EAP バージョン 1.01 の証明書のガイド

内容

概要

このドキュメントでは、Extensible Authentication Protocol（EAP）のさまざまな方式に関連する各証明書のタイプ、形式、および要件をわかりやすく説明します。 このドキュメントで紹介する EAP に関連する証明書のタイプには、サーバ、ルート CA、中間 CA、クライアント、マシンの 5 つがあります。これらの証明書にはさまざまな形式が用意されており、各証明書に関する要件は EAP の実施要件に応じて異なります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

サーバ証明書

サーバ証明書は RADIUS サーバにインストールするもので、EAP における第 1 の目的は、認証情報を保護するための暗号化した Transport Layer Security（TLS）トンネルを作成することです。EAP-MSCHAPv2 を使用する場合、サーバ証明書は、第 2 の役割として、RADIUS サーバが信頼できる認証用のエンティティであるかどうかを識別します。この 2 つめの役割は、Enhanced Key Usage（EKU）フィールドを使用して実現されます。EKU フィールドは、証明書が有効なサーバ認証であるかどうか、およびこの証明書を発行したルート CA が信頼できるルート CA であるかどうかを識別します。これを実施するには、ルート CA 証明書が必要です。Cisco Secure ACS では、証明書が、Base64 エンコードまたは DER エンコードの X.509 v3 バイナリ形式である必要があります。

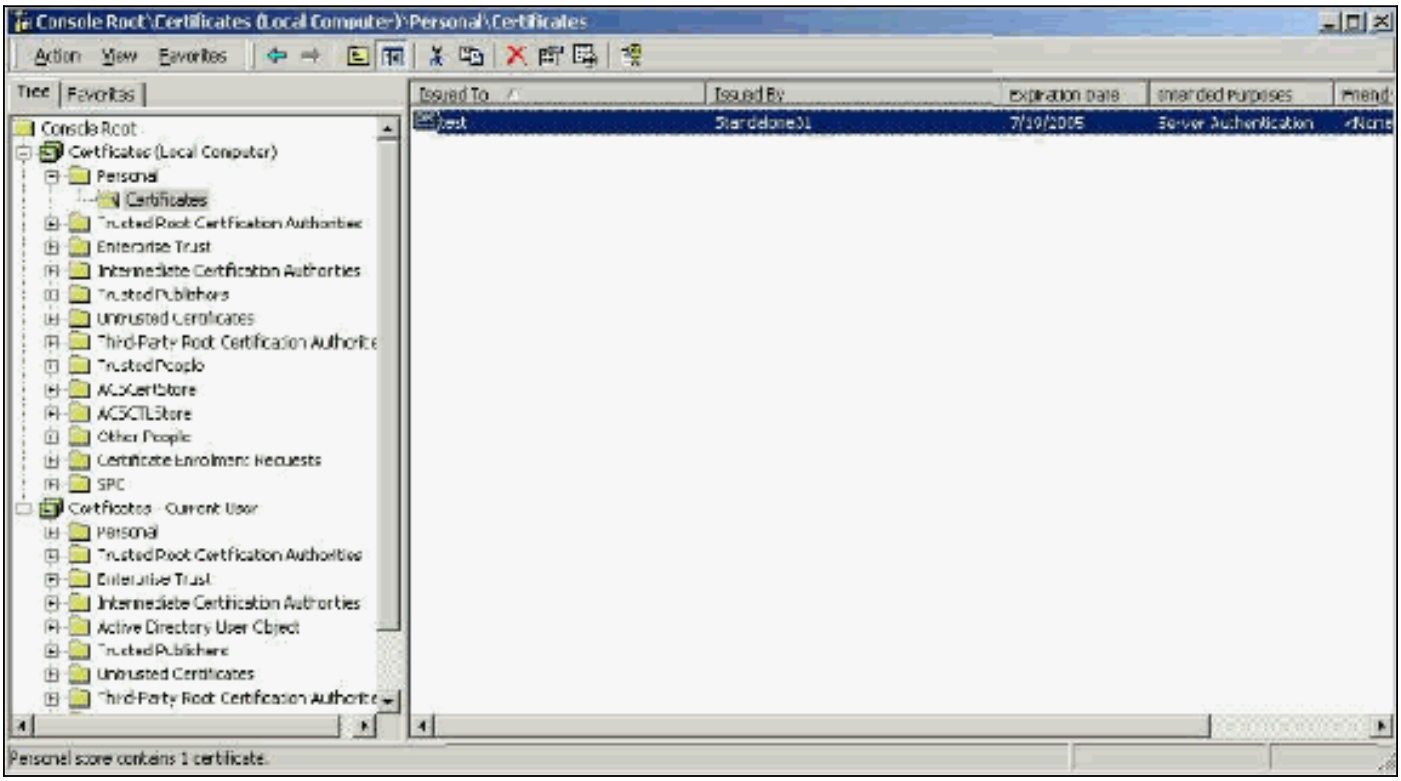
この証明書は、ACS の Certificate Signing Request（CSR; 証明書署名要求）を使用して作成できます。この CSR は CA に送信されます。また、証明書を（Microsoft 証明書サービスのような）社内 CA 証明書の作成フォームを使用して、発行することもできます。サーバ証明書は 1024 より大きい鍵サイズで作成することもできますが、1024 より大きい鍵は PEAP で正しく機能しませんので、注意してください。認証が渡されても、クライアントは続行できません。

証明書の作成に CSR を使用する場合、証明書は .cer、.pem、または .txt 形式で作成されます。まれなケースですが、拡張子が付かないで作成される場合もあります。証明書は、必ず、プレーン テキスト ファイルで、必要に応じて変更できる拡張子の付いたものにしてください（ACS アプライアンスでは、.cer または .pem の拡張子を使用します）。 また、CSR を使用する場合、証明書の秘密鍵は、指定したパスに別のファイルとして作成されます。このファイルは、拡張子が付いている場合もあれば、付いていない場合もあり、パスワードが付いています（このパスワードは、ACS にインストールする場合に必要です）。 拡張子の種類に関係なく、必ず、ファイルはプレーン テキスト ファイルで、必要に応じて変更できる拡張子が付いたものにしてください（ACS アプライアンスでは、.pvk または .pem の拡張子を使用します）。 秘密鍵のパスが指定されていない場合、ACS では、C:\Program Files\CiscoSecure ACS vx.x\CSAdmin\Logs ディレクトリに秘密鍵が保存され、証明書のインストール時に秘密鍵のパスを指定しなかった場合は、このディレクトリが検索されます。

証明書の作成に Microsoft 証明書サービスの発行フォームを使用する場合は、ACS に証明書をインストールできるように、必ずエクスポート可能な鍵としてマークしてください。この方法で証明書を作成すると、インストール処理が非常に簡単になります。作成した証明書は、証明書サービスの Web インターフェイスから Windows の適切なストアに直接インストールできます。さらに後で、CN を参照に使用して、ストレージから ACS にインストールできます。また、ローカル コンピュータのストアにインストールされている証明書は、Windows ストレージからエクスポー

トして、別のコンピュータに簡単にインストールすることもできます。このタイプの証明書をエクスポートする場合は、鍵がエクスポートとマークされている必要があります。また、パスワードが付加されている必要があります。すると、秘密鍵とサーバ証明書を含んだ証明書が、.pfx 形式で作成されます。

Windows 証明書ストアに正しくインストールされたサーバ証明書は、このサンプル ウィンドウに示すように、[Certificates (Local Computer)] > [Personal] > [Certificates] **フォルダに表示される必要があります。**



