Guia de certificado EAP versão 1.01

Contents

Introduction

Este documento esclarece algumas das confusões que acompanham os vários tipos de certificado, formatos e requisitos associados às várias formas do Extensible Authentication Protocol (EAP). Os cinco tipos de certificado relacionados ao EAP discutidos neste documento são Servidor, CA raiz, CA intermediária, Cliente e Máquina. Estes certificados encontram-se em vários formatos e podem existir requisitos diferentes em relação a cada um deles, com base na implementação de PEA em causa.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Certificados de servidor

O certificado do servidor é instalado no servidor RADIUS e seu objetivo principal no EAP é criar o túnel TLS (Transport Layer Security) criptografado que protege as informações de autenticação. Quando você usa EAP-MSCHAPv2, o certificado do servidor assume uma função secundária, que é identificar o servidor RADIUS como uma entidade confiável para autenticação. Essa função secundária é realizada com o uso do campo Enhanced Key Usage (EKU). O campo EKU identifica o certificado como um certificado de servidor válido e verifica se a AC raiz que emitiu o certificado é uma AC raiz fidedigna. Isso exige a presença do certificado CA raiz. O Cisco Secure ACS exige que o certificado seja codificado em base64 ou formato binário codificado em DER X.509 v3.

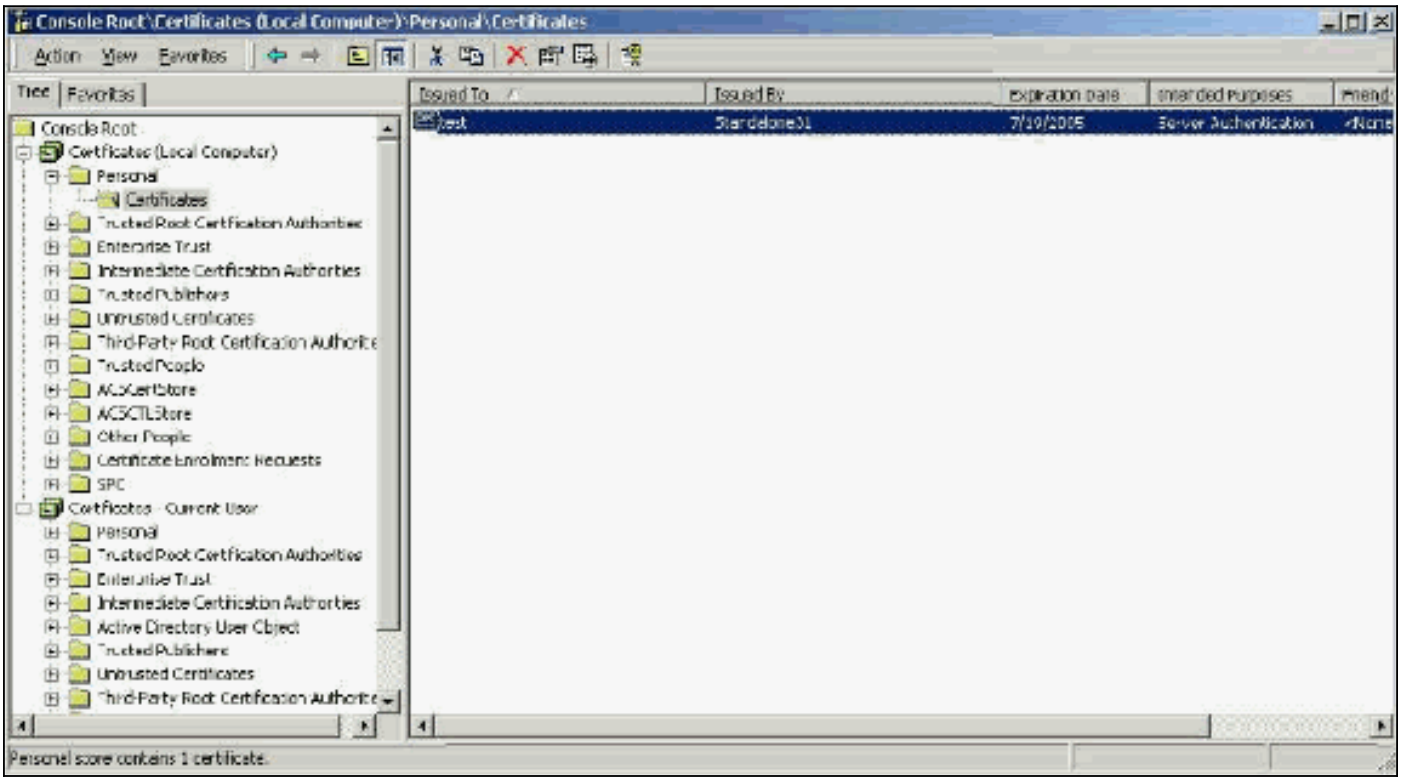
Você pode criar esse certificado usando uma solicitação de assinatura de certificado (CSR) no ACS, que é enviada a uma CA. Ou você também pode cortar o certificado usando um formulário interno de criação de certificado CA (como o Microsoft Certificate Services). É importante observar que, embora você possa criar o certificado do servidor com tamanhos de chave maiores que 1024, qualquer chave maior que 1024 não funciona com PEAP. O cliente trava mesmo se a autenticação passasse.

Se você criar o certificado com o uso de um CSR, ele será criado com um formato .cer, .pem ou .txt. Em raras ocasiões, ele é criado sem extensão. Certifique-se de que seu certificado seja um arquivo de texto simples com uma extensão que você pode alterar conforme necessário (o aplicativo ACS usa a extensão .cer ou .pem). Além disso, se você usar um CSR, a chave privada do certificado será criada no caminho especificado como um arquivo separado que pode ou não ter uma extensão e que tem uma senha associada a ela (a senha é necessária para instalação no ACS). Independentemente da extensão, verifique se é um arquivo de texto simples com uma extensão que você pode alterar conforme necessário (o aplicativo ACS usa a extensão .pvk ou .pem). Se nenhum caminho for especificado para a chave privada, o ACS salvará a chave no diretório C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs e procurará nesse diretório se nenhum caminho for especificado para o arquivo de chave privada quando você instalar o certificado.

Se o certificado for criado com o uso do formulário de envio do certificado do Microsoft Certificate Services, certifique-se de marcar as chaves como exportáveis para que você possa instalar o certificado no ACS. A criação de um certificado dessa forma simplifica significativamente o processo de instalação. Você pode instalá-lo diretamente na loja adequada do Windows na interface da Web Serviços de Certificado e depois instalá-lo no ACS a partir do armazenamento com o uso do CN como referência. Um certificado instalado no armazenamento local do

computador também pode ser exportado do armazenamento do Windows e instalado em outro computador com facilidade. Quando esse tipo de certificado é exportado, as chaves precisam ser marcadas como exportáveis e receber uma senha. O certificado aparece então no formato .pfx, que inclui a chave privada e o certificado do servidor.

Quando instalado corretamente no arquivo de certificados do Windows, o Certificado do Servidor precisa ser exibido na pasta **Certificados (Computador Local) > Pessoal > Certificados** conforme visto nesta janela de exemplo.



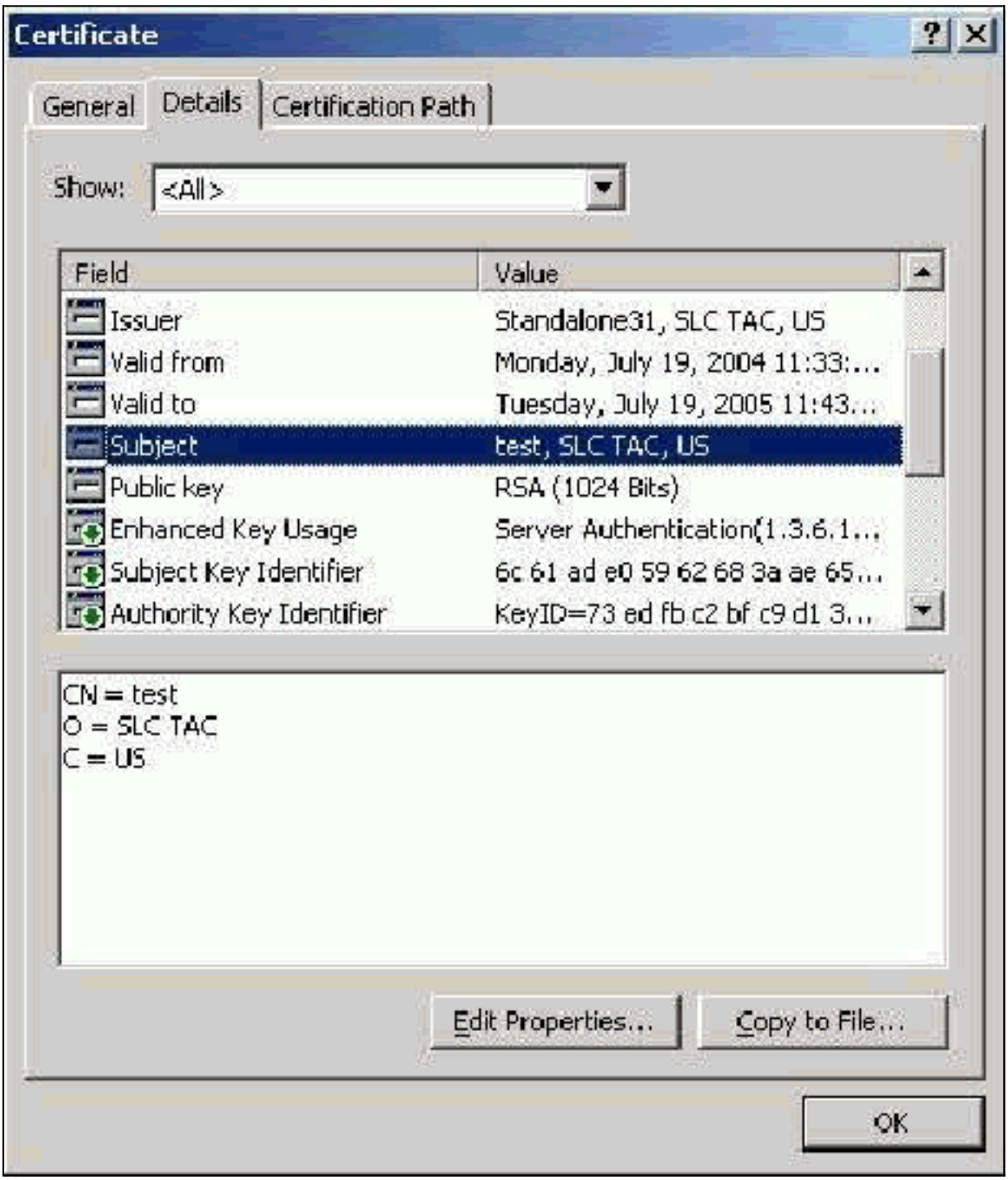
Certificados autoassinados são certificados que você cria sem uma raiz ou o envolvimento intermediário da CA. Eles têm o mesmo valor nos campos de assunto e emissor, como um certificado CA raiz. A maioria dos certificados autoassinados usa o formato X.509 v1. Portanto, eles não funcionam com o ACS. No entanto, a partir da versão 3.3, o ACS tem a capacidade de criar seus próprios certificados autoassinados que você pode usar para EAP-TLS e PEAP. Não utilize um tamanho de chave superior a 1024 para compatibilidade com PEAP e EAP-TLS. Se você usa um certificado autoassinado, o certificado também atua na capacidade do Certificado de CA raiz e deve ser instalado na pasta **Certificados (Computador local) > Autoridades de certificação raiz confiáveis > Certificados** do cliente quando você usa o suplicante do Microsoft EAP. Ele instala automaticamente no arquivo de certificados raiz confiável no servidor. No entanto, ele ainda deve ser confiável na Certificate Trust List (Lista de certificados confiáveis) na configuração do certificado ACS. Consulte a seção Certificados CA raiz para obter mais informações.

