EAP 1.01版證書指南

目錄

簡介

本文檔澄清了與各種形式的可擴展身份驗證協定(EAP)相關的各種證書型別、格式和要求所伴隨的一些混淆。 本文討論的與EAP相關的五種證書型別是伺服器、根CA、中間CA、客戶端和電腦。這些證書有不同的格式，並且根據涉及的EAP實施對每種證書可能有不同的要求。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

伺服器證書

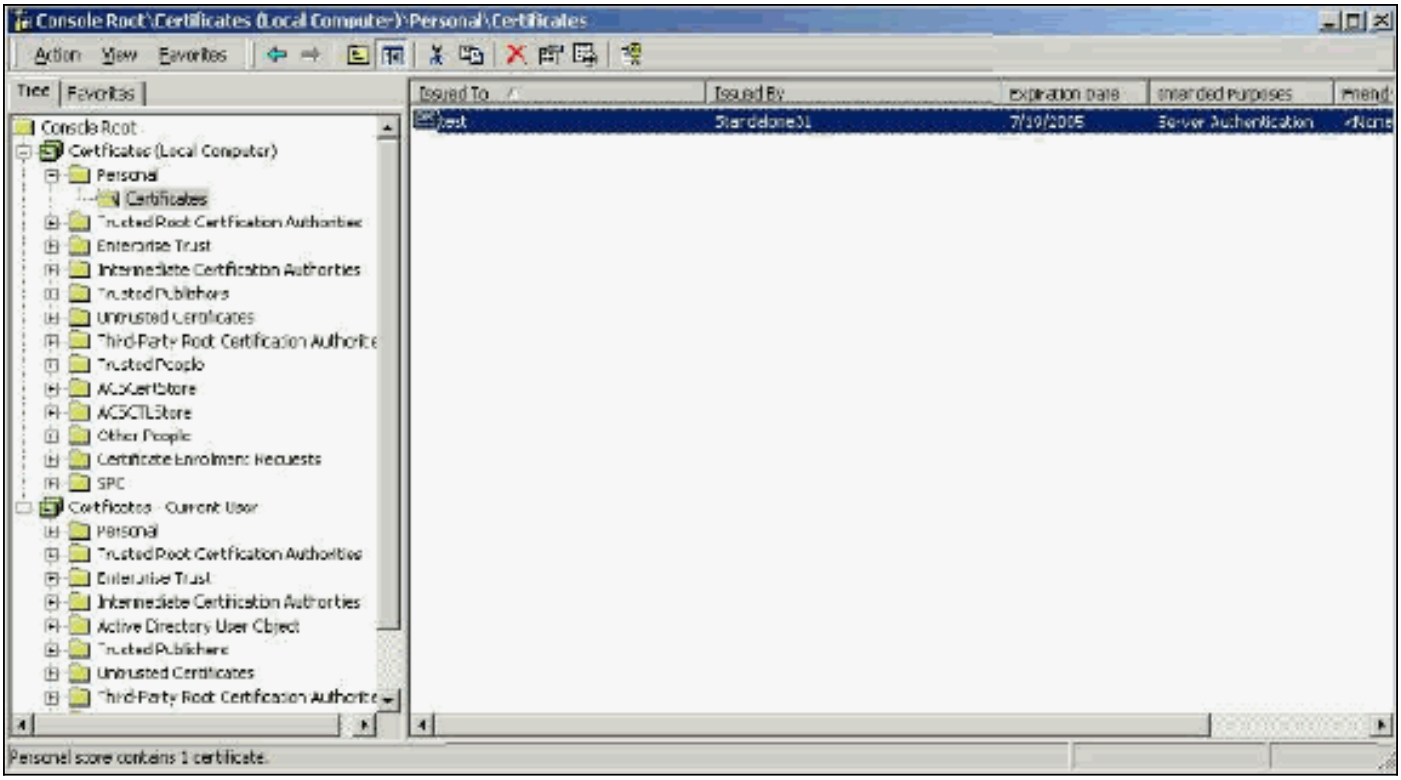
伺服器證書安裝在RADIUS伺服器上，其在EAP中的主要用途是建立加密的傳輸層安全(TLS)隧道，以保護身份驗證資訊。使用EAP-MSCHAPv2時，伺服器證書將承擔輔助角色，該輔助角色將RADIUS伺服器標識為身份驗證的可信實體。此輔助角色是通過使用Enhanced Key Usage(EKU)欄位完成的。EKU欄位將證書標識為有效的伺服器證書，並驗證頒發證書的根CA是否為受信任的根CA。這需要存在根CA證書。Cisco Secure ACS要求證書採用Base64編碼或DER編碼的二進位制X.509 v3格式。

您可以使用提交到CA的ACS中的憑證簽署請求(CSR)建立此憑證。或者，也可以使用內部CA（如Microsoft證書服務）證書建立表單剪下證書。必須注意的是，雖然您可以建立金鑰大小大於1024的伺服器證書，但任何大於1024的金鑰都不適用於PEAP。即使身份驗證通過，客戶端也會掛起。

如果使用CSR建立證書，則會使用.cer、.pem或.txt格式建立證書。在極少數情況下，建立時沒有副檔名。確保您的證書是純文字檔案檔案，其副檔名可以根據需要更改（ACS裝置使用.cer或.pem副檔名）。 此外，如果您使用CSR，則會在您指定的路徑中建立憑證的私密金鑰，該路徑可能包含也可能不包含延伸模組且具有相關聯的密碼（在ACS上安裝時需要該密碼）。 無論副檔名如何，請確保它是具有副檔名的純文字檔案檔案，您可以根據需要對其進行更改（ACS裝置使用.pvk或.pem副檔名）。 如果沒有為私鑰指定路徑，ACS會將金鑰儲存在C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs目錄中，並在安裝證書時沒有為私鑰檔案指定路徑時在此目錄中查詢。

如果使用Microsoft證書服務證書提交表單建立證書，請確保將金鑰標籤為可匯出，以便可以在ACS中安裝證書。以這種方式建立證書可顯著簡化安裝過程。您可以從證書服務Web介面直接將其安裝到正確的Windows應用商店中，然後使用CN作為參考從儲存中安裝到ACS上。安裝在本地電腦儲存中的證書也可以從Windows儲存匯出並輕鬆安裝在另一台電腦上。匯出此類證書時，需要將金鑰標籤為可匯出並給定密碼。證書隨後以.pfx格式顯示，其中包括私鑰和伺服器證書。

在Windows證書儲存中正確安裝後，伺服器證書需要顯示在**Certificates(Local Computer)> Personal > Certificates**資料夾中，如本示例視窗所示。

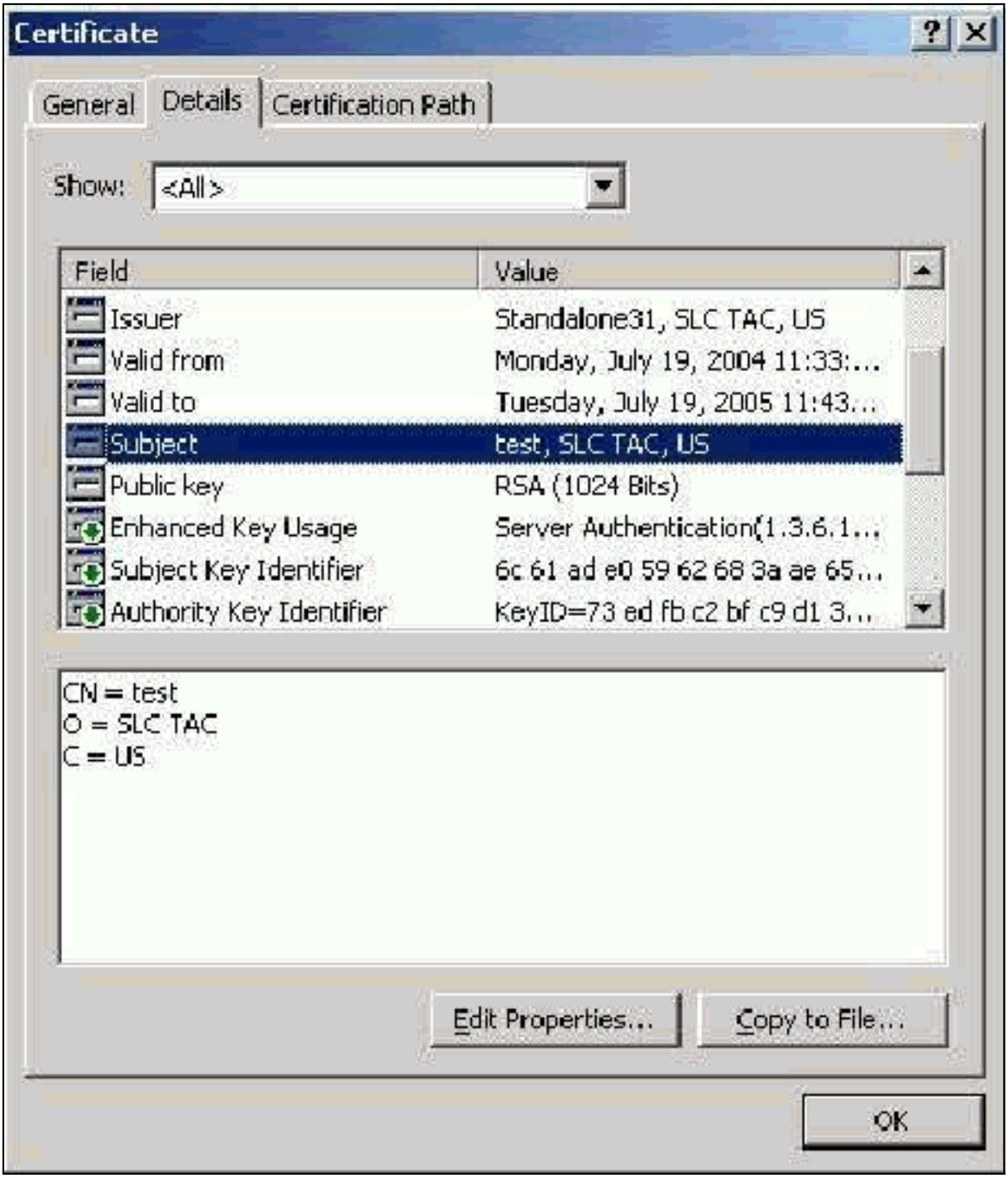


自簽名證書是您建立的沒有根證書或CA中間參與的證書。它們在subject和issuer欄位中具有相同的值，如根CA證書。大多數自簽名證書使用X.509 v1格式。因此，它們不適用於ACS。但是，自版本3.3起，ACS能夠建立自己的自簽名證書，您可以將其用於EAP-TLS和PEAP。請勿使用大於1024的金鑰大小來相容PEAP和EAP-TLS。如果您使用自簽名證書，則證書還以根CA證書的容量運行，並且當您使用Microsoft EAP請求方時，必須安裝在客戶端的**證書（本地電腦）>受信任的根證書頒發機構>證書**資料夾中。它會自動安裝在伺服器上的受信任根證書儲存中。但是，在ACS證書設定中的證書信任清單中仍然必須信任它。如需詳細資訊，請參閱根CA憑證一節。

由於使用Microsoft EAP請求方時，自簽名證書用作伺服器證書的根CA證書，並且由於有效期不能從預設的一年延長，因此Cisco建議您僅將這些證書用於EAP作為臨時措施，直到可以使用傳統CA。

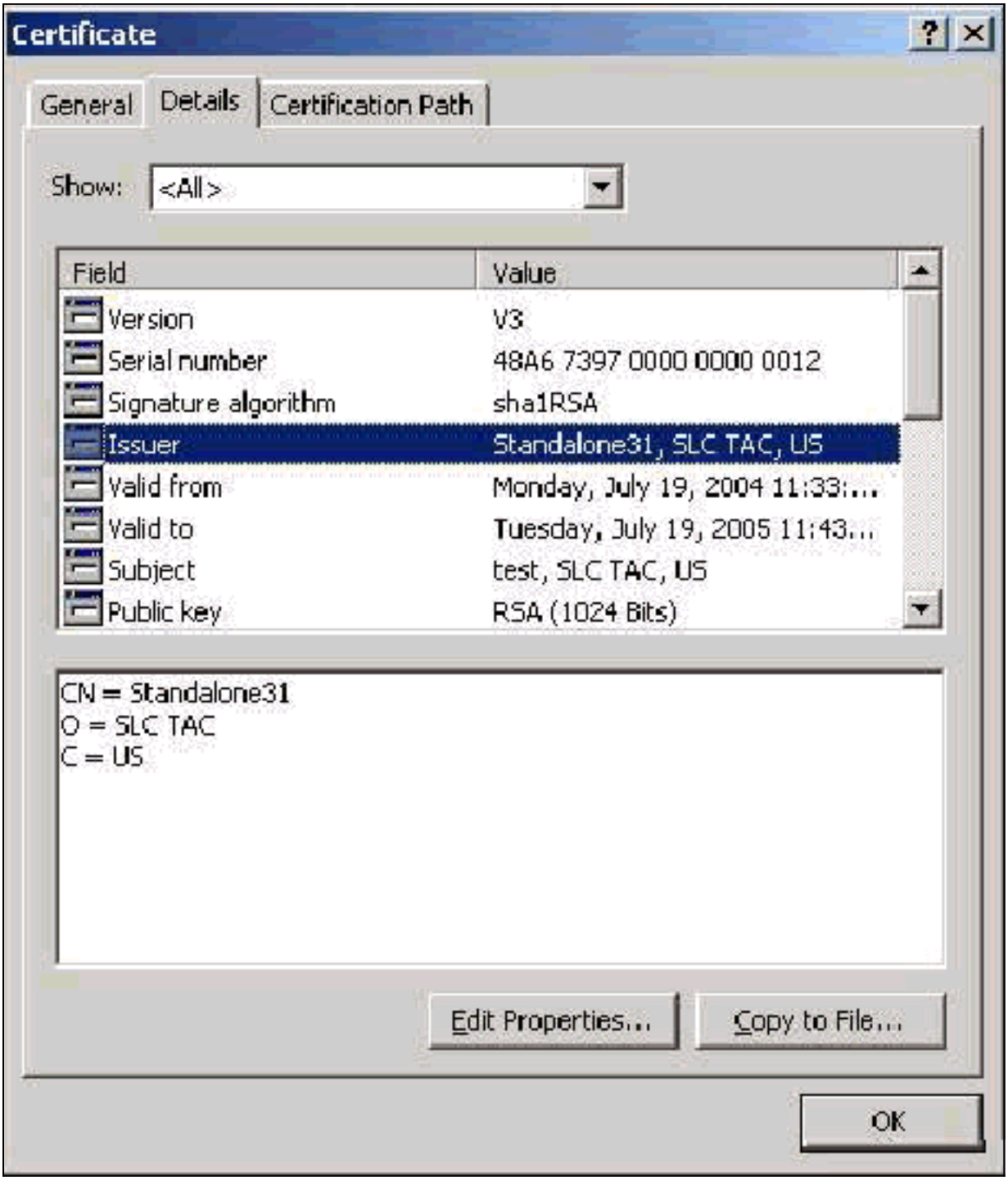
主題欄位

Subject欄位標識證書。CN值用於確定證書的「常規」頁籤中的「頒發給」欄位，並填充了您在ACS「CSR」對話方塊的「證書主題」欄位中輸入的資訊，或填充了Microsoft證書服務中「名稱」欄位的資訊。如果使用了從儲存安裝證書的選項，則CN值用於告知ACS需要在本地電腦證書儲存中使用哪種證書。



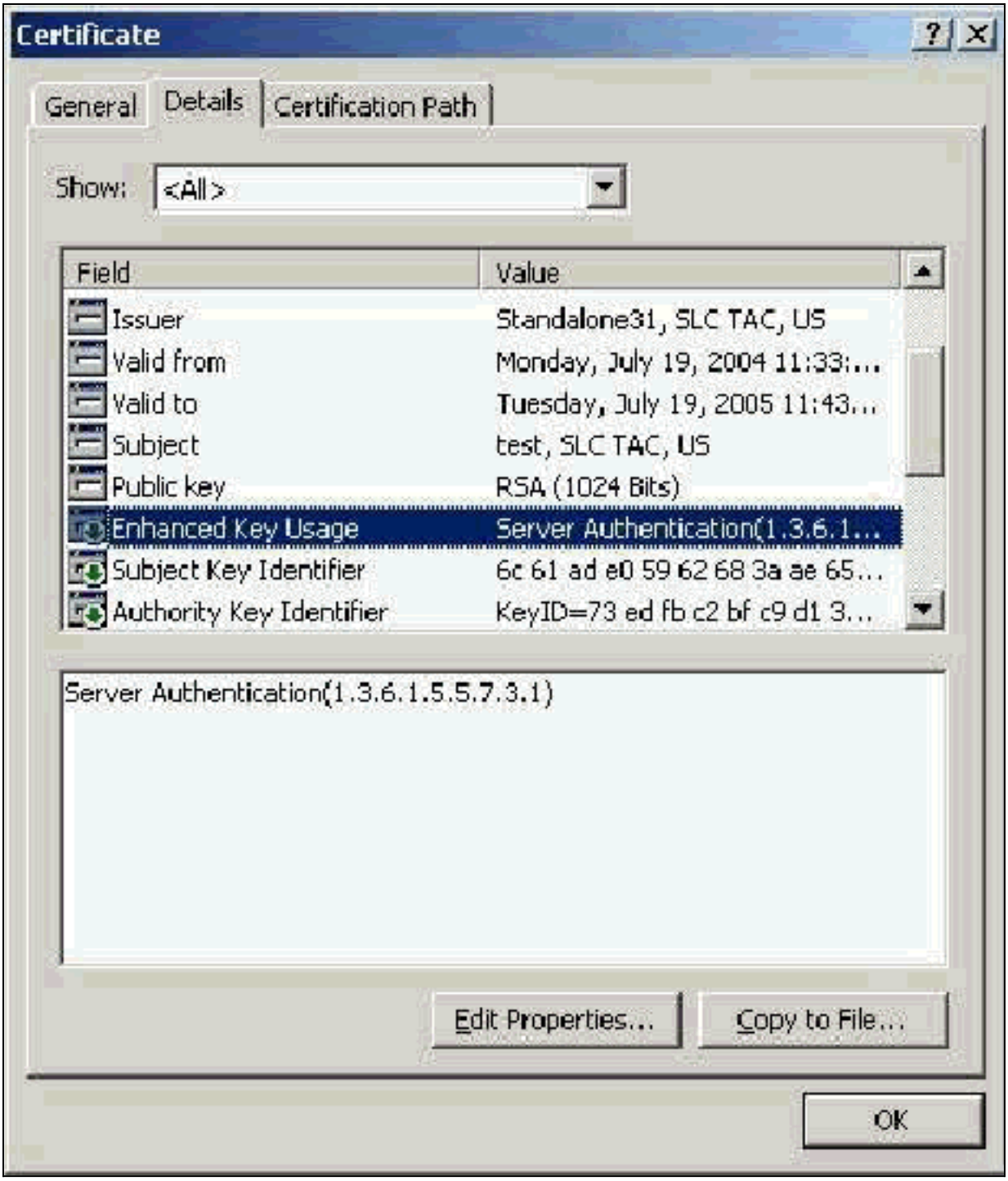
頒發者欄位

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將用CA的名稱填充。



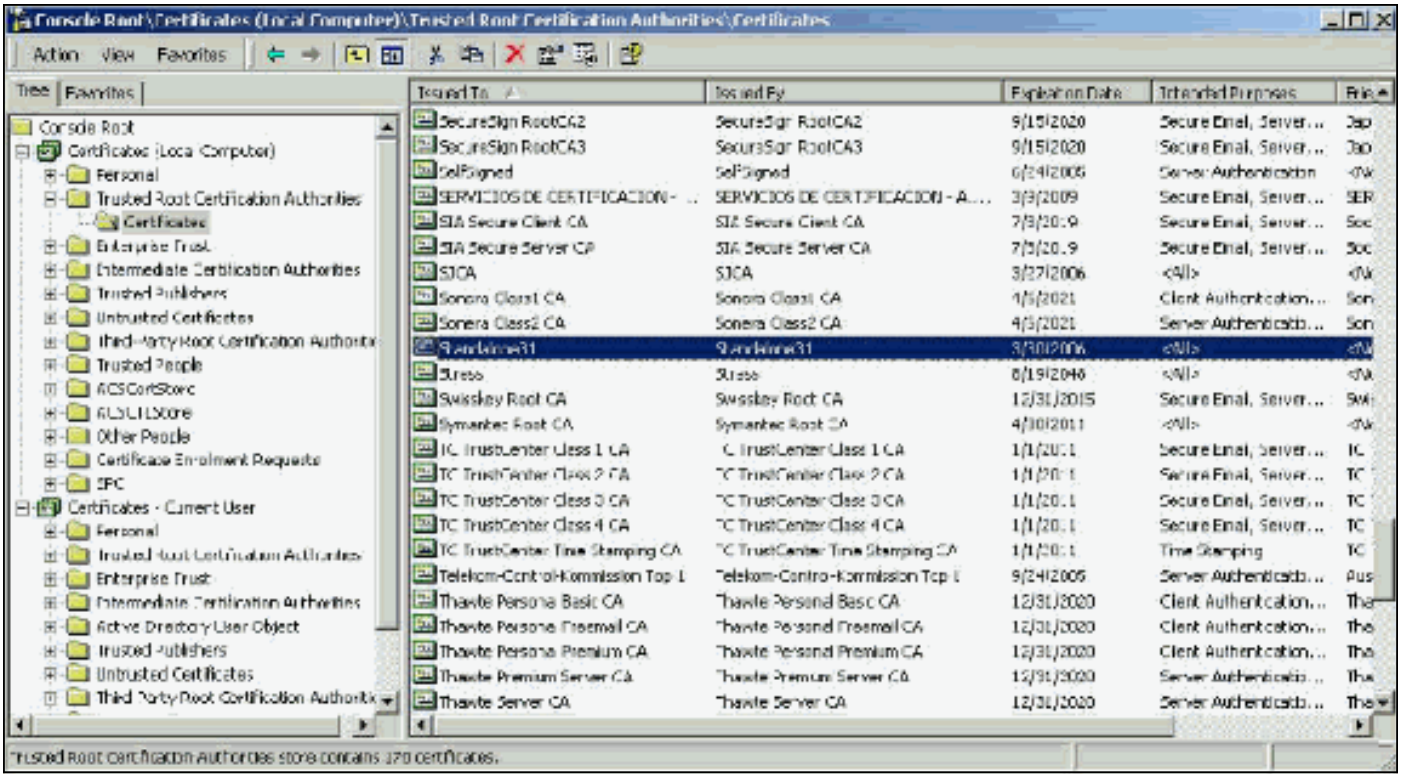
增強型金鑰使用欄位

Enhanced Key Usage欄位可識別憑證的預期用途，需列為「伺服器驗證」。 當您使用Microsoft的PEAP和EAP-TLS請求方時，此欄位為必填欄位。使用Microsoft Certificate Services時，將在獨立CA中配置，並且從「目標用途」下拉選單中選擇**Server Authentication Certificate**，在「企業CA」中配置，並且從「證書模板」下拉選單中選擇**Web Server**。如果您使用具有Microsoft證書服務的CSR來請求證書，則您沒有選擇使用獨立CA指定目標用途。因此，不存在EKU欄位。使用企業CA，您將看到「目標用途」下拉選單。某些CA不使用EKU欄位建立證書，因此當您使用Microsoft EAP請求方時，它們無用。



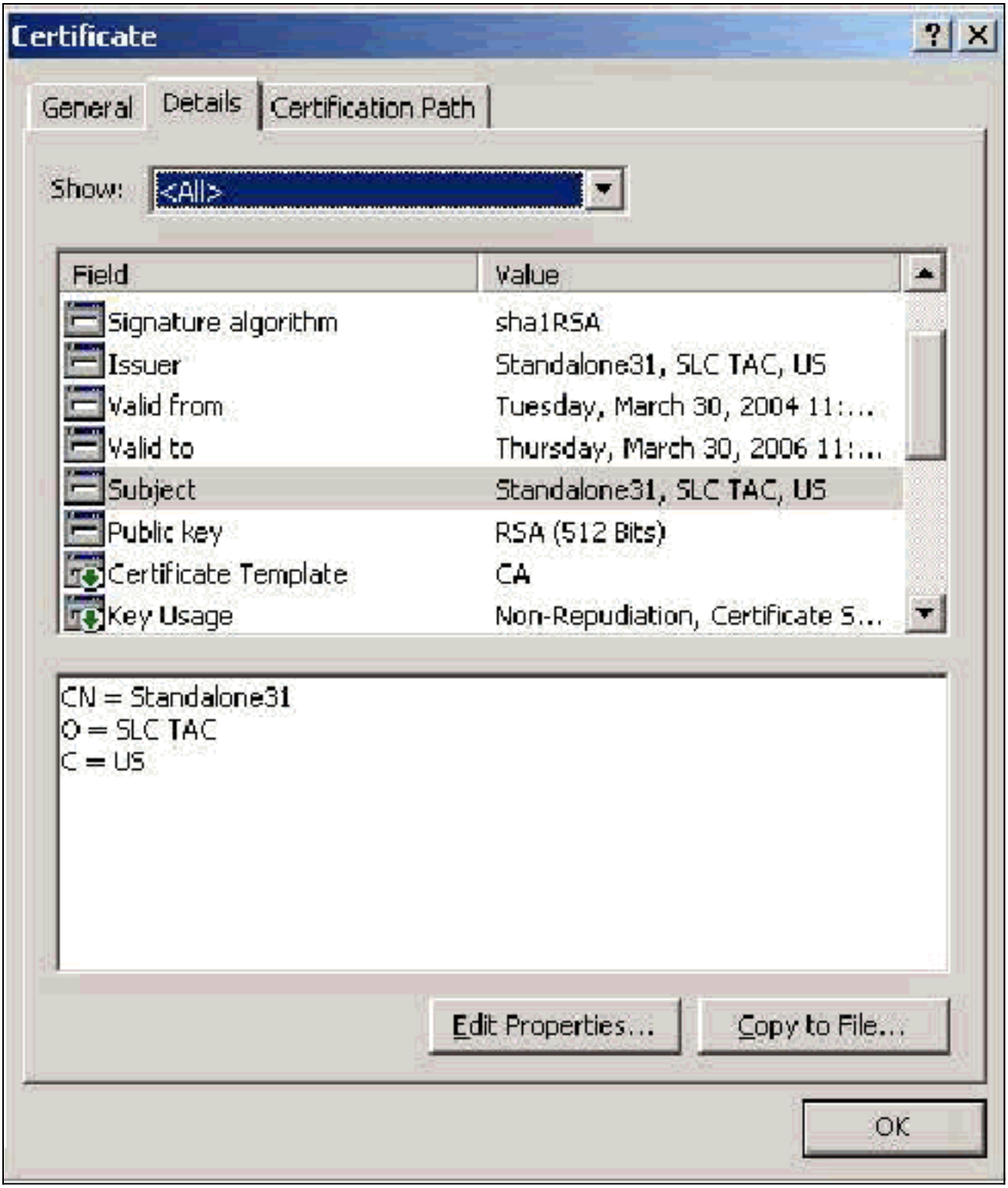
根CA證書

根CA證書的用途之一是將伺服器證書（以及中間CA證書，如果適用）標識為ACS和Windows EAP-MSCHAPv2請求方的受信任證書。它必須位於ACS伺服器上的Windows中的受信任的根憑證授權庫中，如果是EAP-MSCHAPv2，則位於客戶端電腦上。大多數第三方根CA證書都隨Windows一起安裝，因此幾乎不費吹灰之力。如果使用Microsoft證書服務，並且證書伺服器與ACS位於同一電腦上，則自動安裝根CA證書。如果在Windows的受信任的根證書頒發機構儲存中找不到根CA證書，則必須從CA獲取並安裝該證書。在Windows證書儲存中正確安裝後，根CA證書需要顯示在**Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates**資料夾中，如本示例視窗所示。



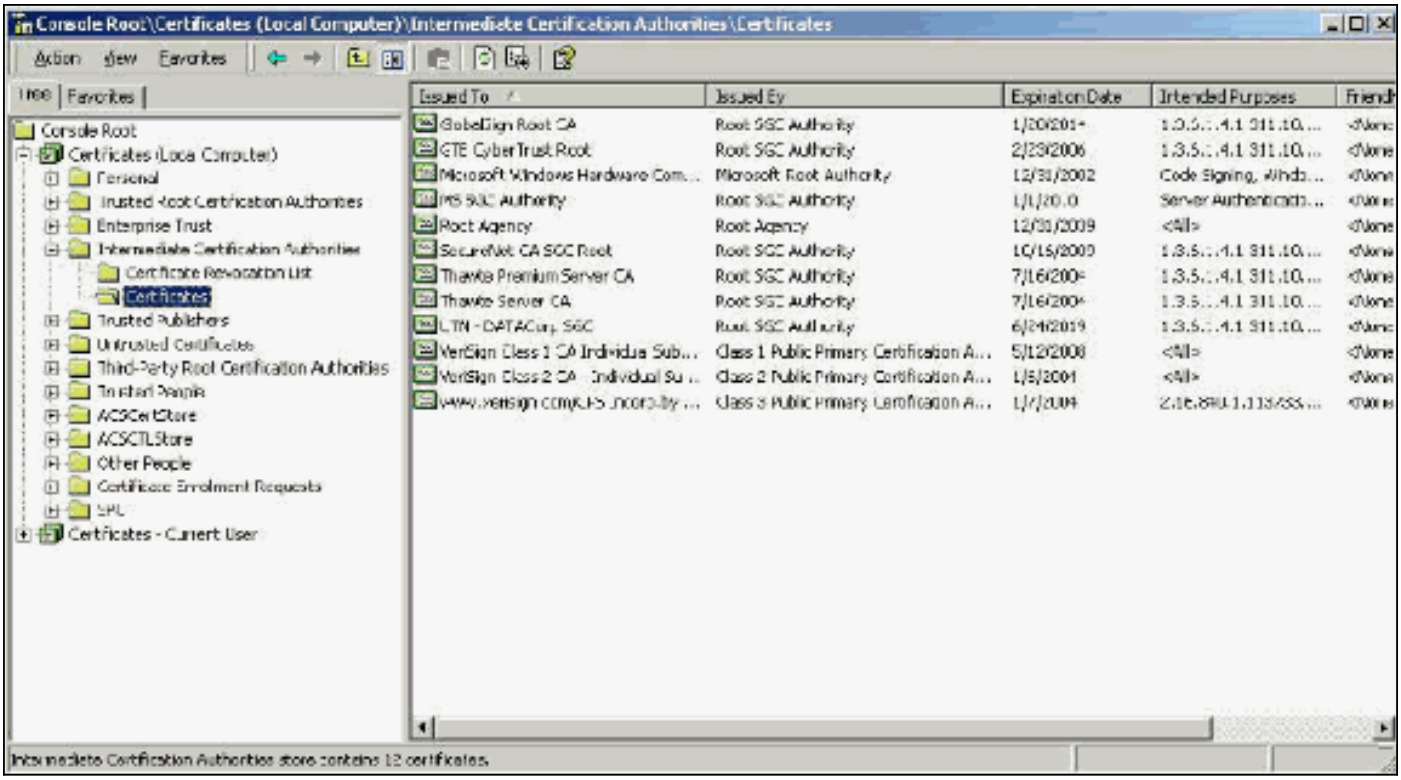
主題和頒發者欄位

Subject和Issuer欄位標識CA，並且需要完全相同。使用這些欄位填充證書的「常規」頁籤中的「頒發給」和「頒發者」欄位。使用根CA的名稱填充。



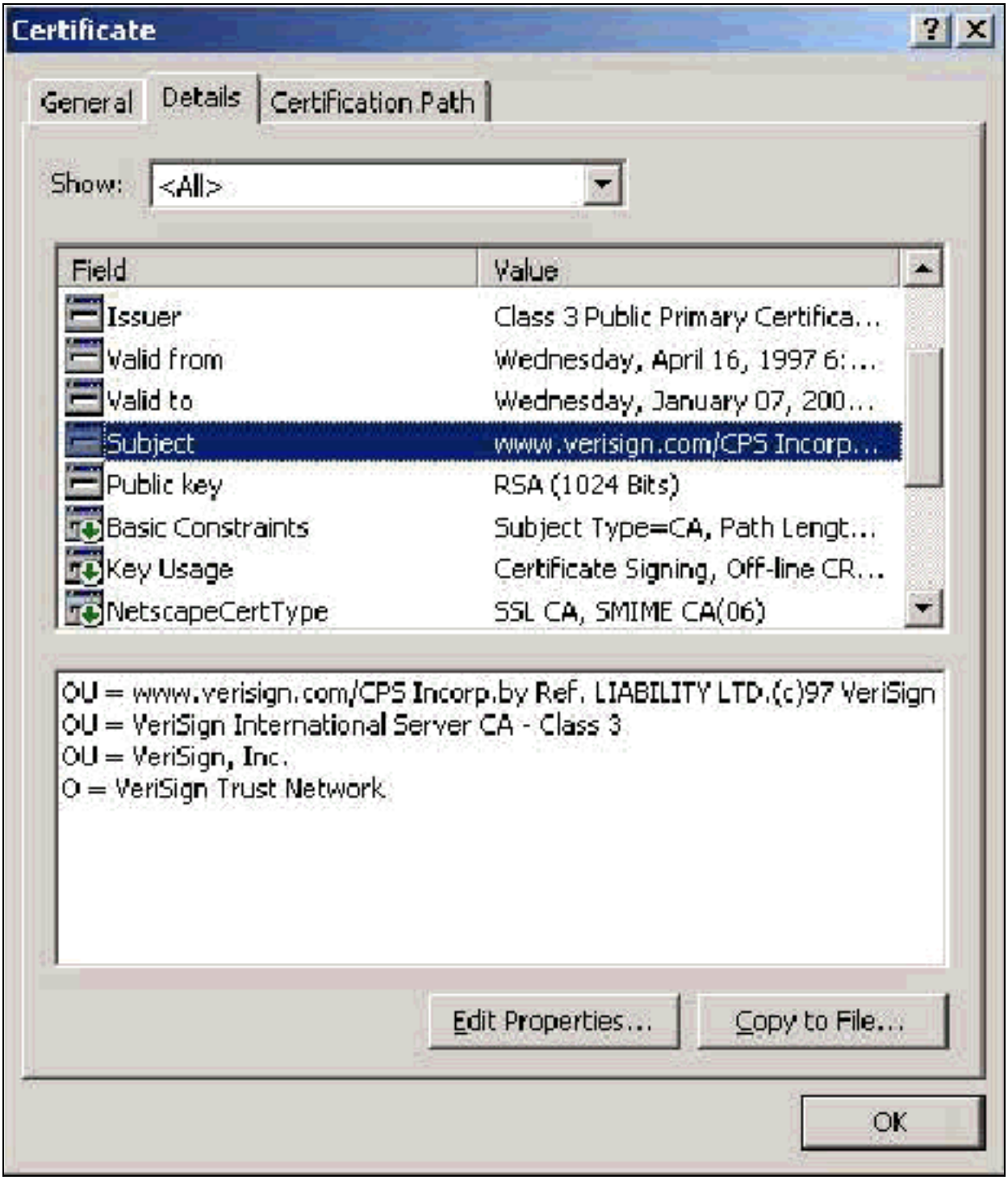
中繼CA憑證

中間CA證書是用來標識從屬於根CA的CA的證書。某些伺服器證書（Verisign的無線證書）是使用中間CA建立的。如果使用中間CA剪下的伺服器證書，則中間CA證書必須安裝在ACS伺服器上本地電腦儲存的中間證書頒發機構區域中。此外，如果在客戶端上使用Microsoft EAP請求方，則建立中間CA證書的根CA的根CA證書也必須位於ACS伺服器和客戶端上的相應儲存區中，以便可以建立信任鏈。根CA證書和中間CA證書必須在ACS和客戶端上標籤為受信任。大多數中繼CA證書未隨Windows一起安裝，因此您可能需要從供應商處獲取這些證書。在Windows證書儲存中正確安裝後，中間CA證書將顯示在**Certificates(Local Computer)> Intermediate Certification Authorities > Certificates**資料夾中，如本示例視窗所示。



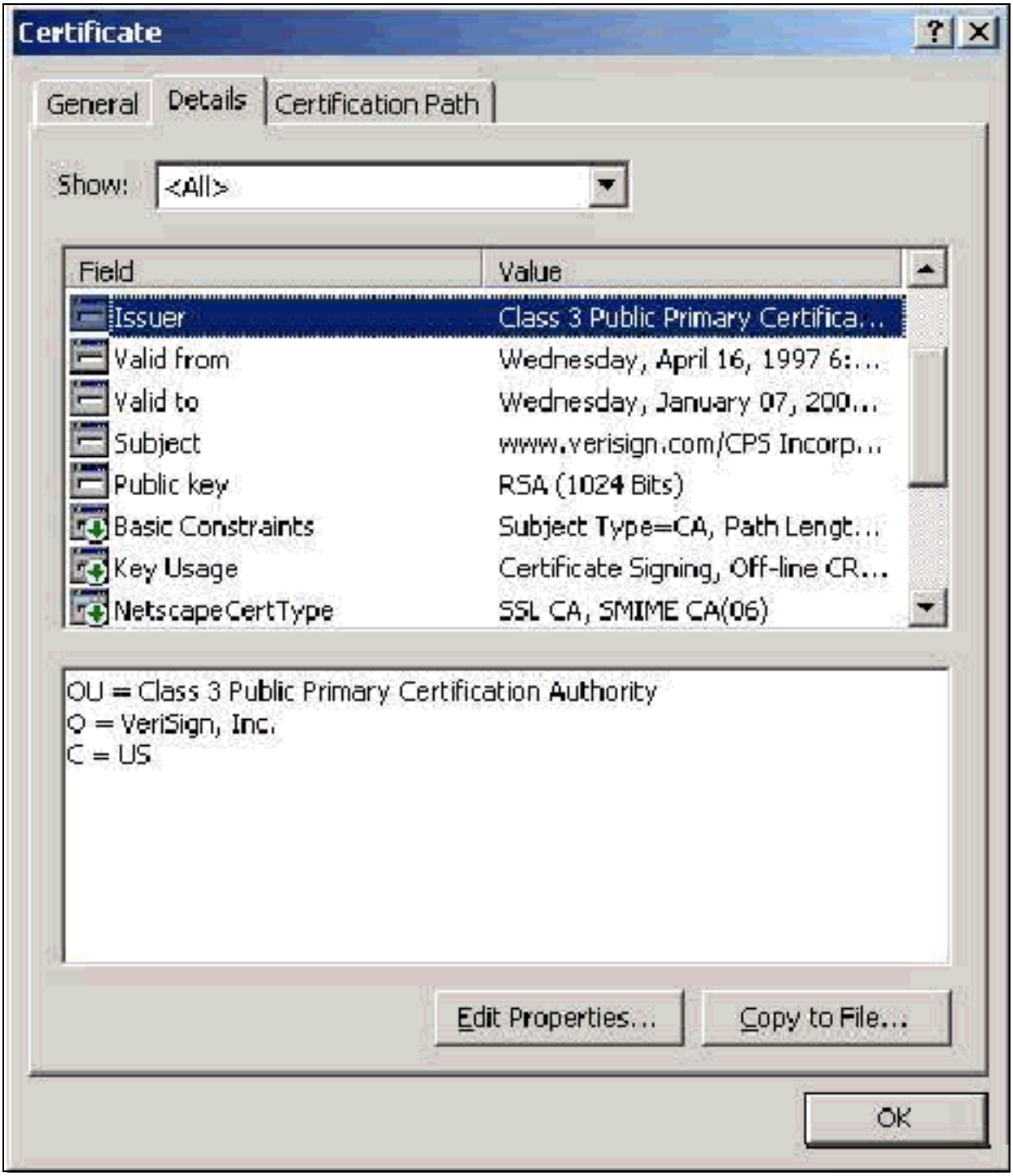
主題欄位

Subject欄位標識中間CA。此值用於確定證書的「常規」頁籤中的「頒發給」欄位。



頒發者欄位

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將用CA的名稱填充。



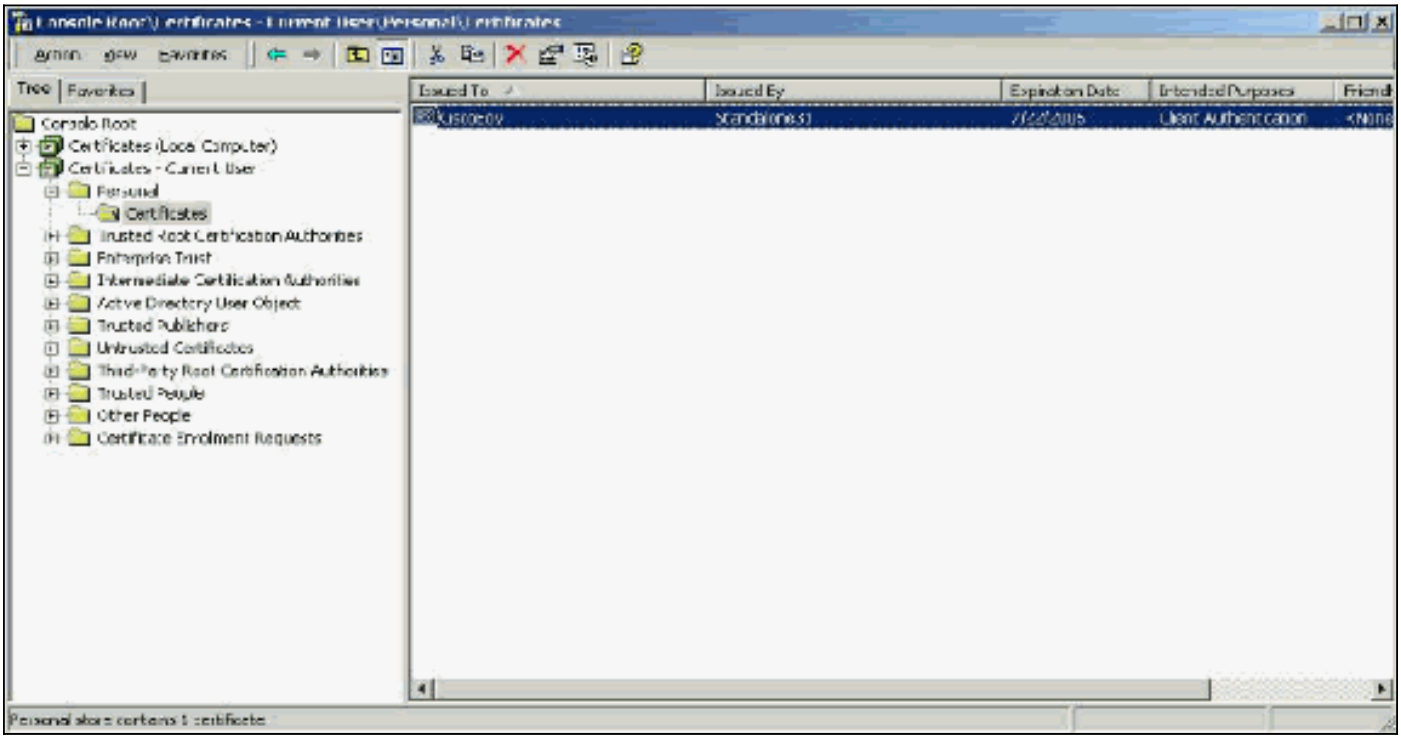
使用者端憑證

「客戶端證書」用於在EAP-TLS中正面標識使用者。它們在構建TLS隧道方面不起作用，不用於加密。通過三種方式之一完成陽性識別：

- **CN（或名稱）Comparison** — 將證書中的CN與資料庫中的使用者名稱進行比較。有關此比較型別的更多資訊包含在證書的Subject欄位的描述中。
- **SAN Comparison** — 將證書中的SAN與資料庫中的使用者名稱進行比較。僅從ACS 3.2開始支援此比較。有關此比較型別的更多資訊包含在證書的「使用者可選名稱」欄位的描述中。
- **Binary Comparison** — 將證書與資料庫中儲存的證書的二進位制副本進行比較（只有AD和LDAP可以做到這一點）。 如果使用證書二進位制比較，必須以二進位制格式儲存使用者證書。此外，對於通用LDAP和Active Directory，儲存證書的屬性必須是名為「usercertificate」的標準LDAP屬性。

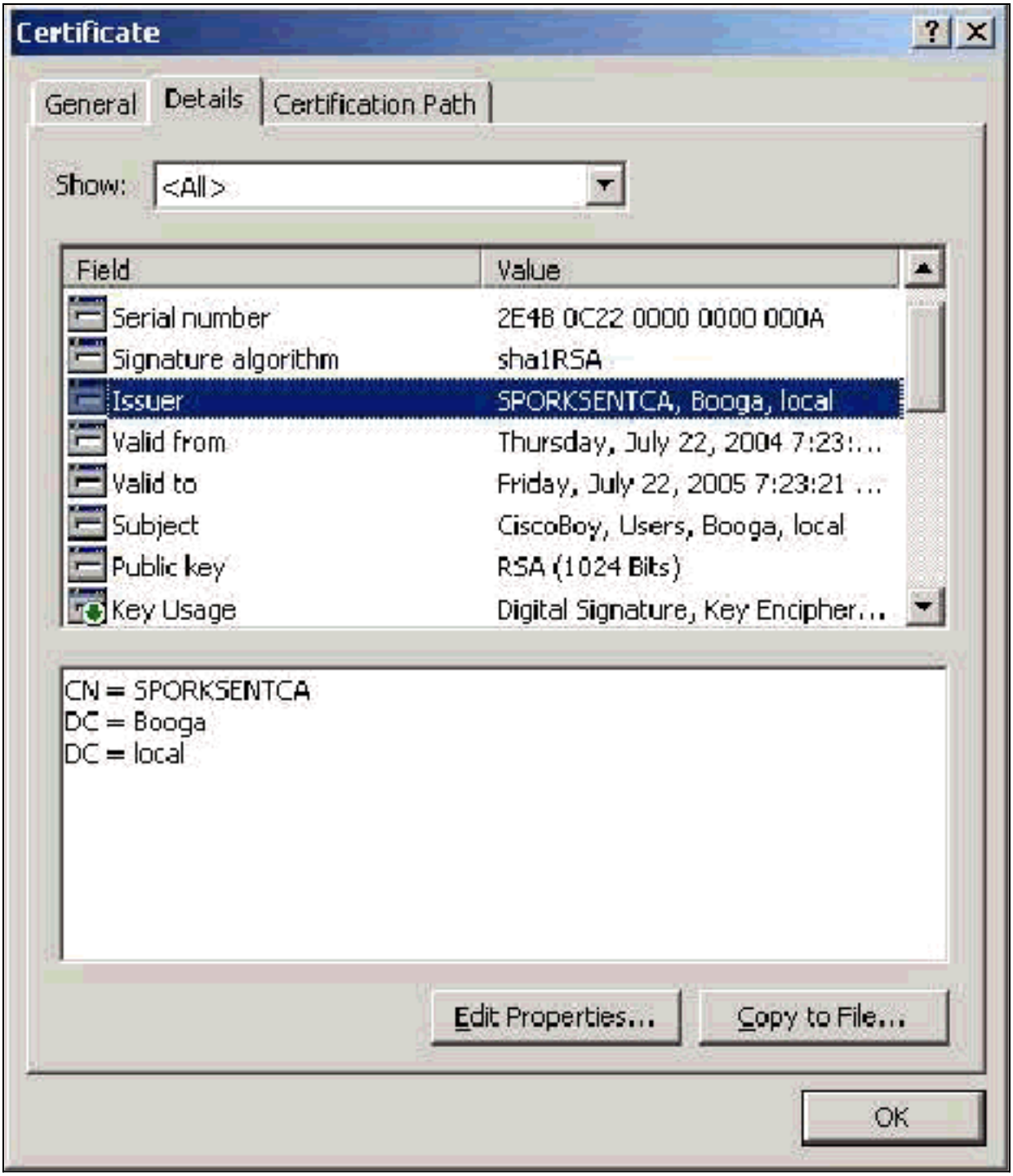
無論使用哪種比較方法，相應欄位（CN或SAN）中的資訊都必須與資料庫用於身份驗證的名稱相匹配。AD在混合模式下使用NetBios名稱進行身份驗證，在本機模式下使用UPN。

本節討論使用Microsoft證書服務生成客戶端證書。EAP-TLS需要唯一的客戶端證書才能對每個使用者進行身份驗證。必須在每台電腦上為每個使用者安裝證書。正確安裝後，憑證位於**Certificates - Current User > Personal > Certificates**資料夾中，如本範例視窗所示。



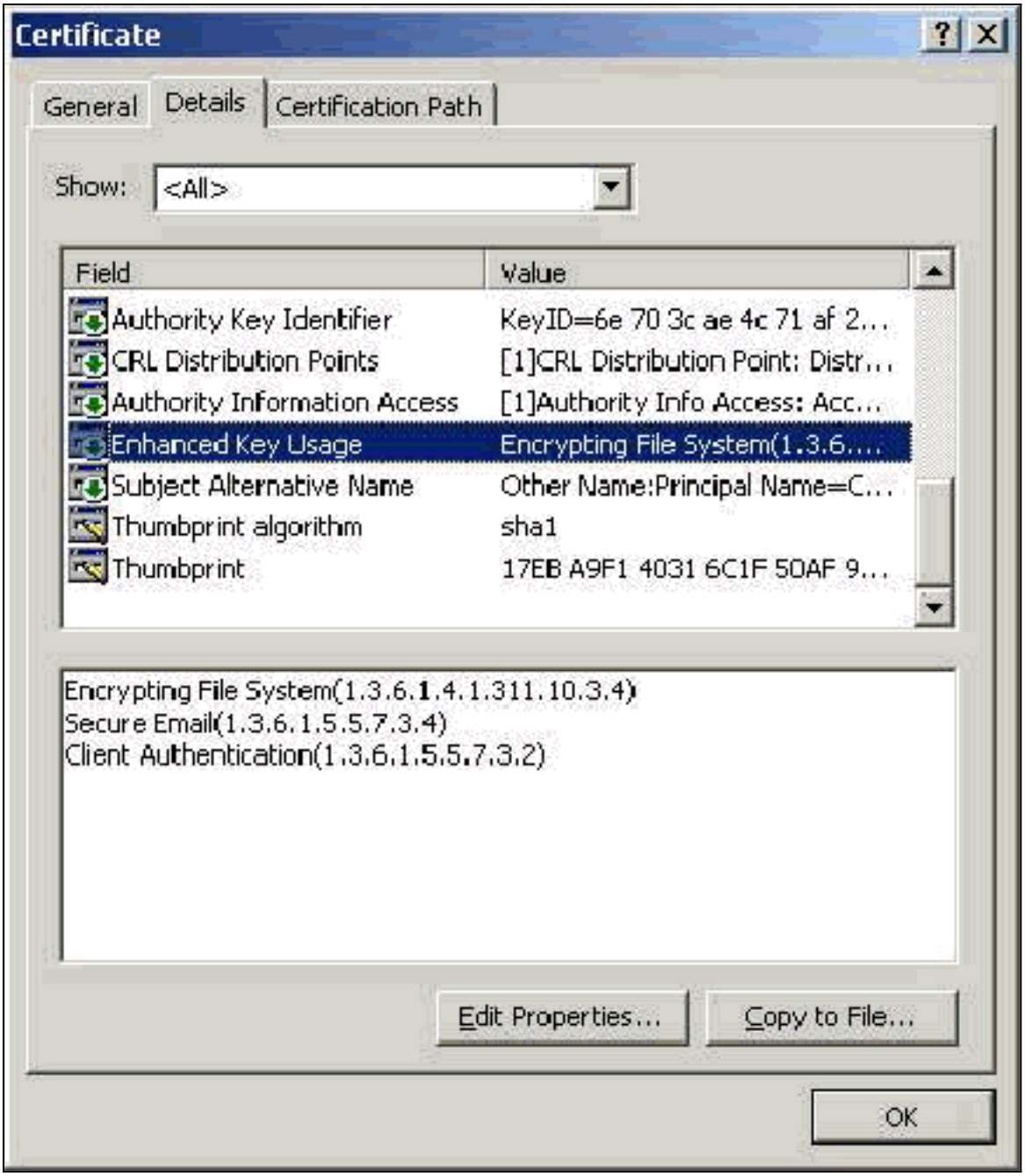
頒發者欄位

Issuer欄位標識削減證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。這將使用CA的名稱填充。



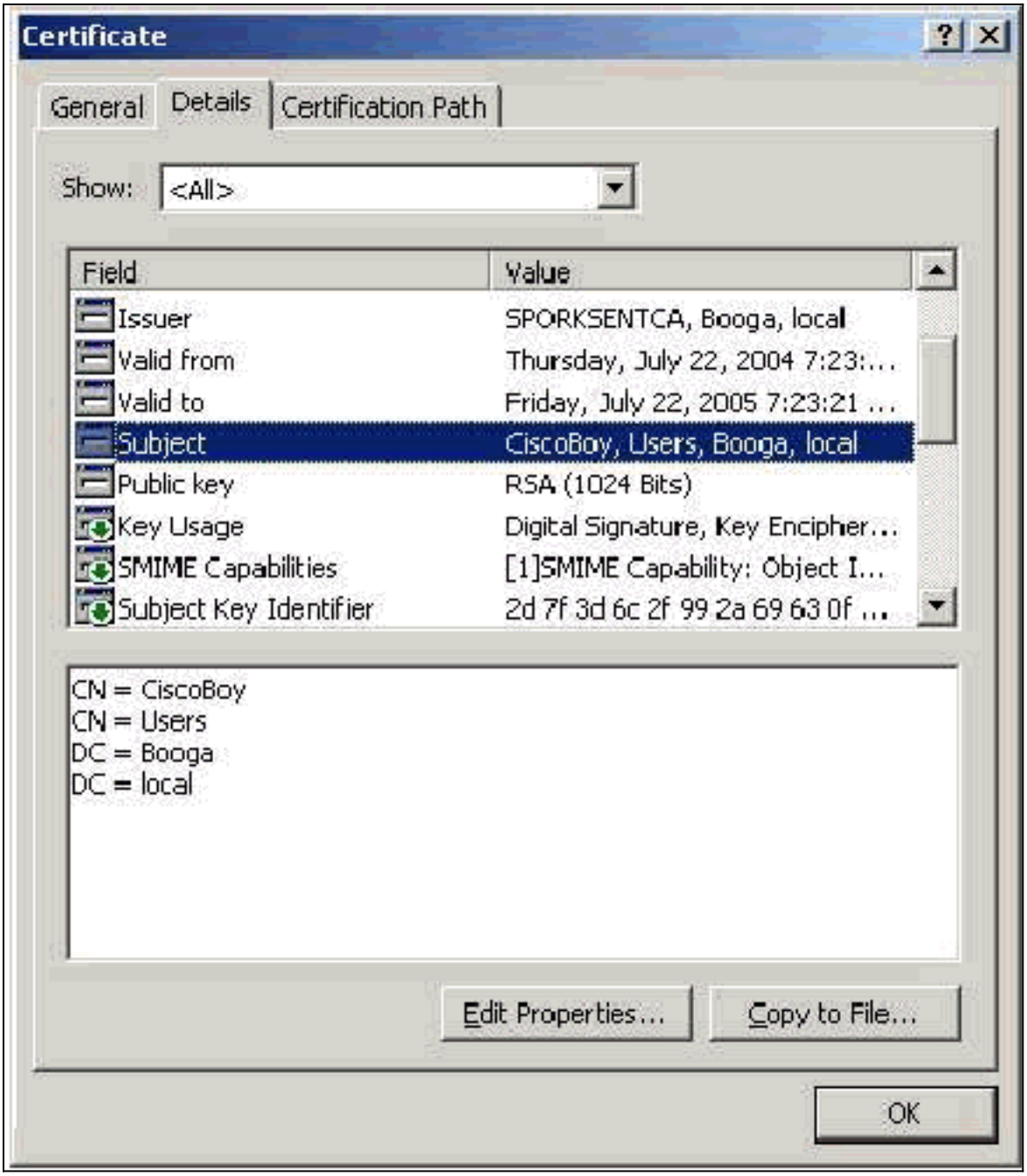
增強型金鑰使用欄位

Enhanced Key Usage欄位會識別憑證的預期用途，並需要包含使用者端驗證。當您使用Microsoft的PEAP和EAP-TLS請求方時，此欄位為必填欄位。使用Microsoft證書服務時，當您從「目標用途」下拉選單中選擇**Client Authentication Certificate**時，會在獨立CA中配置此服務；當您從「證書模板」下拉選單中選擇**User**時，會在企業CA中配置此服務。如果您使用具有Microsoft證書服務的CSR來請求證書，則您沒有選擇使用獨立CA指定目標用途。因此，不存在EKU欄位。使用企業CA，您將看到「目標用途」下拉選單。某些CA不使用EKU欄位建立證書。當您使用Microsoft EAP請求方時，它們毫無用處。



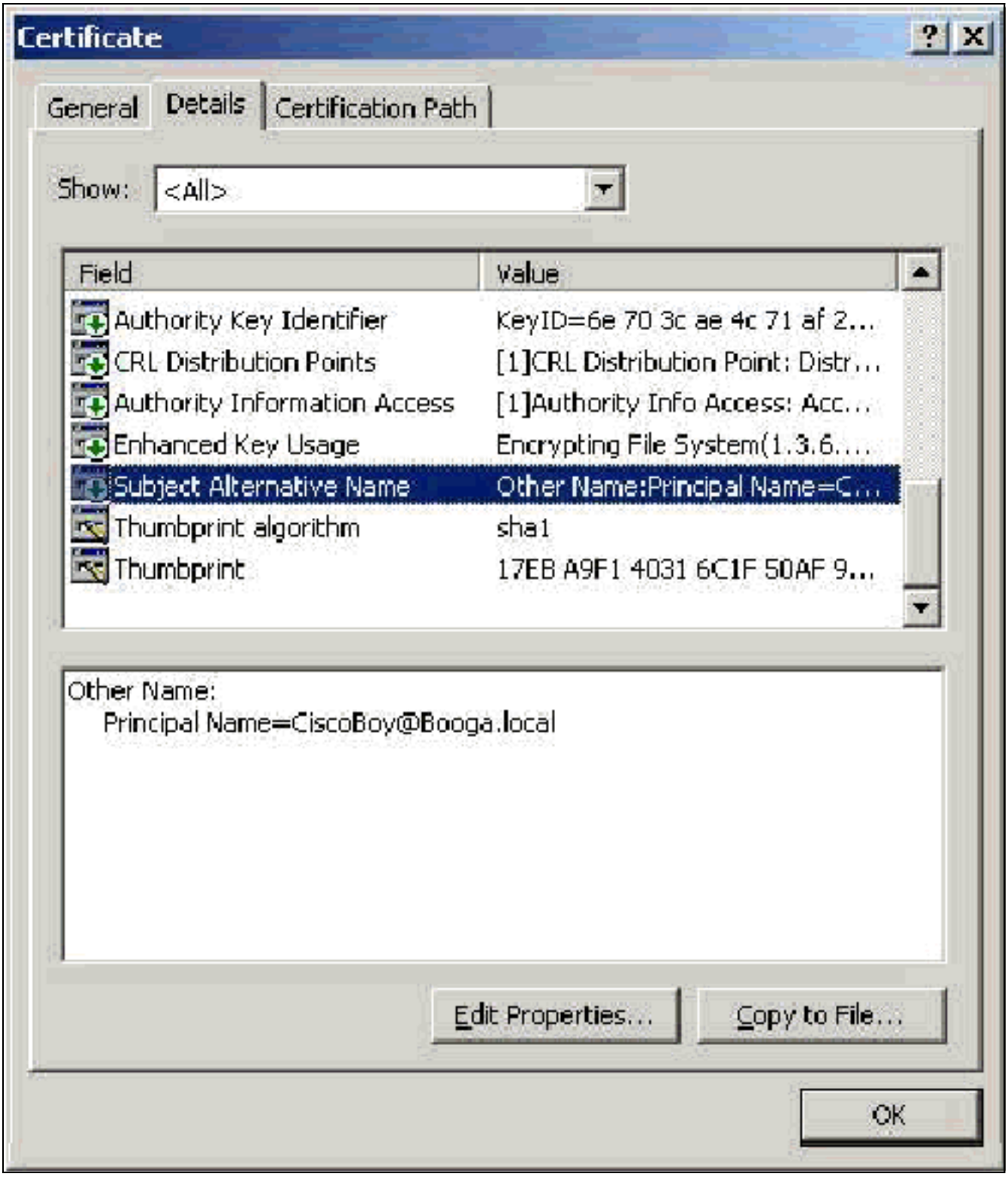
主題欄位

此欄位用於CN比較。將列出的第一個CN與資料庫進行比較以查詢匹配項。如果找到匹配項，則身份驗證成功。如果您使用獨立CA，則CN中會填充您在證書提交表單中Name欄位輸入的任何內容。如果您使用企業CA，則CN會自動填充在Active Directory使用者和電腦控制檯中列出的帳戶名稱（這不一定與UPN或NetBios名稱匹配）。



主題替代名稱欄位

Subject Alternative Name欄位用於SAN比較。將列出的SAN與資料庫進行比較以查詢匹配項。如果找到匹配項，則身份驗證成功。如果您使用企業CA，則SAN會自動填充Active Directory登入名@domain(UPN)。 獨立CA不包括SAN欄位，因此不能使用SAN比較。

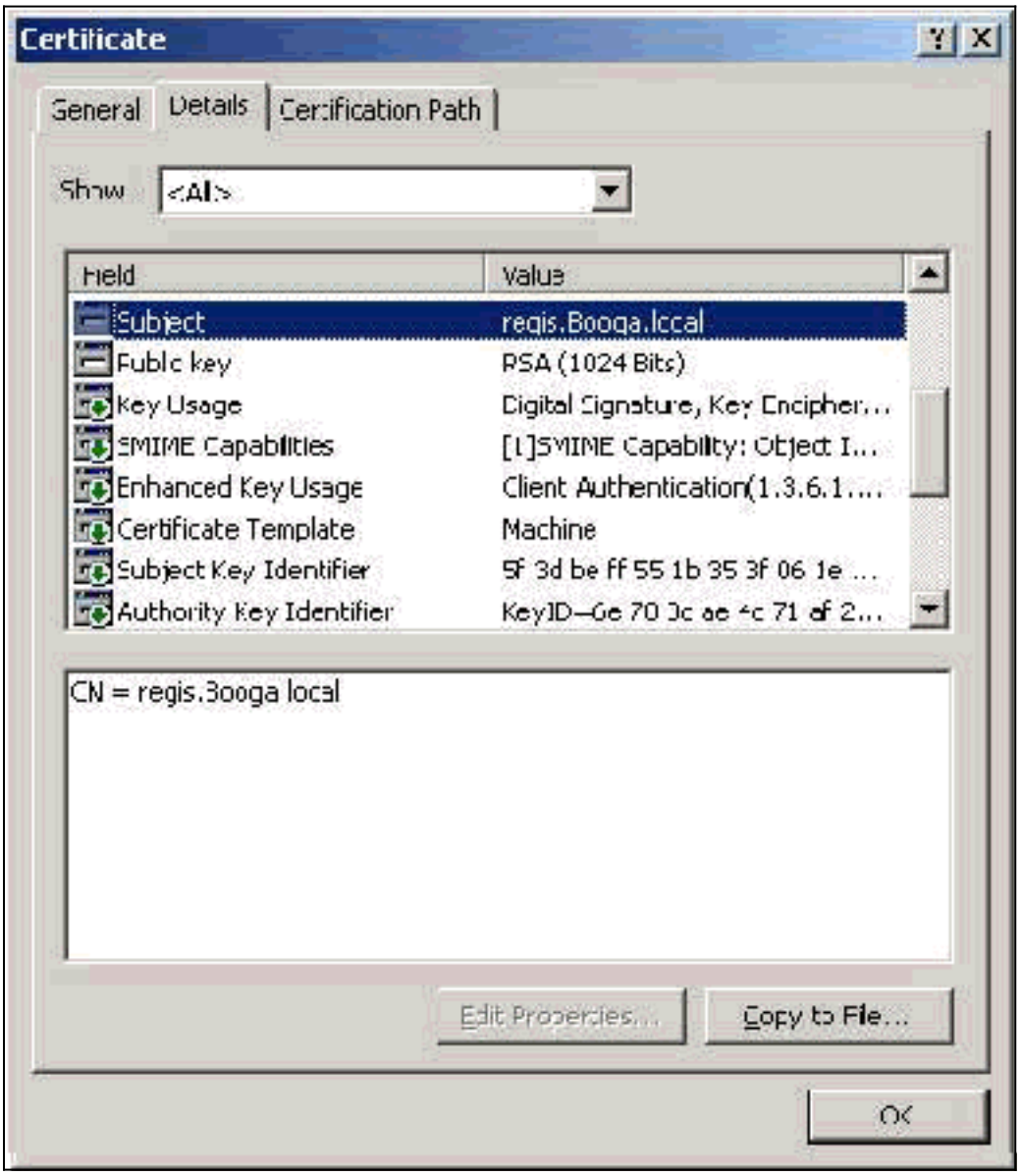


電腦證書

使用電腦身份驗證時，電腦證書在EAP-TLS中使用，以主動識別電腦。只有當您配置Microsoft Enterprise CA進行證書自動註冊並將電腦加入域時，才能訪問這些證書。當您使用電腦的Active Directory憑證並將其安裝在本地電腦儲存中時，將自動建立證書。配置自動註冊之前已是域成員的電腦將在下次Windows重新啟動時收到證書。電腦證書安裝在證書（本地電腦）MMC管理單元的**證書(Certificates)>個人>證書**資料夾中，與伺服器證書一樣。由於無法匯出私鑰，因此無法在任何其他電腦上安裝這些證書。

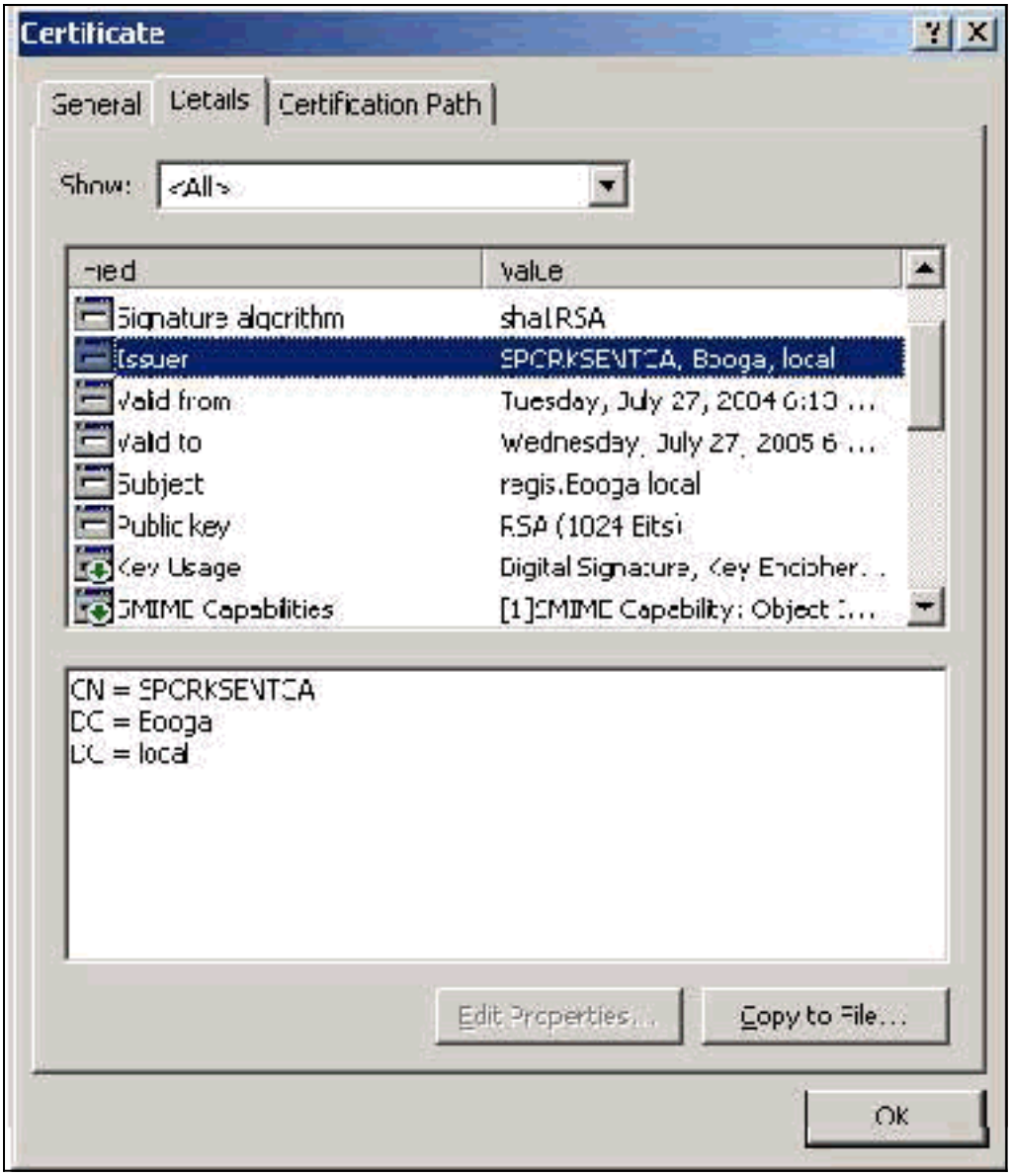
主題和SAN欄位

Subject和SAN欄位標識電腦。該值由電腦的完全限定名稱填充，並用於確定證書的「常規」頁籤中的「頒發給」欄位，對於「主題」和「SAN」欄位都相同。



頒發者欄位

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將用CA的名稱填充。



附錄A — 通用證書擴展

.csr — 這實際上不是證書，而是證書簽名請求。它是採用以下格式的純文字檔案檔案：

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

.pvk — 此擴展表示私鑰，儘管此擴展不保證內容實際是私鑰。內容必須是採用以下格式的純文字檔案：

```
-----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 — 這是一個表示證書的通用擴展。伺服器、根CA和中間CA證書可以採用此格式。它通常是一個副檔名的純文字檔案檔案，您可以根據需要進行更改，可以是DER格式或Base 64格式。可以將此格式匯入Windows證書儲存區。

.pem — 此副檔名為Privacy Enhanced Mail。此擴展通常用於UNIX、Linux、BSD等。它通常用於伺服器證書和私鑰，通常是一個副檔名為.pem到.cer的純文字檔案檔案，您可以根據需要對其進行更改，以便將其匯入到Windows證書儲存區。

.cer和.pem檔案的內部內容通常類似於以下輸出：

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

.pfx — 此副檔名表示個人資訊交換。此格式是一種方法，可用於將證書捆綁到單個檔案中。例如，您可以將伺服器證書及其關聯的私鑰和根CA證書捆綁到一個檔案中，並輕鬆將該檔案匯入適當的Windows證書儲存區。最常用於伺服器和客戶端證書。很遺憾，如果包含根CA證書，則根CA證書始終安裝在當前使用者儲存而不是本地電腦儲存中，即使指定了本地電腦儲存進行安裝。

.p12 -通常只有客戶端證書才會顯示此格式。可以將此格式匯入Windows證書儲存區。

.p7b — 這是將多個證書儲存在一個檔案中的另一種格式。可以將此格式匯入Windows證書儲存區。

附錄B — 證書格式轉換

在大多數情況下，當您更改副檔名（例如，從.pem更改為.cer）時會發生證書轉換，因為證書通常採用純文字檔案格式。有時，證書不是純文字檔案格式，您必須使用OpenSSL 等工具對其進行轉換。例如，ACS解決方案引擎無法安裝.pfx格式的證書。因此，必須將憑證和私鑰轉換為可用格式。以下是OpenSSL的基本命令語法：

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

系統將提示您輸入匯入密碼和PEM密碼短語。這些密碼必須相同，並且是在匯出.pfx時指定的私鑰密碼。輸出是一個.pem檔案，該檔案包含.pfx中的所有證書和私鑰。此檔案可在ACS中同時稱為證書和私鑰檔案，安裝時不會出現問題。

附錄C — 證書有效期

憑證僅在其有效期期間內可用。根CA證書的有效期是在建立根CA時確定的，可以變化。中間CA證書的有效期在建立CA時確定，並且不能超過其從屬的根CA的有效期。使用Microsoft證書服務，伺服器、客戶端和電腦證書的有效期將自動設定為一年。只有當您按照Microsoft知識庫文章254632對Windows登錄檔進行駭客攻擊時，才能更改此值，並且此值不能超過根CA的有效期。ACS生成的自簽名證書的有效期始終為一年，在當前版本中無法更改。

相關資訊

- RADIUS 支援頁面
- 要求建議 (RFC)
- 技術支援 - Cisco Systems