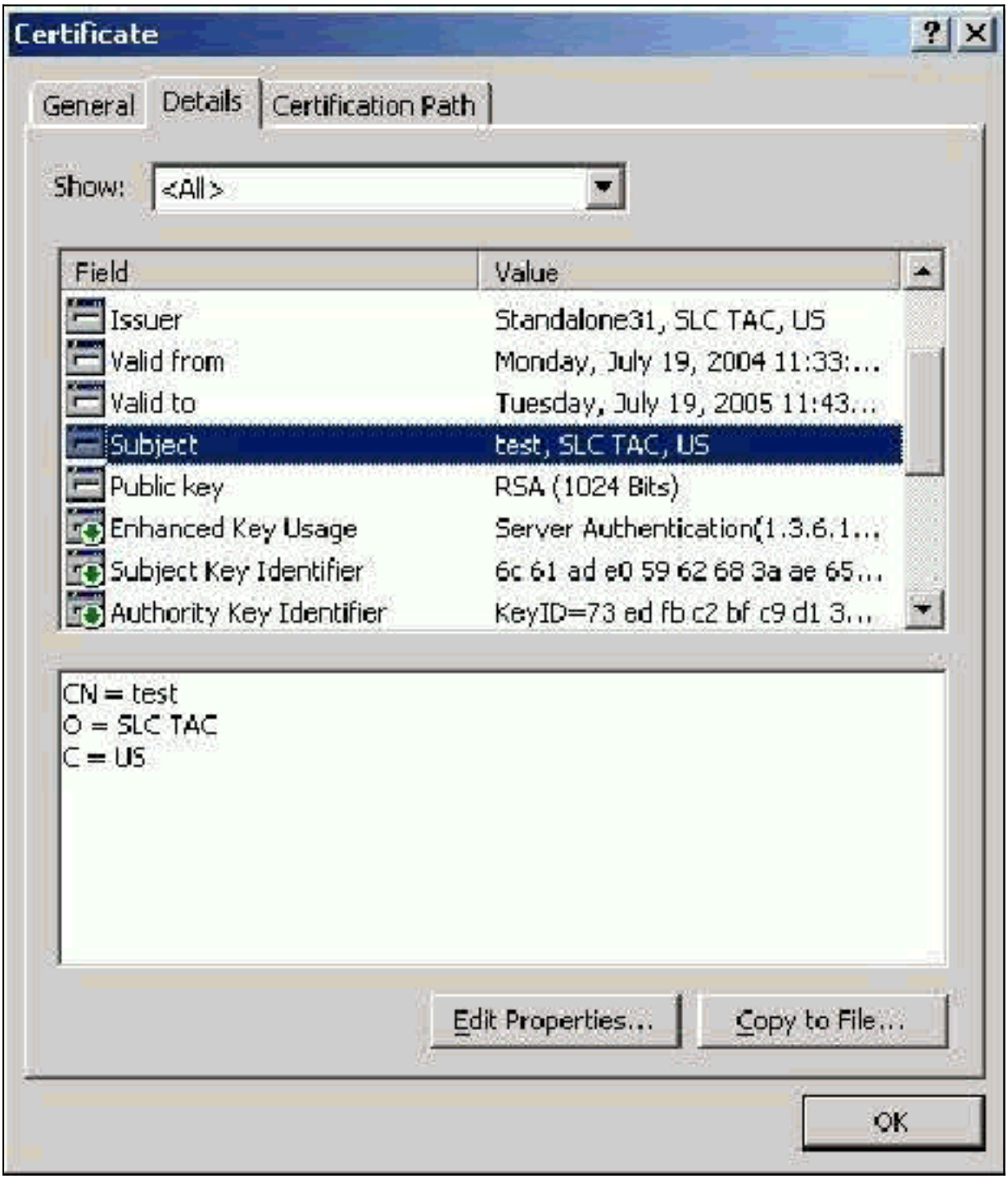
自己署名証明書とは、作成にルート CA および中間 CA が関与していない証明書です。この証明書では、ルート CA 証明書のように、subject フィールドと issuer フィールドに同じ値が含まれています。ほとんどの自己署名証明書では、X.509 v1 形式を使用します。そのため、このような証明書は ACS では使用できません。ただし、ACS のバージョン 3.3 では、EAP-TLS および PEAP で使用可能な独自の自己署名証明書の作成機能が用意されています。PEAP および EAP-TLS との互換性を保つため、1024 より大きい鍵サイズを使用しないでください。自己署名証明書を使用する場合は、その証明書がルート CA 証明書としても機能するため、Microsoft EAP サプリカントを使用するときに、クライアントの [Certificates (Local Computer)] > [Trusted Root Certification Authorities] > [Certificates] **フォルダにインストールする必要があります。**自己署名証明書は、自動的にサーバの「信頼されたルート証明書」ストアにインストールされます。ただし、ACS の Certificate Setup の Certificate Trust List でも信頼されている必要があります。詳細については、「ルート CA 証明書」のセクションを参照してください。

自己署名証明書は、Microsoft EAP サプリカントを使用している場合には、サーバ証明書を検証するときのルート CA 証明書としても使用されてしまいます。また、有効期間をデフォルトの 1 年から延長できませんので、この証明書は、EAP で従来の CA が使用できるようになるまでの一時的な対策としてだけ使用することをお勧めします。

Subject フィールド

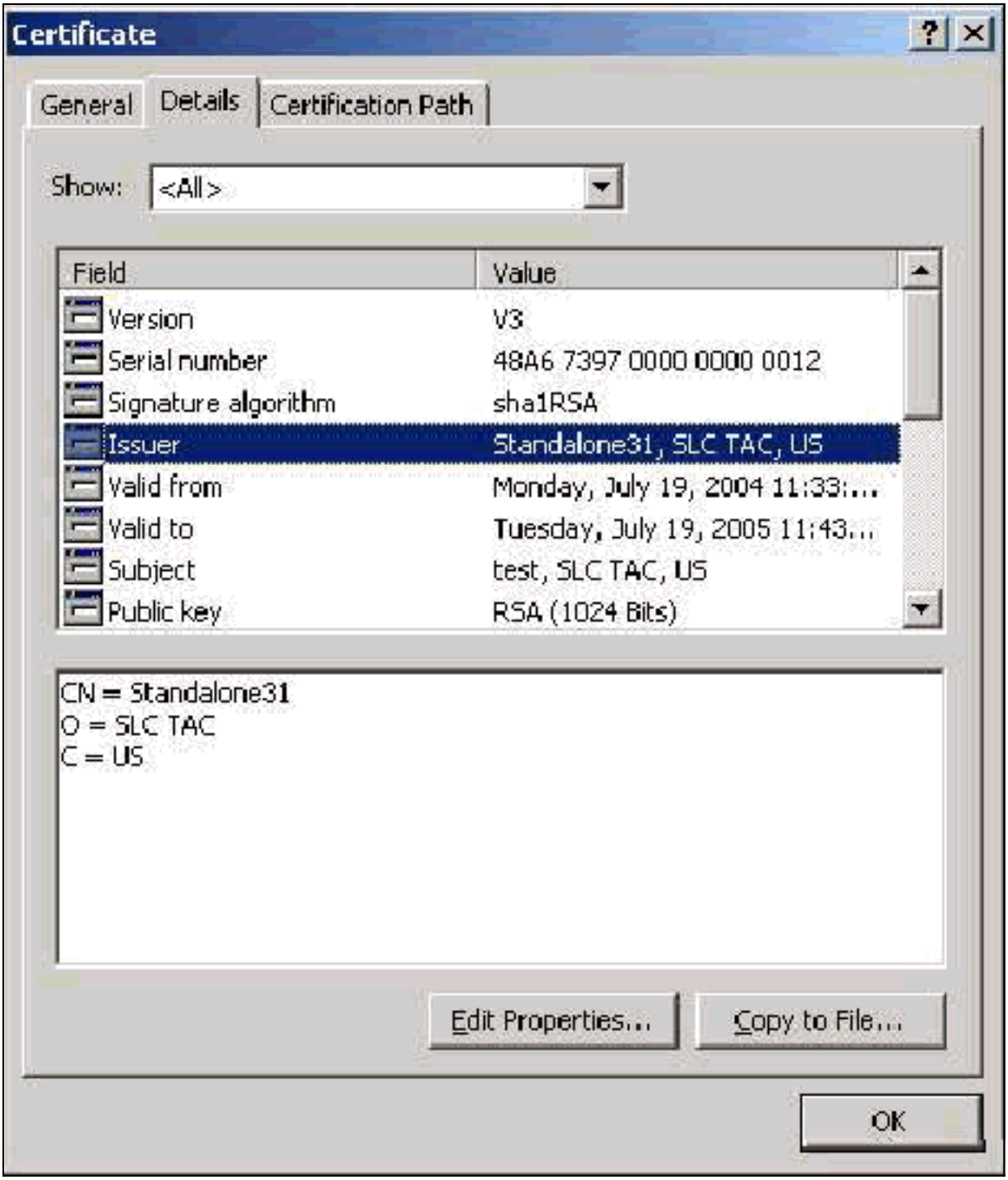
Subject フィールドは、証明書を識別します。CN の値は、証明書の General タブの Issued to フィールドを設定するのに使用します。この値には、ACS の CSR ダイアログの Certificate subject フィールドで入力した情報、または Microsoft 証明書サービスの Name フィールドの情報が入力

されます。CN の値は、ストレージの証明書をインストールするオプションが使用された場合に、ローカル マシンの証明書ストアから使用する証明書を ACS に通知するために使用します。



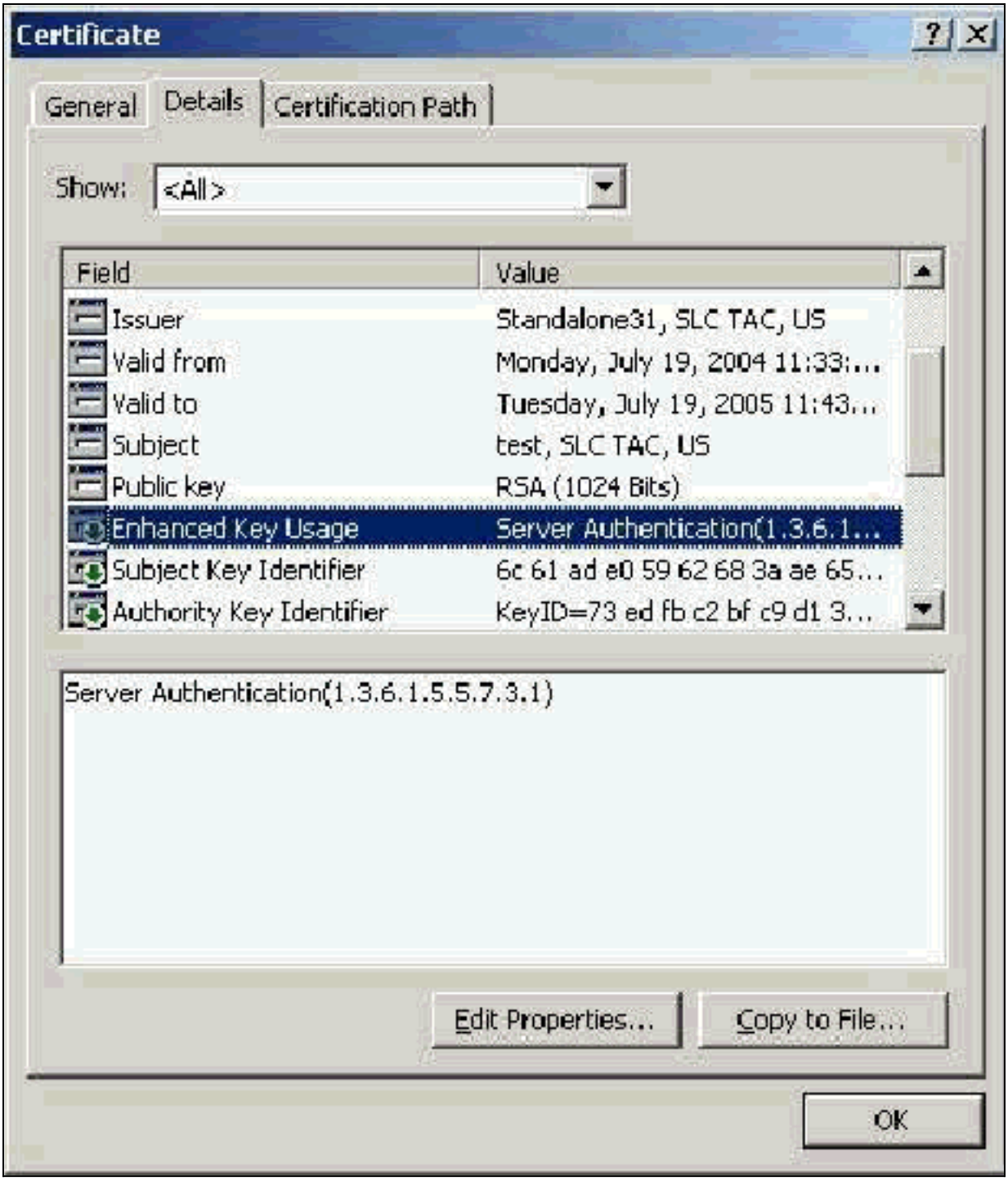
Issuer フィールド

Issuer フィールドは、証明書を発行した CA を識別します。この値は、証明書の General タブの Issued by フィールドの値を設定するのに使用します。値には、CA の名前が入力されています。