Como os certificados autoassinados são usados como certificado de CA raiz para validação de certificado de servidor quando você usa o suplicante Microsoft EAP e como o período de validade não pode ser aumentado do padrão de um ano, a Cisco recomenda que você os use somente para EAP como medida temporária até que você possa usar uma CA tradicional.

Campo de assunto

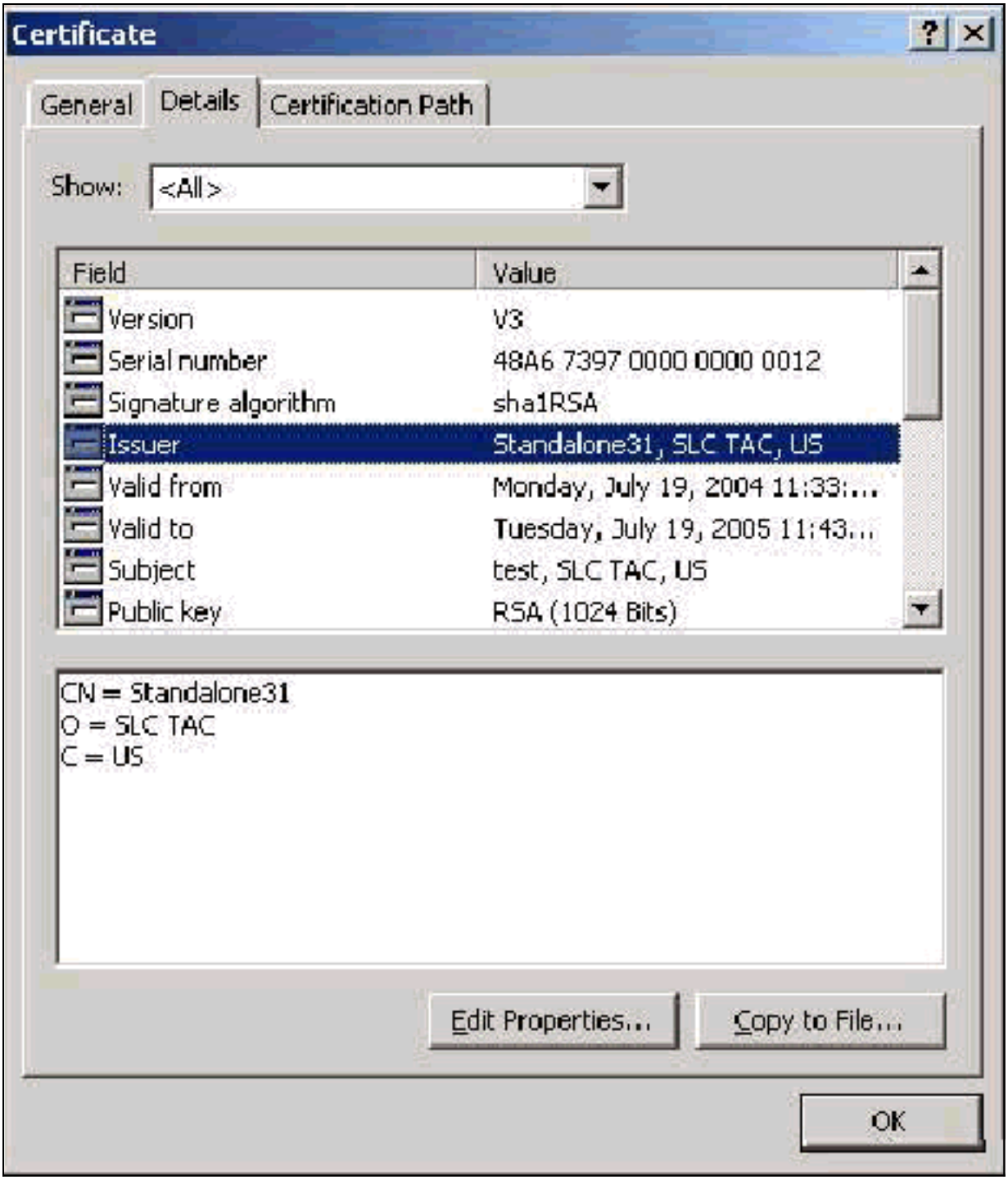
O campo Assunto identifica o certificado. O valor CN é usado para determinar o campo Emitido para na guia Geral do certificado e é preenchido com as informações que você insere no campo

Assunto do certificado na caixa de diálogo CSR do ACS ou com as informações do campo Nome nos Serviços de Certificado da Microsoft. O valor CN é usado para informar ao ACS qual certificado ele precisa usar do repositório de certificados da máquina local se a opção de instalar o certificado do armazenamento for usada.



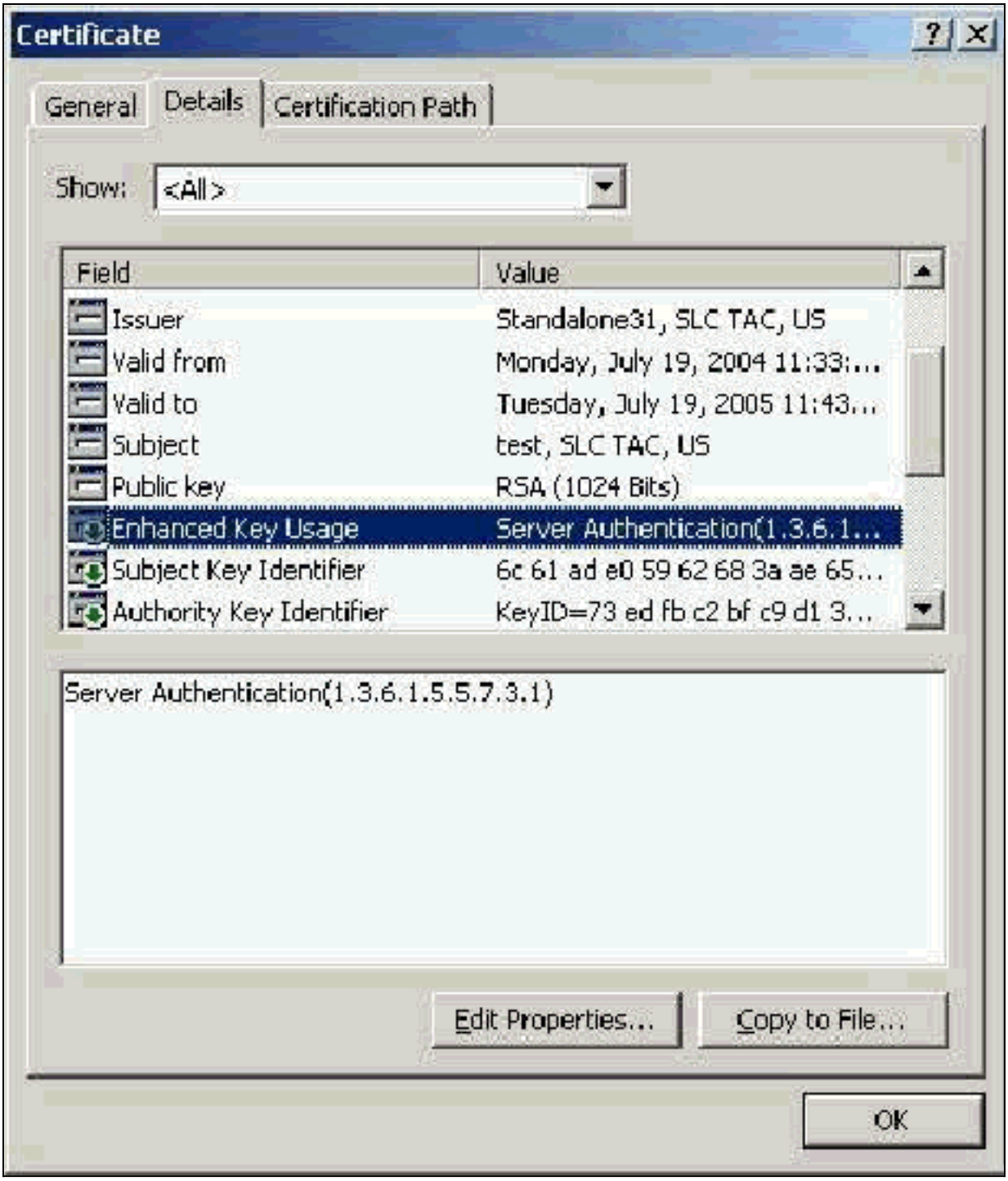
Campo do emissor

O campo Emitente identifica a CA que cortou o certificado. Use esse valor para determinar o valor do campo Emitido por na guia Geral do certificado. Ele é preenchido com o nome da CA.



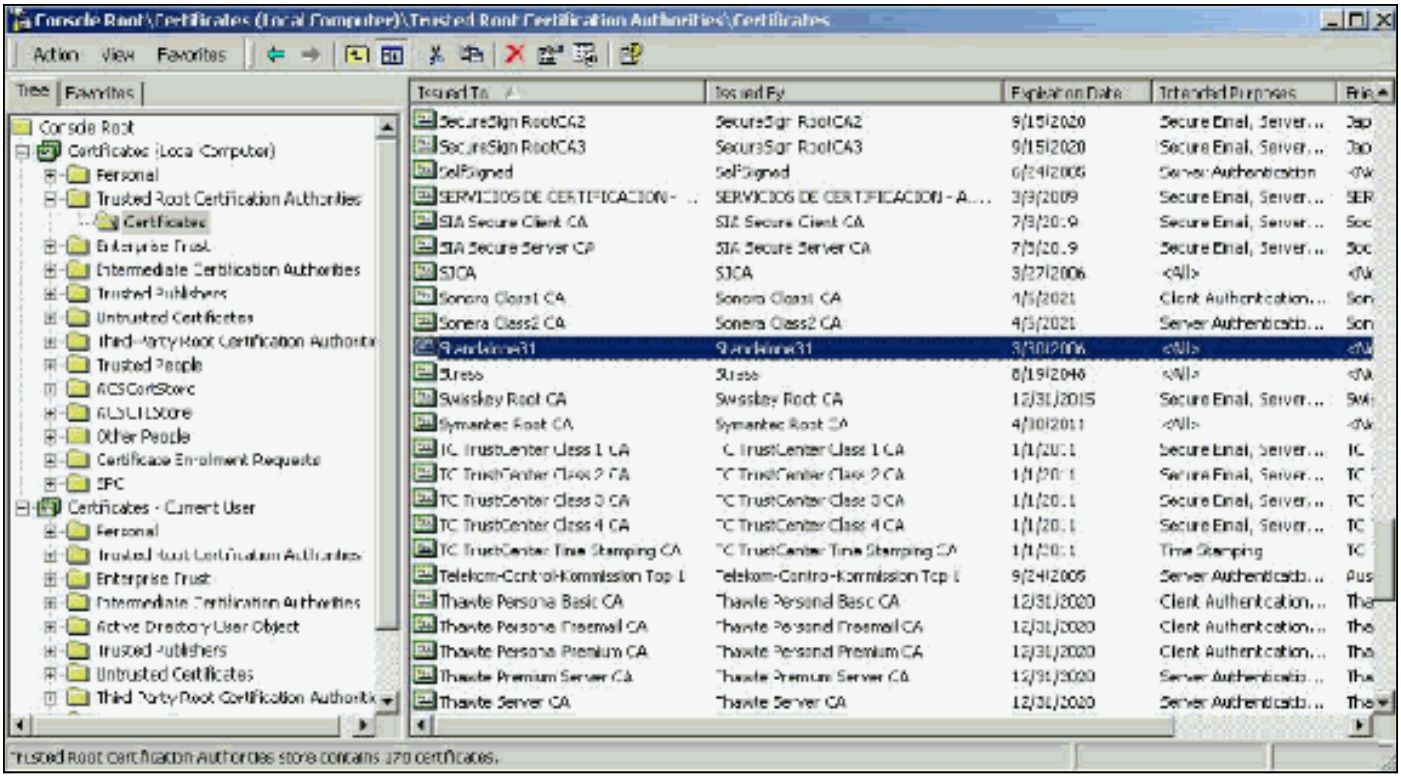
Campo de uso de chave aprimorado

O campo Enhanced Key Usage identifica a finalidade do certificado e precisa ser listado como "Autenticação de servidor". Este campo é obrigatório quando você usa o suplicante da Microsoft para PEAP e EAP-TLS. Quando você usa o Microsoft Certificate Services, ele é configurado na CA independente com a seleção de **Server Authentication Certificate** no menu suspenso Finalidade pretendida e na AC corporativa com a seleção de **Servidor Web** no menu suspenso Certificate Template. Se você solicitar um certificado com o uso de um CSR com o Microsoft Certificate Services, não terá a opção de especificar a Finalidade com a CA independente. Portanto, o campo EKU está ausente. Com a CA corporativa, você tem o menu suspenso Finalidade. Algumas CAs não criam certificados com um campo EKU, portanto, são inúteis quando você usa o suplicante EAP da Microsoft.



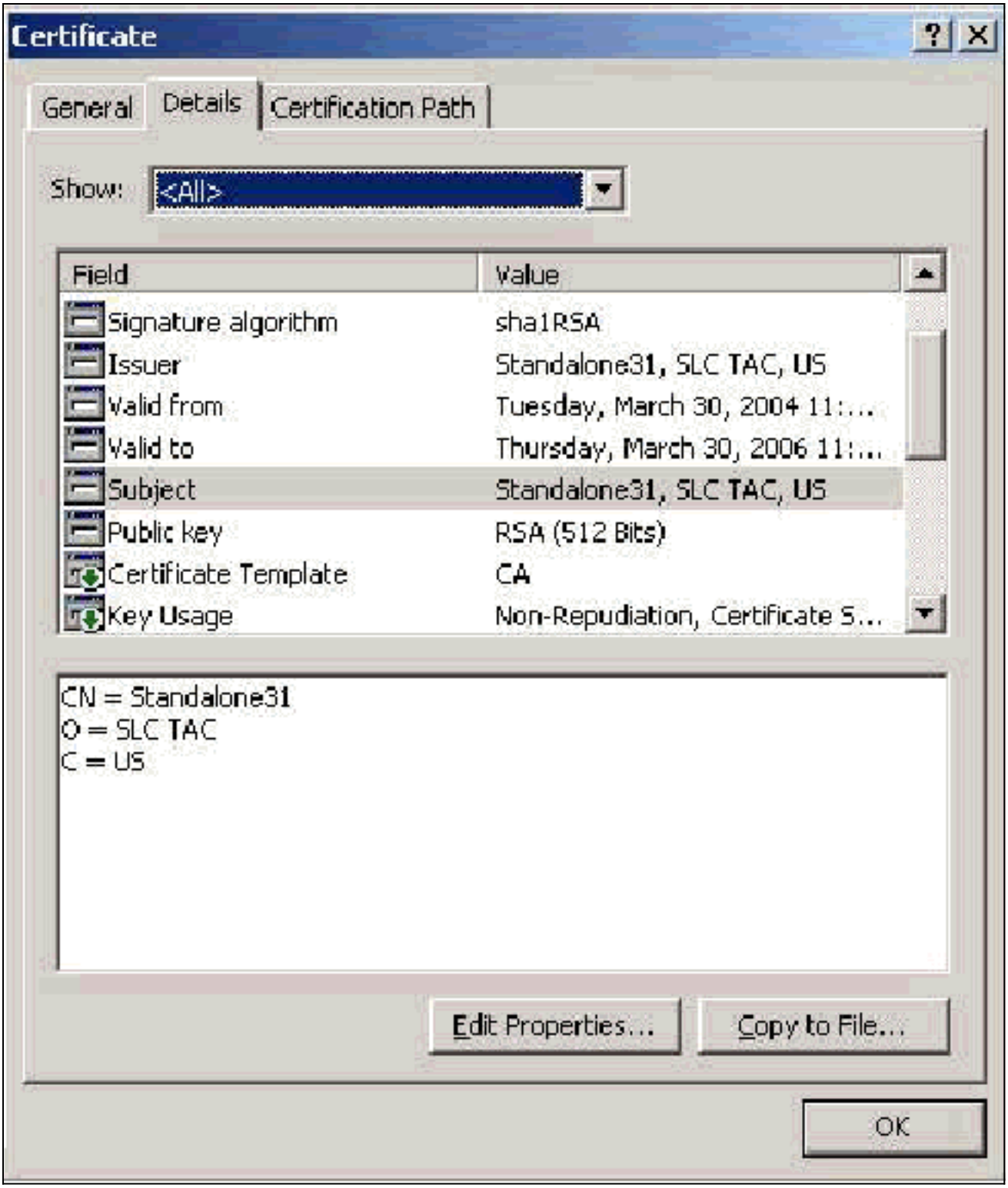
Certificados CA raiz

A única finalidade do certificado CA raiz é identificar o certificado do servidor (e o certificado CA intermediário, se aplicável) como um certificado confiável para o ACS e para o suplicante do Windows EAP-MSCHAPv2. Ele deve estar localizado no repositório das Autoridades de Certificação de Raiz Confiáveis no Windows no servidor ACS e, no caso do EAP-MSCHAPv2, no computador cliente. A maioria dos certificados CA raiz de terceiros está instalada com o Windows e há pouco esforço envolvido com isso. Se o Microsoft Certificate Services for usado e o servidor de certificado estiver na mesma máquina que o ACS, o certificado CA raiz será instalado automaticamente. Se o certificado CA raiz não for encontrado no arquivo de Autoridades de Certificação de Raiz Confiáveis no Windows, ele deverá ser adquirido da AC e instalado. Quando instalado corretamente no arquivo de certificados do Windows, o certificado CA raiz precisa aparecer na pasta **Certificados (Computador local) > Autoridades de certificação raiz confiáveis > Certificados** conforme visto nesta janela de exemplo.



