EAP版本1.01证书指南

目录

简介

本文档澄清了与各种形式的可扩展身份验证协议(EAP)相关的各种证书类型、格式和要求所伴随的一些混淆。 本文档讨论的与EAP相关的五种证书类型是服务器、根CA、中间CA、客户端和计算机。这些证书以各种格式发现，并且根据涉及的EAP实施，与每个证书相关的要求可能不同。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

服务器证书

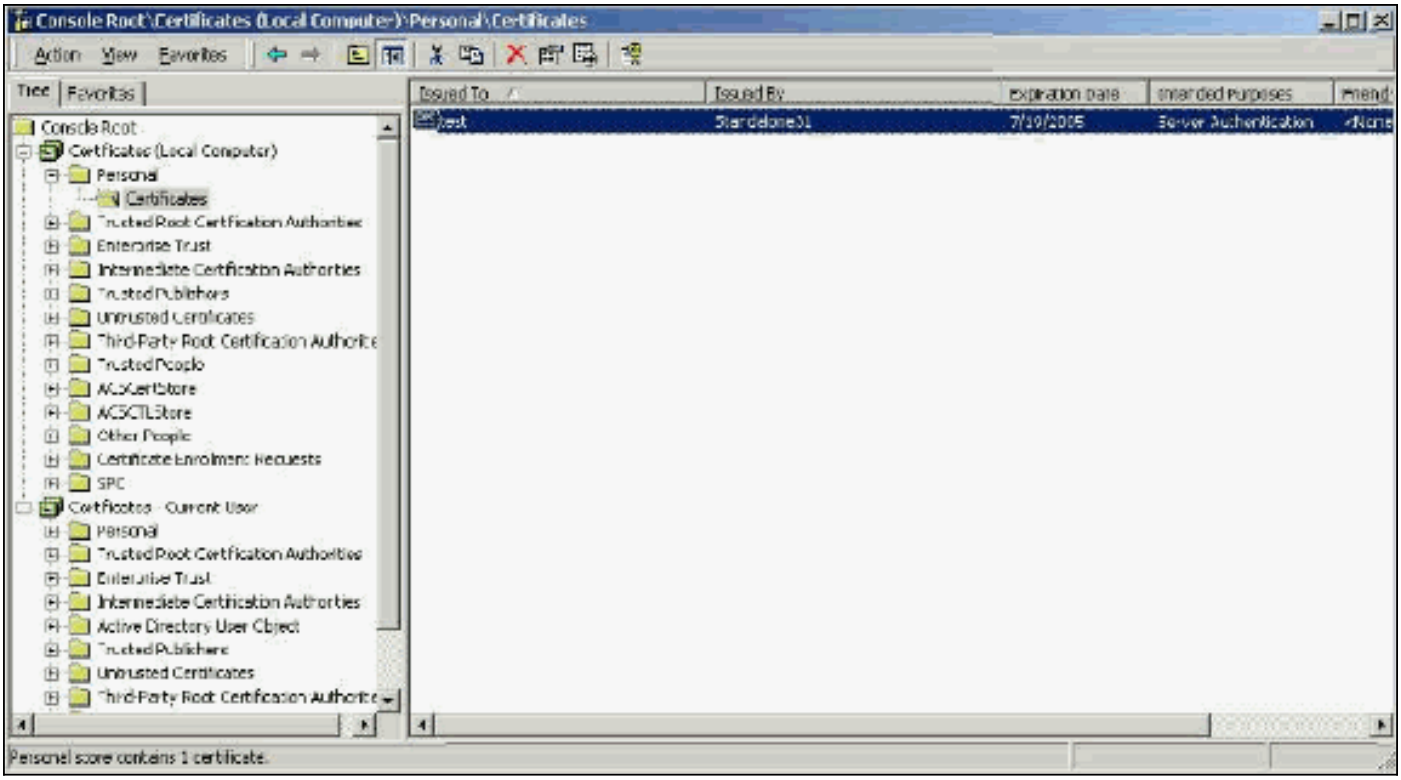
服务器证书安装在RADIUS服务器上，其在EAP中的主要用途是创建加密的传输层安全(TLS)隧道，以保护身份验证信息。使用EAP-MSCHAPv2时，服务器证书承担辅助角色，即将RADIUS服务器标识为身份验证的受信任实体。此辅助角色通过使用增强密钥使用(EKU)字段完成。EKU字段将证书标识为有效的服务器证书，并验证颁发证书的根CA是受信任的根CA。这要求存在根CA证书。Cisco Secure ACS要求证书采用Base64编码或DER编码的二进制X.509 v3格式。

您可以使用ACS中的证书签名请求(CSR)创建此证书，该请求会提交到CA。或者，您也可以使用内部CA（如Microsoft证书服务）证书创建表单剪切证书。请注意，虽然您可以创建密钥大小大于1024的服务器证书，但任何大于1024的密钥都不能与PEAP配合使用。即使身份验证通过，客户端也会挂起。

如果使用CSR创建证书，则使用.cer、.pem或.txt格式创建证书。在极少数情况下，创建时没有扩展。确保证书是带扩展名的纯文本文件，您可以根据需要进行更改（ACS设备使用.cer或.pem扩展名）。 此外，如果使用CSR，则证书的私钥会在您指定的路径中创建，该路径是可能具有扩展名或可能不具有扩展名且具有与其关联的密码（在ACS上安装时需要密码）的单独文件。 无论扩展名是什么，请确保它是具有可根据需要更改的扩展名的纯文本文件（ACS装置使用.pvk或.pem扩展名）。如果没有为私钥指定路径，则ACS会将密钥保存在C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs目录中，并在安装证书时，如果没有为私钥文件指定路径，则查看此目录。

如果证书是使用Microsoft Certificate Services证书提交表创建的，请确保将密钥标记为可导出，以便可以在ACS中安装证书。以这种方式创建证书可显着简化安装过程。您可以从证书服务Web界面直接将其安装到正确的Windows存储中，然后使用CN作为参考从存储中安装到ACS上。本地计算机存储中安装的证书也可以从Windows存储中导出并轻松安装在另一台计算机上。导出此类证书时，需要将密钥标记为可导出并指定密码。然后，证书以.pfx格式显示，包括私钥和服务器证书。

在Windows证书存储中正确安装后，服务器证书需要显示在“证书（本地计算机）”>“个人”>“证书”文件夹中，如本例窗口中所示。

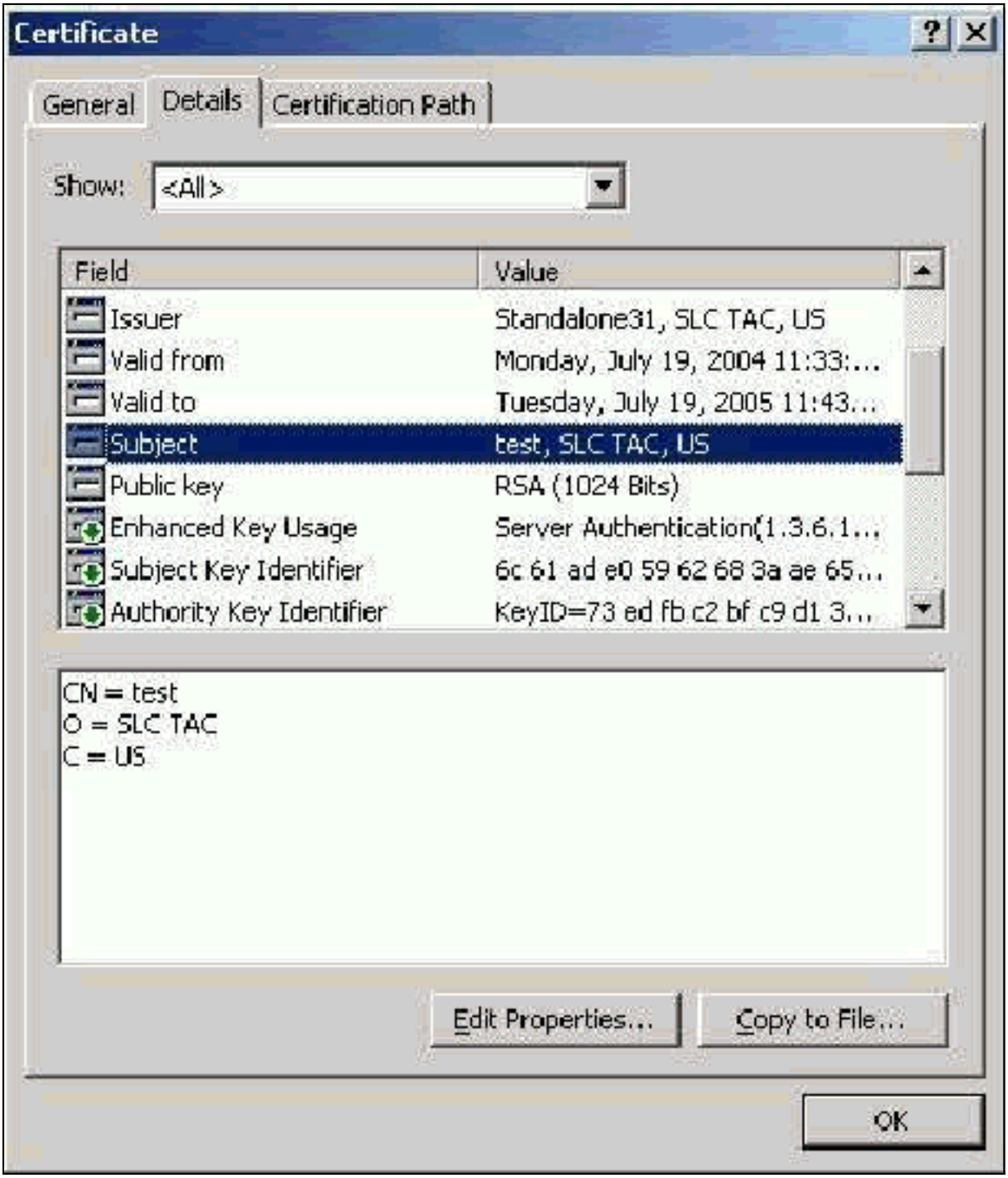


自签名证书是您创建的证书，无需CA的根或中间参与。它们在主题和颁发者字段（如根CA证书）中具有相同的值。大多数自签名证书使用X.509 v1格式。因此，它们不能与ACS配合使用。但是，从版本3.3开始，ACS能够创建自己的自签名证书，您可以将其用于EAP-TLS和PEAP。请勿使用大于1024的密钥大小与PEAP和EAP-TLS兼容。如果使用自签名证书，则证书也以根CA证书的容量运行，并且在使用Microsoft EAP请求方时必须安装在客户端的**Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates**文件夹中。它会自动安装在服务器上的受信任根证书存储区中。但是，它仍必须在ACS Certificate Setup的Certificate Trust List（证书信任列表）中受信任。有关详细信息，请参阅根CA证书部分。

由于使用Microsoft EAP请求方时，自签名证书用作服务器证书验证的根CA证书，并且由于有效期不能从默认的一年延长，因此Cisco建议您仅将其用作EAP作为临时措施，直到您可以使用传统CA。

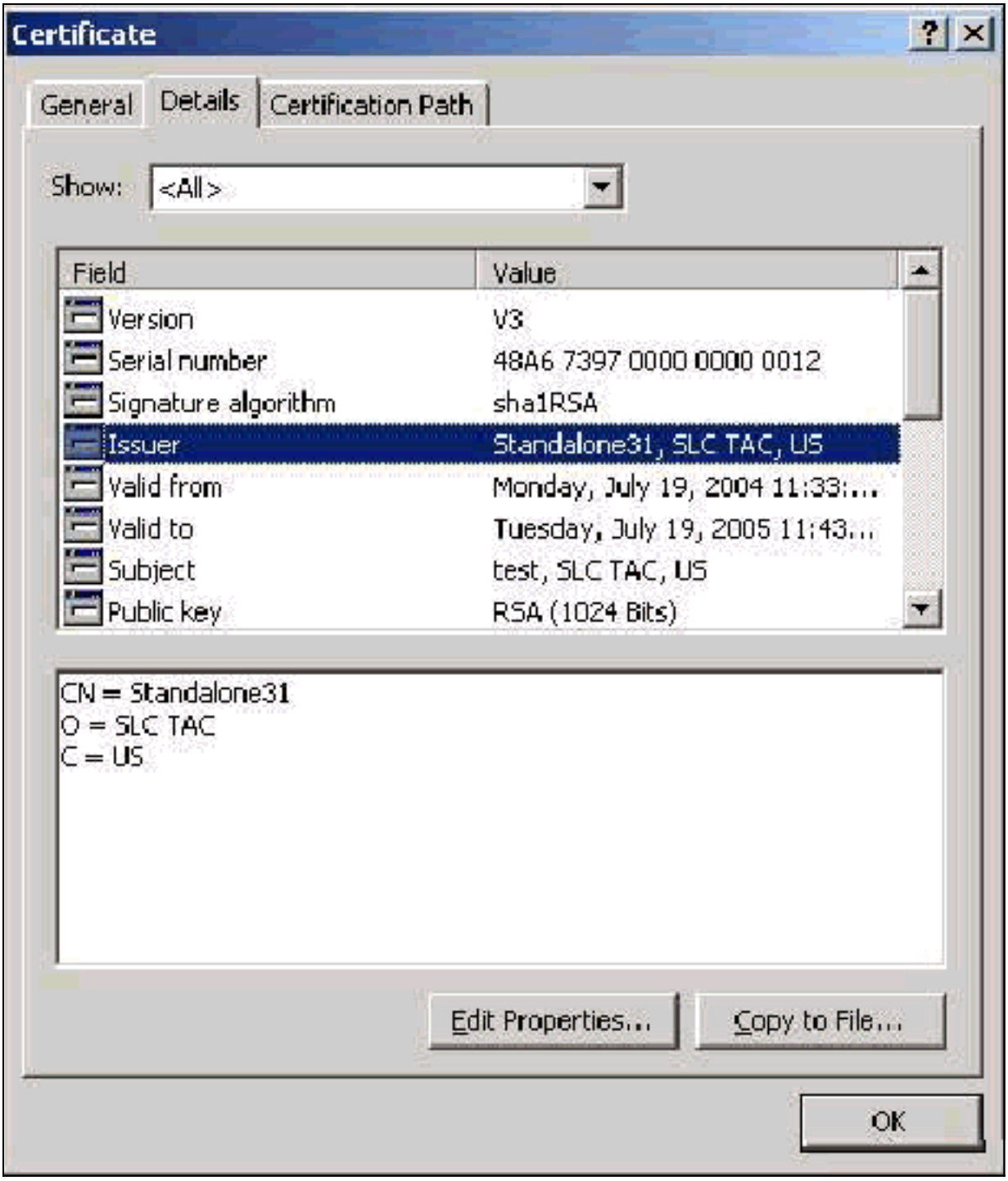
主题字段

Subject字段标识证书。CN值用于确定证书“常规”(General)选项卡中的“颁发给”(Issued to)字段，并填充您在ACS“CSR”(CSR)对话框的“证书主题”(Certificate subject)字段中输入的信息，或Microsoft Certificate Services中“名称”(Name)字段的信息。CN值用于告诉ACS，如果使用从存储安装证书的选项，它需要从本地计算机证书存储区使用什么证书。



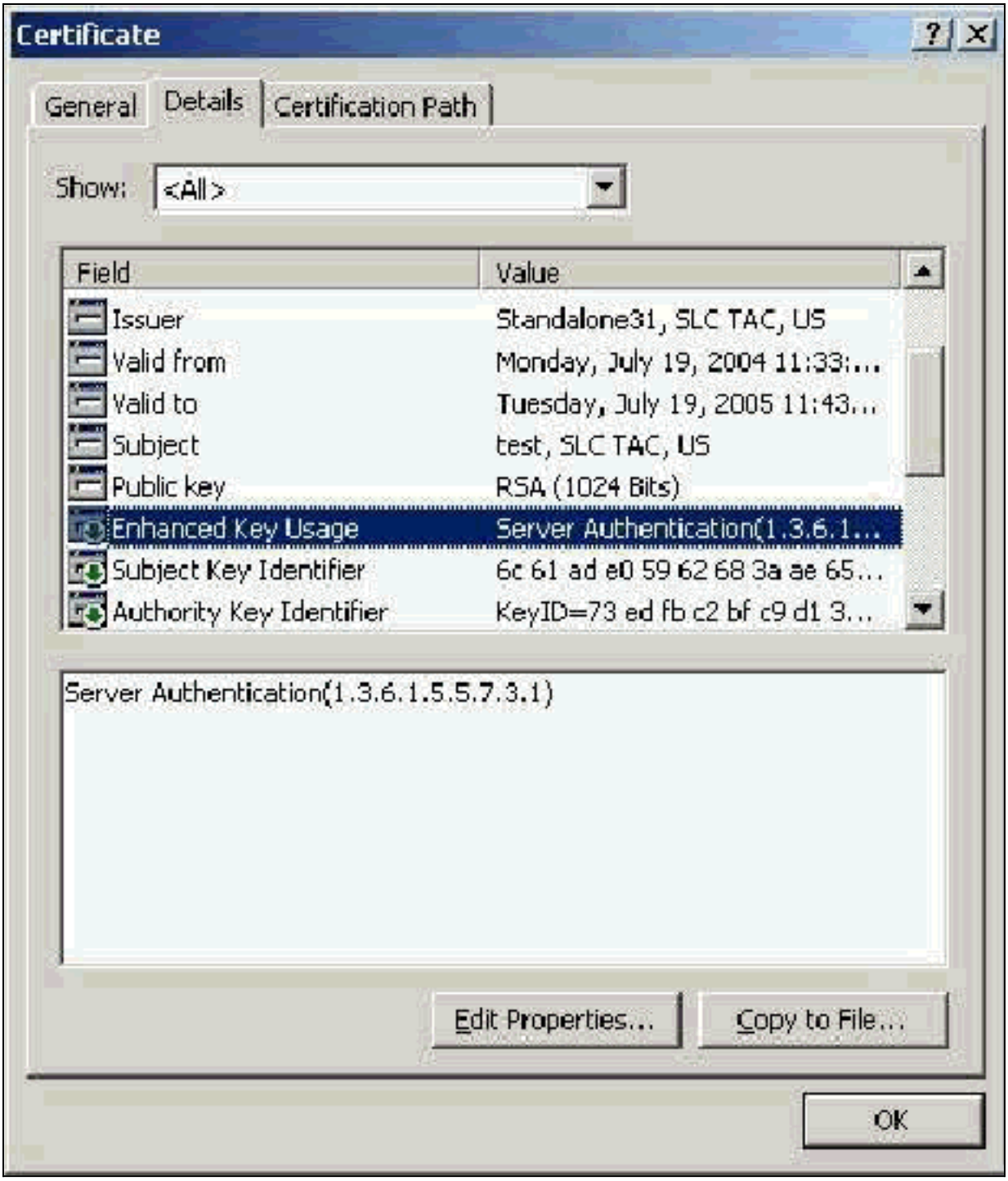
颁发者字段

颁发者字段标识剪切证书的CA。使用此值可确定证书“常规”(General)选项卡中“颁发者”(Issued by)字段的值。它填充了CA的名称。



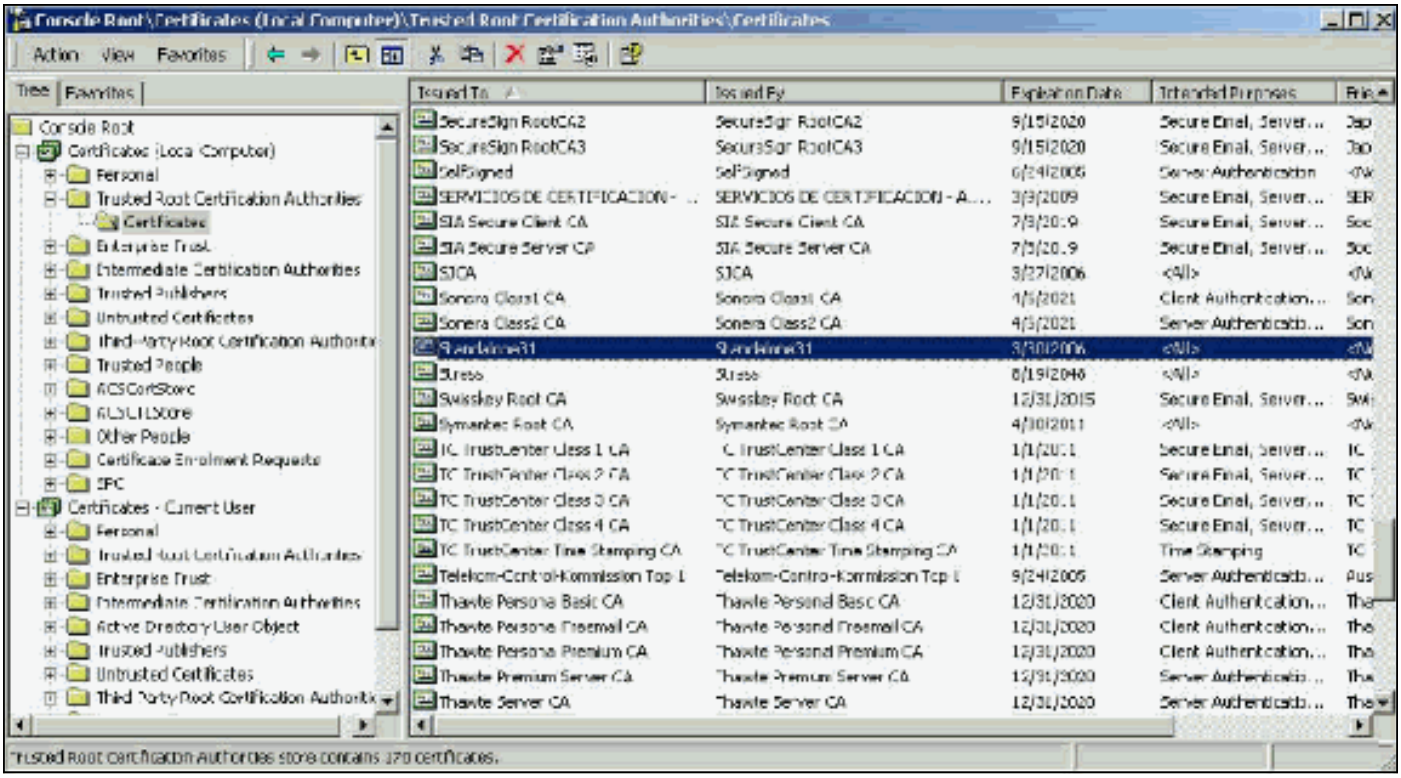
增强的密钥使用字段

“增强的密钥使用”(Enhanced Key Usage)字段标识证书的预期用途，需要列为“服务器身份验证”(Server Authentication)。 当您将Microsoft请求方用于PEAP和EAP-TLS时，此字段为必填字段。使用Microsoft证书服务时，在独立CA中配置此选项，从“目标用途”下拉菜单中选择**Server Authentication Certificate**，在企业CA中配置此选项，从“证书模板”下拉菜单中选择**Web Server**。如果您使用CSR和Microsoft证书服务请求证书，则您不能选择使用独立CA指定目标用途。因此，EKU字段不存在。使用企业CA，您将看到目标用途下拉列表。某些CA不使用EKU字段创建证书，因此在您使用Microsoft EAP请求方时，这些证书是无用的。



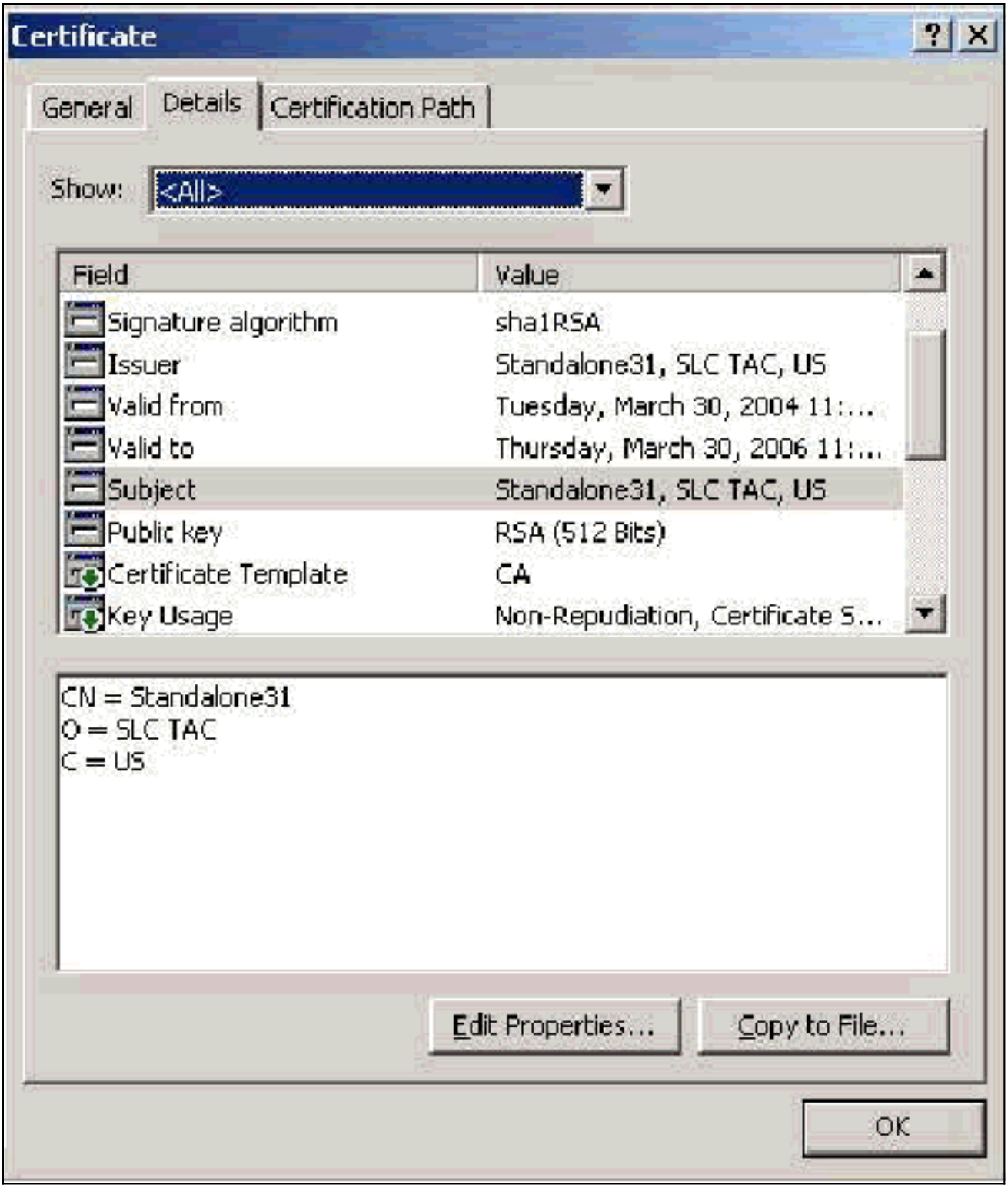
根CA证书

根CA证书的一个用途是将服务器证书(和中间CA证书（如果适用）)标识为ACS和Windows EAP-MSCHAPv2请求方的受信任证书。它必须位于ACS服务器上Windows中的受信任根证书颁发机构存储中，如果是EAP-MSCHAPv2，则位于客户端计算机上。大多数第三方根CA证书都安装在Windows中，而且几乎不用做任何工作。如果使用Microsoft证书服务，且证书服务器与ACS位于同一台计算机上，则会自动安装根CA证书。如果在Windows中的受信任根证书颁发机构存储中未找到根CA证书，则必须从CA获取并安装该证书。在Windows证书存储中正确安装后，根CA证书需要显示在**Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates文件夹中，如本示例窗口**所示。



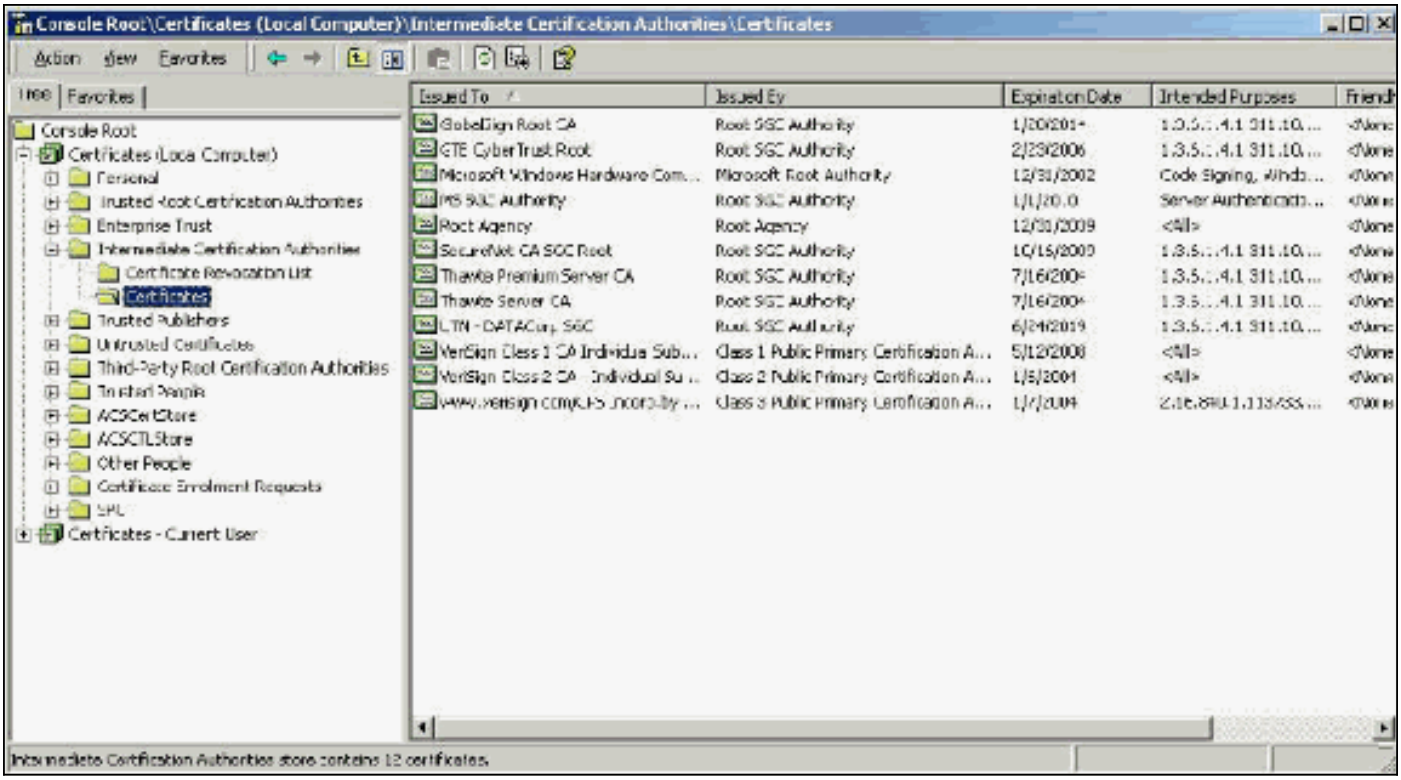
主题和颁发者字段

“主题”(Subject)和“颁发者”(Issuer)字段标识CA，并且需要完全相同。使用这些字段填充证书“常规”(General)选项卡中的“颁发给”(Issued to)和“颁发者”(Issued by)字段。它们填充了根CA的名称。



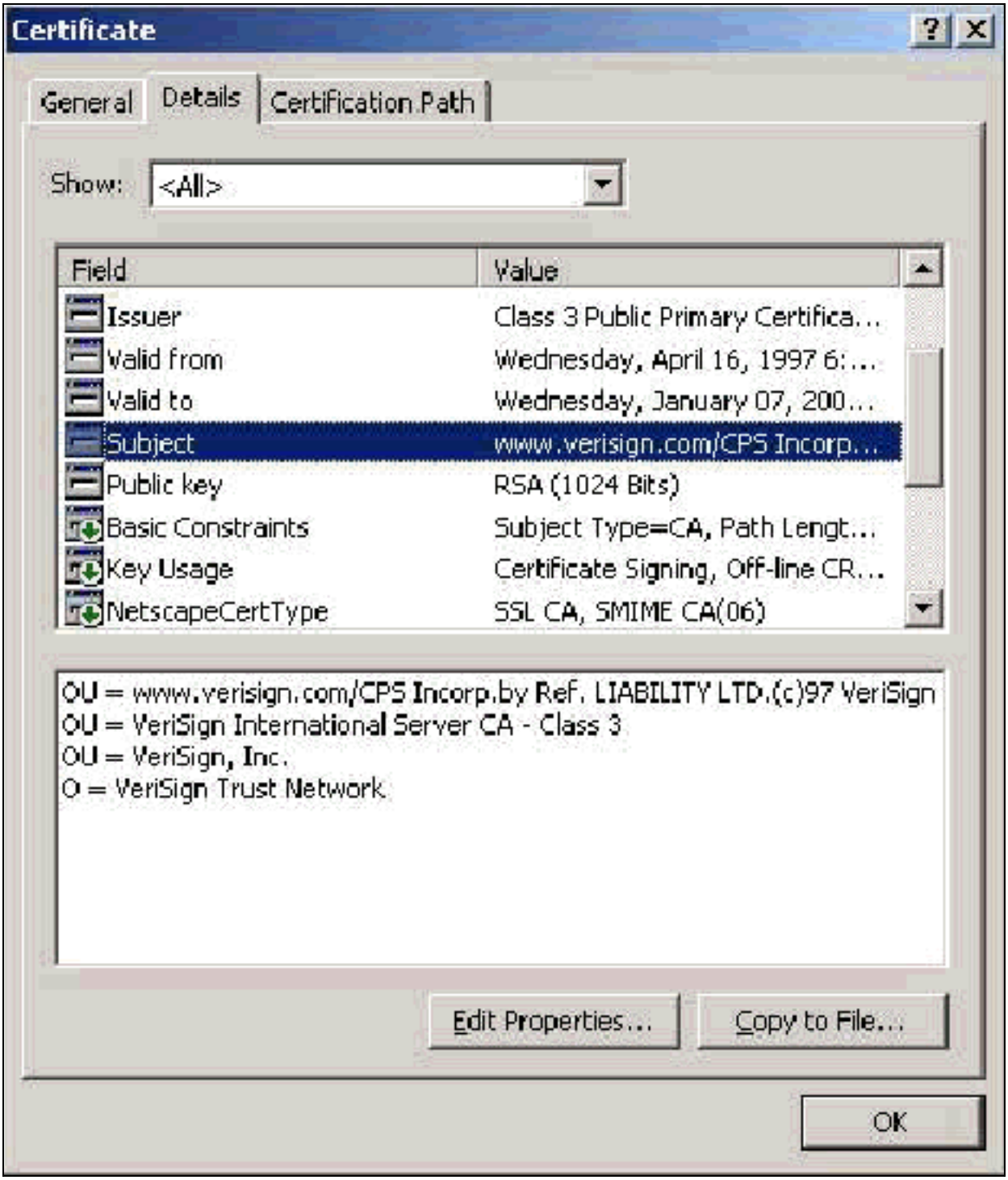
中间CA证书

中间CA证书是用于标识从属于根CA的CA的证书。使用中间CA创建某些服务器证书（Verisign的无线证书）。如果使用由中间CA剪切的服务器证书，则必须在ACS服务器上本地计算机存储的中间证书颁发机构区域中安装中间CA证书。此外，如果客户端上使用Microsoft EAP请求方，则创建中间CA证书的根CA的根CA证书也必须位于ACS服务器和客户端上的适当存储中，以便建立信任链。根CA证书和中间CA证书必须在ACS和客户端上标记为受信任。大多数中间CA证书未与Windows一起安装，因此您最可能需要从供应商处获取这些证书。在Windows证书存储中正确安装后，中间CA证书将显示在**Certificates(Local Computer)> Intermediate Certification Authorities > Certificates文件夹中，如本示例窗口**所示。



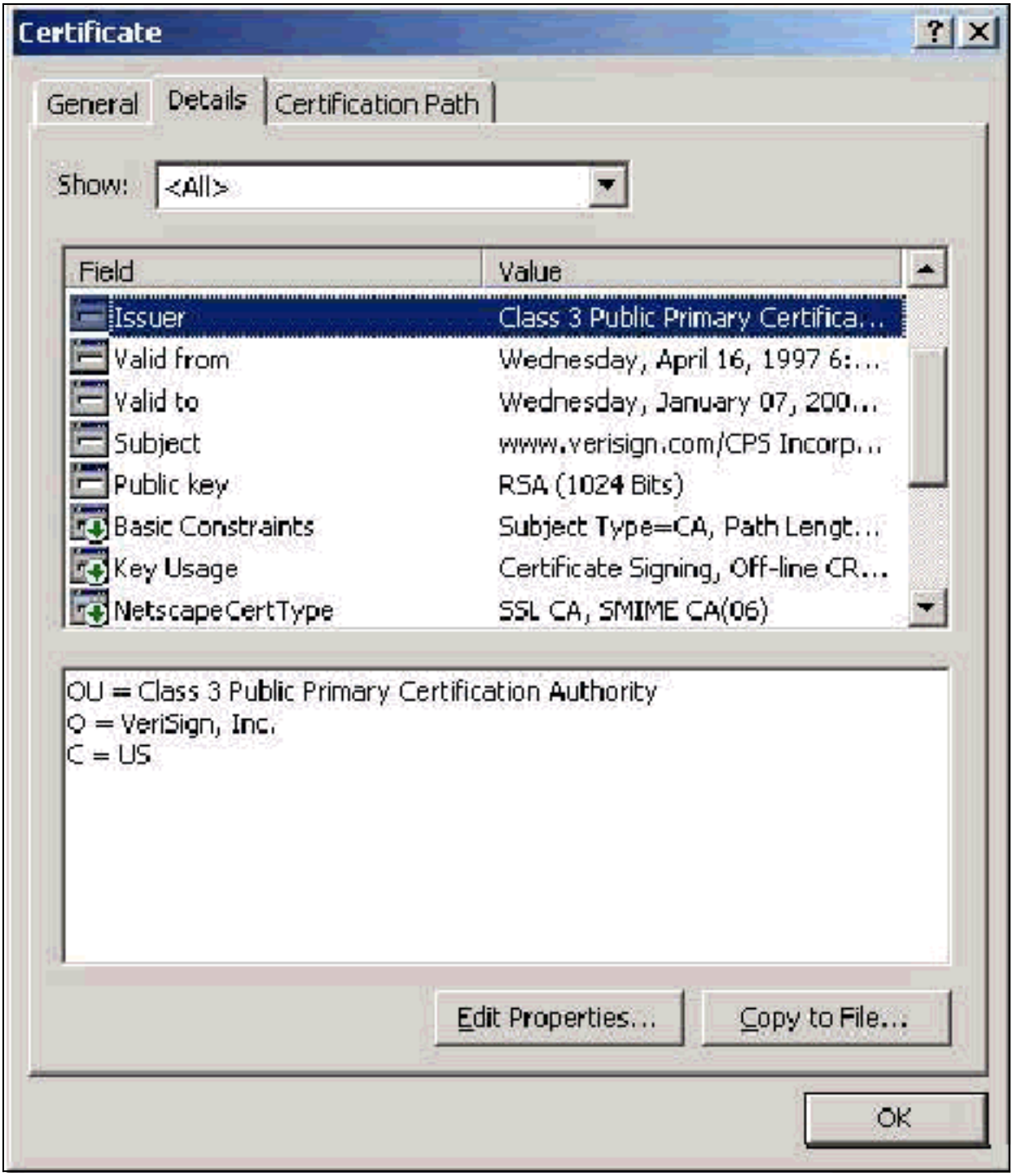
主题字段

Subject字段标识中间CA。此值用于确定证书“常规”(General)选项卡中的“已颁发给”(Issued to)字段。



颁发者字段

颁发者字段标识剪切证书的CA。使用此值可确定证书“常规”(General)选项卡中“颁发者”(Issued by)字段的值。它填充了CA的名称。



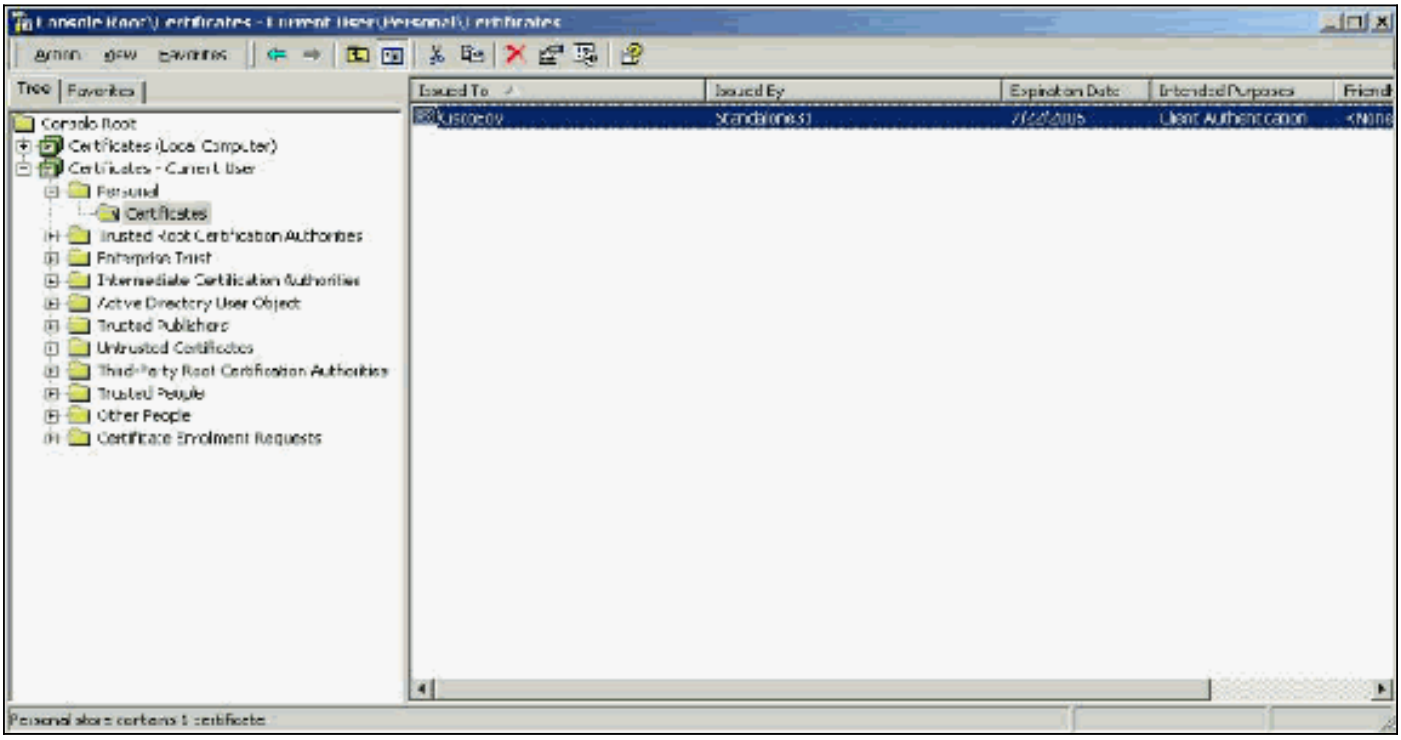
客户端证书

客户端证书用于在EAP-TLS中正确标识用户。它们在构建TLS隧道时不起任何作用，不用于加密。正确识别通过以下三种方法之一实现：

- **CN（或名称）Comparison** — 将证书中的CN与数据库中的用户名进行比较。有关此比较类型的详细信息包含在证书的Subject字段的说明中。
- **SAN比较** — 将证书中的SAN与数据库中的用户名进行比较。这仅在ACS 3.2中受支持。有关此比较类型的详细信息包含在证书的“使用者备用名称”字段的说明中。
- **Binary Comparison** — 将证书与存储在数据库中的证书的二进制副本进行比较（只有AD和LDAP可以执行此操作）。 如果使用证书二进制比较，则必须以二进制格式存储用户证书。此外，对于通用LDAP和Active Directory，存储证书的属性必须是名为“usercertificate”的标准LDAP属性。

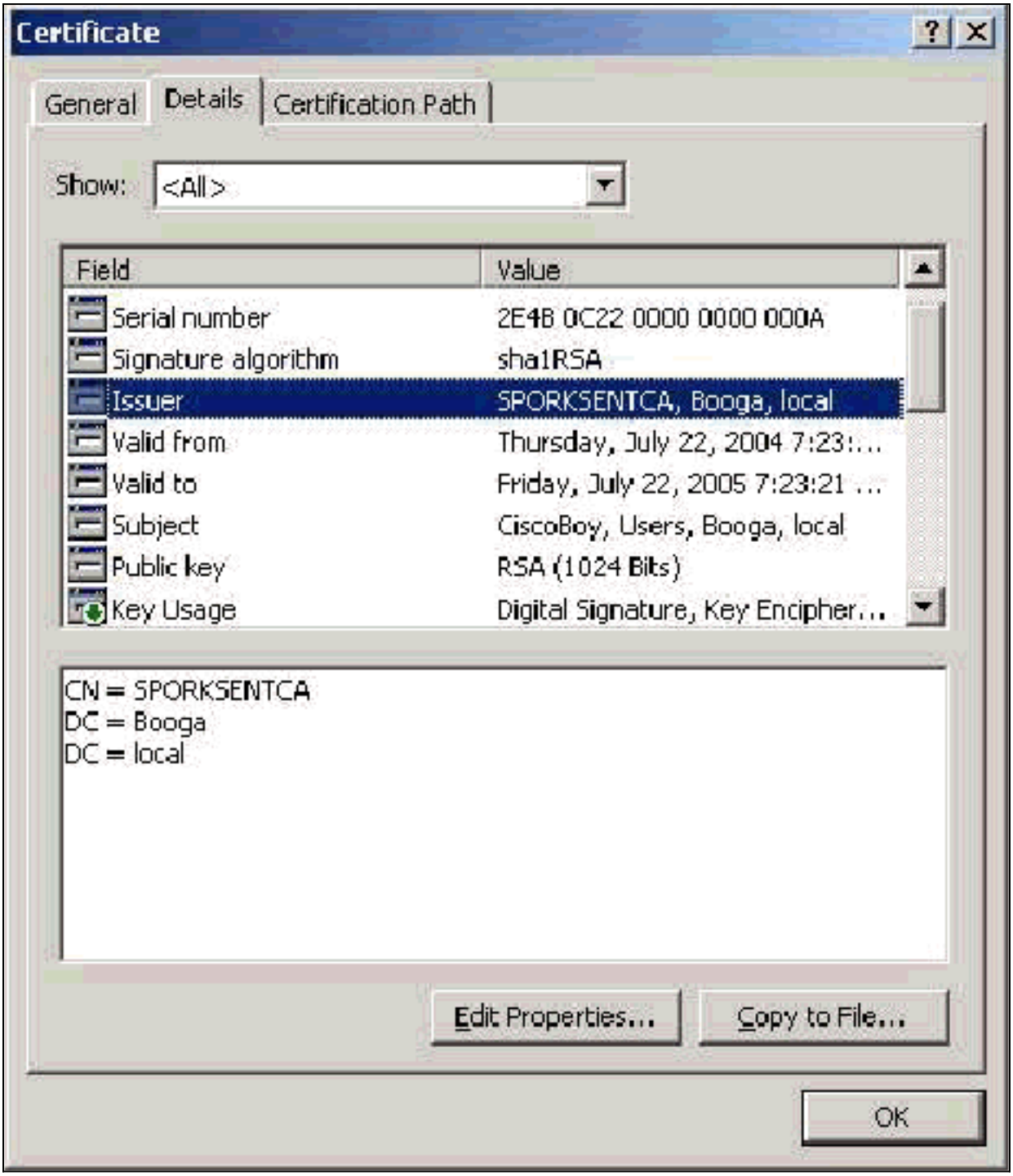
无论使用哪种比较方法，相应字段（CN或SAN）中的信息都必须与数据库用于身份验证的名称相匹配。AD在混合模式下使用NetBios名称进行身份验证，在本地模式下使用UPN。

本节讨论使用Microsoft证书服务生成客户端证书。EAP-TLS要求唯一的客户端证书，以便每个用户进行身份验证。必须为每个用户在每台计算机上安装证书。正确安装后，证书位于Certificates - Current User > Personal > Certificates文件夹中，如本示例窗口所示。



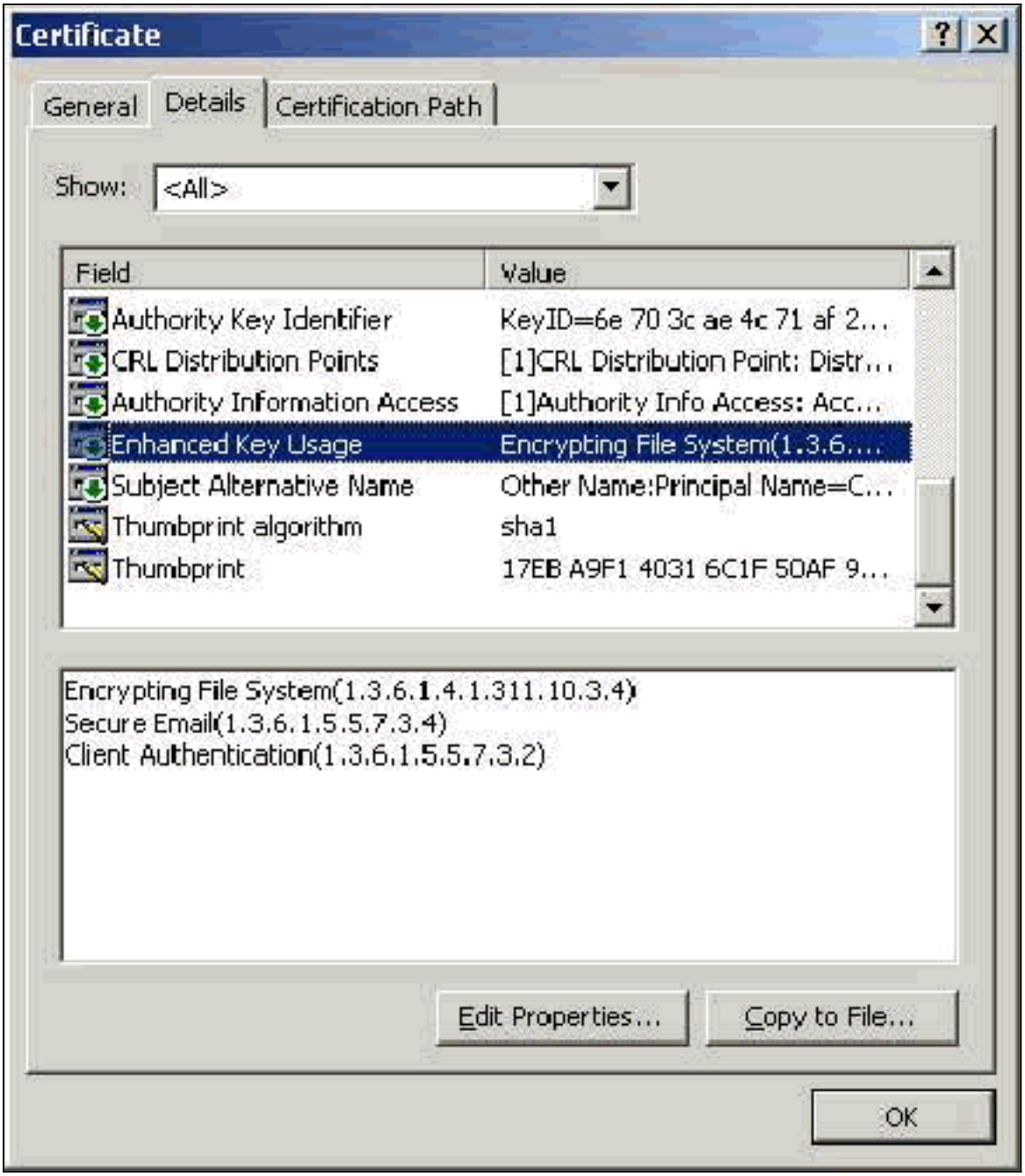
颁发者字段

Issuer字段标识剪切证书的CA。使用此值可确定证书“常规”(General)选项卡中“颁发者”(Issued by)字段的值。这将填充CA的名称。



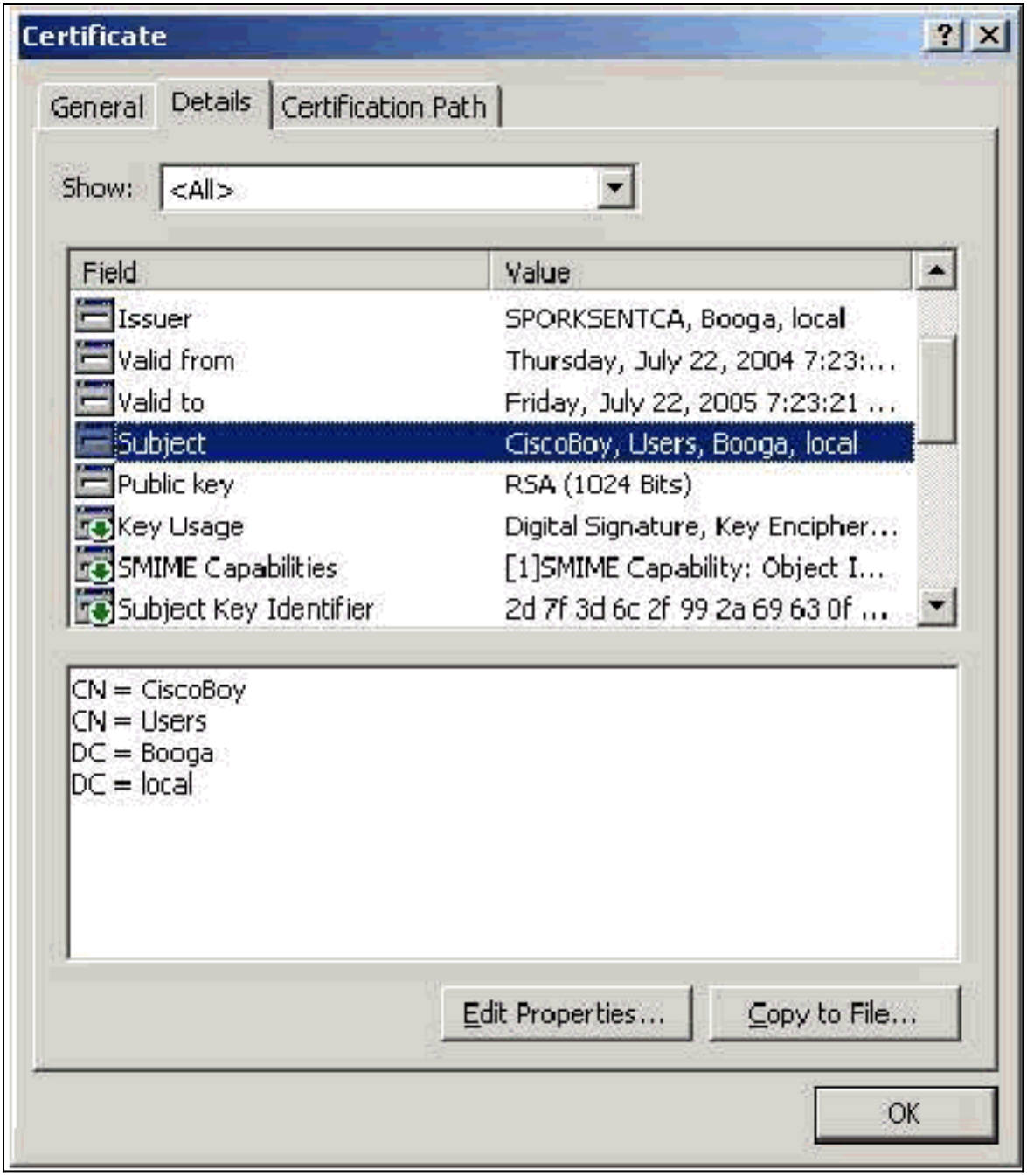
增强的密钥使用字段

Enhanced Key Usage字段标识证书的预期用途，并需要包含客户端身份验证。当您将Microsoft请求方用于PEAP和EAP-TLS时，此字段为必填字段。使用Microsoft证书服务时，当您从“目标用途”(Intended Purpose)下拉列表中选择**客户端身份验证证书**(Client Authentication Certificate)时，在“独立CA”(Standolane CA)中配置此功能，从“证书模板”(Certificate Template)下拉列表中选择**用户**(User)。如果您使用CSR和Microsoft证书服务请求证书，则您不能选择使用独立CA指定目标用途。因此，EKU字段不存在。使用企业CA，您将看到目标用途下拉列表。某些CA不使用EKU字段创建证书。当您使用Microsoft EAP请求方时，它们无用。



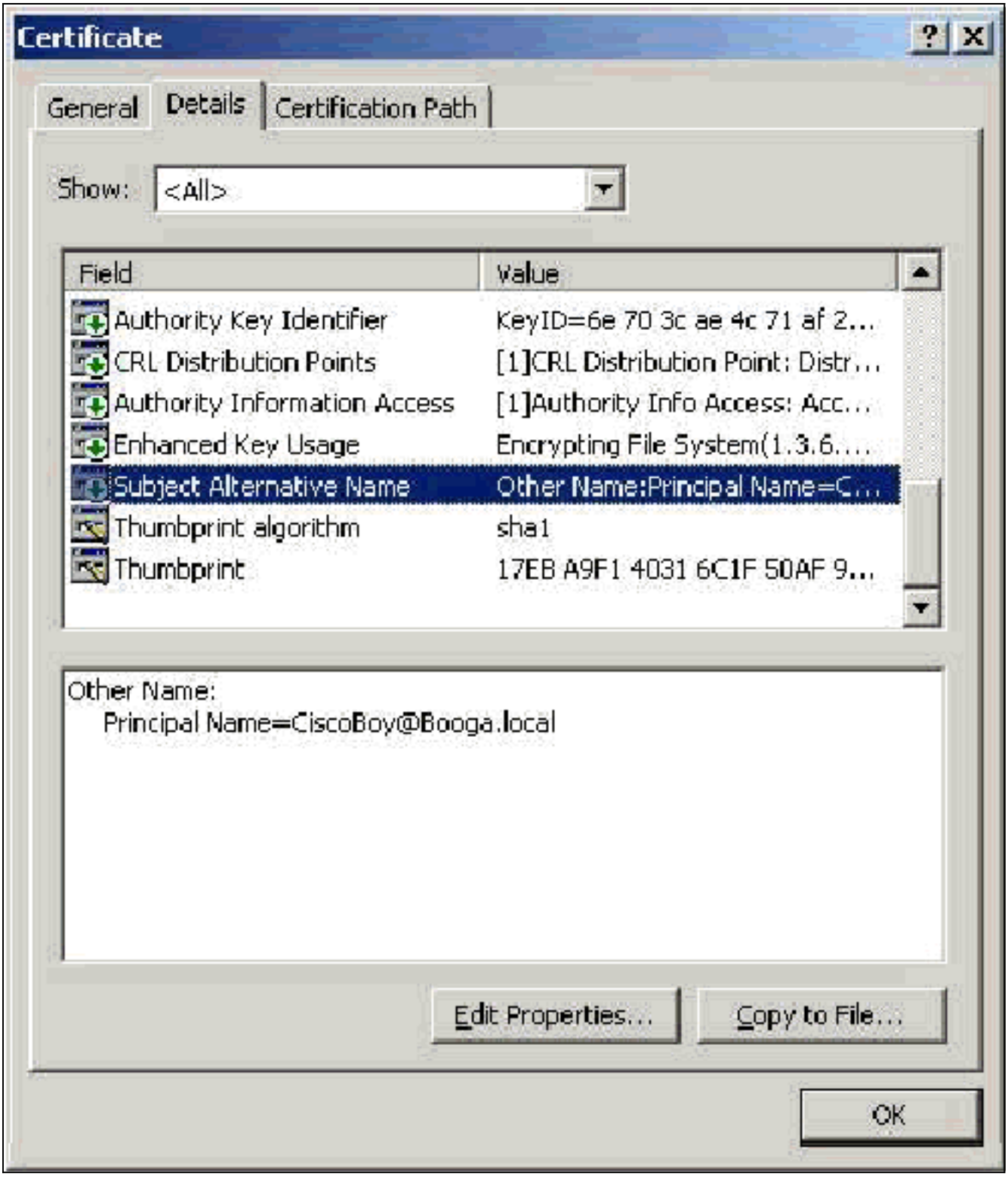
主题字段

此字段用于CN比较。将列出的第一个CN与数据库进行比较以查找匹配项。如果找到匹配项，身份验证成功。如果使用独立CA，则CN将填入您在证书提交表单的“名称”(Name)字段中输入的任何内容。如果使用企业CA，CN会自动填充Active Directory用户和计算机控制台中列出的帐户名称（这不一定与UPN或NetBios名称匹配）。



主题备用名称字段

SAN比较中使用“主题备用名称”字段。将列出的SAN与数据库进行比较以查找匹配项。如果找到匹配项，身份验证成功。如果使用企业CA，SAN会自动填充Active Directory登录名@domain(UPN)。独立CA不包含SAN字段，因此您不能使用SAN比较。

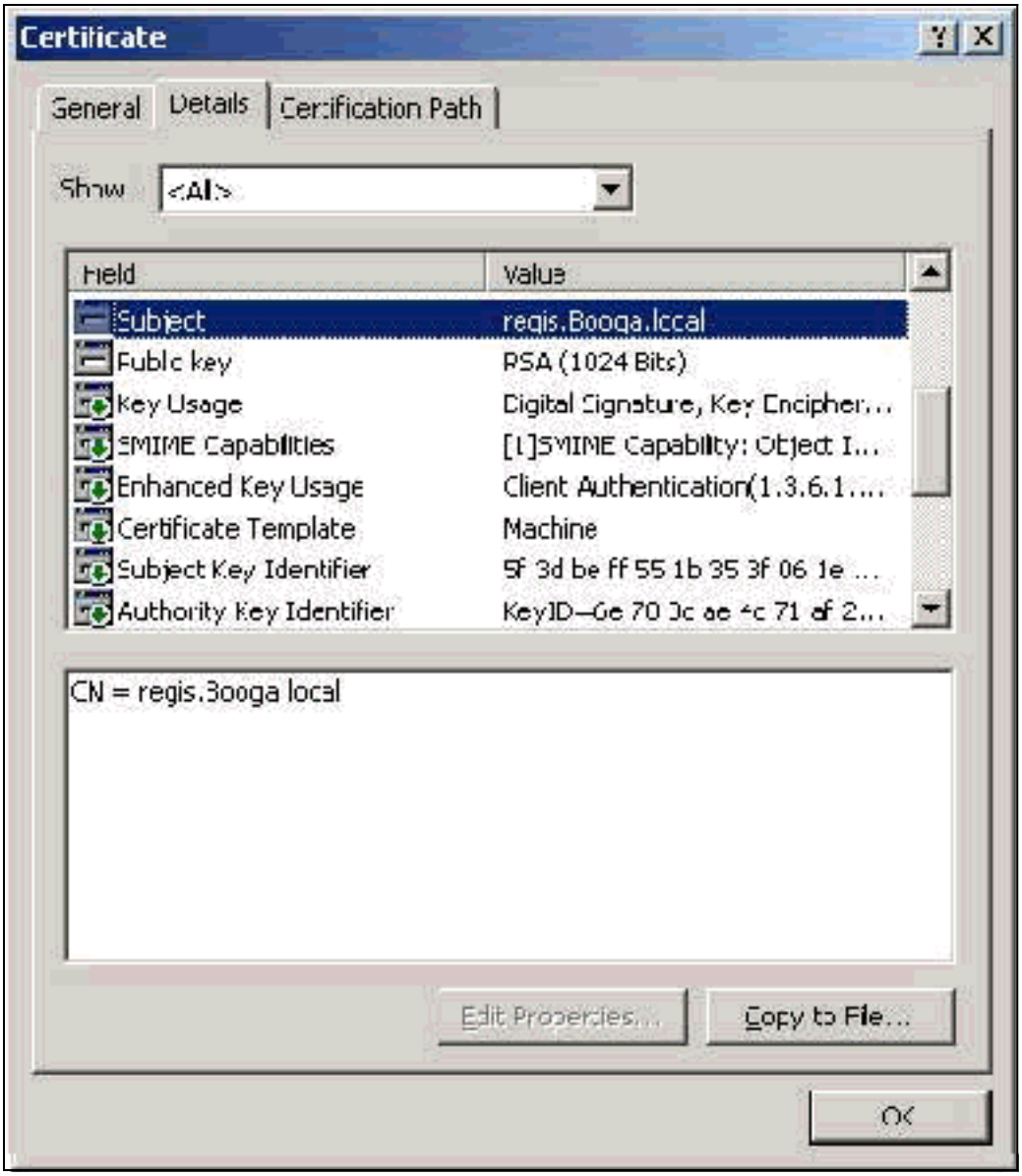


计算机证书

计算机证书在EAP-TLS中使用，以在您使用计算机身份验证时正确标识计算机。只有在为证书自动注册配置Microsoft企业CA并将计算机加入域时，才能访问这些证书。当您使用计算机的Active Directory凭据并将其安装到本地计算机存储时，会自动创建证书。在您配置自动注册之前已经是域成员的计算机在Windows下次重新启动时收到证书。计算机证书安装在证书(本**地计算机)>个人>证书**文件夹中，与服务器证书一样。由于无法导出私钥，因此无法在任何其他计算机上安装这些证书。

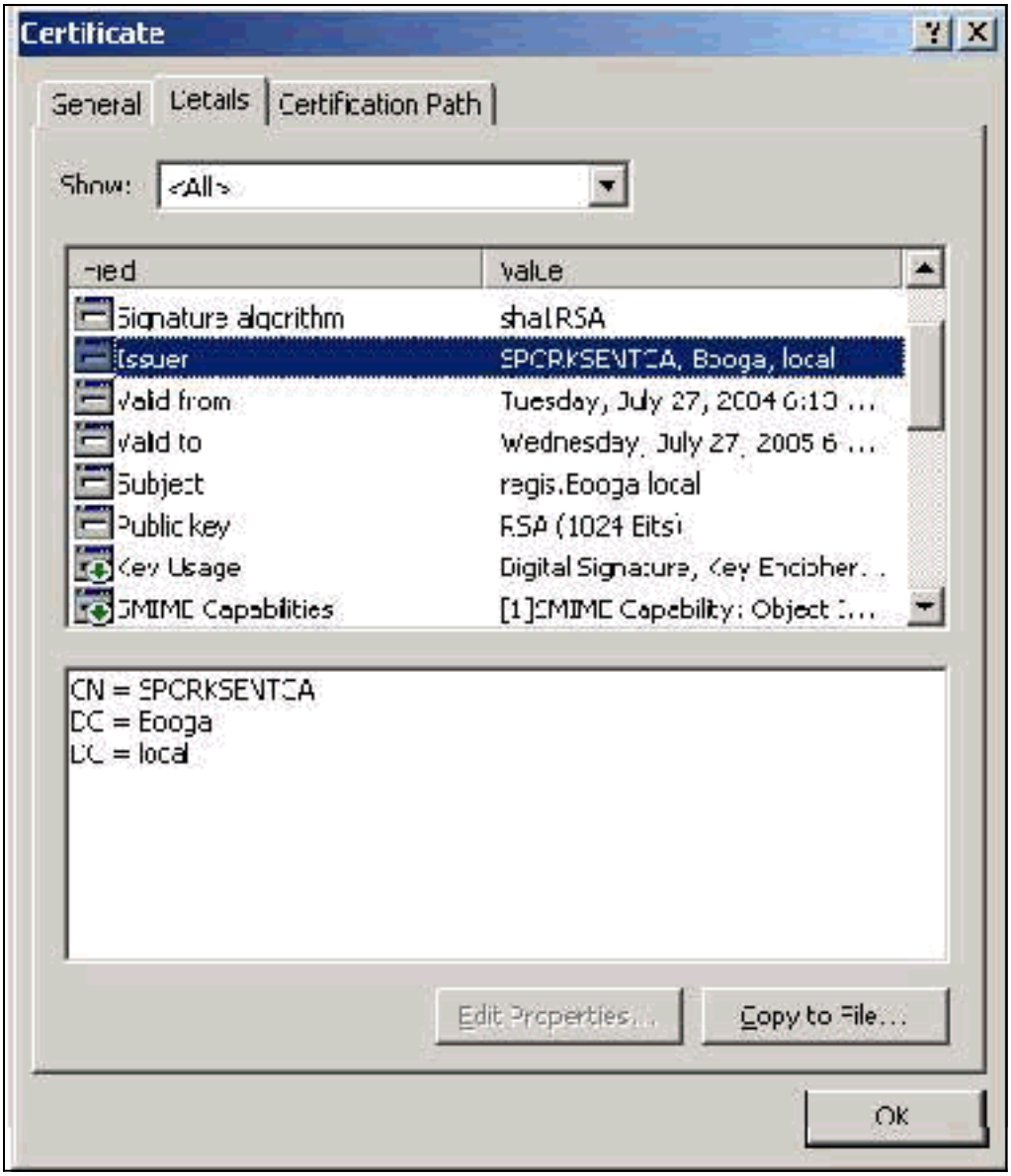
主题和SAN字段

“主题”和“SAN”字段标识计算机。该值由计算机的完全限定名称填充，用于确定证书“常规”(General)选项卡中的“已颁发给”(Issued to)字段，并且对于“主题”(Subject)和“SAN”(SAN)字段相同。



颁发者字段

颁发者字段标识剪切证书的CA。使用此值可确定证书“常规”(General)选项卡中“颁发者”(Issued by)字段的值。它填充了CA的名称。



附录A — 通用证书扩展

.csr — 这实际上不是证书，而是证书签名请求。它是一个纯文本文件，格式如下：

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

.pvk — 此扩展表示私钥，但该扩展并不保证内容实际是私钥。内容需要采用以下格式的纯文本：

```
-----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 — 这是表示证书的通用扩展。服务器、根CA和中间CA证书可以采用此格式。它通常是带扩展名的纯文本文件，您可以根据需要更改，可以是DER或Base 64格式。您可以将此格式导入到Windows证书存储区。

.pem — 此分机代表“隐私增强型邮件”。此扩展通常用于UNIX、Linux、BSD等。它通常用于服务器证书和私钥，并且通常是扩展名为.pem的纯文本文件，您可以根据需要将其从.pem更改为.cer，以便将其导入Windows证书存储。

.cer和.pem文件的内部内容通常类似于以下输出：

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAy+gAwIBAgIKSKZzlwAAAAAEjANBgkqhkiG9w0BAQUFADA2MQswCQYD
VQQGEwJVUzEQMA4GA1UEChMHU0xDIFRBQzEVMBMGA1UEAxMMU3RhbmRhbG9uZTMx
MB4XDTA0MDcxOTE3MzMyNVoXDTA1MDcxOTE3NDMyNVowLjELMAkGA1UEBhMCVVMx
AAQAGBvkDy7BaMBJgFRuS+QU8o2XfH5aAQiCcyKu/jK6mMt64QyCy9k=
-----END CERTIFICATE-----
```

.pfx — 此分机代表个人信息交换。此格式可用于将证书捆绑到单个文件中。例如，您可以将服务器证书及其关联的私钥和根CA证书捆绑到一个文件中，并轻松将文件导入相应的Windows证书存储。它最常用于服务器和客户端证书。遗憾的是，如果包含根CA证书，则根CA证书始终安装在当前用户存储中，而不是本地计算机存储中，即使指定安装本地计算机存储。

.p12 — 此格式通常仅在客户端证书中显示。您可以将此格式导入到Windows证书存储区。

.p7b — 这是另一种格式，它将多个证书存储在一个文件中。您可以将此格式导入到Windows证书存储区。

附录B — 证书格式转换

在大多数情况下，证书转换发生在您更改扩展名（例如，从.pem更改为.cer）时，因为证书通常采用纯文本格式。有时，证书不是明文格式，您必须使用OpenSSL等工具对其进行转换 。例如，ACS解决方案引擎无法安装.pfx格式的证书。因此，您必须将证书和私钥转换为可用格式。以下是OpenSSL的基本命令语法：

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

系统将提示您输入导入密码和PEM密码短语。这些密码必须相同，并且是导出.pfx时指定的私钥密码。输出是一个.pem文件，包含.pfx中的所有证书和私钥。此文件在ACS中可以同时用作证书和私

钥文件，且安装时没有问题。

附录C — 证书有效期

证书仅在其有效期内可用。根CA证书的有效期在建立根CA时确定，并且可能有所不同。中间CA证书的有效期是在建立CA时确定的，并且不能超过它所属的根CA的有效期。使用Microsoft证书服务，服务器、客户端和计算机证书的有效期自动设置为一年。仅当您按照Microsoft知识库文章254632对Windows注册表进行黑客攻击时，此更改不能超过根CA的有效期。ACS生成的自签名证书的有效期始终为一年，在当前版本中无法更改。

相关信息

- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持 - Cisco Systems