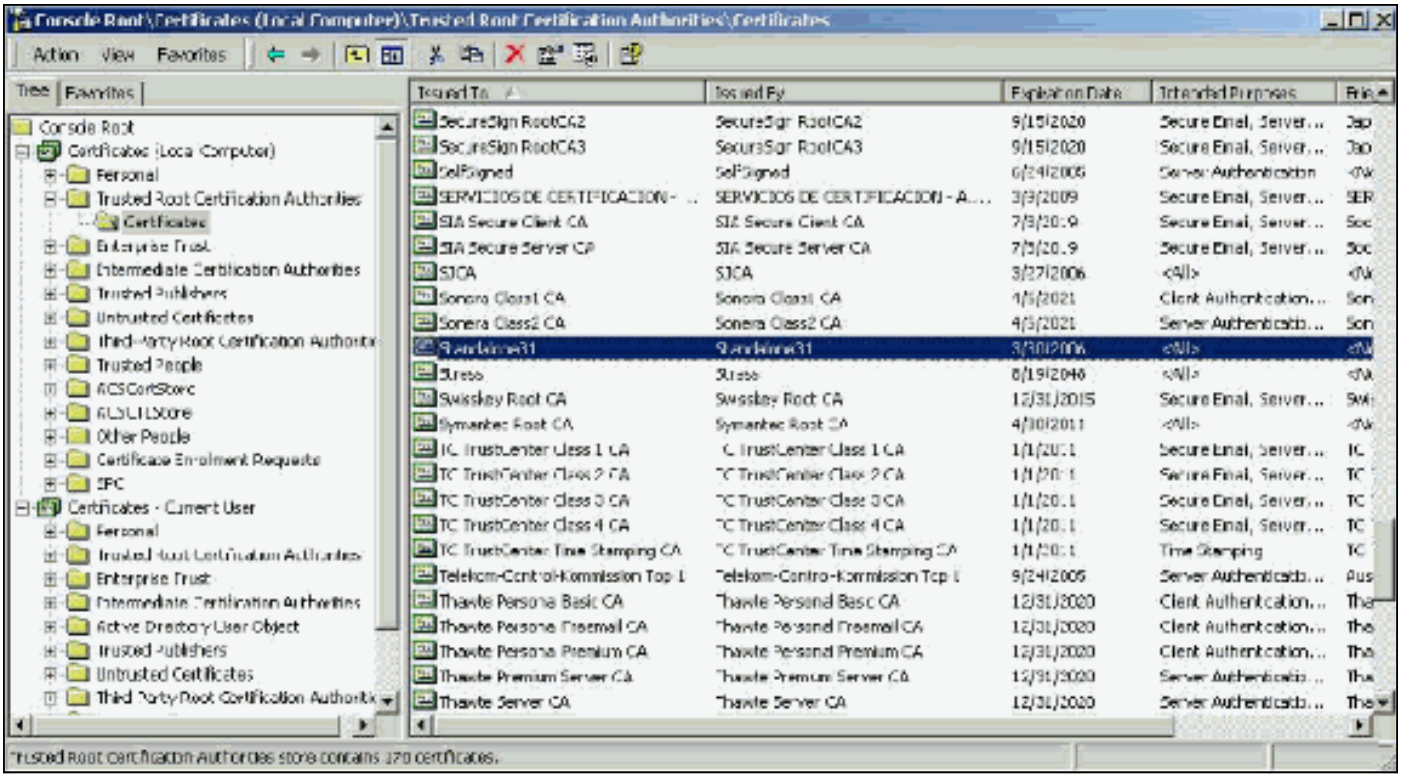
Enhanced Key Usage フィールド

Enhanced Key Usage フィールドは、証明書の使用目的を識別するもので、「Server Authentication」と表示されている必要があります。 PEAP および EAP-TLS で Microsoft サプリカントを使用する場合、このフィールドは必須です。Microsoft 証明書サービスを使用する場合、スタンドアロン CA では Intended Purpose ドロップダウンで Server Authentication Certificate を選択すると、エンタープライズ CA では Certificate Template ドロップダウンで Web Server を選択すると、このフィールドが設定されます。CSR と Microsoft 証明書サービスを使用して証明書を要求する場合、スタンドアロン CA で Intended Purpose を指定するオプションはありません。そのため、EKU フィールドは存在しません。エンタープライズ CA の場合は、Intended Purpose ドロップダウンが使用できます。CA によっては、EKU フィールドをともなう証明書を作成していない場合がありますが、Microsoft EAP サプリカントを使用している場合、このような証明書は使用できません。



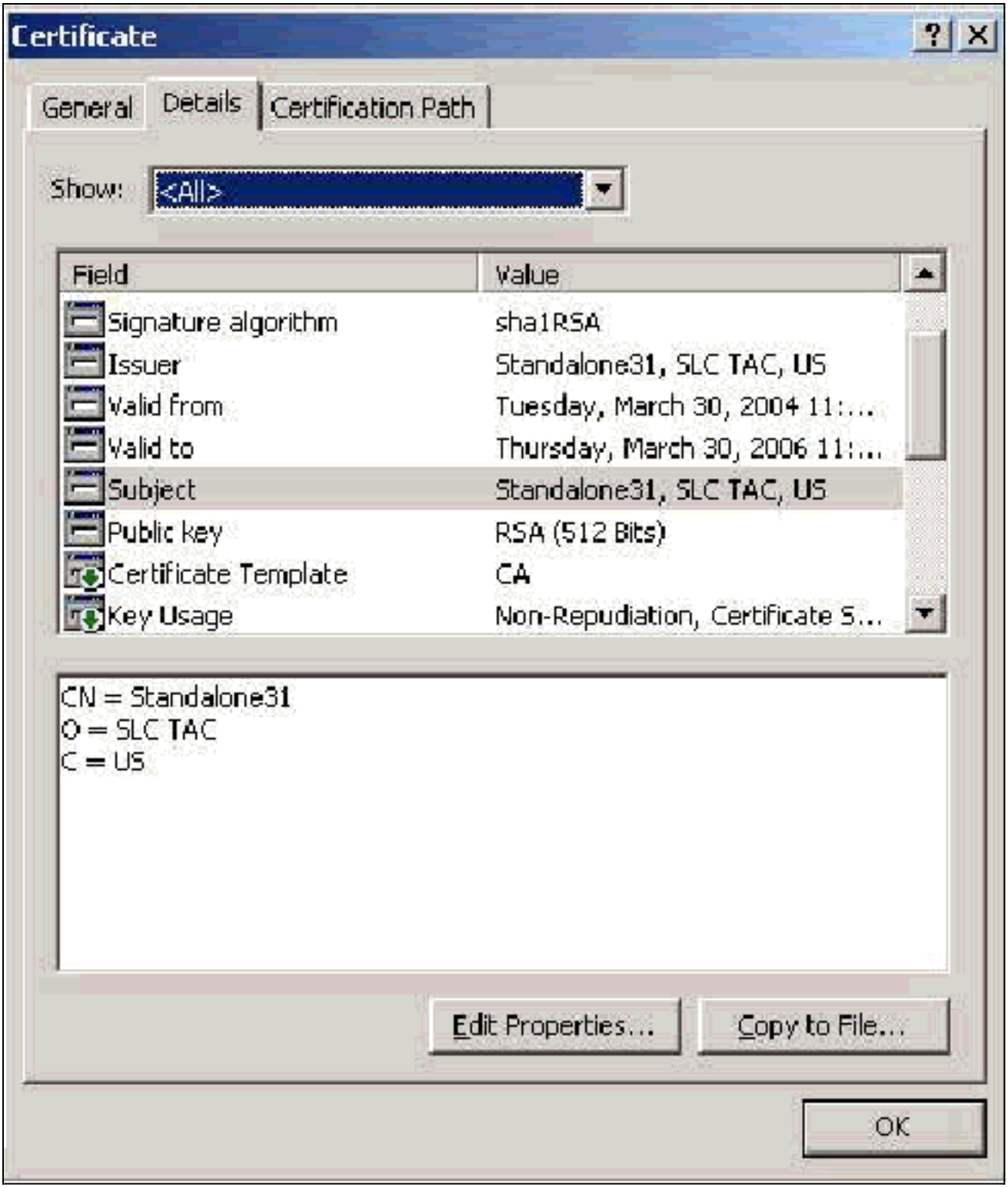
ルート CA 証明書

ルート CA 証明書の目的の一つは、サーバ証明書（および中間 CA 証明書（該当する場合））が、ACS および Windows EAP-MSCHAPv2 サプリカントにとって信頼できる証明書であるかどうかを識別することです。この証明書は、ACS サーバと（EAP-MSCHAPv2 の場合は）クライアント コンピュータの Windows の「信頼されたルート証明機関」ストアに保存しておく必要があります。ほとんどのサード パーティのルート CA 証明書は、Windows と一緒にインストールされるため、これに関する作業はほとんど必要ありません。Microsoft 証明書サービスを使用していて、証明書のサーバが ACS と同じマシンである場合、ルート CA 証明書は自動的にインストールされます。ルート CA 証明書が Windows の「信頼されたルート証明機関」ストアに見つからない場合は、お客様の CA から入手してインストールする必要があります。Windows 証明書ストアに正しくインストールされたルート CA 証明書は、このサンプル ウィンドウに示すように、[Certificates (Local Computer)] > [Trusted Root Certification Authorities] > [Certificates] **フォルダに表示される必要があります。**