Campos do assunto e do emissor

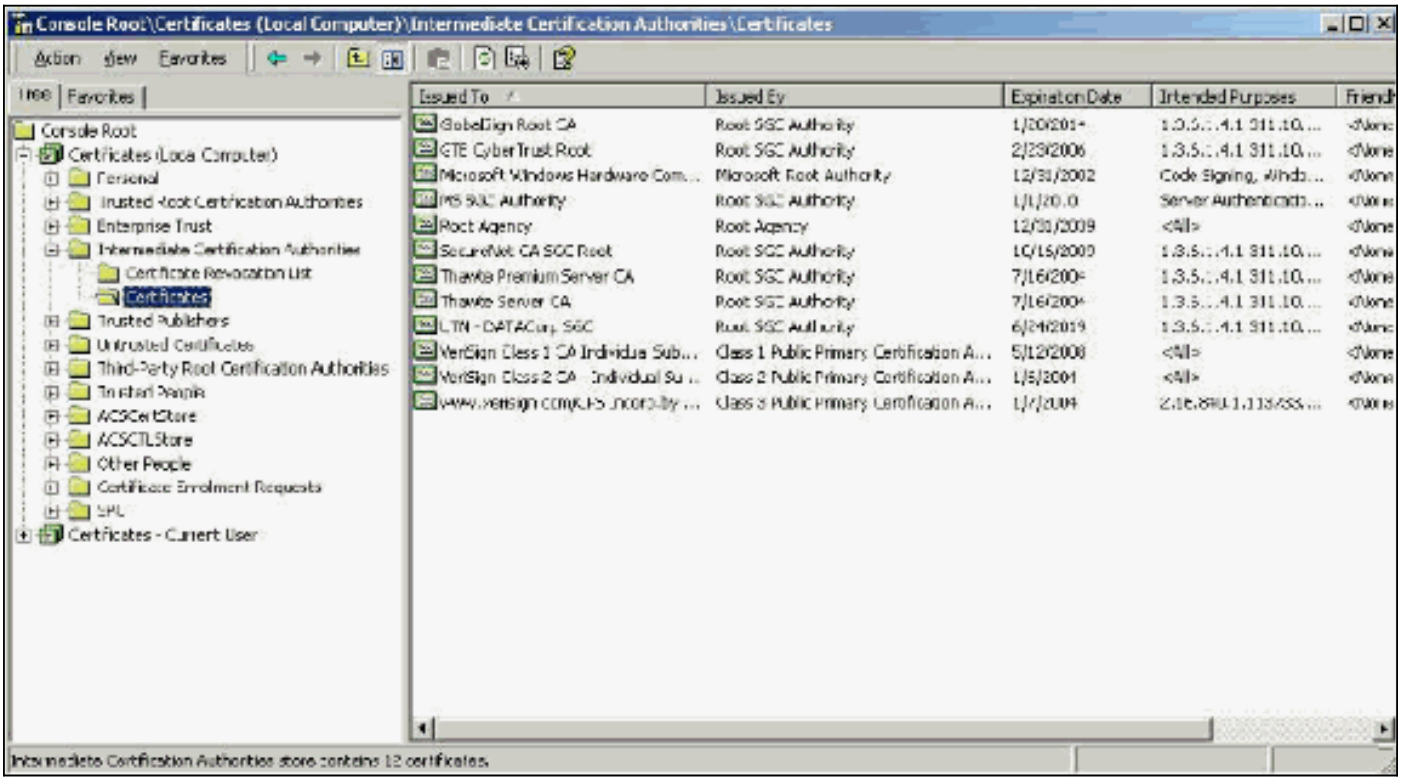
Os campos Assunto e Emitente identificam a CA e precisam ser exatamente os mesmos. Use esses campos para preencher os campos Emitido e Emitido por na guia Geral do certificado. Eles são preenchidos com o nome da CA raiz.



Certificados CA intermediários

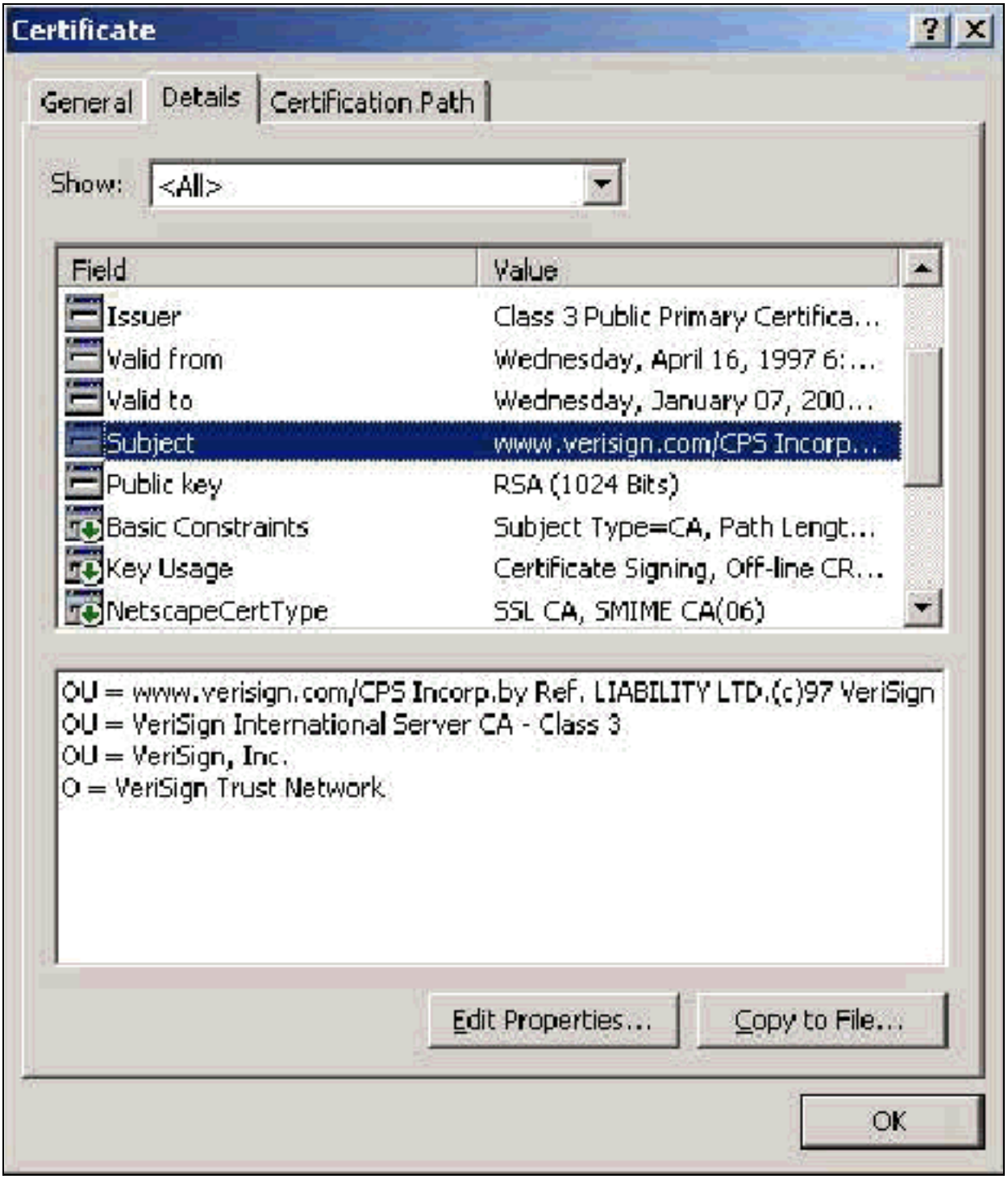
Certificados CA intermediários são certificados que você usa para identificar uma CA subordinada a uma CA raiz. Alguns certificados de servidor (certificados sem fio da Verisign) são criados com o uso de uma CA intermediária. Se for usado um certificado de servidor cortado por uma CA intermediária, o certificado CA intermediário deve ser instalado na área Autoridades de certificação intermediárias do armazenamento de máquina local no servidor ACS. Além disso, se o suplicante EAP da Microsoft for usado no cliente, o Certificado CA raiz da CA raiz que criou o Certificado CA intermediário também deverá estar no armazenamento apropriado no servidor ACS e no cliente para que a cadeia de confiança possa ser estabelecida. O certificado CA raiz e o certificado CA intermediário devem ser marcados como confiáveis no ACS e no cliente. A maioria

dos certificados CA intermediários não está instalada com o Windows, por isso é muito provável que você precise adquiri-los do fornecedor. Quando instalado corretamente no arquivo de certificados do Windows, o Certificado de CA intermediário aparece na pasta **Certificados (Computador local) > Autoridades de certificação intermediárias > Certificados**, como visto nesta janela de exemplo.



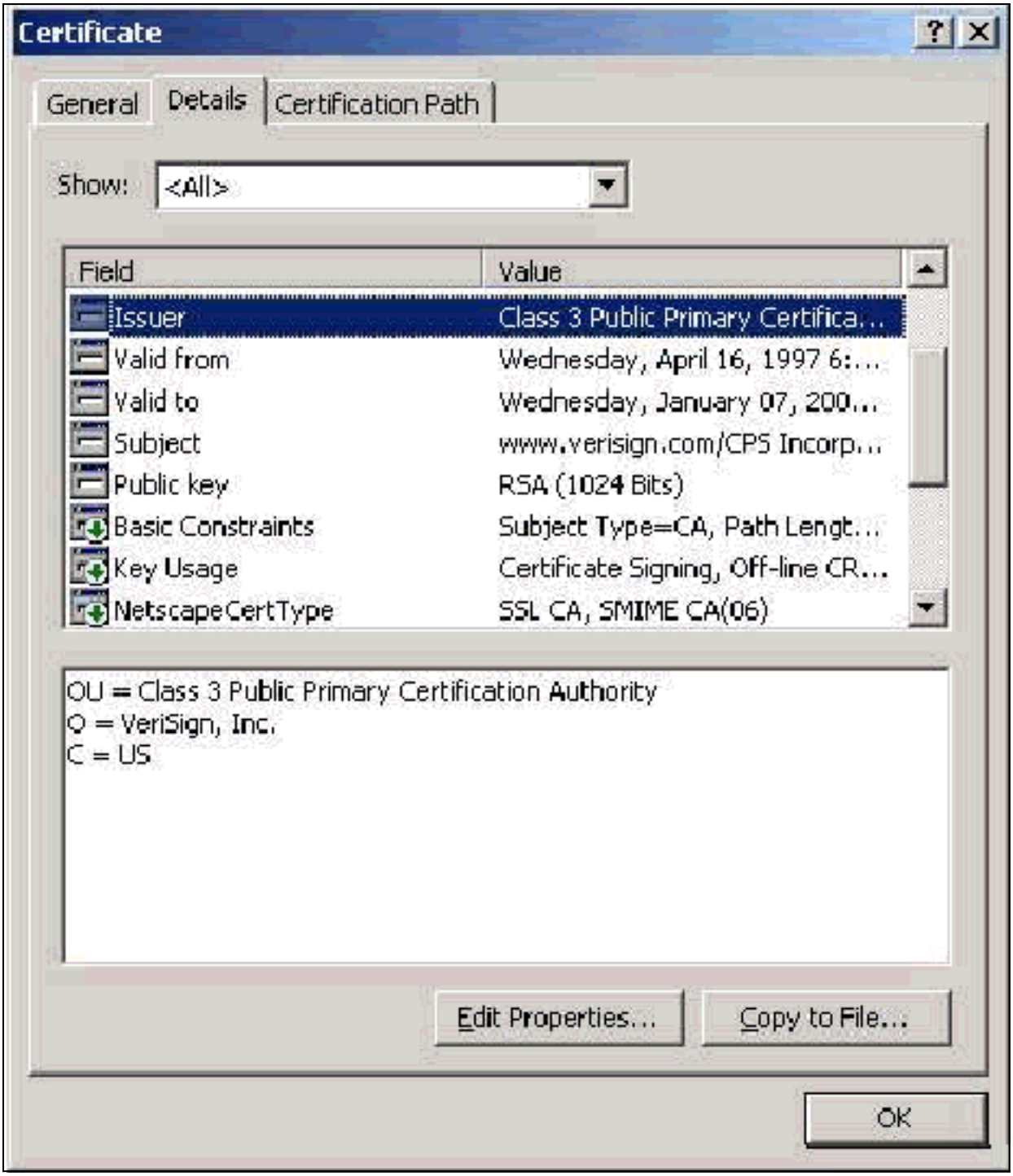
Campo de assunto

O campo Assunto identifica a CA intermediária. Esse valor é usado para determinar o campo Emitido para na guia Geral do certificado.



Campo do emissor

O campo Emitente identifica a CA que cortou o certificado. Use esse valor para determinar o valor do campo Emitido por na guia Geral do certificado. Ele é preenchido com o nome da CA.



Certificados de cliente

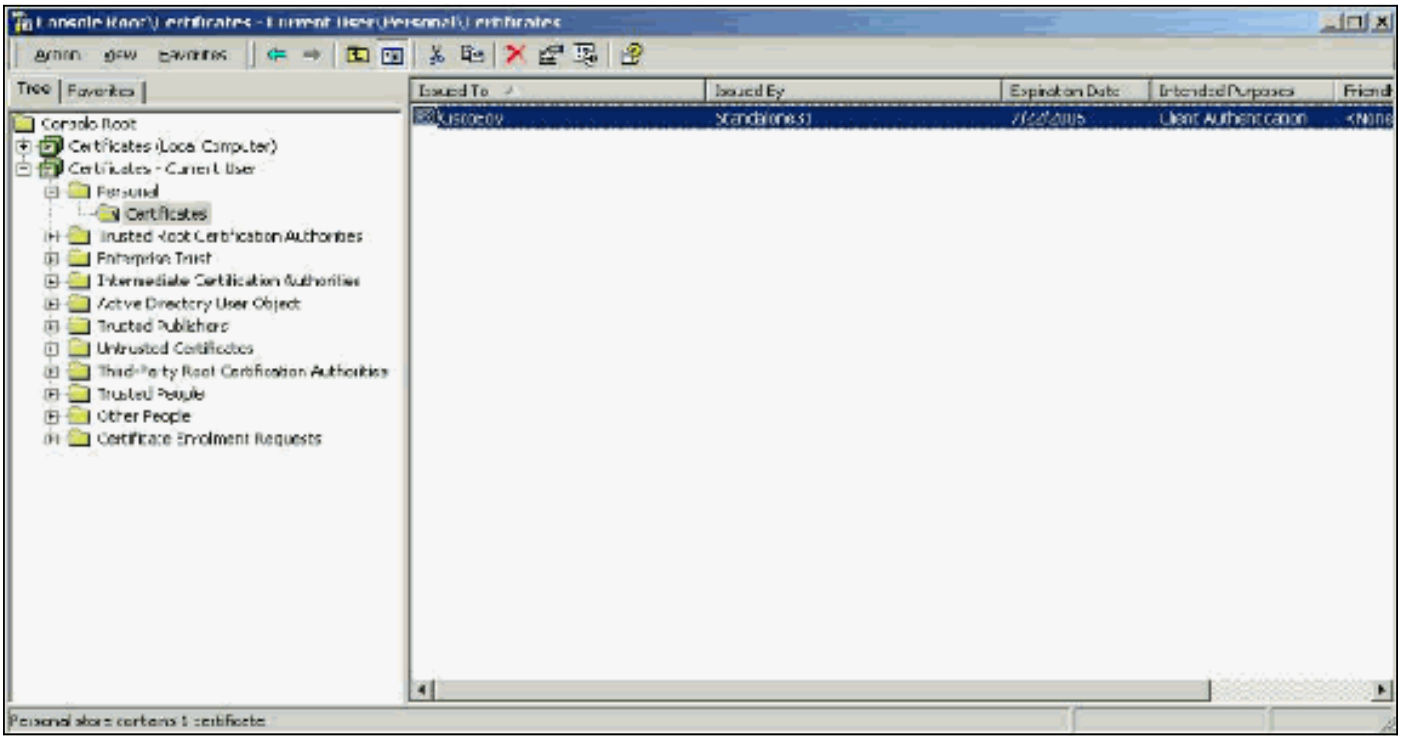
Os certificados do cliente são usados para identificar positivamente o usuário no EAP-TLS. Eles não têm nenhuma função na construção do túnel TLS e não são usados para criptografia. A identificação positiva é realizada por um de três meios:

- **CN (ou Name)Comparison** — Compara o CN no certificado com o nome de usuário no banco de dados. Mais informações sobre esse tipo de comparação estão incluídas na descrição do campo Assunto do certificado.
- **Comparação de SAN** — Compara a SAN no certificado com o nome de usuário no banco de dados. Isso só é suportado a partir do ACS 3.2. Mais informações sobre esse tipo de comparação estão incluídas na descrição do campo Nome alternativo do assunto do certificado.

- **Comparação binária** —Compara o certificado com uma cópia binária do certificado armazenado no banco de dados (somente AD e LDAP podem fazer isso). Se você usar a comparação binária de certificado, deverá armazenar o certificado de usuário em um formato binário. Além disso, para LDAP genérico e Ative Diretory, o atributo que armazena o certificado deve ser o atributo LDAP padrão chamado "usercertificate".

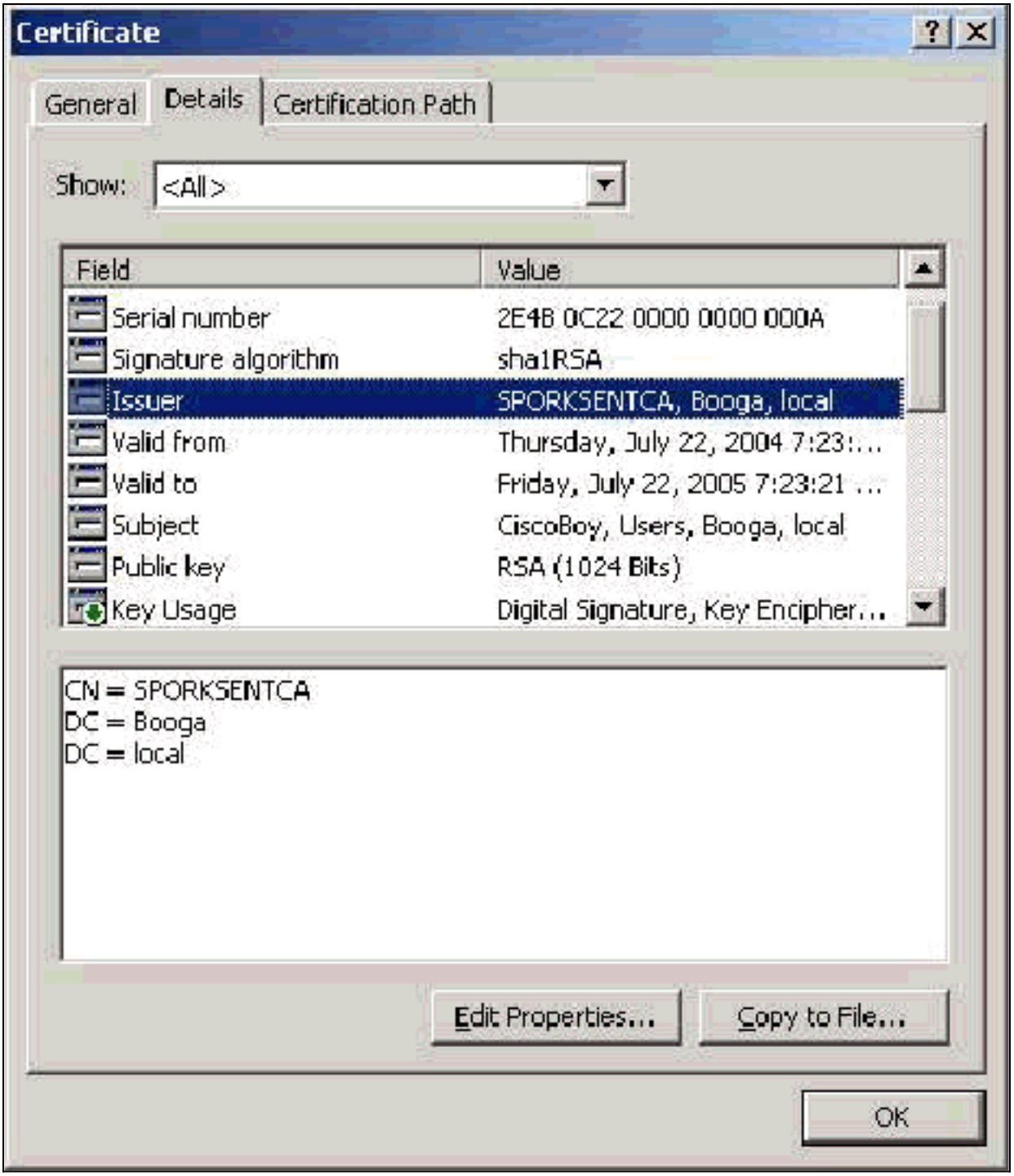
Seja qual for o método de comparação usado, as informações no campo apropriado (CN ou SAN) devem corresponder ao nome que seu banco de dados usa para autenticação. O AD usa o nome do NetBios para autenticação em modo misto e o UPN em modo nativo.

Esta seção discute a geração de certificado do cliente com o uso dos Serviços de certificado da Microsoft. O EAP-TLS requer um certificado de cliente exclusivo para que cada usuário seja autenticado. O certificado deve ser instalado em cada computador para cada usuário. Quando instalado corretamente, o certificado está localizado na pasta **Certificados - Usuário Atual > Pessoal > Certificados**, conforme visto nesta janela de exemplo.



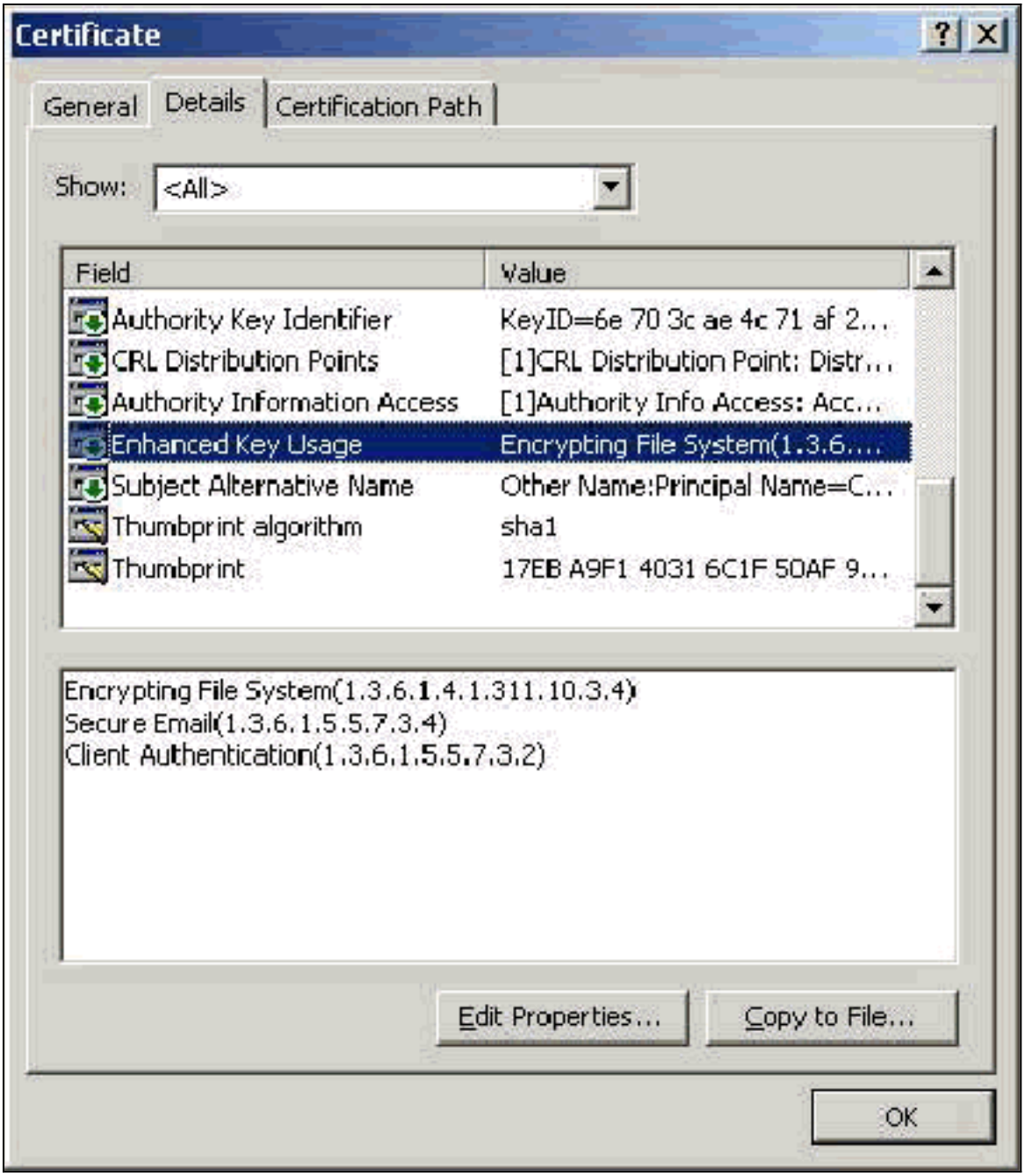
Campo do emissor

O campo Emitente identifica a CA que corta o certificado. Use esse valor para determinar o valor do campo Emitido por na guia Geral do certificado. Isso é preenchido com o nome da CA.



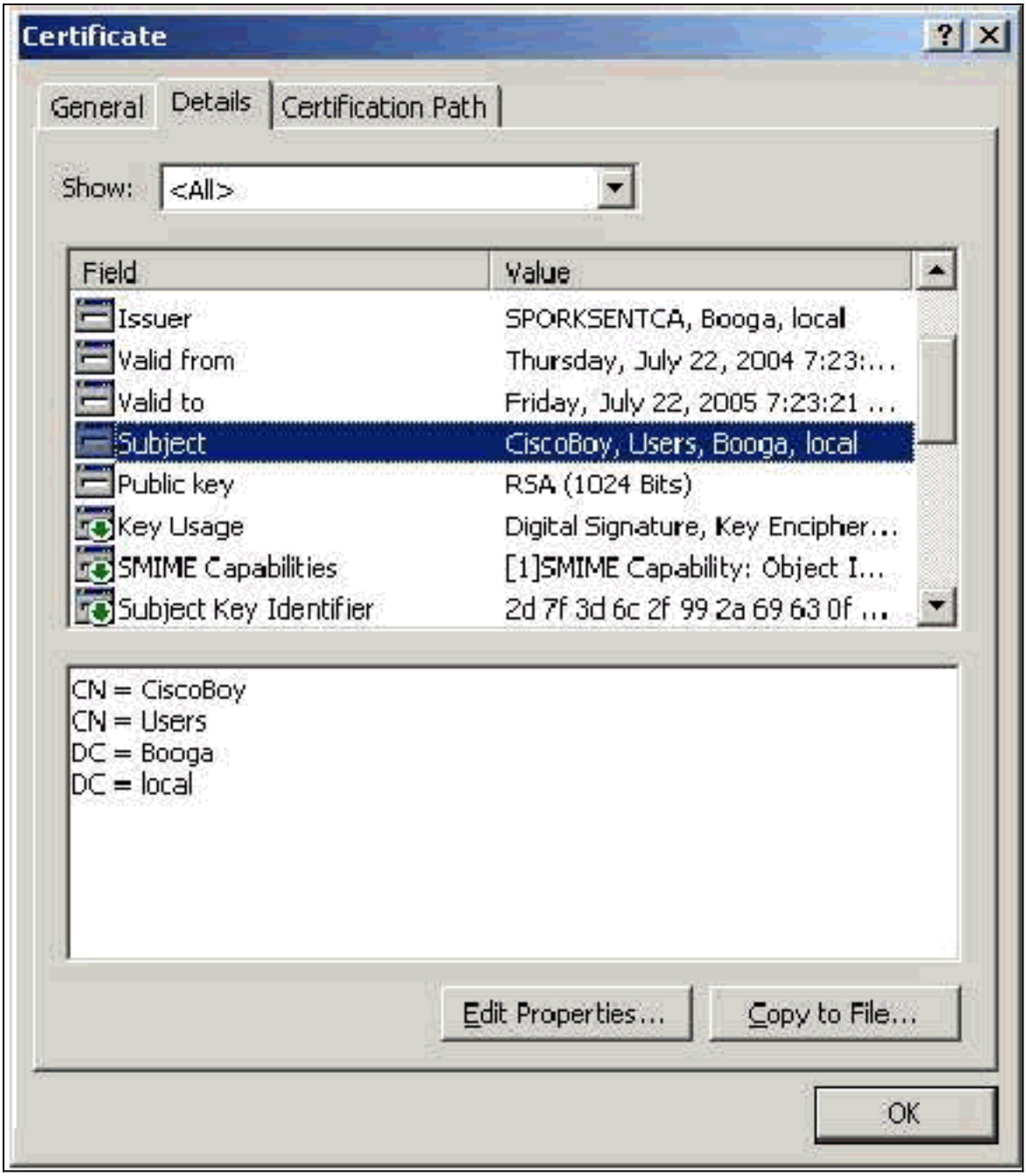
Campo de uso de chave aprimorado

O campo Enhanced Key Usage identifica a finalidade do certificado e precisa conter a autenticação do cliente. Este campo é obrigatório quando você usa o suplicante da Microsoft para PEAP e EAP-TLS. Quando você usa o Microsoft Certificate Services, ele é configurado na CA independente quando você seleciona **Certificado de Autenticação de Cliente** no menu suspenso Finalidade pretendida e na CA corporativa quando você seleciona **Usuário** no menu suspenso Modelo de Certificado. Se você solicitar um certificado com o uso de um CSR com o Microsoft Certificate Services, não terá a opção de especificar a Finalidade com a CA independente. Portanto, o campo EKU está ausente. Com a CA corporativa, você tem o menu suspenso Finalidade. Algumas CAs não criam certificados com um campo EKU. Eles são inúteis quando você usa o suplicante EAP da Microsoft.



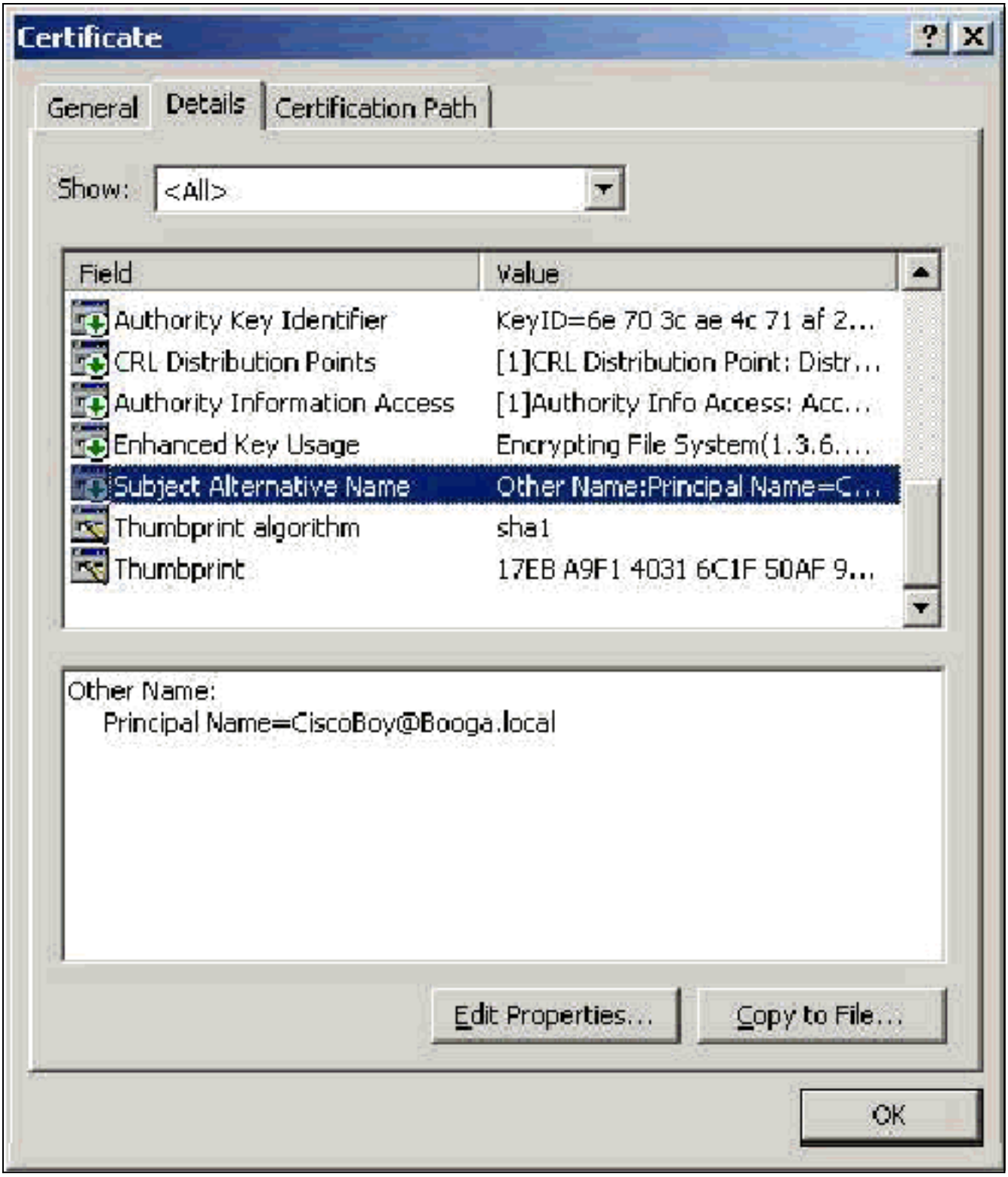
Campo de assunto

Este campo é usado na comparação da NC. O primeiro CN listado é comparado ao banco de dados para encontrar uma correspondência. Se uma correspondência for encontrada, a autenticação será bem-sucedida. Se você usar uma CA independente, a CN será preenchida com o que você colocar no campo Nome no formulário de envio do certificado. Se você usar a CA corporativa, a CN será preenchida automaticamente com o nome da conta conforme listado no console Usuários e Computadores do Ative Diretory (isso não corresponde necessariamente ao UPN ou ao nome do NetBios).



Campo de nome alternativo do assunto

O campo Nome alternativo do assunto é usado na comparação da SAN. A SAN listada é comparada ao banco de dados para encontrar uma correspondência. Se uma correspondência for encontrada, a autenticação será bem-sucedida. Se você usar a CA corporativa, a SAN será preenchida automaticamente com o nome de logon @domain (UPN) do Ative Diretory. A CA autônoma não inclui um campo SAN, por isso não é possível utilizar a comparação da SAN.



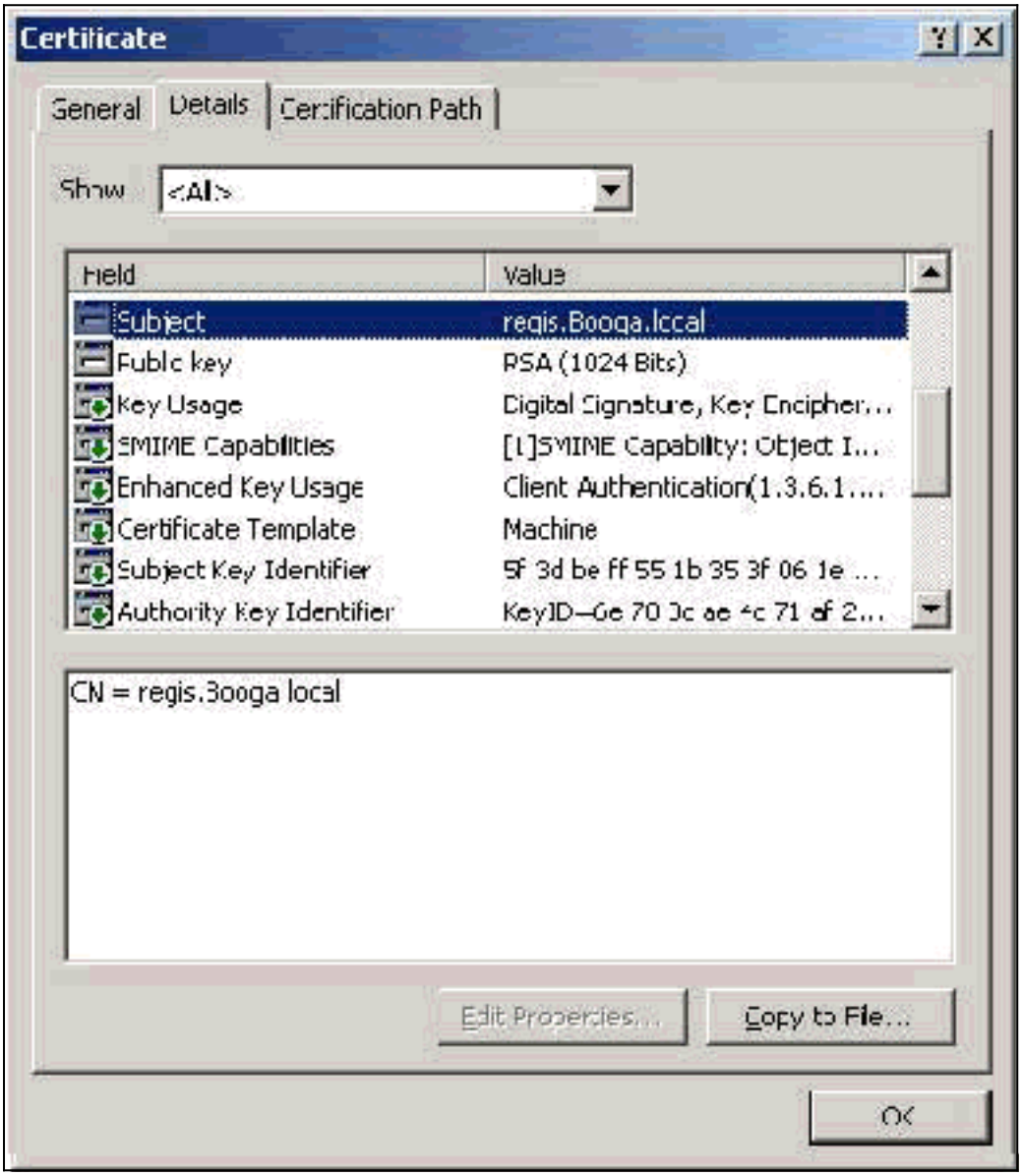
Certificados de máquina

Os certificados de máquina são usados em EAP-TLS para identificar positivamente o computador quando você usa a autenticação da máquina. Você só pode acessar esses certificados quando configura sua AC do Microsoft Enterprise para inscrição automática de certificado e ingressa no computador no domínio. O certificado é criado automaticamente quando você usa as credenciais do Ative Diretory do computador e as instala no armazenamento local do computador. Os computadores que já são membros do domínio antes de você configurar a inscrição automática receberão um certificado na próxima vez que o Windows for reiniciado. O Certificado da Máquina é instalado na **pasta Certificados (Computador Local) > Pessoal > Certificados** do snap-in MMC Certificados (Computador Local) da mesma forma que Certificados de Servidor. Não é possível

instalar esses certificados em nenhuma outra máquina, pois não é possível exportar a chave privada.

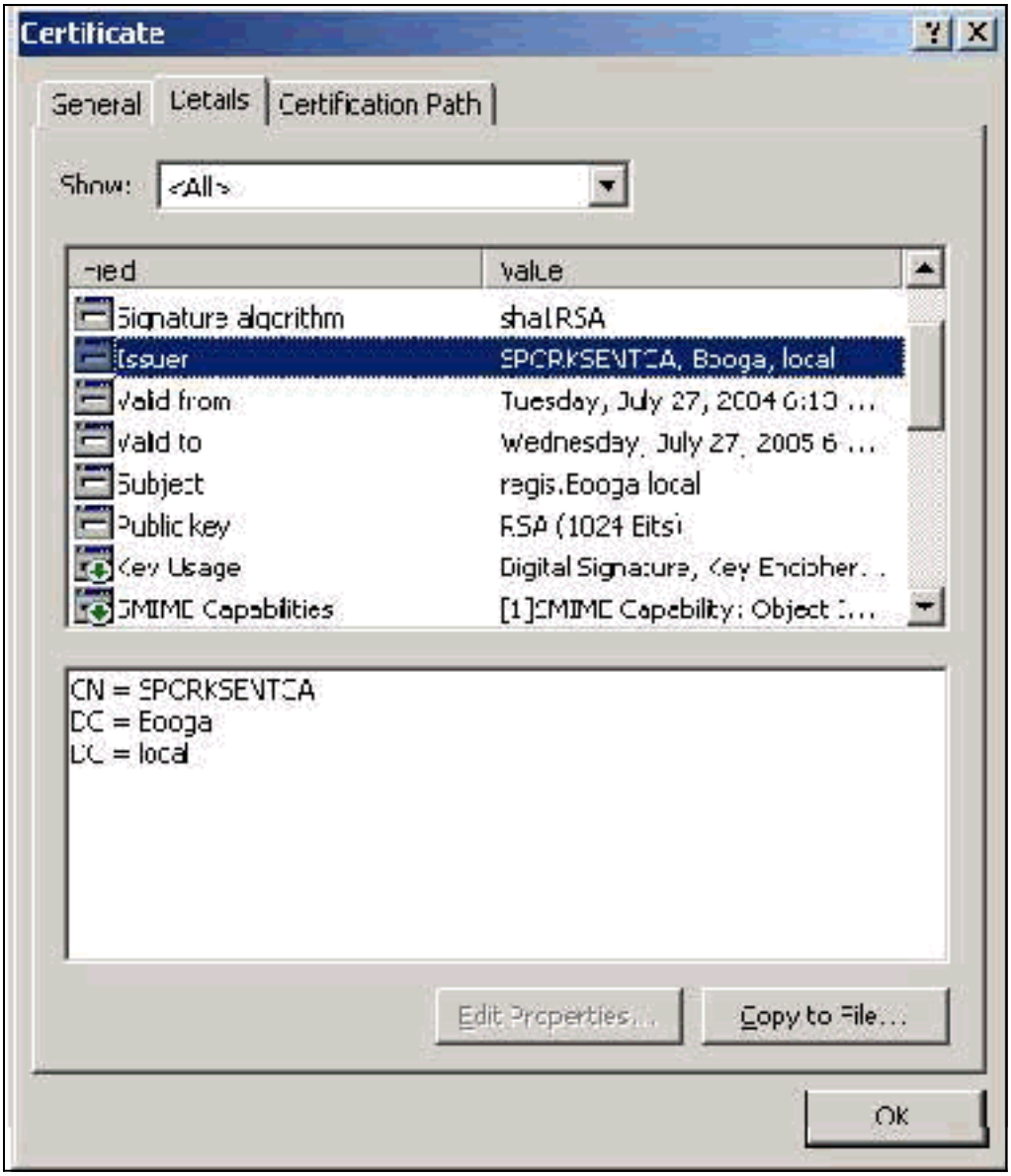
Campos de assunto e SAN

Os campos Assunto e SAN identificam o computador. O valor é preenchido pelo nome totalmente qualificado do computador e é usado para determinar o campo Emitido para na guia Geral do certificado e é o mesmo para os campos Assunto e SAN.



Campo do emissor

O campo Emitente identifica a CA que cortou o certificado. Use esse valor para determinar o valor do campo Emitido por na guia Geral do certificado. Ele é preenchido com o nome da CA.



Apêndice A - Extensões de certificado comuns

.csr — Na verdade, não é um certificado, mas sim uma solicitação de assinatura de certificado. É um arquivo de texto simples com este formato:

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

.pvk — Esta extensão denota uma chave privada, embora a extensão não garanta que o conteúdo é realmente uma chave privada. O conteúdo precisa ser um texto simples com 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 — Este é um ramal genérico que denota um certificado. Os certificados de servidor, CA raiz e CA intermediário podem estar neste formato. Geralmente, é um arquivo de texto simples com uma extensão que pode ser alterada conforme necessário e pode ser do formato DER ou Base 64. Você pode importar esse formato para o repositório de certificados do Windows.

.pem — Esta extensão significa Privacy Enhanced Mail. Essa extensão é comumente usada com UNIX, Linux, BSD e assim por diante. Geralmente, é usado para certificados de servidor e chaves privadas, e geralmente é um arquivo de texto simples com uma extensão que você pode alterar conforme necessário de .pem para .cer para que você possa importá-lo para o repositório de certificados do Windows.

O conteúdo interno dos arquivos .cer e .pem geralmente se parece com esta saída:

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

.pfx — Esta extensão significa Personal Information Exchange (Intercâmbio de informações pessoais). Esse formato é um método que você pode usar para agrupar certificados em um único arquivo. Por exemplo, você pode agrupar um certificado de servidor e sua chave privada associada e certificado CA raiz em um arquivo e importar facilmente o arquivo para o repositório de certificados do Windows apropriado. É mais comumente usado para certificados de servidor e cliente. Infelizmente, se um certificado CA raiz for incluído, o certificado CA raiz será sempre instalado no repositório do usuário atual em vez do repositório do computador local, mesmo que o repositório do computador local seja especificado para instalação.

.p12 —Geralmente, esse formato é visto apenas com um certificado do cliente. Você pode importar esse formato para o repositório de certificados do Windows.

.p7b — Este é outro formato que armazena vários certificados em um arquivo. Você pode importar esse formato para o repositório de certificados do Windows.

Apêndice B - Conversão do formato do certificado

Na maioria dos casos, a conversão de certificado ocorre quando você altera o ramal (por exemplo, de .pem para .cer), pois os certificados geralmente estão em formato de texto simples. Às vezes, um certificado não está no formato de texto simples e você deve convertê-lo com o uso

de uma ferramenta como OpenSSL . Por exemplo, o Mecanismo de Solução ACS não pode instalar certificados no formato .pfx. Portanto, você deve converter o certificado e a chave privada em um formato utilizável. Esta é a sintaxe básica do comando OpenSSL:

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

Você será solicitado a inserir a senha de importação e a senha PEM. Essas senhas precisam ser iguais e são a senha de chave privada especificada quando o .pfx é exportado. A saída é um único arquivo .pem que estão incluídos todos os certificados e chaves privadas no .pfx. Esse arquivo pode ser chamado no ACS como o certificado e o arquivo de chave privada e é instalado sem problemas.

Apêndice C - Período de validade do certificado

Um certificado só pode ser usado durante o período de validade. O período de validade de um certificado CA raiz é determinado quando a CA raiz é estabelecida e pode variar. O período de validade de um certificado CA intermediário é determinado quando a CA é estabelecida e não pode exceder o período de validade da CA raiz à qual está subordinada. O período de validade dos certificados de servidor, cliente e máquina é automaticamente definido para um ano com o Microsoft Certificate Services. Isso só pode ser alterado quando você hackeia o registro do Windows de acordo com o artigo 254632 da Base de conhecimento Microsoft e não pode exceder o período de validade da CA raiz. O período de validade dos certificados autoassinados que o ACS gera é sempre de um ano e não pode ser alterado nas versões atuais.

Informações Relacionadas

- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems