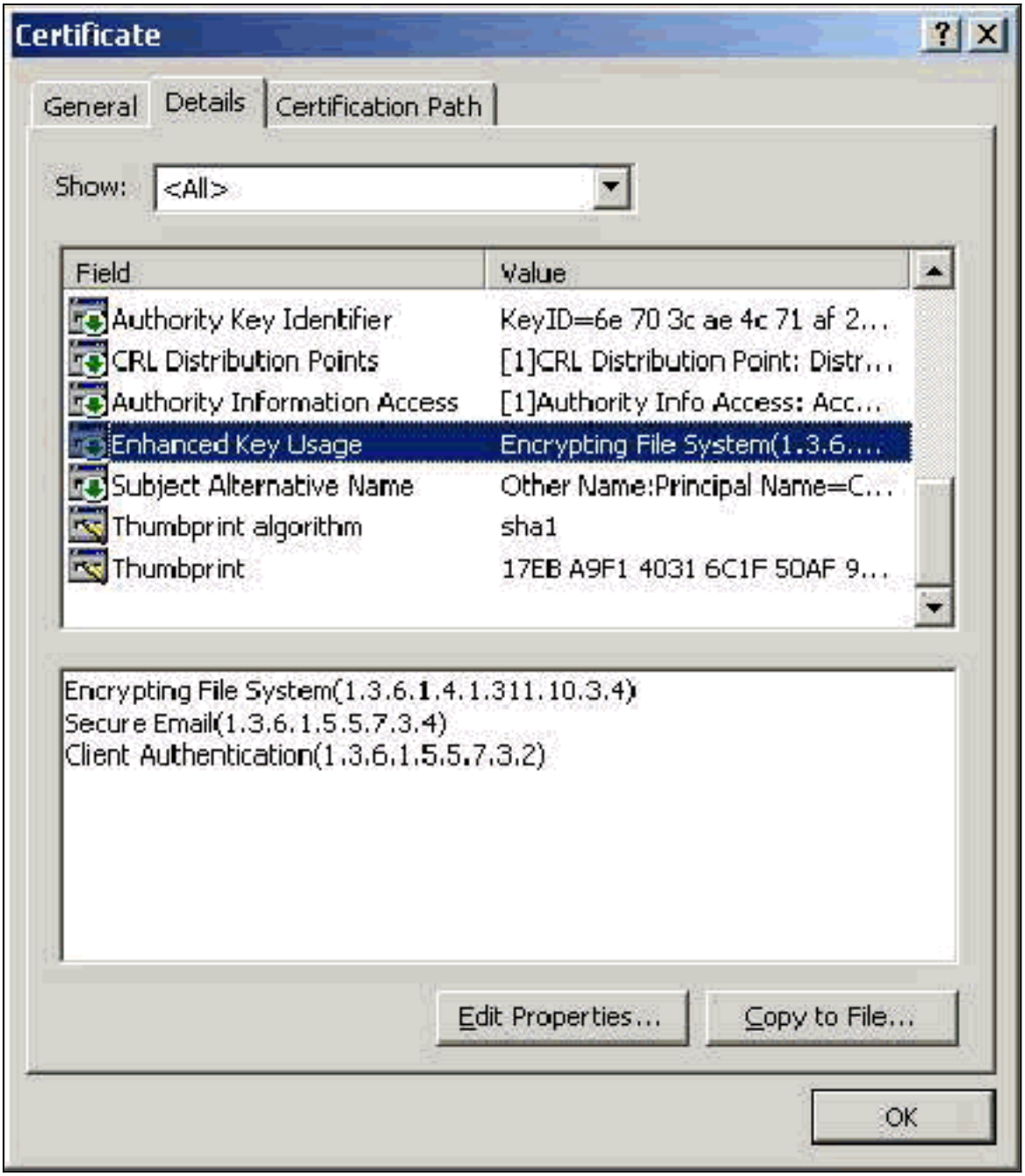
Campo del emisor

El campo Emisor identifica la CA que corta el certificado. Utilice este valor para determinar el valor del campo Emitido por en la ficha General del certificado. Esto se rellena con el nombre de la CA.



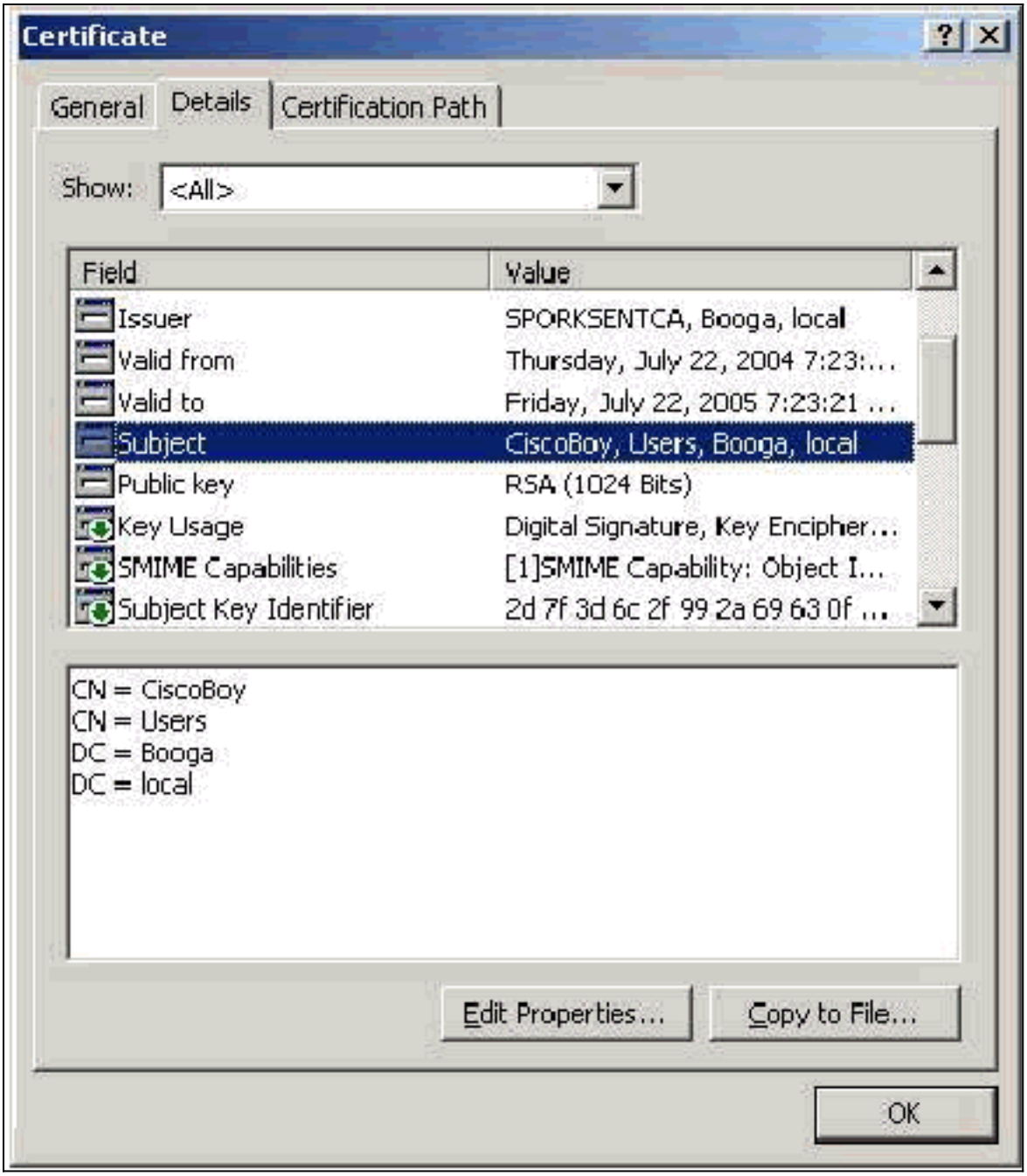
Campo de uso de clave mejorado

El campo Uso mejorado de claves identifica el propósito deseado del certificado y necesita contener la autenticación del cliente. Este campo es obligatorio cuando utiliza el suplicante de Microsoft para PEAP y EAP-TLS. Cuando utiliza Microsoft Certificate Services, esto se configura en la CA independiente cuando selecciona **Client Authentication Certificate** en la lista desplegable Depósito esperado y en la CA empresarial cuando selecciona **User** en la lista desplegable Certificate Template. Si solicita un certificado con el uso de un CSR con Microsoft Certificate Services, no tiene la opción de especificar el propósito esperado con la CA independiente. Por lo tanto, el campo EKU está ausente. Con la CA empresarial, tiene el menú desplegable Objetivo esperado. Algunas CA no crean certificados con un campo EKU. Son inútiles cuando se utiliza el suplicante EAP de Microsoft.



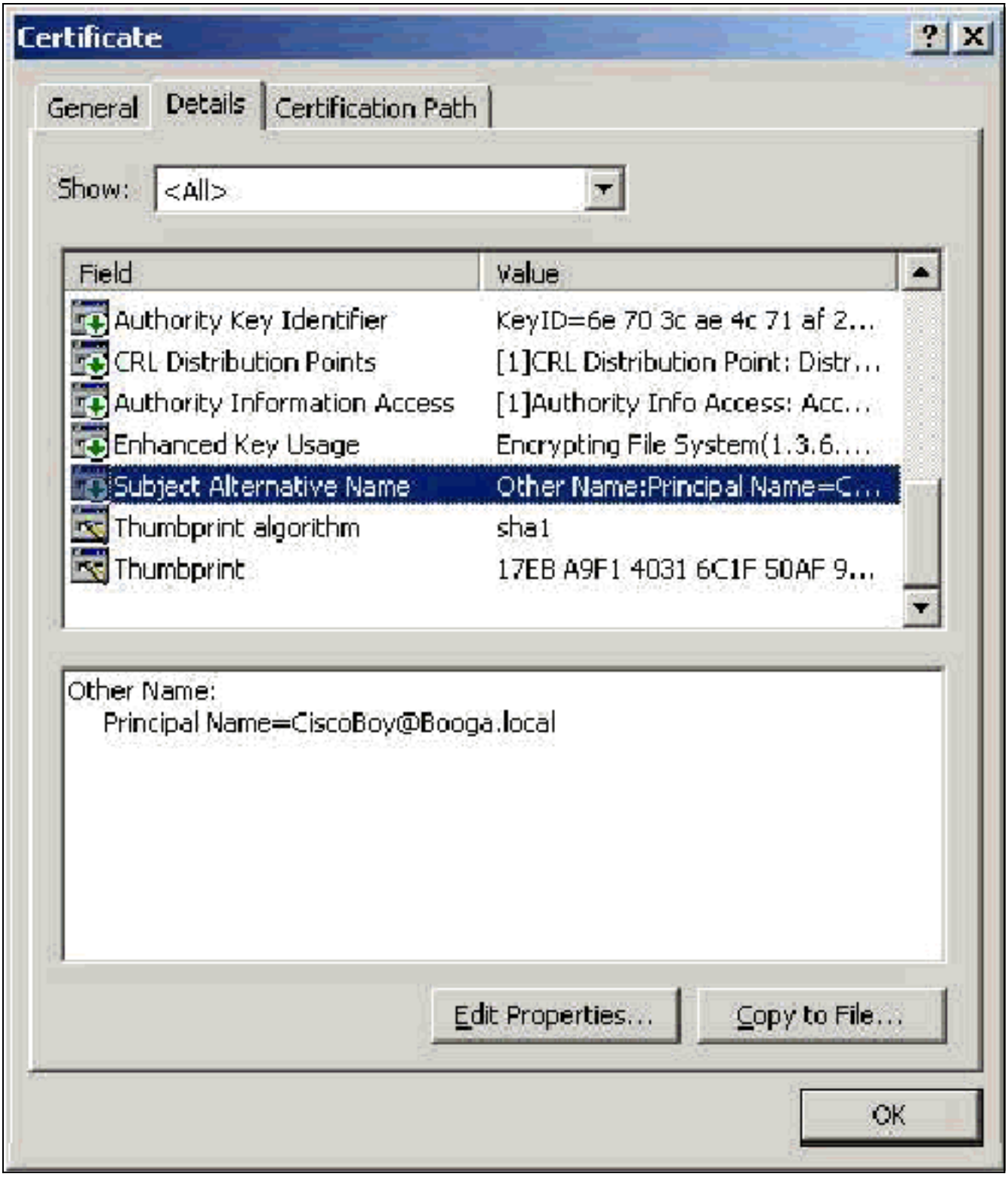
Campo Asunto

Este campo se utiliza en la comparación CN. El primer CN listado se compara con la base de datos para encontrar una coincidencia. Si se encuentra una coincidencia, la autenticación se realiza correctamente. Si utiliza una CA independiente, el CN se rellena con lo que introduzca en el campo Nombre del formulario de envío de certificado. Si utiliza la CA de empresa, la CN se rellena automáticamente con el nombre de la cuenta como se muestra en la consola Usuarios y equipos de Active Directory (esto no necesariamente coincide con el UPN o el nombre de NetBios).



Campo Nombre alternativo del asunto

El campo Nombre alternativo del sujeto se utiliza en la comparación de SAN. La SAN enumerada se compara con la base de datos para encontrar una coincidencia. Si se encuentra una coincidencia, la autenticación se realiza correctamente. Si utiliza la CA empresarial, la SAN se rellena automáticamente con el nombre de inicio de sesión de Active Directory @domain (UPN). La CA independiente no incluye un campo SAN, por lo que no puede utilizar la comparación de SAN.



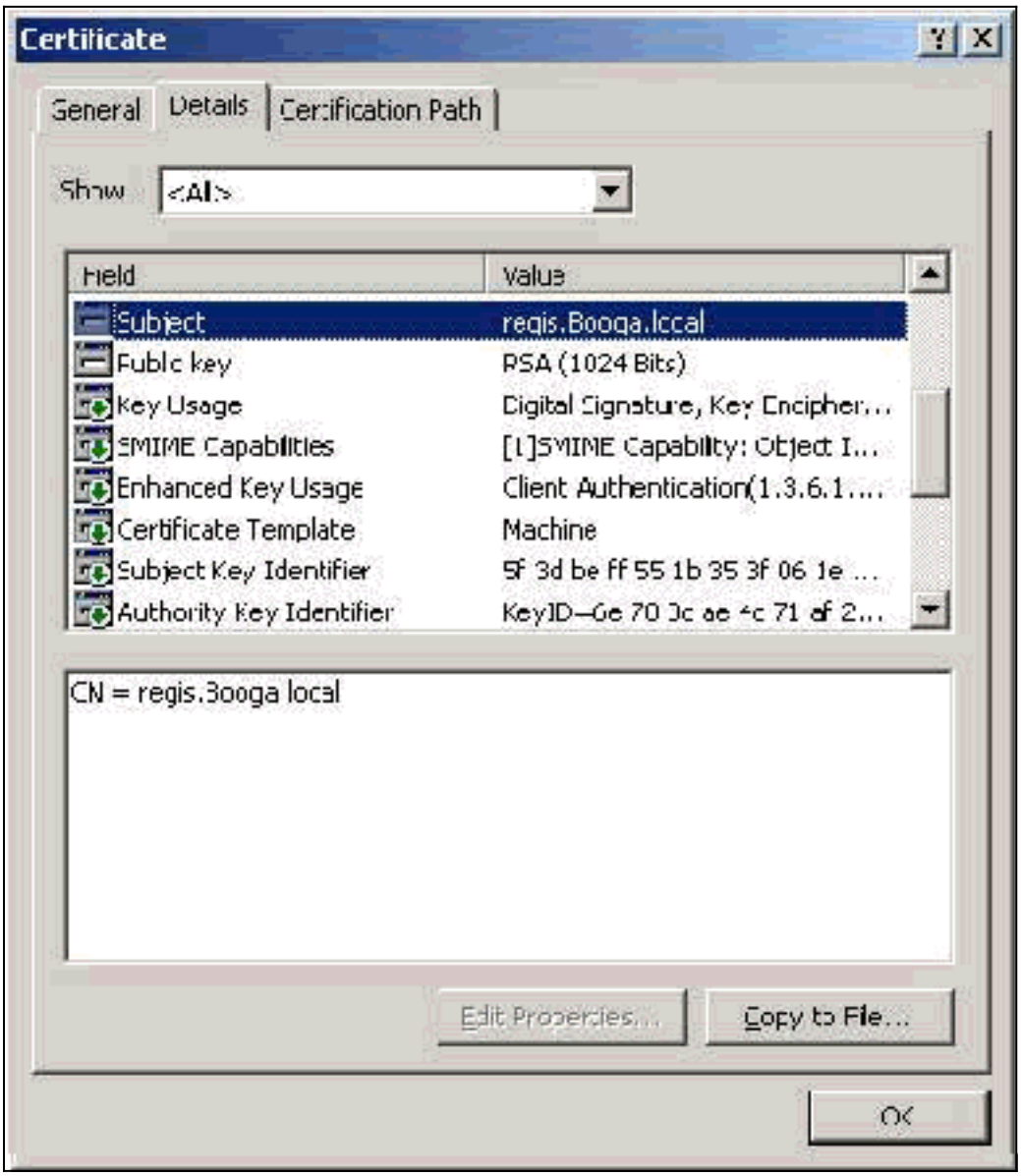
Certificados de equipo

Los certificados de equipo se utilizan en EAP-TLS para identificar positivamente el equipo cuando se utiliza la autenticación de equipo. Solo puede acceder a estos certificados cuando configure la CA de Microsoft Enterprise para la inscripción automática de certificados y se una al equipo al dominio. El certificado se crea automáticamente cuando se utilizan las credenciales de Active Directory del equipo y se instalan en el almacén de equipos local. Los equipos que ya son miembros del dominio antes de configurar la inscripción automática recibirán un certificado la próxima vez que se reinicie Windows. El certificado de equipo está instalado en la carpeta Certificados (equipo local) > Personal > Certificados del complemento MMC Certificados (equipo local), al igual que los certificados de servidor. No puede instalar estos certificados en ningún otro

equipo porque no puede exportar la clave privada.

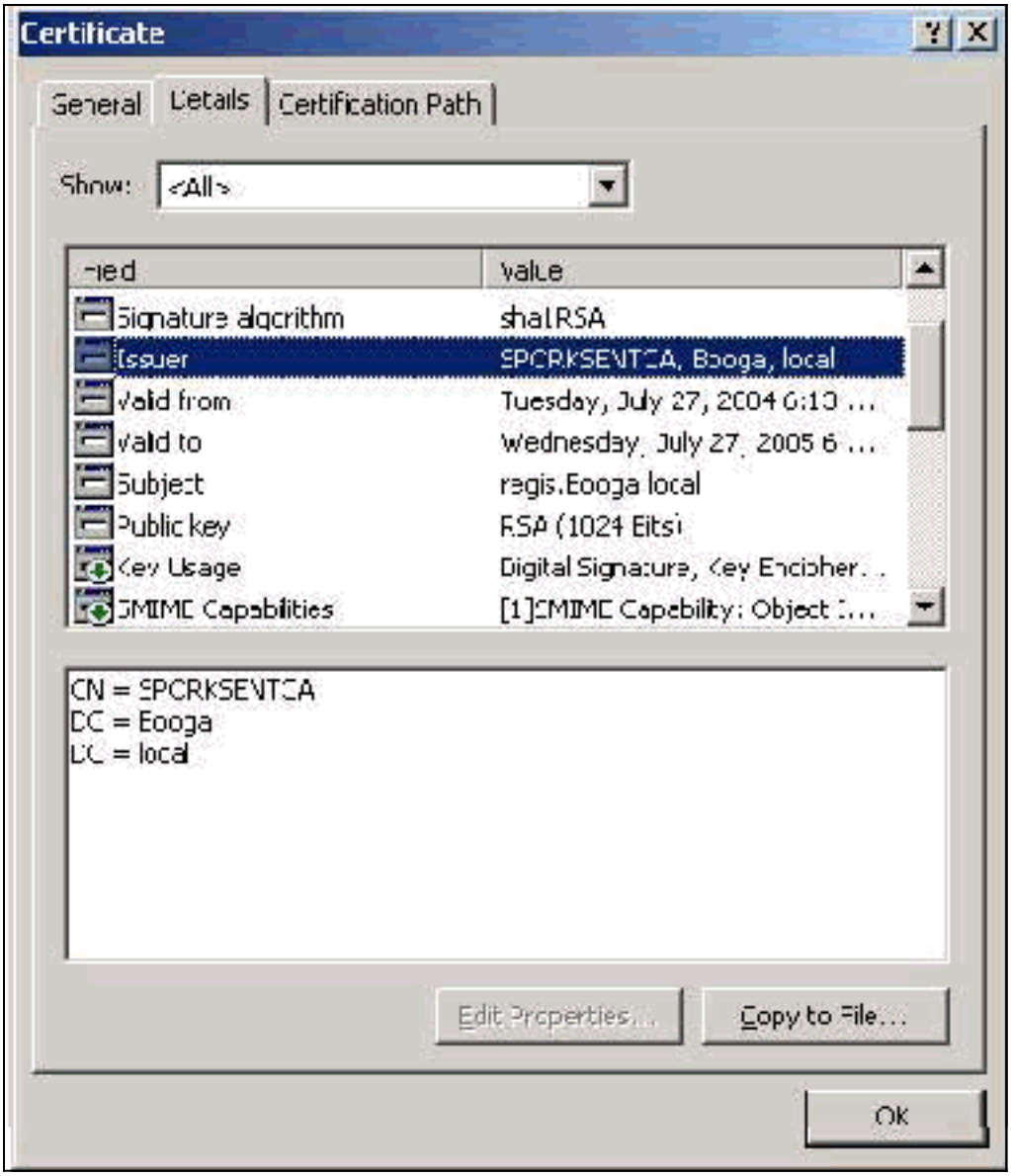
Campos de Asunto y SAN

Los campos Subject (Asunto) y SAN (SAN) identifican el ordenador. El valor se rellena con el nombre completo del equipo y se utiliza para determinar el campo Emitido para en la ficha General del certificado y es el mismo para los campos Asunto y SAN.



Campo del emisor

El campo Emisor identifica la CA que cortó el certificado. Utilice este valor para determinar el valor del campo Emitido por en la ficha General del certificado. Se rellena con el nombre de la CA.



Apéndice A: Extensiones de certificados comunes

.csr: en realidad no es un certificado sino una solicitud de firma de certificado. Se trata de un archivo de texto sin formato 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 sea en realidad una clave privada. El contenido debe ser texto plano 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: extensión genérica que denota un certificado. Los certificados CA de servidor, raíz y media pueden tener este formato. Normalmente es un archivo de texto sin formato con una extensión que puede cambiar según sea necesario y puede tener formato DER o Base 64. Puede importar este formato al almacén de certificados de Windows.

.pem: esta extensión significa Correo de privacidad mejorada. Esta extensión se utiliza comúnmente con UNIX, Linux, BSD, etc. Normalmente se utiliza para certificados de servidor y claves privadas, y normalmente es un archivo de texto sin formato con una extensión que puede cambiar según sea necesario de .pem a .cer para poder importarlo al almacén de certificados de Windows.

El contenido interno de los archivos .cer y .pem generalmente tiene el siguiente aspecto:

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

.pfx: esta extensión significa Intercambio de información personal. Este formato es un método que puede utilizar para agrupar certificados en un solo archivo. Por ejemplo, puede agrupar un certificado de servidor y su clave privada asociada y el certificado de CA raíz en un archivo e importar fácilmente el archivo en el almacén de certificados de Windows adecuado. Se utiliza habitualmente para certificados de servidor y cliente. Desafortunadamente, si se incluye un certificado de CA raíz, el certificado de CA raíz siempre se instala en el almacén de usuario actual en lugar del almacén de equipo local incluso si se especifica el almacén de equipos locales para la instalación.

.p12: este formato sólo se ve generalmente con un certificado de cliente. Puede importar este formato al almacén de certificados de Windows.

.p7b: este es otro formato que almacena varios certificados en un archivo. Puede importar este formato al almacén de certificados de Windows.

Apéndice B: Conversión de formato de certificado

En la mayoría de los casos, la conversión de certificados se produce cuando se cambia la extensión (por ejemplo, de .pem a .cer), ya que los certificados suelen estar en formato de texto sin formato. A veces, un certificado no está en formato de texto simple y debe convertirlo con el

uso de una herramienta como OpenSSL . Por ejemplo, ACS Solution Engine no puede instalar certificados en el formato .pfx. Por lo tanto, debe convertir el certificado y la clave privada en un formato utilizable. Esta es la sintaxis básica del comando para OpenSSL:

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

Se le solicitarán la contraseña de importación y la frase de paso PEM. Estas contraseñas deben ser las mismas y son la contraseña de clave privada especificada cuando se exporta .pfx. El resultado es un único archivo .pem que incluye todos los certificados y claves privadas en .pfx. Este archivo puede ser referido en ACS como el certificado y el archivo de clave privada y se instala sin problemas.

Apéndice C: Período de validez del certificado

Un certificado sólo se puede utilizar durante su período de validez. El período de validez para un certificado de CA raíz se determina cuando se establece la CA raíz y puede variar. El período de validez de un certificado CA intermedio se determina cuando se establece la CA y no puede exceder el período de validez de la CA raíz a la que está subordinada. El período de validez para los certificados de servidor, cliente y equipo se establece automáticamente en un año con Microsoft Certificate Services. Esto sólo se puede cambiar cuando se hackea el registro de Windows según el artículo 254632 de Microsoft Knowledge Base y no puede exceder el período de validez de la CA raíz. El período de validez de los certificados autofirmados que genera ACS es siempre de 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