Subject フィールドと Issuer フィールド

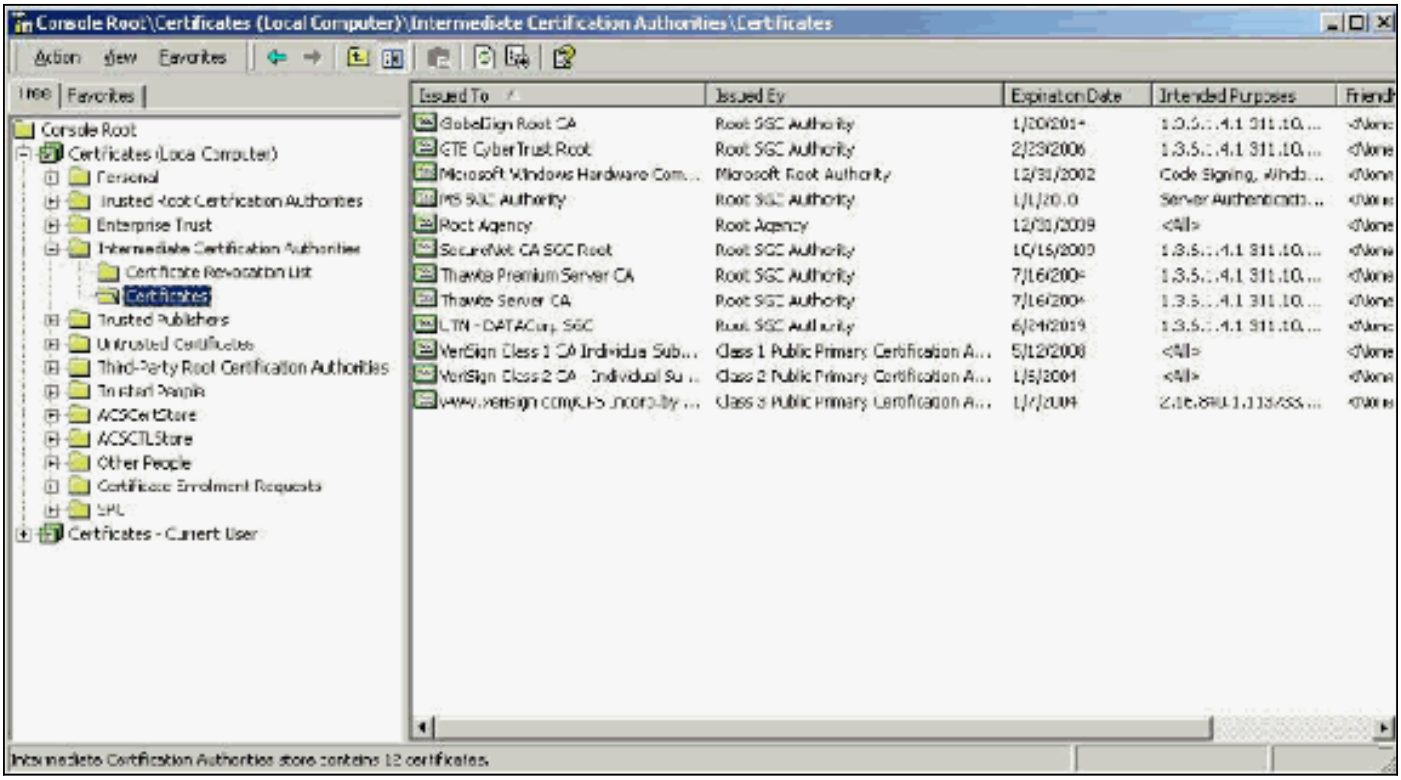
Subject フィールドと Issuer フィールドは、CA を識別するもので、完全に一致している必要があります。これらのフィールドは、証明書の General タブの Issued to フィールドと Issued by フィールドを設定するのに使用します。これらのフィールドには、ルート CA の名前が入力されています。



中間 CA 証明書

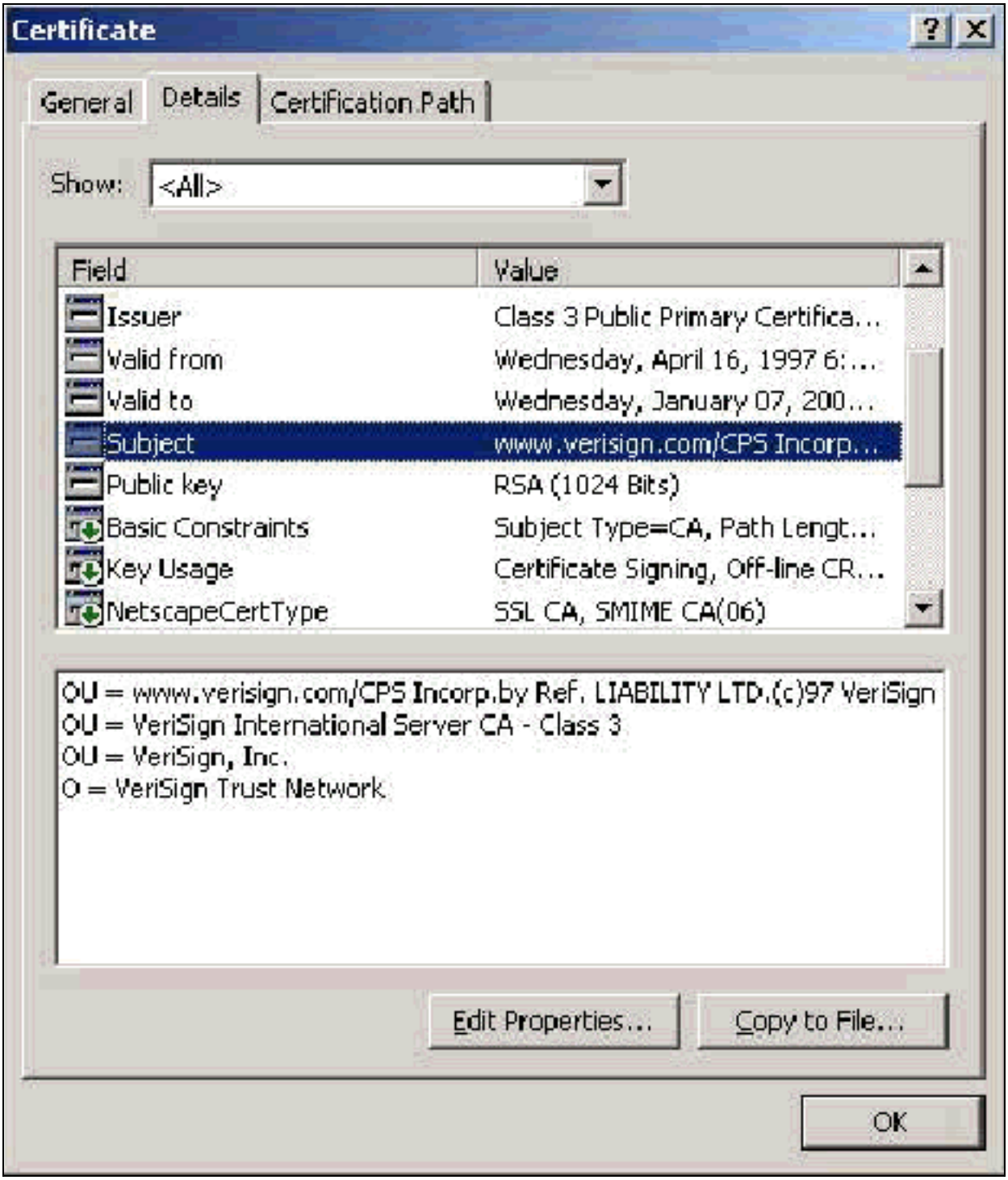
中間 CA 証明書は、ルート CA の下位の CA を識別するのに使用する証明書です。一部のサーバ証明書（Verisign の無線証明書）は、中間 CA を使用して作成されています。中間 CA により発行されたサーバ証明書を使用している場合は、ACS サーバのローカル マシン ストアの「中間証明機関」のエリアに、中間 CA 証明書がインストールされている必要があります。また、クライアントで Microsoft EAP サプリカントを使用している場合は、ACS サーバとクライアントの該当するストアに、中間 CA 証明書を作成したルート CA のルート CA 証明書がインストールされ、信頼のチェーンが確立できるようになっている必要があります。ルート CA 証明書と中間 CA 証明書はいずれも、ACS およびクライアントで信頼されたものとしてマークされている必要があります。ほとんどの中間 CA 証明書は、Windows と一緒にはインストールされないため、通常はベ

ンダーから入手する必要があります。Windows 証明書ストアに正しくインストールされた中間 CA 証明書は、このサンプル ウィンドウに示すように、[Certificates (Local Computer)] > [Intermediate Certification Authorities] > [Certificates] **フォルダに表示される必要があります。**



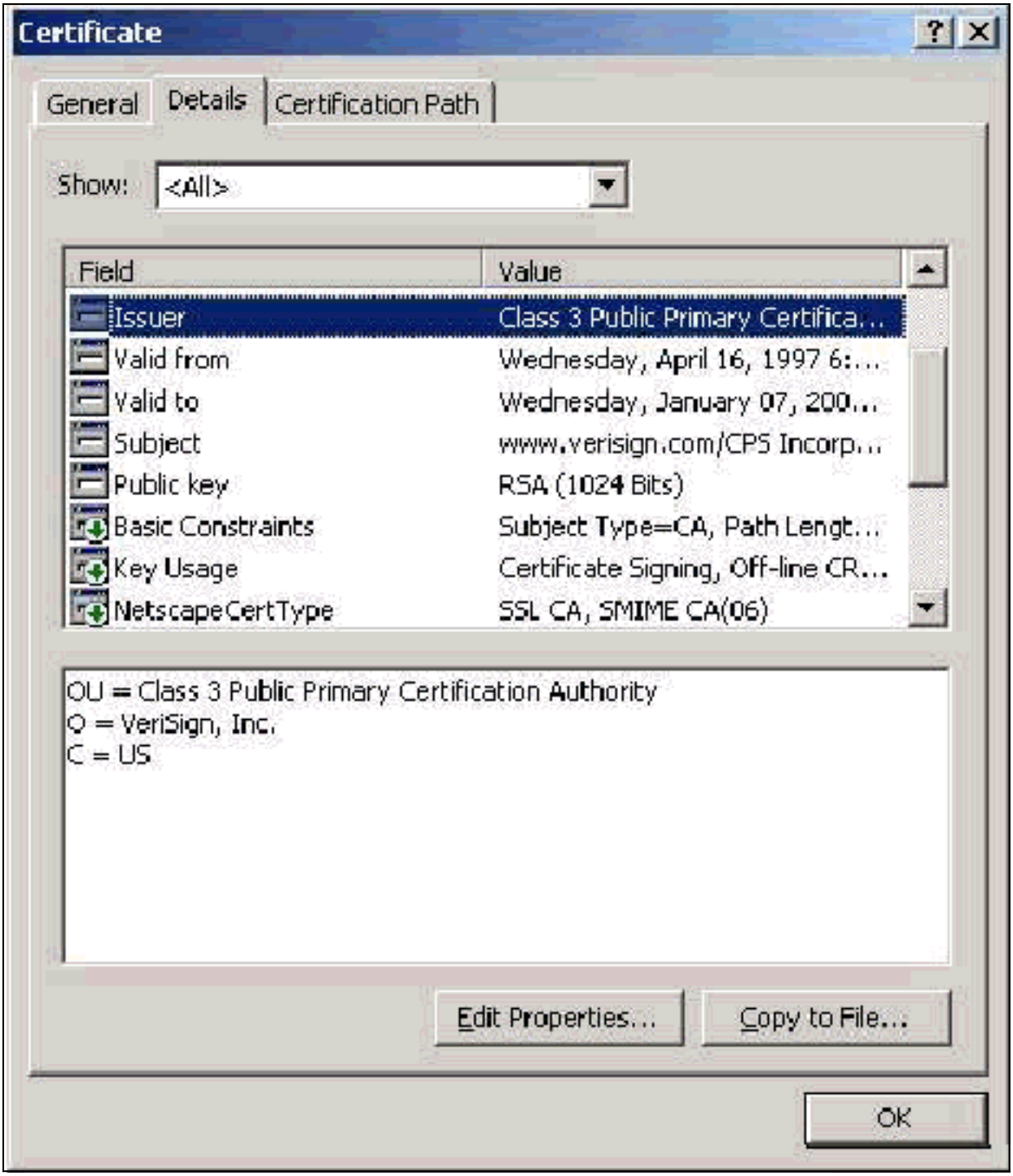
Subject フィールド

Subject フィールドは、中間 CA を識別します。この値は、証明書の General タブの Issued to フィールドを設定するのに使用します。



Issuer フィールド

Issuer フィールドは、証明書を発行した CA を識別します。この値は、証明書の General タブの Issued by フィールドの値を設定するのに使用します。値には、CA の名前が入力されています。



クライアント証明書

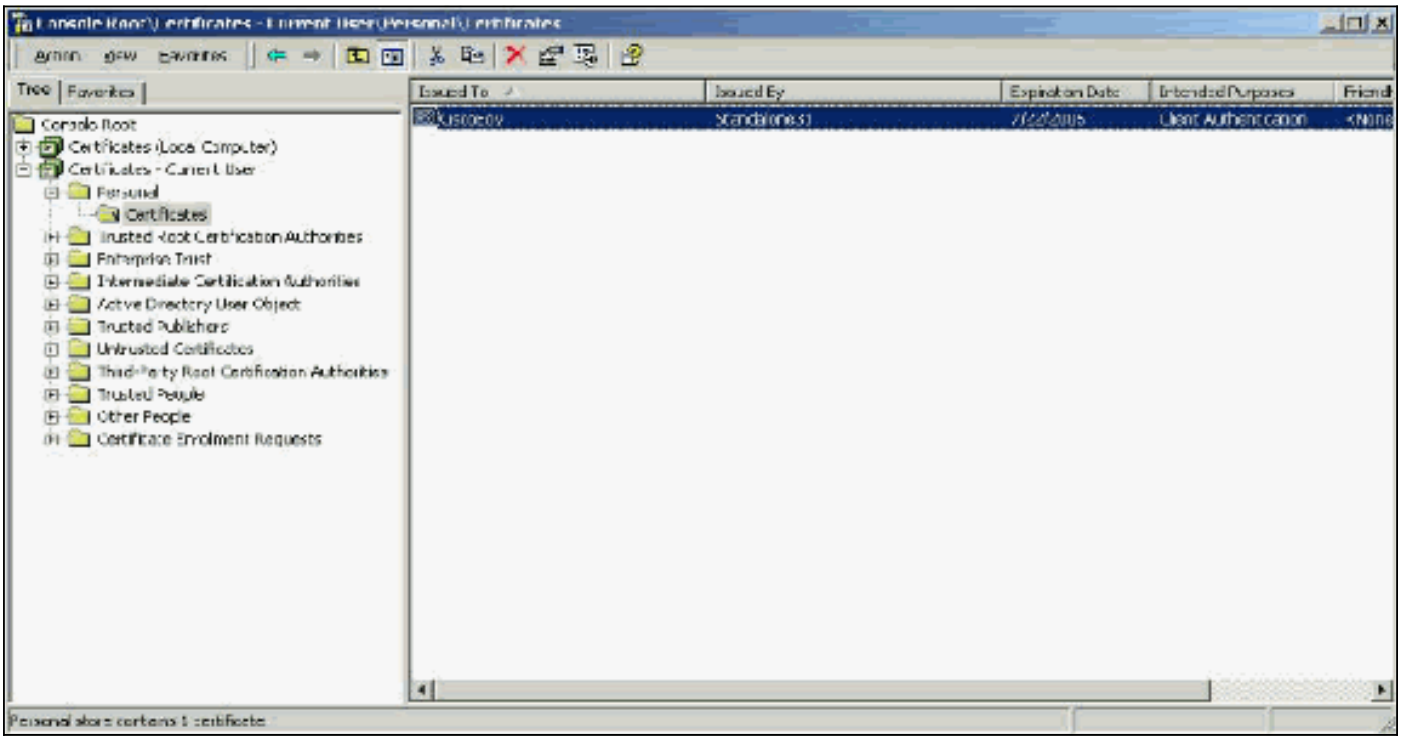
クライアント証明書は、EAP-TLS でユーザを明確に識別するために使用します。TLS トンネルを作成する役割はないので、暗号化には使用されません。明確な識別は、次の 3 つの方法のいずれかによって実現されます。

- **CN（または名前）比較：証明書内の CN とデータベース内のユーザ名を比較します。**この比較タイプに関連する情報については、証明書の Subject フィールドで説明しています。
- **SAN 比較：証明書内の SAN とデータベース内のユーザ名を比較します。**これは、ACS 3.2以降でのみサポートされています。この比較タイプの詳細は、証明書の[Subject Alternative Name]フィールドの説明に記載されています。
- **バイナリ比較：証明書とデータベースに保存されている証明書のバイナリ コピーを比較します（AD と LDAP のみで実行できます）。** 証明書のバイナリ比較を使用する場合は、ユーザ

証明書をバイナリ形式で保存する必要があります。また、汎用的な LDAP および Active Directory の場合、証明書を保存するアトリビュートは、「usercertificate」という名前の標準 LDAP アトリビュートである必要があります。

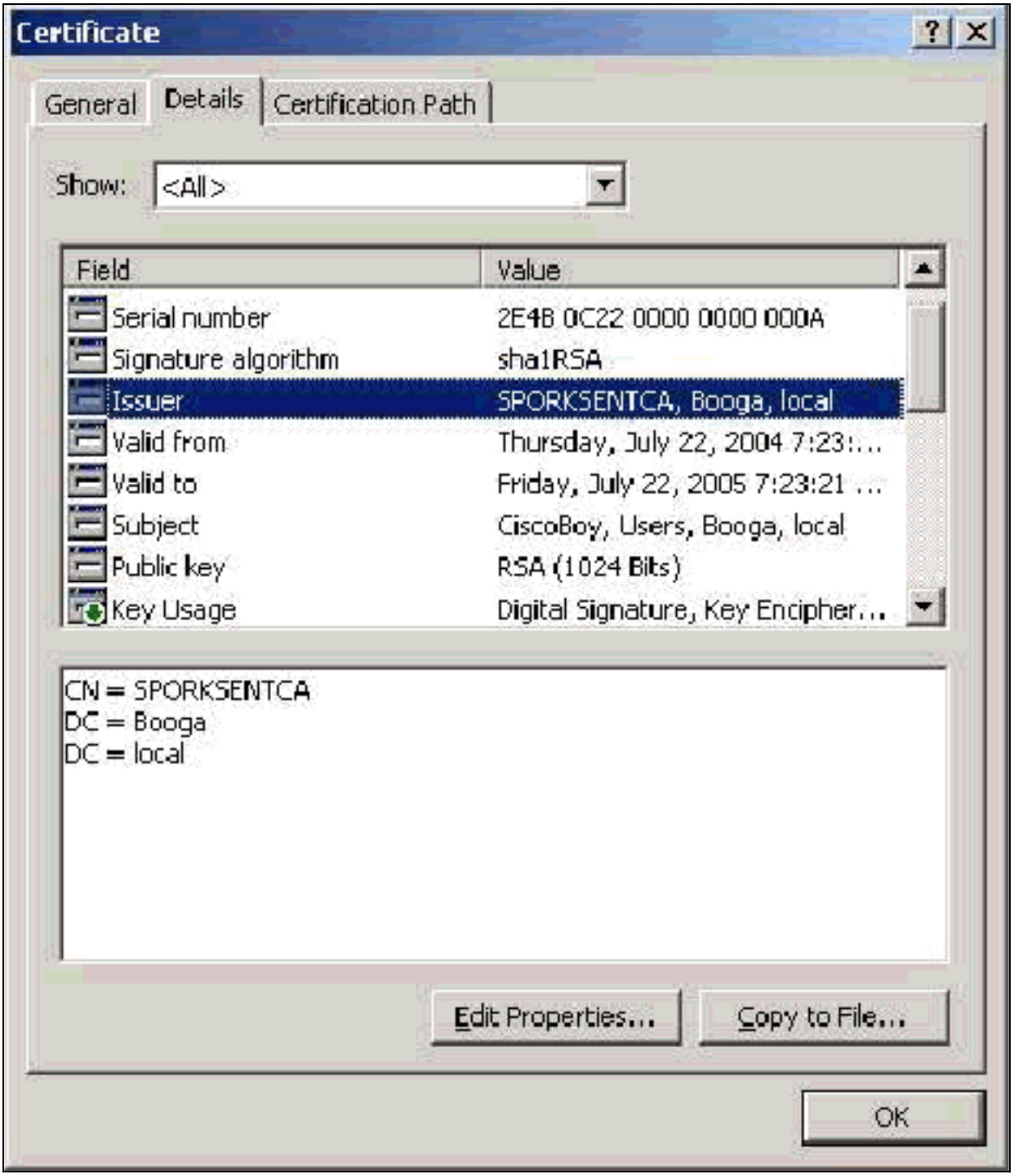
いずれの比較方法を使用する場合も、適切なフィールド（CN または SAN）の情報と、データベースが認証に使用する名前が一致する必要があります。AD では、混合モードの認証用の NetBios 名と、ネイティブ モードの UPN を使用します。

このセクションでは、Microsoft 証明書サービスを使用したクライアント証明書の生成について説明します。EAP-TLS では、各ユーザを認証するために、一意のクライアント証明書が必要です。証明書は、各コンピュータに各ユーザごとにインストールする必要があります。正しくインストールされた証明書は、このサンプル ウィンドウに示すように、[Certificates -Current User] > [Personal] > [Certificates] **フォルダに配置されます。**



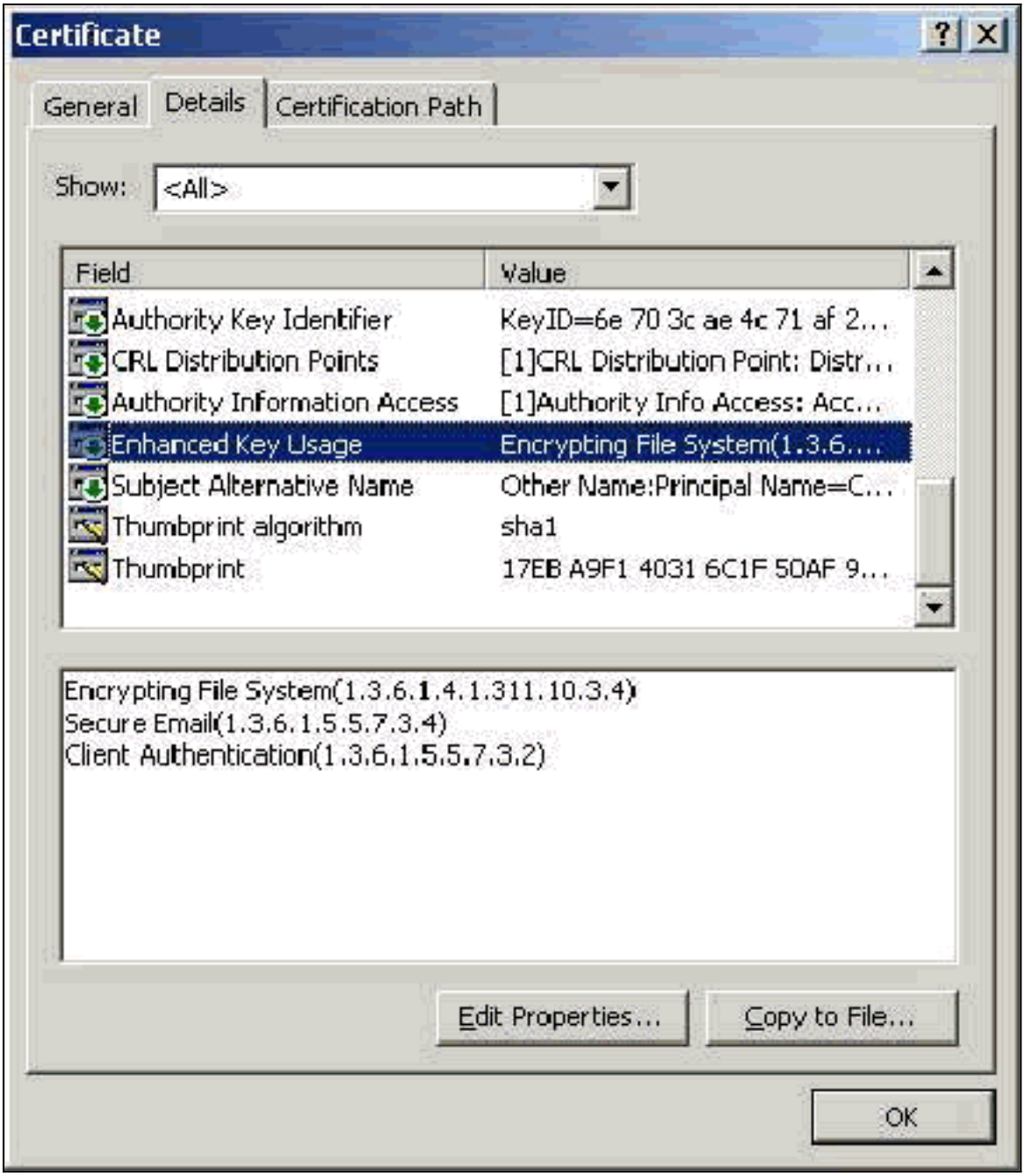
Issuer フィールド

Issuer フィールドは、証明書を発行した CA を識別します。この値は、証明書の General タブの Issued by フィールドの値を設定するのに使用します。値には、CA の名前が入力されています。



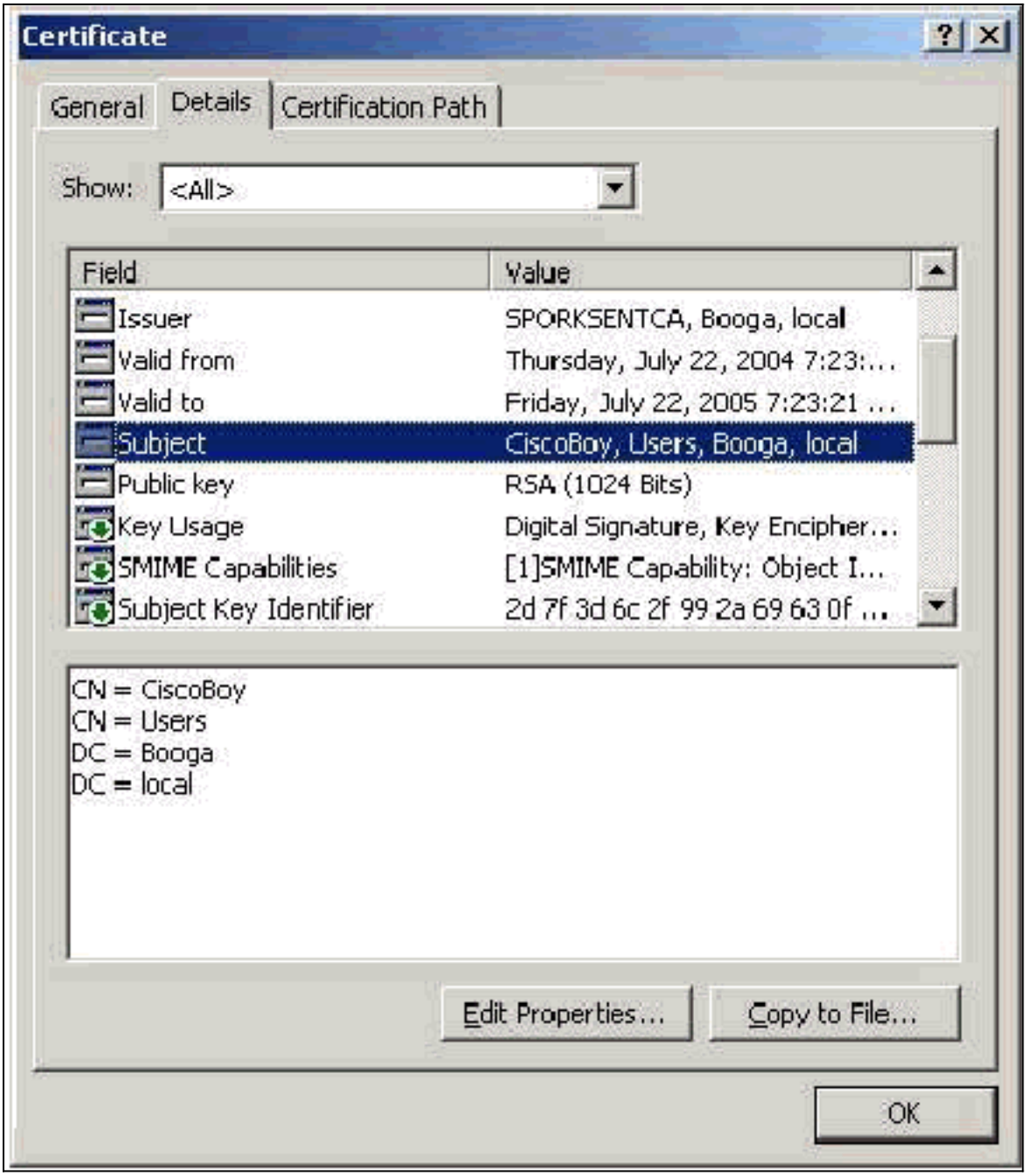
Enhanced Key Usage フィールド

Enhanced Key Usage フィールドは、証明書の使用目的を識別するもので、「Client Authentication」と入力されている必要があります。PEAP および EAP-TLS で Microsoft サプリカントを使用する場合、このフィールドは必須です。Microsoft 証明書サービスを使用する場合、スタンドアロン CA では Intended Purpose ドロップダウンで Client Authentication Certificate を選択すると、エンタープライズ CA では Certificate Template ドロップダウンで User を選択すると、このフィールドが設定されます。CSR と Microsoft 証明書サービスを使用して証明書を要求する場合、スタンドアロン CA で Intended Purpose を指定するオプションはありません。そのため、EKU フィールドは存在しません。エンタープライズ CA の場合は、Intended Purpose ドロップダウンが使用できます。CA によっては、EKU フィールドをともなう証明書を作成していない場合があります。Microsoft EAP サプリカントを使用している場合、このような証明書は使用できません。



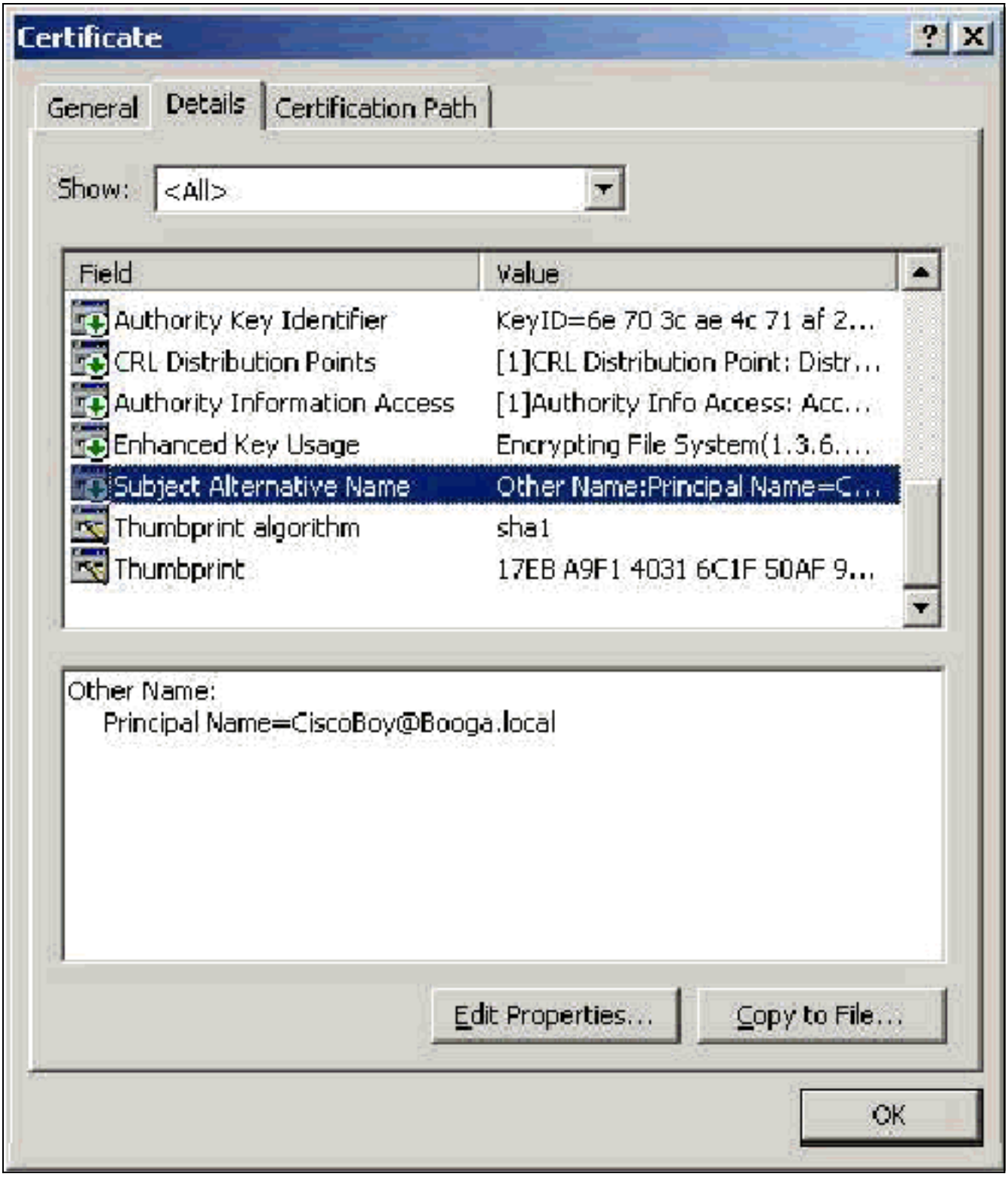
Subject フィールド

このフィールドは、CN の比較で使用します。表示されている先頭の CN がデータベースに比較され、一致するエントリが検索されます。一致するエントリが見つかると、認証は成功します。スタンドアロン CA を使用している場合、CN には、証明書の発行フォームの Name フィールドに入力した内容が設定されています。エンタープライズ CA を使用している場合、CN には、Active Directory Users and Computers コンソールに表示されるアカウントの名前が自動的に設定されています（UPN または NetBios 名と一致している必要はありません）。



Subject Alternative Name フィールド

Subject Alternative Name フィールドは、SAN の比較で使用します。表示されている SAN がデータベースに比較され、一致するエントリが検索されます。一致するエントリが見つかると、認証は成功します。エンタープライズ CA を使用している場合、SAN には、Active Directory のログイン名 @domain (UPN) が自動的に設定されています。 スタンドアロン CA には SAN フィールドが含まれていないため、SAN の比較は使用できません。



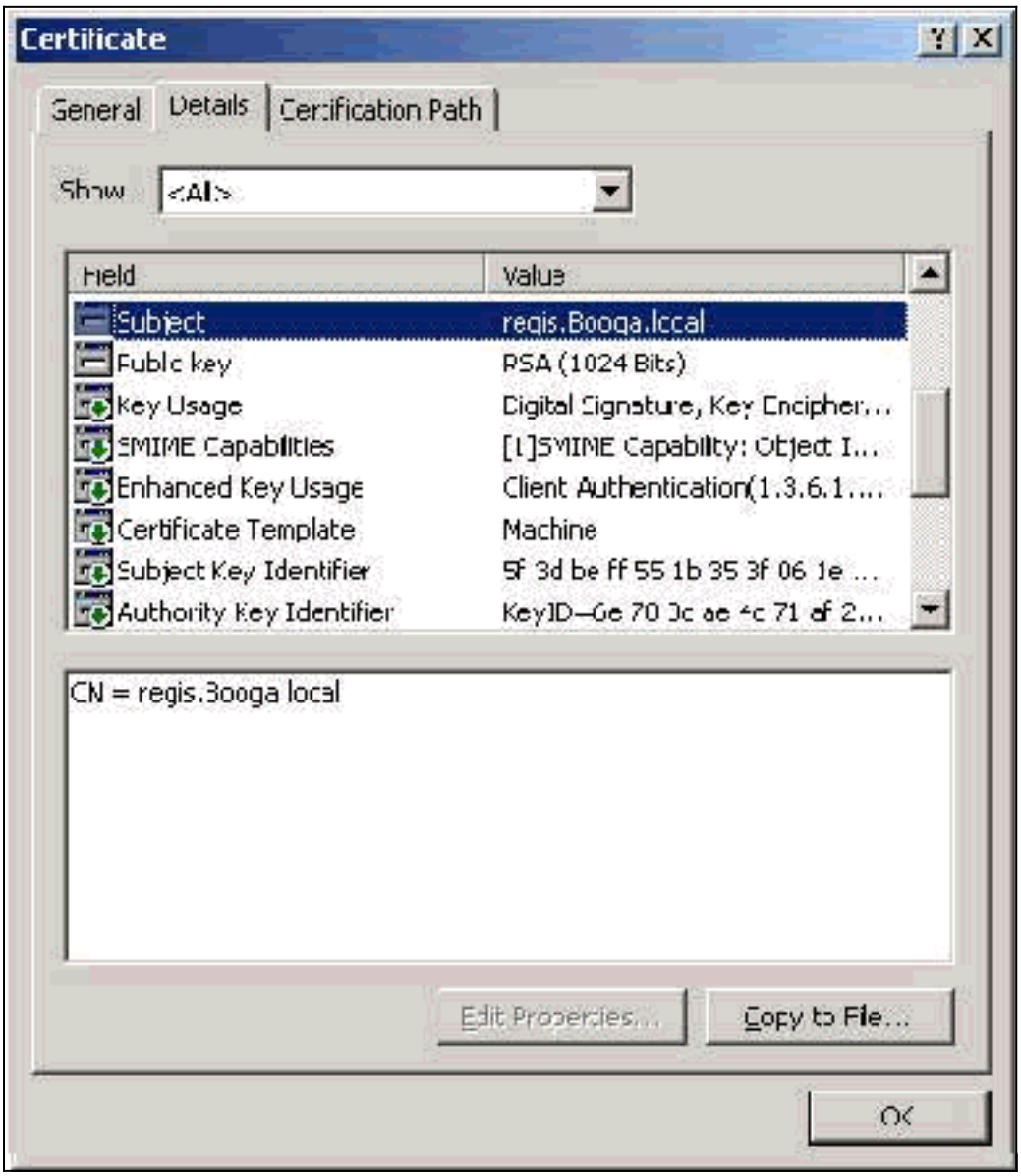
マシン証明書

マシン証明書は、マシン認証を使用するときに、EAP-TLS でコンピュータを明確に識別するために使用します。この証明書が使用できるのは、Microsoft エンタープライズ CA を証明書の自動登録用に設定していて、さらにコンピュータがドメインに参加している場合だけです。コンピュータの Active Directory のクレデンシャルを使用していて、このクレデンシャルをローカル コンピュータのストアにインストールすると、自動的に証明書が作成されます。自動登録を設定する前からドメインのメンバになっていたコンピュータは、次に Windows の再起動をしたときに証明書を受信します。マシン証明書は、サーバ証明書と同様に、Certificates (Local Computer) MMC スナップインの [Certificates (Local Computer)] > [Personal] > [Certificates] **フォルダにインストールされます。**この証明書は、秘密鍵をエクスポートできないため、ほかのマシンにはインストー

ルできません。

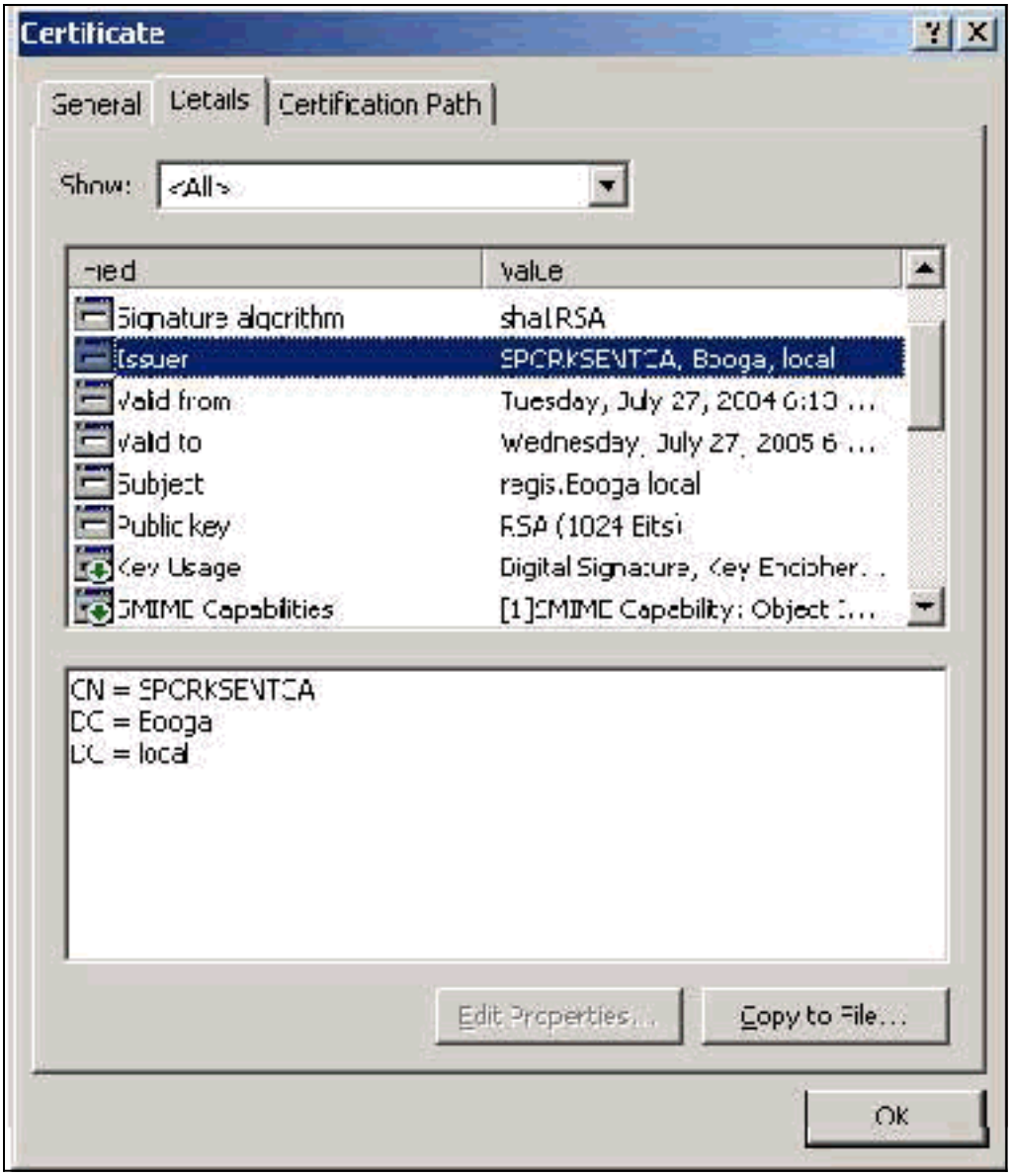
Subject フィールドと SAN フィールド

Subject フィールドと SAN フィールドは、コンピュータを識別します。これらの値には、コンピュータの完全修飾名が入力されており、証明書の General タブの Issued to フィールドを設定するのに使用します。Subject フィールドと SAN フィールドは、同じ値になります。



Issuer フィールド

Issuer フィールドは、証明書を発行した CA を識別します。この値は、証明書の General タブの Issued by フィールドの値を設定するのに使用します。値には、CA の名前が入力されています。



付録 A - 証明書の一般的な拡張子

.csr：これは、実際には証明書ではなく、証明書署名要求です。プレーン テキスト ファイルで、次のようなフォーマットになります。

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

.pvk：この拡張子は秘密キーを表しますが、中身が本当に秘密キーかどうかは保証されません。中身はプレーン テキストで、次のようなフォーマットになっている必要があります。

```
-----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：これは、証明書を表す一般的な拡張子です。サーバ証明書、ルート CA 証明書、および中間 CA 証明書は、この形式で作成できます。通常は、プレーン テキスト ファイルに拡張子が付いたものです。拡張子は、必要に応じて変更できます。また、DER 形式と Base 64 形式のいずれかを選択できます。この形式は、Windows の証明書ストアにインポートできます。

.pem：この拡張子は、プライバシー強化メールを意味します。通常、この拡張子は UNIX、Linux、BSD などで使用します。主に、サーバ証明書と秘密鍵で使用します。通常は、プレーン テキスト ファイルに拡張子が付いたものです。拡張子は、必要に応じて .pem から .cer に変更できるため、Windows の証明書ストアにインポートすることもできます。

通常、.cer ファイルおよび .pem ファイルの中身は、次の出力のようになります。

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

.pfx：この拡張子は、個人情報交換を示します。この形式を使用すると、複数の証明書を 1 つのファイルにバンドルできます。たとえば、サーバ証明書とそれに対応する秘密鍵、さらにルート CA 証明書を 1 つのファイルにバンドルしたり、バンドルしたファイルを Windows の適切な証明書ストアに簡単にインポートできます。通常は、サーバ証明書とクライアント証明書で使用します。残念ながら、ルート CA 証明書が含まれている場合、インストール先に「ローカル コンピュータ」ストアが指定されていても、ルート CA 証明書は「ローカル コンピュータ」ストアでなく、必ず、「現在のユーザー」ストアにインストールされます。

.p12：この形式は通常、クライアント証明書でのみ表示されます。この形式は、Windows の証明書ストアにインポートできます。

.p7b：これは、1つのファイルに複数の証明書を保存するもう1つの形式です。この形式は、Windows の証明書ストアにインポートできます。

付録 B - 証明書の形式の変換

ほとんどの場合、証明書はプレーン テキスト形式であるため、拡張子を変更すると (たとえば .pem から .cer) 、証明書の変換が実行されます。ただし、証明書がプレーン テキスト形式でない場合は、OpenSSL などのツールを使用して、証明書の変換を実行する必要があります。 たとえば、ACS Solution Engine では .pfx 形式の証明書をインストールできません。そのため、証明書と秘密鍵を使用可能な形式に変換する必要があります。OpenSSL の基本的なコマンド構文は

次のとおりです。

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

Import Password と PEM パス フレーズを入力するように指示されます。これらは、同じパスワードである必要があります。パスワードは、.pfx をエクスポートしたときに指定した秘密鍵のパスワードです。出力は 1 つの .pem ファイルで、.pfx の証明書と秘密鍵がすべて含まれています。このファイルは、ACS で、証明書と秘密鍵の両方のファイルとして参照でき、インストールも問題なく実行できます。

付録 C - 証明書の有効期間

証明書が使用できるのは、その有効期間の間だけです。ルート CA 証明書の有効期間は、ルート CA が設立されたときに決定されており、それぞれ異なります。中間 CA 証明書の有効期間は、CA が設立されたときに決定されますが、上位のルート CA の有効期間を超えることはできません。サーバ証明書、クライアント証明書、およびマシン証明書の有効期間は、Microsoft 証明書サービスを使用した場合、自動的に 1 年が設定されます。これは、Microsoft Knowledge Baseの記事254632に従ってWindowsレジストリをハックする場合にのみ変更できます 。ルートCAの有効期間を超えることはできません。ACS で生成する自己署名証明書の有効期間は、常に 1 年で、現在のバージョンでは変更できません。

関連情報

- RADIUS に関するサポート ページ
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems