Zertifikatsleitfaden für EAP Version 1.01

Inhalt

Einführung

Dieses Dokument verdeutlicht einige der Verwirrung, die mit den verschiedenen Zertifikatstypen, -formaten und -anforderungen im Zusammenhang mit den verschiedenen Formen des Extensible Authentication Protocol (EAP) einhergeht. Die fünf in diesem Dokument behandelten Zertifikatstypen für EAP sind Server, Root CA, Intermediate CA, Client und Machine. Diese Zertifikate sind in verschiedenen Formaten verfügbar, und es können je nach der jeweiligen EAP-Implementierung unterschiedliche Anforderungen für jede dieser Formate bestehen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Serverzertifikate

Das Serverzertifikat wird auf dem RADIUS-Server installiert, und der Hauptzweck des EAP besteht darin, den verschlüsselten Transport Layer Security (TLS)-Tunnel zu erstellen, der die Authentifizierungsinformationen schützt. Wenn Sie EAP-MSCHAPv2 verwenden, übernimmt das Serverzertifikat eine sekundäre Rolle, nämlich den RADIUS-Server als vertrauenswürdige Einheit für die Authentifizierung zu identifizieren. Diese sekundäre Rolle wird mithilfe des Felds Enhanced Key Usage (EKU) erreicht. Das EKU-Feld identifiziert das Zertifikat als gültiges Serverzertifikat und verifiziert, dass die Root-Zertifizierungsstelle, die das Zertifikat ausgestellt hat, eine vertrauenswürdige Root-Zertifizierungsstelle ist. Dazu muss das Zertifikat der Stammzertifizierungsstelle vorhanden sein. Für Cisco Secure ACS ist es erforderlich, dass das Zertifikat entweder Base64-codiert oder DER-codiert im binären X.509 v3-Format vorliegt.

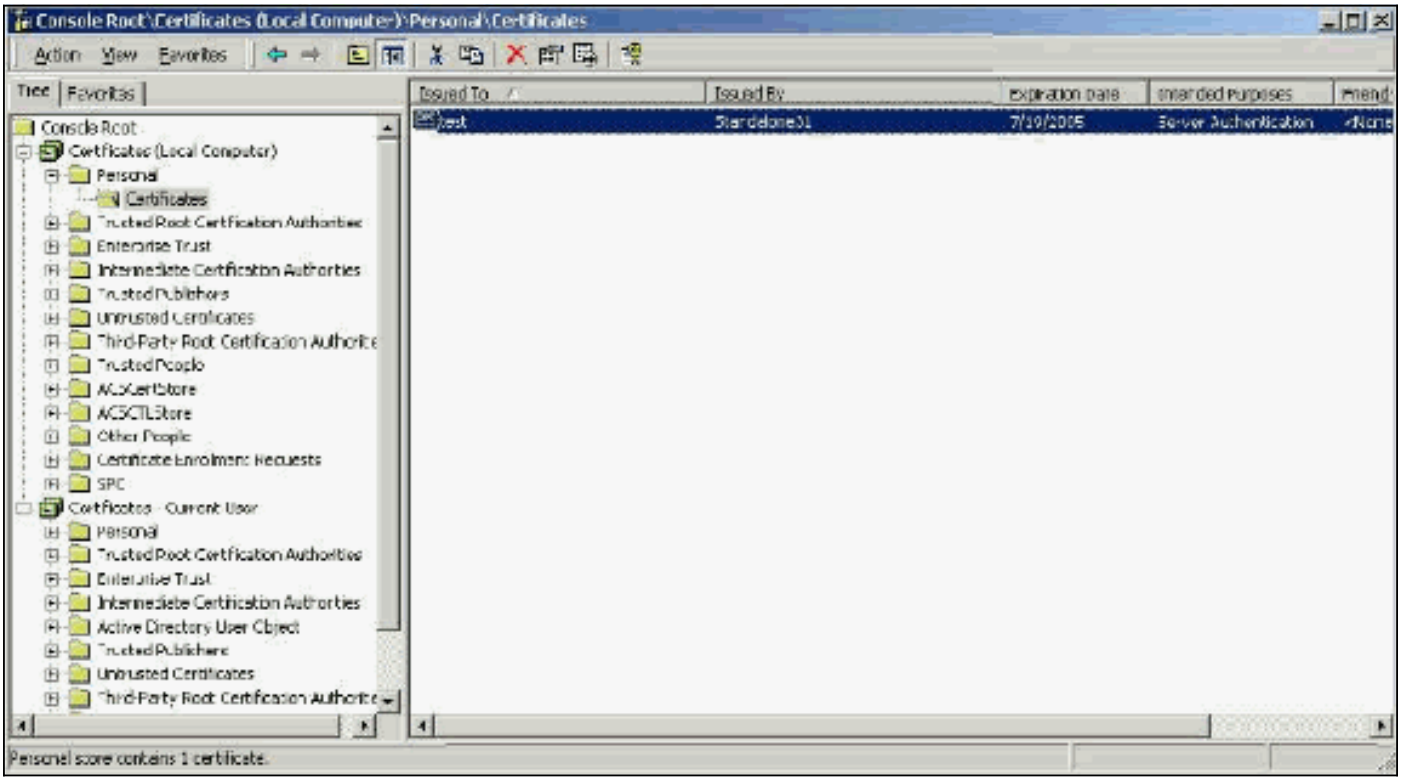
Sie können dieses Zertifikat entweder mithilfe einer Zertifikatssignierungsanfrage (Certificate Signing Request, CSR) im ACS erstellen, die an eine Zertifizierungsstelle übermittelt wird. Sie können das Zertifikat auch mithilfe eines internen Zertifizierungsstellen-Formulars (wie z. B. Microsoft Certificate Services) ausschneiden. Beachten Sie, dass Sie zwar ein Serverzertifikat mit Schlüssellängen von mehr als 1024 erstellen können, dass jedoch ein Schlüssel größer als 1024 nicht mit PEAP kompatibel ist. Der Client stürzt selbst bei erfolgreicher Authentifizierung ab.

Wenn Sie das Zertifikat mithilfe eines CSR erstellen, wird es im .cer-, .pem- oder .txt-Format erstellt. In seltenen Fällen wird sie ohne Erweiterung erstellt. Stellen Sie sicher, dass das Zertifikat eine Nur-Text-Datei mit einer Erweiterung ist, die Sie bei Bedarf ändern können (die ACS-Appliance verwendet die Erweiterung .cer oder .pem). Wenn Sie einen CSR verwenden, wird der private Schlüssel des Zertifikats im Pfad erstellt, den Sie als separate Datei angeben, die möglicherweise über eine Erweiterung verfügt und mit der ein Kennwort verknüpft ist (das Kennwort ist für die Installation auf dem ACS erforderlich). Unabhängig von der Erweiterung stellen Sie sicher, dass es sich um eine Textdatei mit einer Erweiterung handelt, die Sie bei Bedarf ändern können (die ACS-Appliance verwendet die Erweiterung .pvk oder .pem). Wenn für den privaten Schlüssel kein Pfad angegeben ist, speichert ACS den Schlüssel im Verzeichnis C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs und sucht in diesem Verzeichnis, wenn bei der Installation des Zertifikats kein Pfad für die private Schlüsseldatei angegeben ist.

Wenn das Zertifikat mithilfe des Formulars zum Einreichen des Zertifikats von Microsoft Certificate Services erstellt wird, müssen Sie die Schlüssel als exportierbar markieren, damit Sie das Zertifikat in ACS installieren können. Die Erstellung eines Zertifikats vereinfacht den Installationsprozess erheblich. Sie können es direkt in den entsprechenden Windows-Speicher über die Webschnittstelle der Zertifikatsdienste installieren und dann auf dem ACS mithilfe des CN

als Referenz vom Speicher installieren. Ein im lokalen Computerspeicher installiertes Zertifikat kann auch aus dem Windows-Speicher exportiert und problemlos auf einem anderen Computer installiert werden. Wenn dieser Zertifikatstyp exportiert wird, müssen die Schlüssel als exportierbar gekennzeichnet und mit einem Kennwort versehen werden. Das Zertifikat wird dann im PFX-Format angezeigt, das den privaten Schlüssel und das Serverzertifikat enthält.

Wenn das Serverzertifikat ordnungsgemäß im Windows-Zertifikatsspeicher installiert wurde, muss es im Ordner **Certificates (Local Computer) > Personal > Certificates** (**Lokaler Computer)** angezeigt werden, wie in diesem Beispielfenster gezeigt.

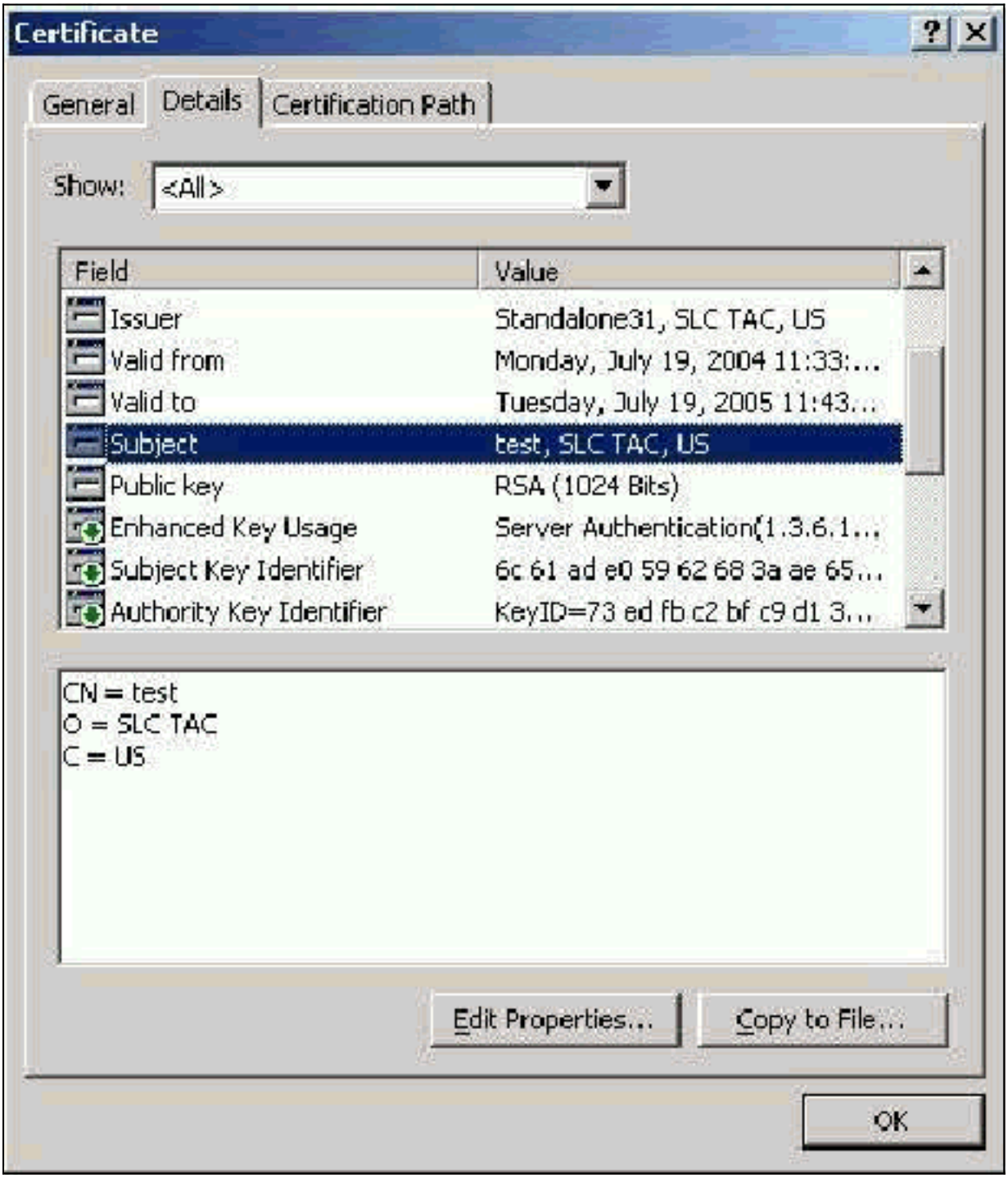


Selbstsignierte Zertifikate sind Zertifikate, die Sie ohne Root oder die zwischengeschaltete Einbindung der CA erstellen. Sie haben den gleichen Wert sowohl im Betreff- als auch im Emittentenfeld wie ein Zertifikat der Stammzertifizierungsstelle. Die meisten selbstsignierten Zertifikate verwenden das X.509 v1-Format. Daher arbeiten sie nicht mit ACS zusammen. Ab Version 3.3 kann ACS jedoch eigene selbstsignierte Zertifikate erstellen, die Sie für EAP-TLS und PEAP verwenden können. Verwenden Sie zur Kompatibilität mit PEAP und EAP-TLS keine Schlüssellänge größer als 1024. Wenn Sie ein selbstsigniertes Zertifikat verwenden, übernimmt das Zertifikat auch die Funktion des Zertifikats der Stammzertifizierungsstelle und muss im Ordner **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** folder (**Lokaler Computer) des** Clients installiert werden, wenn Sie die Microsoft EAP-Komponente verwenden. Sie wird automatisch im vertrauenswürdigen Stammzertifikatspeicher des Servers installiert. Sie muss jedoch in der Zertifikatsvertrauenswürdigkeitsliste der ACS-Zertifikateinrichtung vertrauenswürdig sein. Weitere Informationen finden Sie im Abschnitt Wurzelzertifikate der Zertifizierungsstelle.

Da selbstsignierte Zertifikate als Stammzertifizierungszertifikat für die Serverzertifikatvalidierung verwendet werden, wenn Sie den Microsoft EAP-Supplicant verwenden, und da die Gültigkeitsdauer von der Standardeinstellung von einem Jahr nicht verlängert werden kann, empfiehlt Cisco, diese Zertifikate nur als temporäre Maßnahme für EAP zu verwenden, bis Sie eine herkömmliche Zertifizierungsstelle verwenden können.

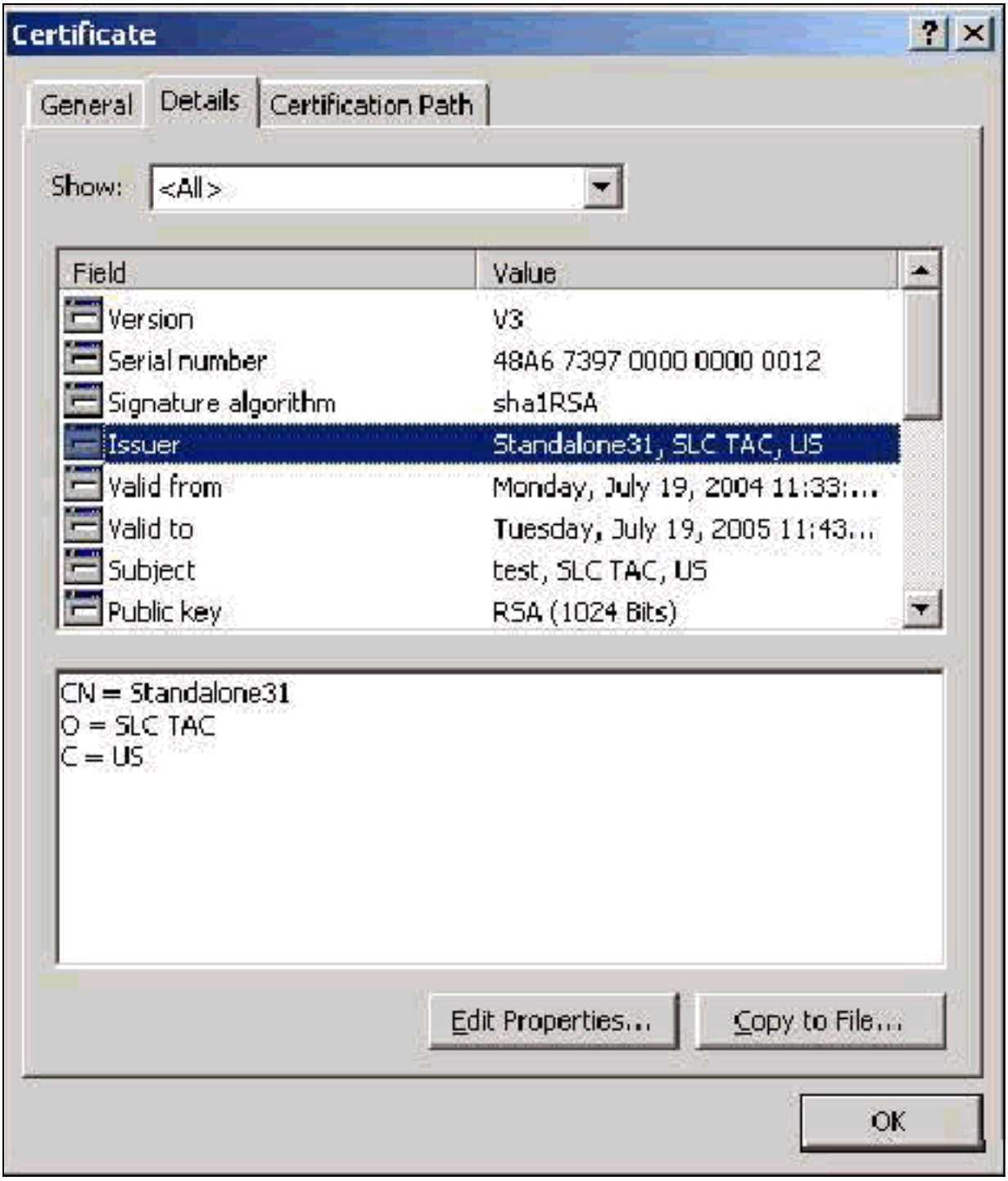
Fachgebiet

Das Betreff-Feld identifiziert das Zertifikat. Der KN-Wert wird verwendet, um das Feld "Issued to" (Ausgestellt für) auf der Registerkarte "General" (Allgemein) des Zertifikats zu bestimmen. Er wird mit den Informationen gefüllt, die Sie im Dialogfeld "CSR" des ACS in das Feld "Certificate subject" eingeben, oder mit den Informationen aus dem Feld "Name" in Microsoft Certificate Services. Der CN-Wert wird verwendet, um ACS mitzuteilen, welches Zertifikat vom Zertifikatsspeicher des lokalen Systems verwendet werden muss, wenn die Option zum Installieren des Zertifikats aus dem Speicher verwendet wird.



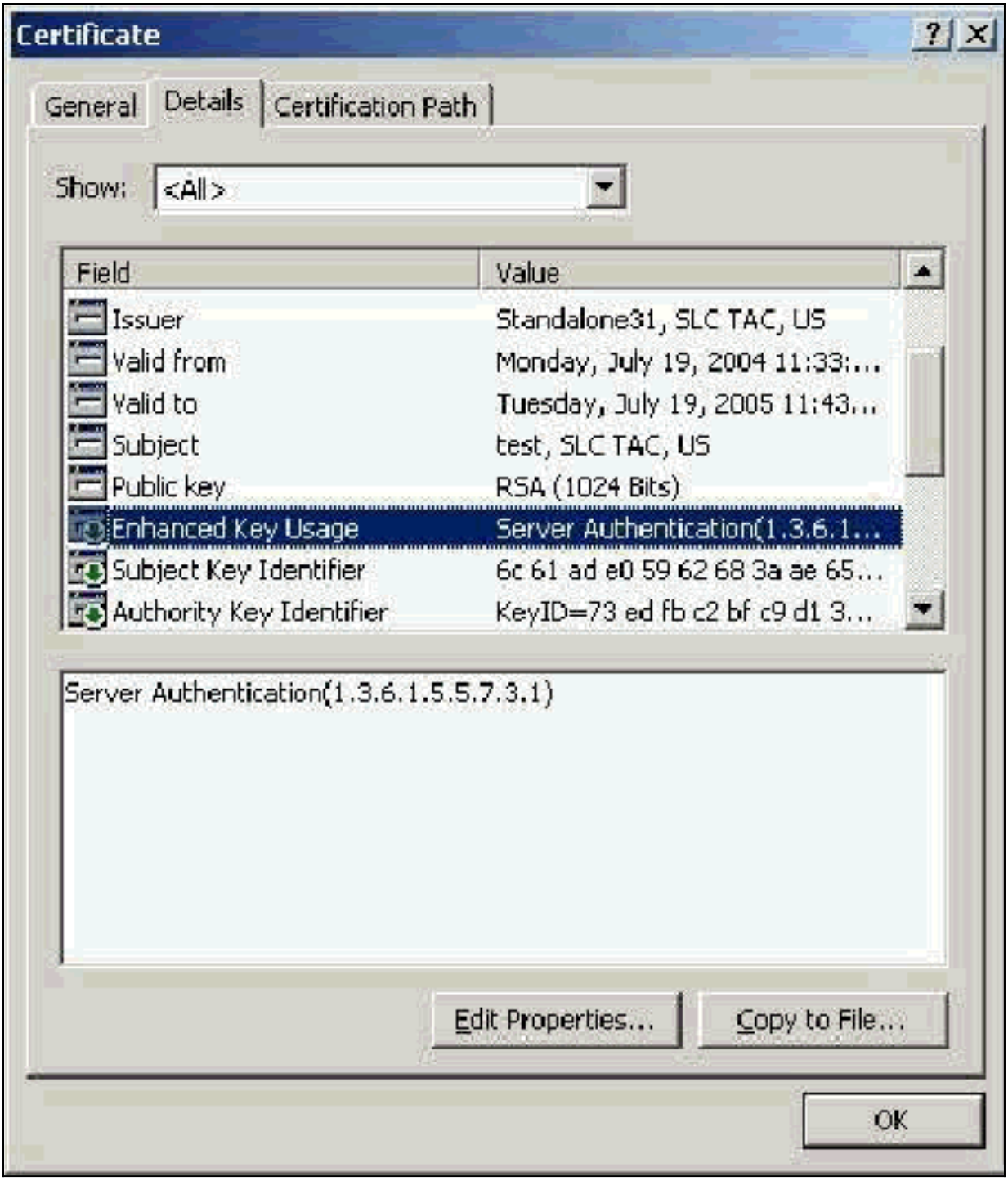
Ausgabefeld

Das Ausstellungsfeld identifiziert die Zertifizierungsstelle, die das Zertifikat ausgeschnitten hat. Verwenden Sie diesen Wert, um den Wert des Felds Issued by (Ausgestellt nach) auf der Registerkarte General (Allgemein) des Zertifikats zu bestimmen. Es wird mit dem Namen der CA ausgefüllt.



Verbesserte Schlüsselverwendungsfelder

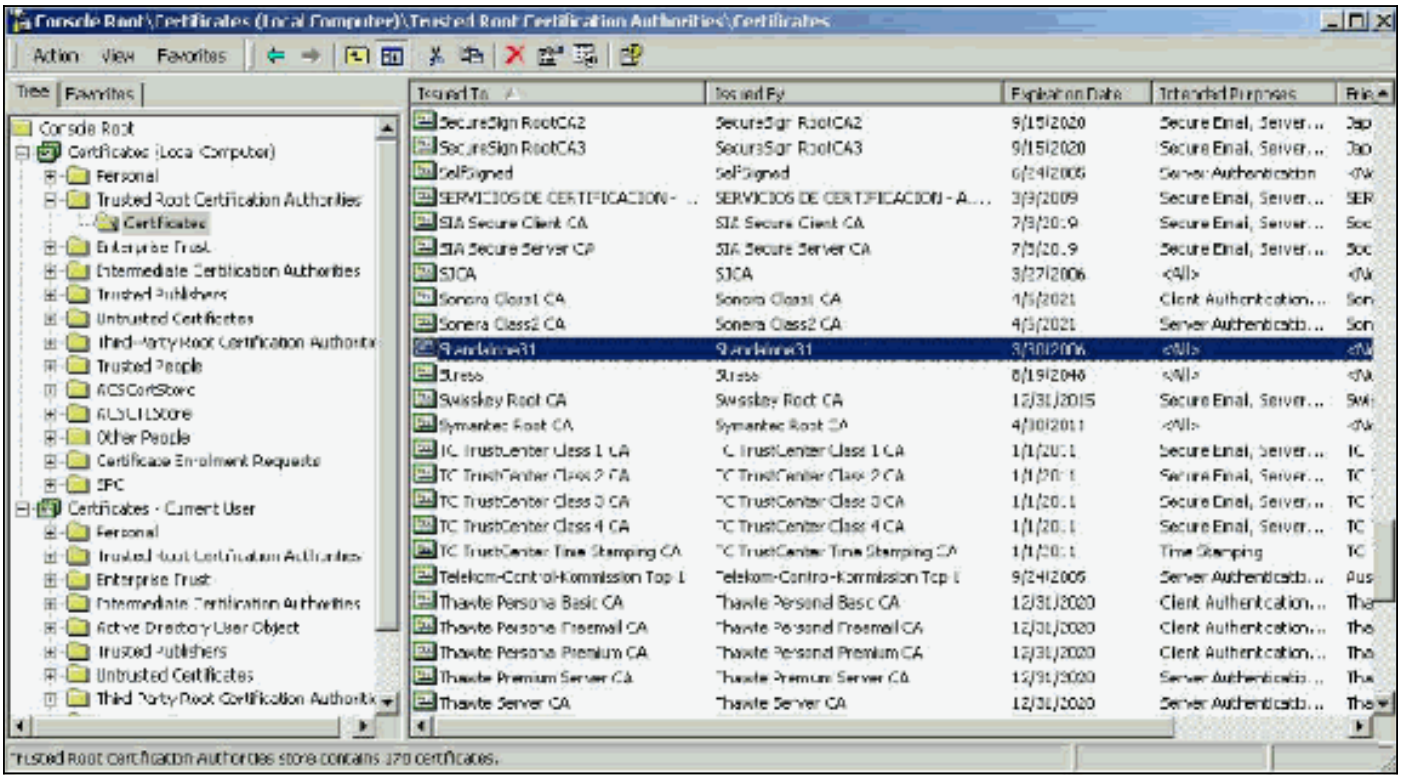
Das Feld "Enhanced Key Usage" (Erweiterte Schlüsselverwendung) gibt den beabsichtigten Zweck des Zertifikats an und muss als "Server Authentication" (Serverauthentifizierung) aufgeführt werden. Dieses Feld ist obligatorisch, wenn Sie die Microsoft-Komponente für PEAP und EAP-TLS verwenden. Wenn Sie Microsoft Zertifikatsdienste verwenden, wird dies in der eigenständigen CA mit der Auswahl des **Serverauthentifizierungszertifikats** aus dem Dropdown-Menü "Beabsichtigte Verwendung" und in der Enterprise CA mit der Auswahl des **Webservers** aus dem Dropdown-Menü "Zertifikatsvorlage" konfiguriert. Wenn Sie ein Zertifikat mit der Verwendung eines CSR mit Microsoft-Zertifikatsdiensten anfordern, haben Sie nicht die Möglichkeit, den beabsichtigten Zweck mit der eigenständigen Zertifizierungsstelle anzugeben. Daher ist das EKU-Feld nicht vorhanden. Bei der Enterprise-CA befindet sich die Dropdown-Liste "Beabsichtigte Verwendung". Einige CAs erstellen keine Zertifikate mit einem EKU-Feld, sodass sie bei Verwendung der Microsoft EAP-Komponente nutzlos sind.



Zertifikate der Stammzertifizierungsstelle

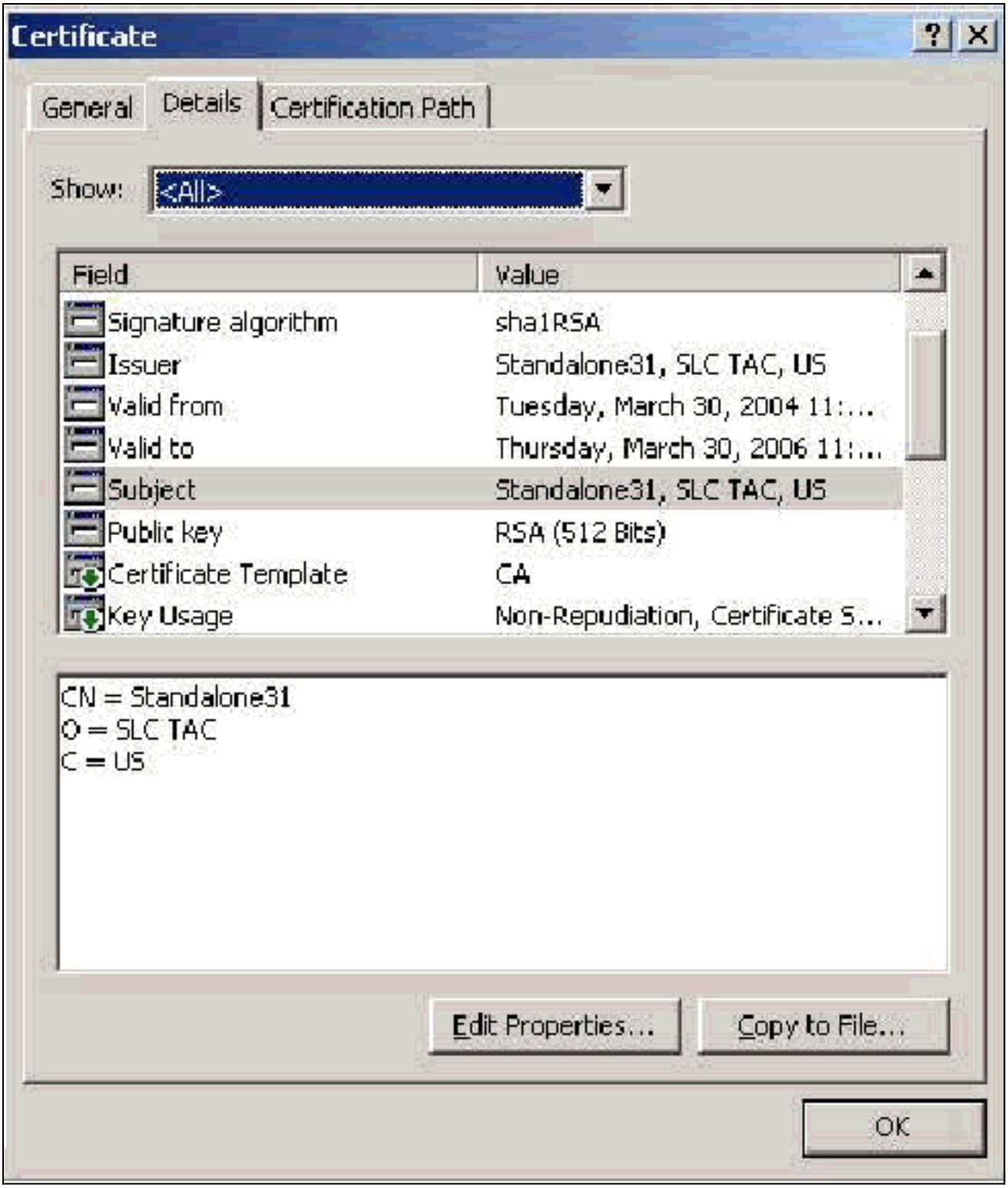
Mit dem Zertifikat der Stammzertifizierungsstelle wird das Serverzertifikat (und ggf. das Zertifikat der erweiterten Zertifizierungsstelle) als vertrauenswürdiges Zertifikat für den ACS und den Windows EAP-MSCHAPv2-Supplicant identifiziert. Sie muss sich sowohl auf dem ACS-Server als auch, im Fall von EAP-MSCHAPv2, auf dem Client-Computer im Speicher der Trusted Root Certification Authority befinden. Die meisten Zertifikate von Drittanbietern werden mit Windows installiert, und es ist wenig Aufwand damit verbunden. Wenn Microsoft Certificate Services verwendet wird und sich der Zertifikatsserver auf demselben Computer wie ACS befindet, wird das Zertifikat der Stammzertifizierungsstelle automatisch installiert. Wenn das Zertifikat der Stammzertifizierungsstelle nicht im Ordner Trusted Root Certification Authority in Windows gefunden wird, muss es von Ihrer Zertifizierungsstelle erworben und installiert werden. Wenn das Zertifikat der Stammzertifizierungsstelle ordnungsgemäß im Windows-Zertifikatsspeicher installiert wurde, muss es im Ordner **Certificates (Local Computer) > Trusted Root Certification Authorities >**

Certificates (**Lokaler Computer)** angezeigt werden, wie in diesem Beispielfenster gezeigt.



Betreff- und Ausgabefelder

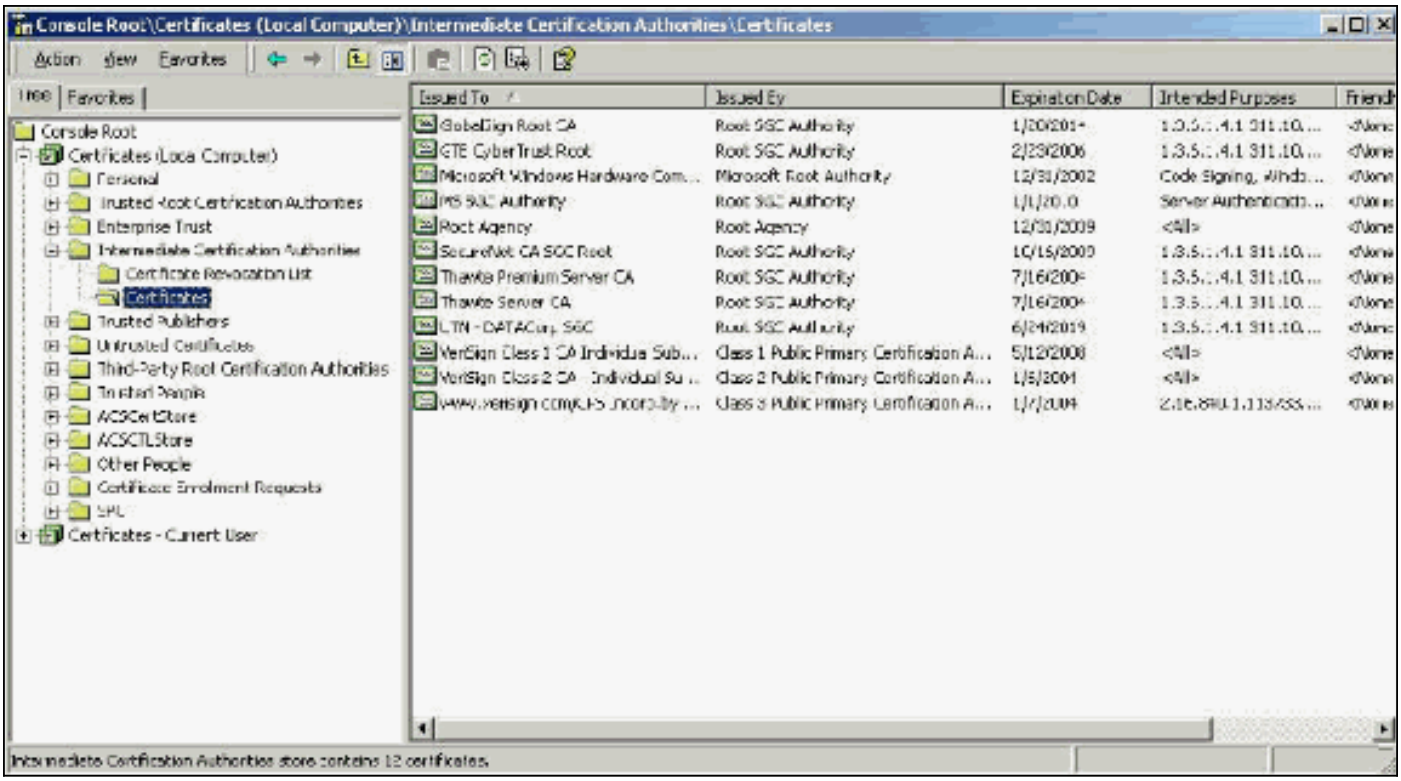
Die Felder "Betreff" und "Issuer" identifizieren die CA und müssen identisch sein. Verwenden Sie diese Felder, um die Felder Ausgabe an und Ausgabe durch auf der Registerkarte Allgemein des Zertifikats auszufüllen. Sie werden mit dem Namen der Root-CA gefüllt.



Zertifizierungsstellenzertifikate

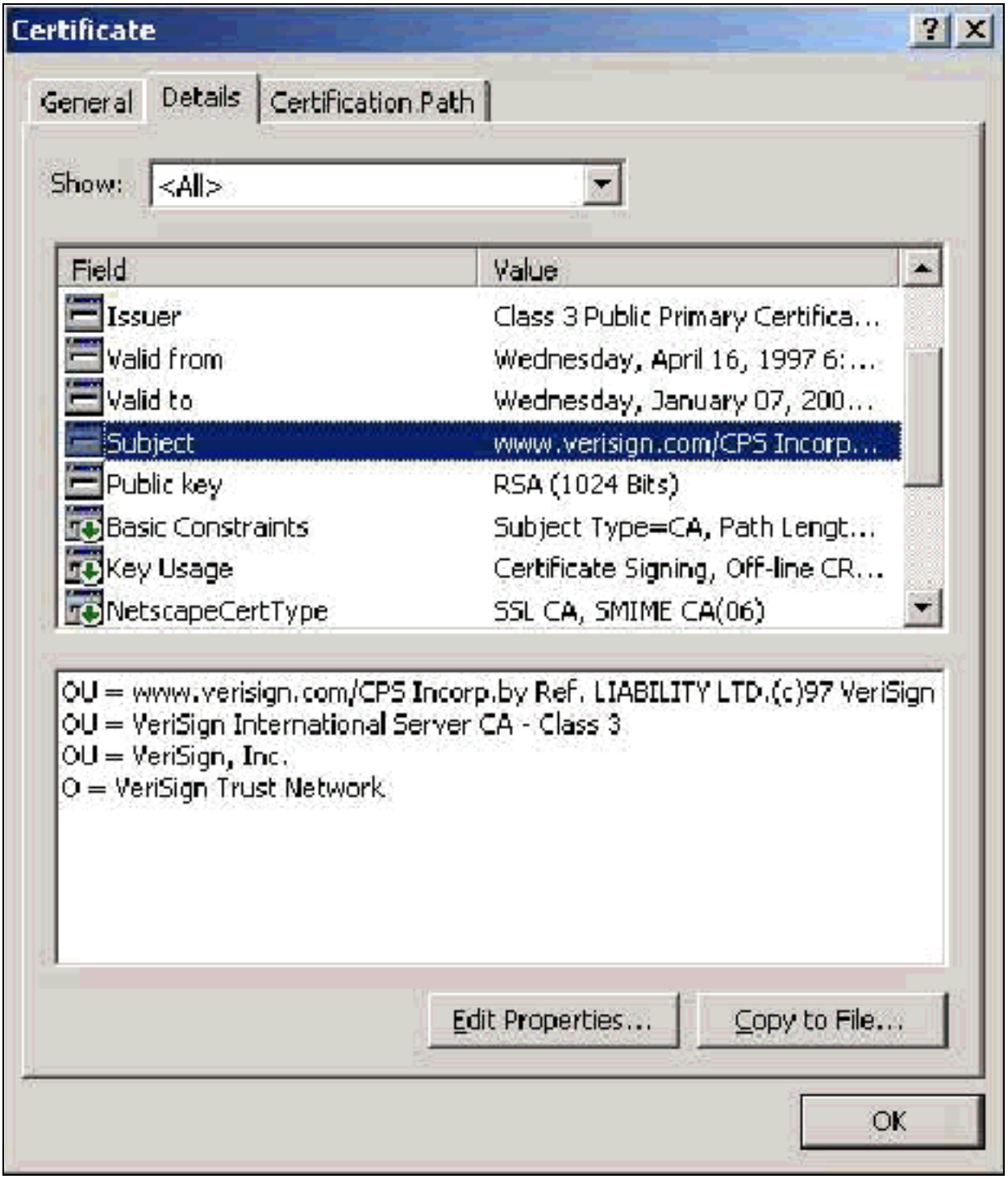
Zwischenzertifikate für Zertifizierungsstellen sind Zertifikate, die Sie verwenden, um eine Zertifizierungsstelle zu identifizieren, die einer Stammzertifizierungsstelle untergeordnet ist. Einige Serverzertifikate (Verisign's wireless certificate) werden mit einer Zwischen-CA erstellt. Wenn ein Serverzertifikat verwendet wird, das von einer zwischengeschalteten Zertifizierungsstelle abgeschnitten wird, muss das Zertifikat der erweiterten Zertifizierungsstelle im Bereich Erweiterte Zertifizierungsstellen des lokalen Maschinenspeichers auf dem ACS-Server installiert werden. Wenn auf dem Client die Microsoft EAP-Komponente verwendet wird, muss sich das Stammzertifizierungszertifikat der Stammzertifizierungsstelle, die das Zertifikat der Zwischen-Zertifizierungsstelle erstellt hat, ebenfalls im entsprechenden Speicher auf dem ACS-Server und -

Client befinden, damit die Vertrauenskette eingerichtet werden kann. Sowohl das Zertifikat der Stammzertifizierungsstelle als auch das Zertifikat der Zwischen-Zertifizierungsstelle müssen in ACS und auf dem Client als vertrauenswürdig gekennzeichnet werden. Die meisten Zertifizierungsstellenzertifikate sind nicht mit Windows installiert, daher müssen Sie sie höchstwahrscheinlich vom Anbieter erwerben. Wenn das Zertifikat der Zwischen-Zertifizierungsstelle ordnungsgemäß im Windows-Zertifikatsspeicher installiert wurde, wird es im Ordner **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates (Lokaler Computer)** angezeigt, wie in diesem Beispielfenster gezeigt.



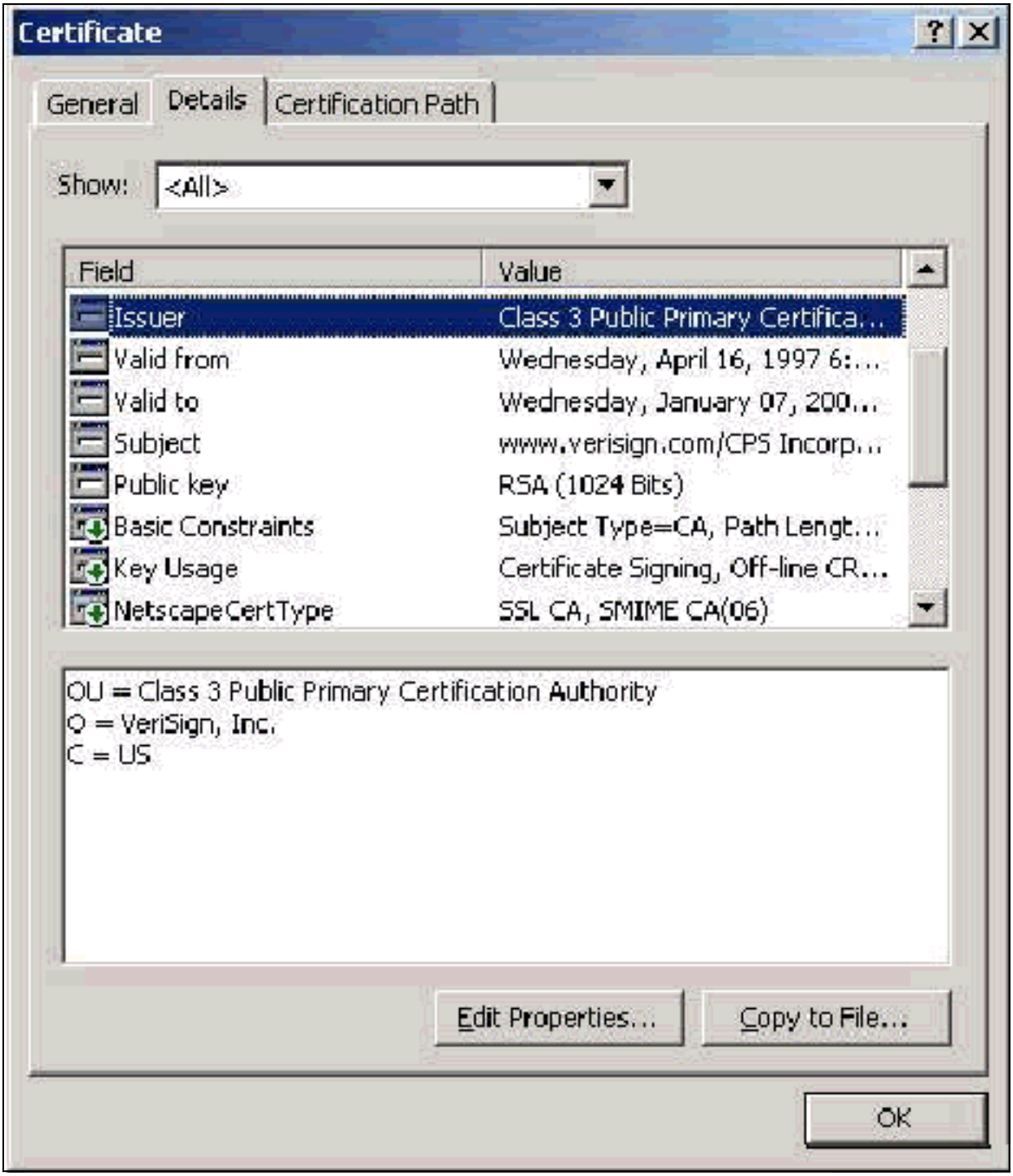
Fachgebiet

Das Betreff-Feld identifiziert die Erweiterte Zertifizierungsstelle. Dieser Wert wird verwendet, um das Feld "Ausgestellt für" auf der Registerkarte "Allgemein" des Zertifikats zu bestimmen.



Ausgabefeld

Das Ausstellungsfeld identifiziert die Zertifizierungsstelle, die das Zertifikat ausgeschnitten hat. Verwenden Sie diesen Wert, um den Wert des Felds Issued by (Ausgestellt nach) auf der Registerkarte General (Allgemein) des Zertifikats zu bestimmen. Es wird mit dem Namen der CA ausgefüllt.



Client-Zertifikate

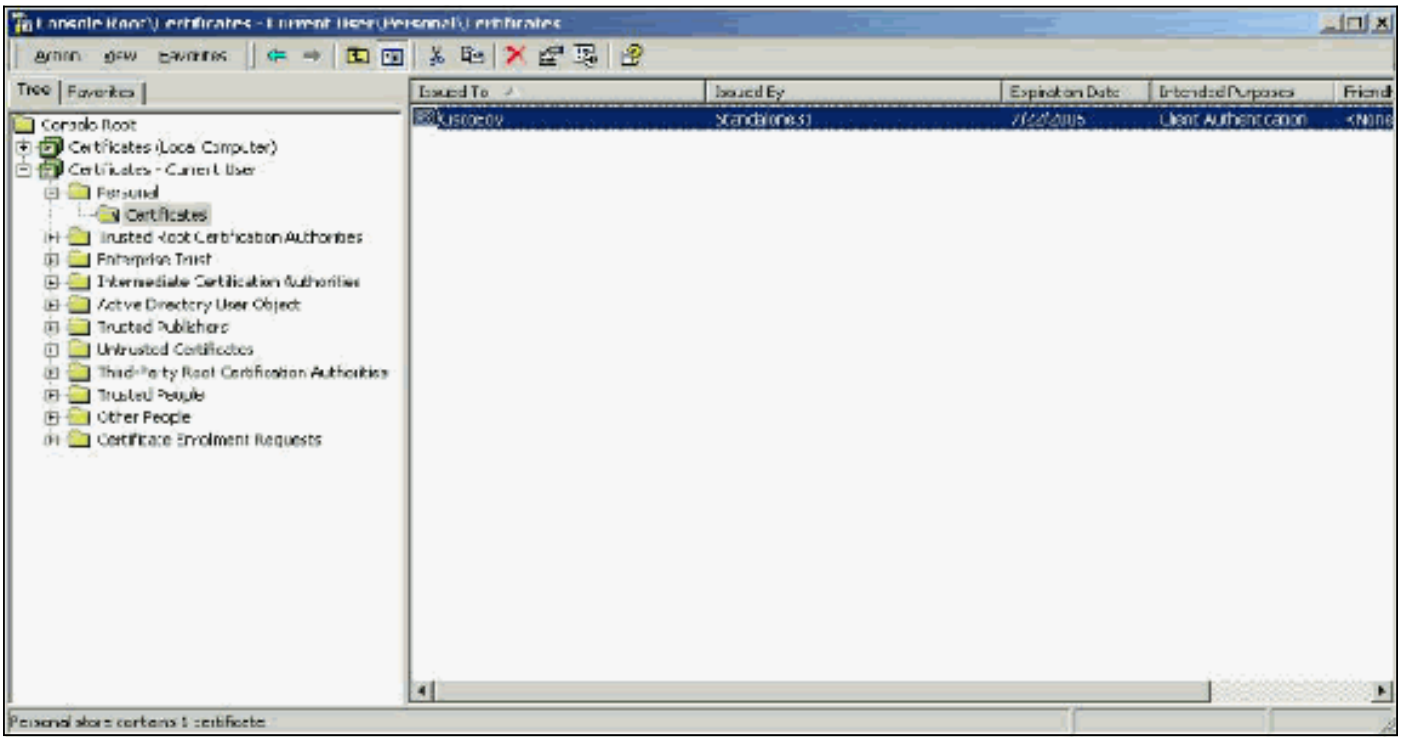
Client-Zertifikate werden verwendet, um den Benutzer in EAP-TLS positiv zu identifizieren. Sie spielen keine Rolle beim Aufbau des TLS-Tunnels und werden nicht für die Verschlüsselung verwendet. Die positive Identifizierung erfolgt mit einem von drei Mitteln:

- **CN (oder Name)Comparison** - Vergleicht den CN im Zertifikat mit dem Benutzernamen in der Datenbank. Weitere Informationen zu diesem Vergleichstyp finden Sie in der Beschreibung des Felds Betreff des Zertifikats.
- **SAN Comparison** (SAN-Vergleich) - Vergleicht das SAN im Zertifikat mit dem Benutzernamen in der Datenbank. Dies wird nur ab ACS 3.2 unterstützt. Weitere Informationen zu diesem Vergleichstyp finden Sie in der Beschreibung des Felds "Subject Alternative Name" des Zertifikats.

- **Binärer Vergleich**: Vergleicht das Zertifikat mit einer Binärkopie des in der Datenbank gespeicherten Zertifikats (nur AD und LDAP können dies tun). Wenn Sie den Binärvergleich für Zertifikate verwenden, müssen Sie das Benutzerzertifikat in einem Binärformat speichern. Außerdem muss das Attribut, das das Zertifikat speichert, für generische LDAP und Active Directory das standardmäßige LDAP-Attribut mit dem Namen "usercertificate" sein.

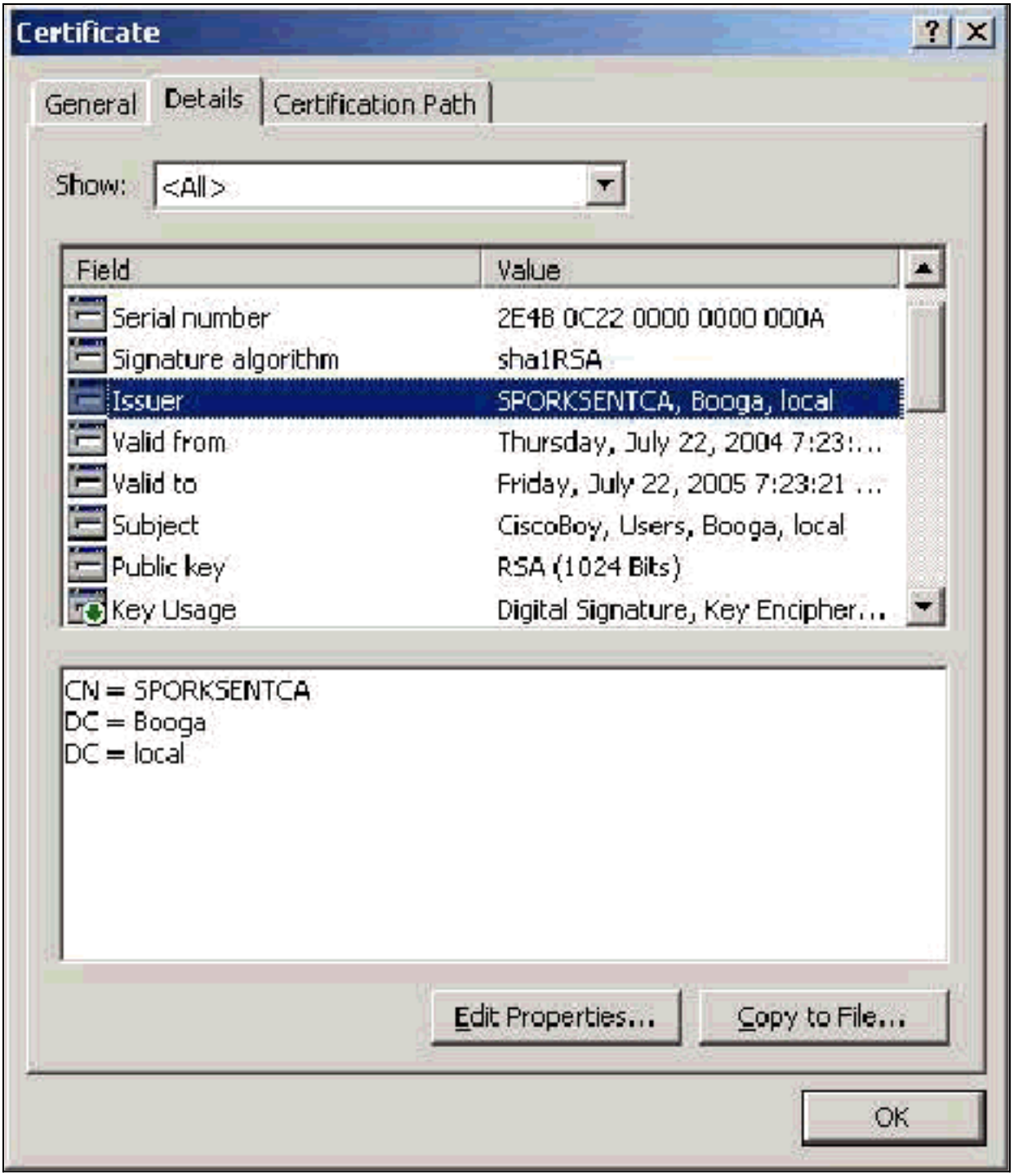
Unabhängig von der verwendeten Vergleichsmethode müssen die Informationen im entsprechenden Feld (CN oder SAN) mit dem Namen übereinstimmen, den die Datenbank für die Authentifizierung verwendet. AD verwendet den NetBios-Namen für die Authentifizierung im gemischten Modus und den UPN im nativen Modus.

In diesem Abschnitt wird die Generierung von Clientzertifikaten unter Verwendung von Microsoft-Zertifikatsdiensten erläutert. EAP-TLS erfordert ein eindeutiges Client-Zertifikat, damit jeder Benutzer authentifiziert werden kann. Das Zertifikat muss auf jedem Computer für jeden Benutzer installiert sein. Bei ordnungsgemäßer Installation befindet sich das Zertifikat im Ordner **Certificates -Current User > Personal > Certificates** (Zertifikate **-aktueller Benutzer > Personal > Zertifikate**), wie in diesem Beispielfenster gezeigt.



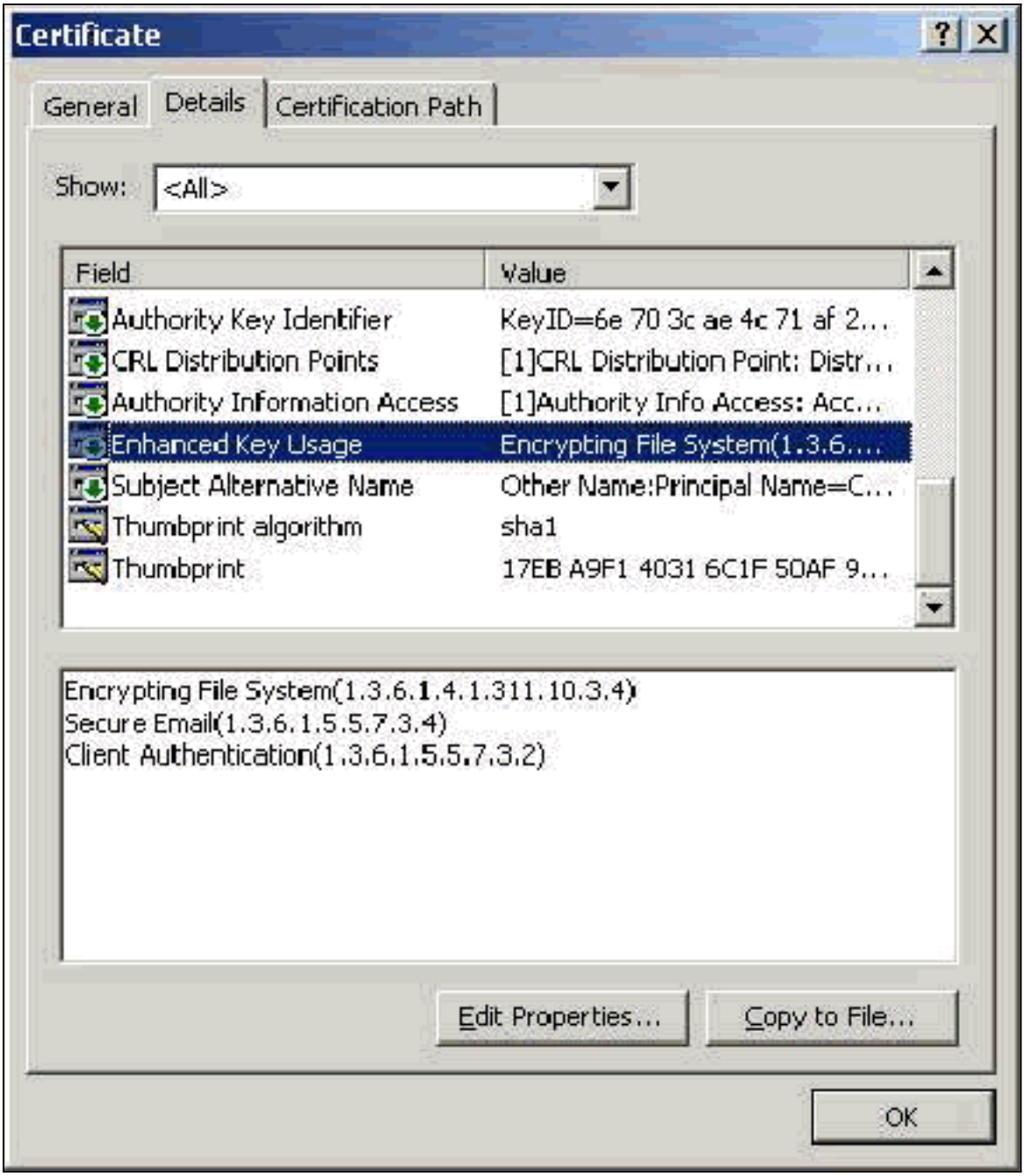
Ausgabefeld

Das Ausstellungsfeld identifiziert die Zertifizierungsstelle, die das Zertifikat auslöst. Verwenden Sie diesen Wert, um den Wert des Felds Issued by (Ausgestellt nach) auf der Registerkarte General (Allgemein) des Zertifikats zu bestimmen. In diesem Feld wird der Name der CA eingetragen.



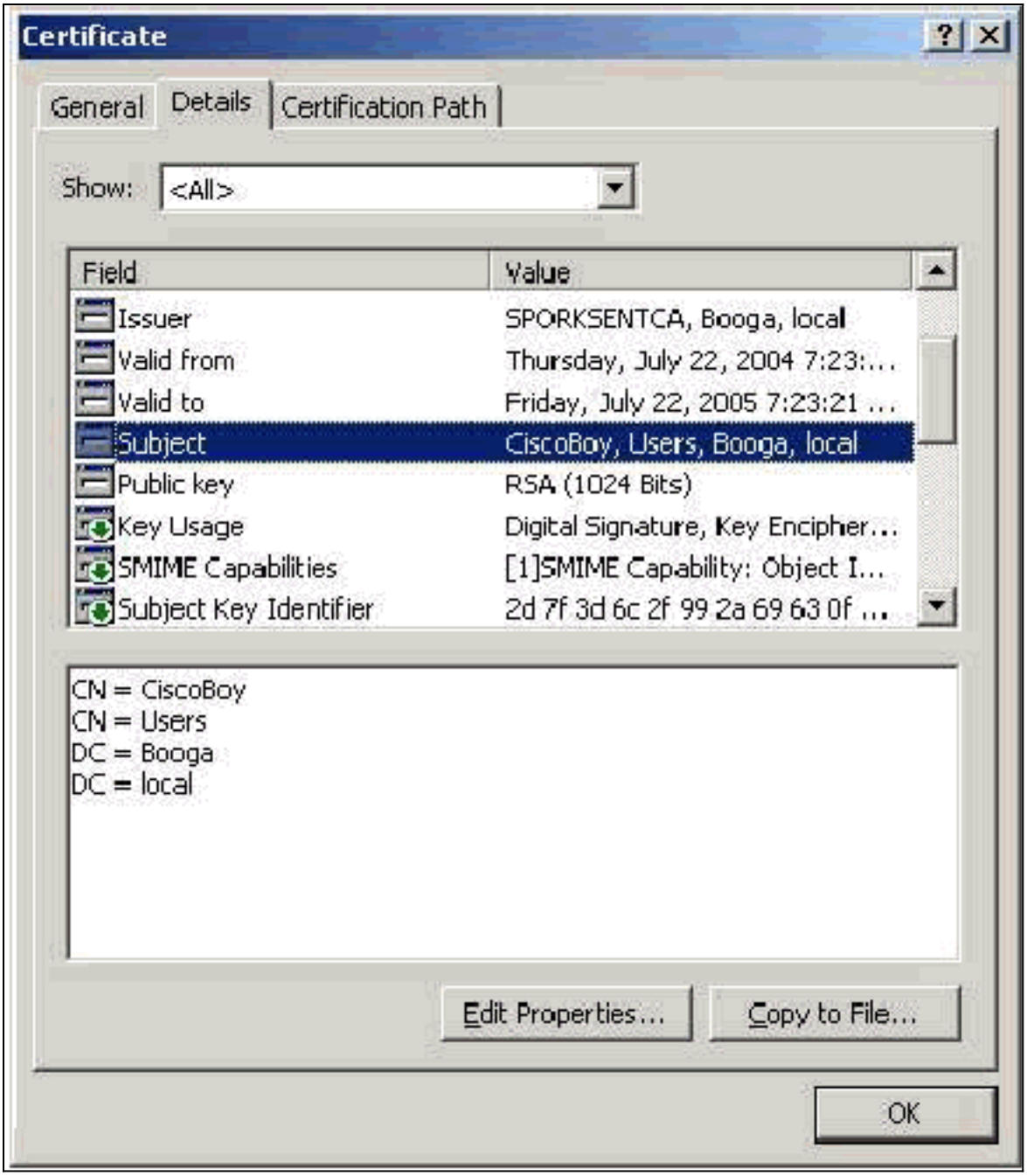
Verbesserte Schlüsselverwendungsfelder

Das Feld Enhanced Key Usage (Erweiterte Schlüsselverwendung) gibt den beabsichtigten Zweck des Zertifikats an und muss die Clientauthentifizierung enthalten. Dieses Feld ist obligatorisch, wenn Sie die Microsoft-Komponente für PEAP und EAP-TLS verwenden. Wenn Sie Microsoft-Zertifikatsdienste verwenden, wird dies in der eigenständigen Zertifizierungsstelle konfiguriert, wenn Sie im Dropdown-Menü "Beabsichtigte Verwendung" das **Client Authentication Certificate** (**Client-Authentifizierungszertifikat**) auswählen, und in der Enterprise-Zertifizierungsstelle, wenn Sie **Benutzer** aus dem Dropdown-Menü Zertifikatvorlage auswählen. Wenn Sie ein Zertifikat mit der Verwendung eines CSR mit Microsoft-Zertifikatsdiensten anfordern, haben Sie nicht die Möglichkeit, den beabsichtigten Zweck mit der eigenständigen Zertifizierungsstelle anzugeben. Daher ist das EKU-Feld nicht vorhanden. Bei der Enterprise-CA befindet sich die Dropdown-Liste "Beabsichtigte Verwendung". Einige CAs erstellen keine Zertifikate mit einem EKU-Feld. Sie sind nutzlos, wenn Sie die Microsoft EAP-Komponente verwenden.



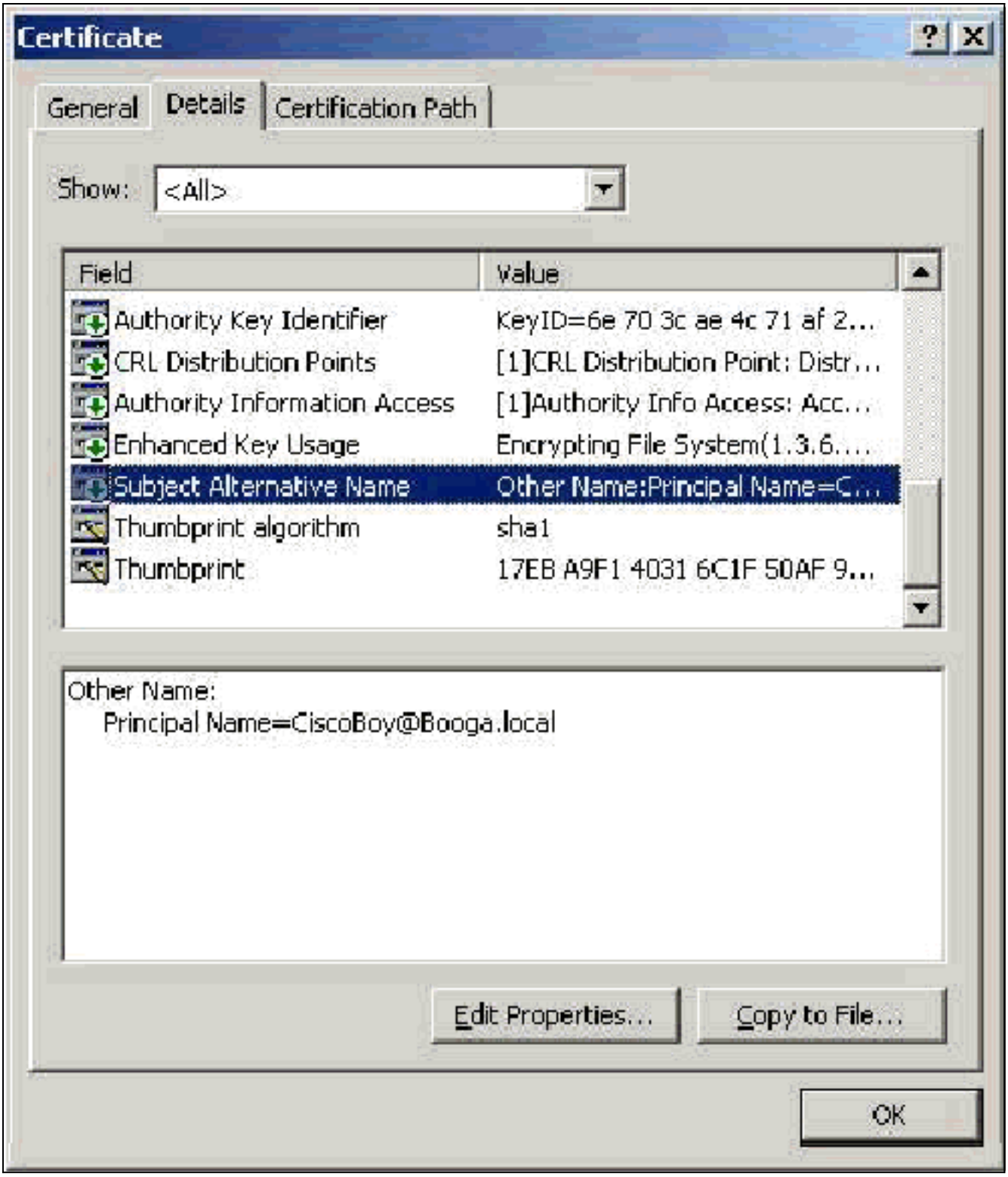
Fachgebiet

Dieses Feld wird beim Vergleich von CN verwendet. Die erste aufgeführte CN wird mit der Datenbank verglichen, um eine Übereinstimmung zu finden. Wenn eine Übereinstimmung gefunden wird, ist die Authentifizierung erfolgreich. Wenn Sie eine eigenständige Zertifizierungsstelle verwenden, wird der CN mit dem Inhalt des Felds Name im Formular für die Einreichung von Zertifikaten ausgefüllt. Wenn Sie die Enterprise-CA verwenden, wird der CN automatisch der in der Konsole Active Directory-Benutzer und -Computer aufgelistete Kontoname hinzugefügt (dies entspricht nicht unbedingt dem UPN oder dem NetBios-Namen).



Feld "Subject Alternative Name"

Das Feld "Subject Alternative Name" wird im SAN-Vergleich verwendet. Das aufgelistete SAN wird mit der Datenbank verglichen, um eine Übereinstimmung zu finden. Wenn eine Übereinstimmung gefunden wird, ist die Authentifizierung erfolgreich. Wenn Sie die Enterprise-CA verwenden, wird das SAN automatisch mit dem Active Directory-Anmeldenamen @domäne (UPN) versehen. Die Standalone-CA enthält kein SAN-Feld, sodass Sie keinen SAN-Vergleich verwenden können.



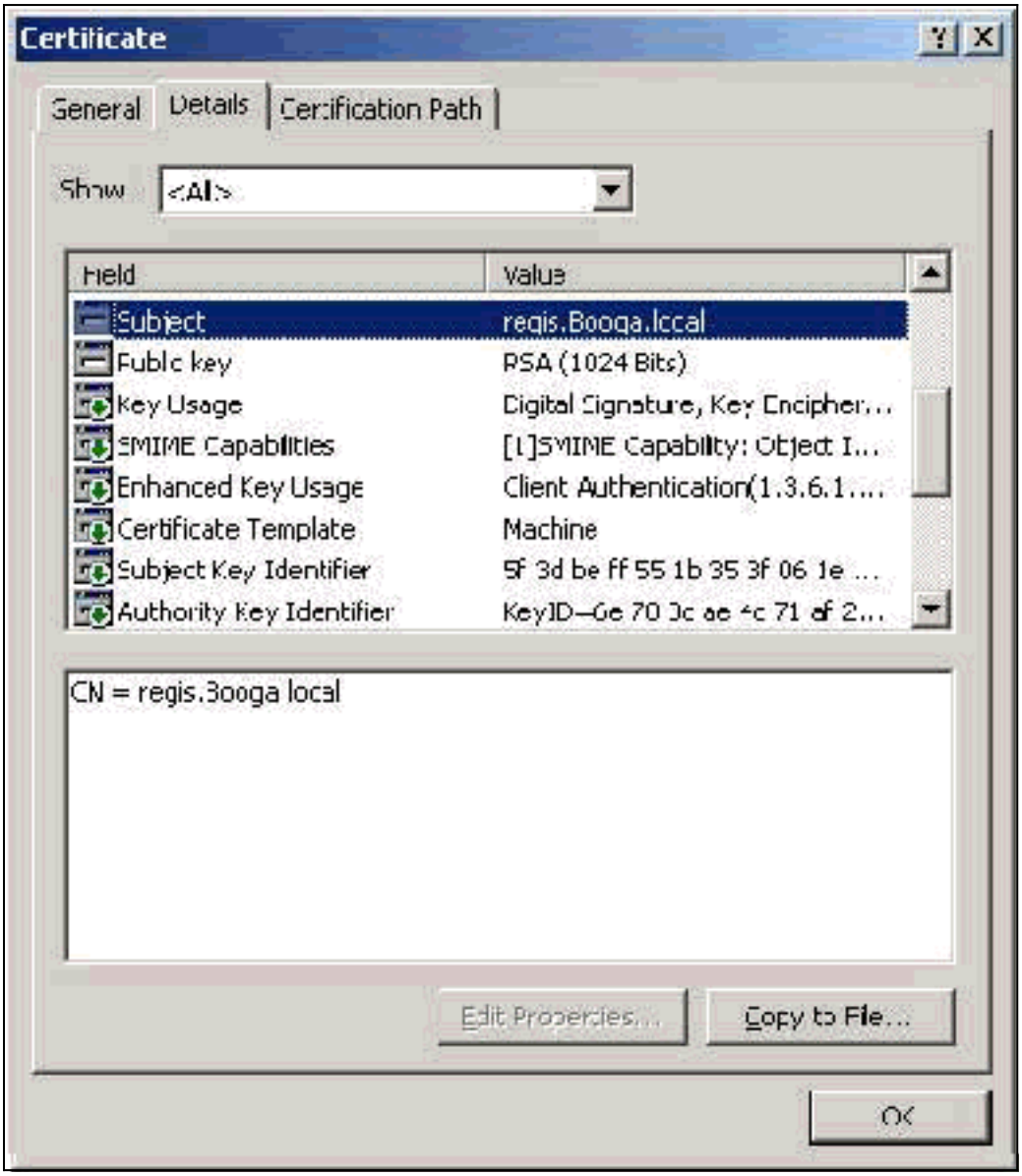
Computerzertifikate

In EAP-TLS werden Computerzertifikate verwendet, um den Computer bei der Verwendung der Computerauthentifizierung positiv zu identifizieren. Sie können auf diese Zertifikate nur zugreifen, wenn Sie Ihre Microsoft Enterprise-CA für die automatische Registrierung von Zertifikaten konfigurieren und dem Computer der Domäne beitreten. Das Zertifikat wird automatisch erstellt, wenn Sie die Active Directory-Anmeldeinformationen des Computers verwenden und diese im lokalen Computerspeicher installieren. Computer, die bereits Mitglieder der Domäne sind, bevor Sie die automatische Registrierung konfigurieren, erhalten beim nächsten Neustart von Windows ein Zertifikat. Das Computerzertifikat wird im MMC-Snap-In **Certificates (Local Computer) > Personal > Certificates (Personal > Certificates** folder (**Personal > Certificates** folder) (Local

Computer) wie in Server Certificates (Serverzertifikate) installiert. Sie können diese Zertifikate nicht auf einem anderen Computer installieren, da Sie den privaten Schlüssel nicht exportieren können.

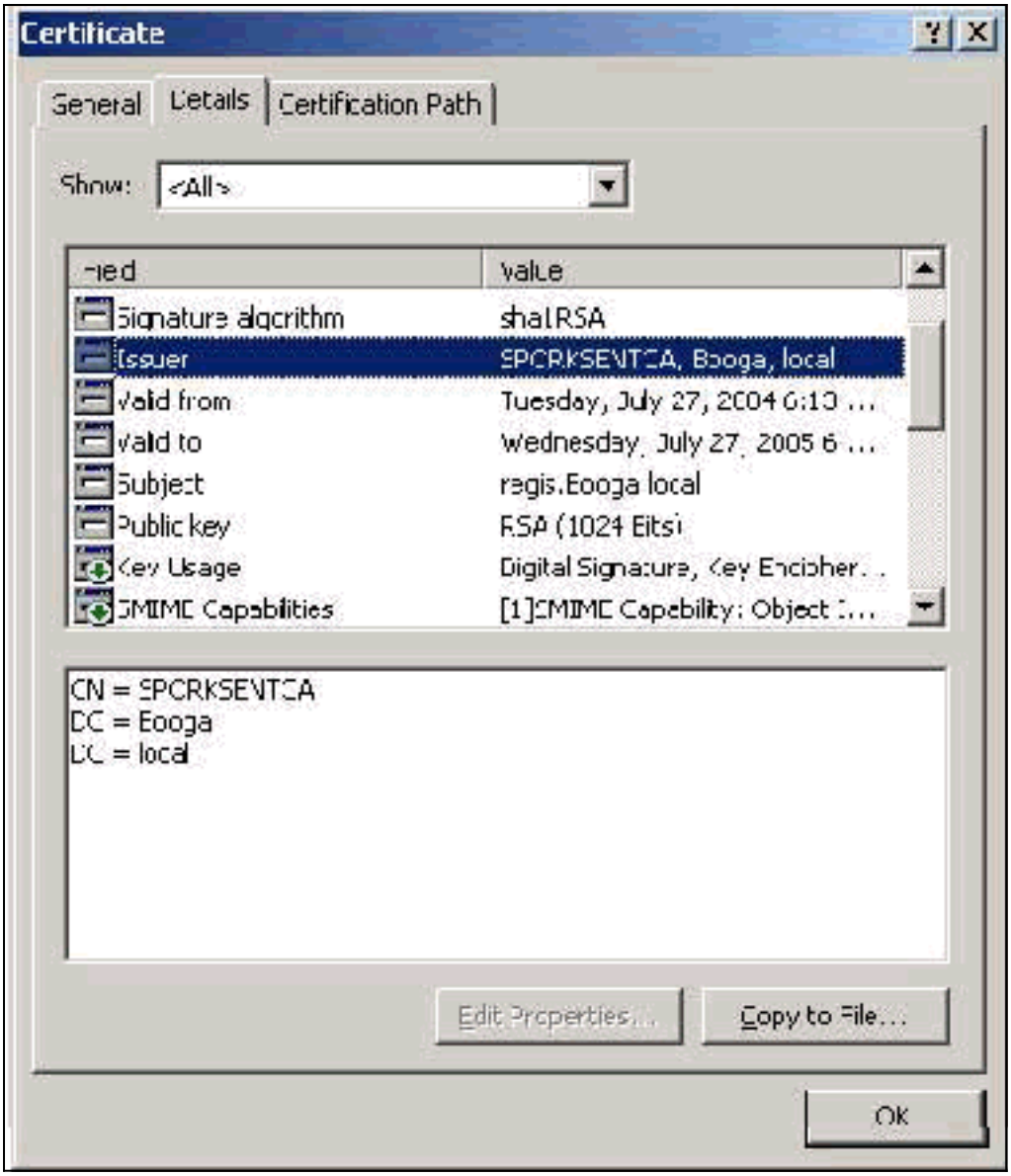
Betreff- und SAN-Felder

Die Felder Betreff und SAN identifizieren den Computer. Der Wert wird durch den vollqualifizierten Namen des Computers eingetragen und wird zur Bestimmung des Felds "Issued to" (Ausgestellt für) auf der Registerkarte "General" (Allgemein) des Zertifikats verwendet. Er ist für die Felder "Subject" (Betreff) und "SAN" identisch.



Ausgabefeld

Das Ausstellungsfeld identifiziert die Zertifizierungsstelle, die das Zertifikat ausgeschnitten hat. Verwenden Sie diesen Wert, um den Wert des Felds Issued by (Ausgestellt nach) auf der Registerkarte General (Allgemein) des Zertifikats zu bestimmen. Es wird mit dem Namen der CA ausgefüllt.



Anhang A: Allgemeine Zertifikaterweiterungen

.csr: Dies ist eigentlich kein Zertifikat, sondern eine Zertifikatssignierungsanforderung. Es handelt sich um eine Textdatei mit folgendem Format:

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

.pvk: Diese Erweiterung gibt einen privaten Schlüssel an, obwohl die Erweiterung nicht garantiert, dass der Inhalt tatsächlich ein privater Schlüssel ist. Der Inhalt muss in einem einfachen Text mit folgendem Format vorliegen:

```
-----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: Dies ist eine generische Erweiterung, die ein Zertifikat kennzeichnet. Server-, Root CA- und Intermediate CA-Zertifikate können in diesem Format vorliegen. Es handelt sich in der Regel um eine einfache Textdatei mit einer Erweiterung, die Sie nach Bedarf ändern können. Sie kann entweder DAS- oder Base 64-Format sein. Sie können dieses Format in den Windows-Zertifikatsspeicher importieren.

.pem - Diese Erweiterung steht für Privacy Enhanced Mail. Diese Erweiterung wird häufig unter UNIX, Linux, BSD usw. verwendet. Sie wird in der Regel für Serverzertifikate und private Schlüssel verwendet und ist in der Regel eine Textdatei mit einer Erweiterung, die Sie bei Bedarf von .pem zu .cer ändern können, um sie in den Windows-Zertifikatsspeicher zu importieren.

Der interne Inhalt von .cer- und .pem-Dateien sieht im Allgemeinen wie die folgende Ausgabe aus:

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

.pfx - Diese Erweiterung steht für Personal Information Exchange. Dieses Format ist eine Methode, mit der Sie Zertifikate in einer einzigen Datei bündeln können. Beispielsweise können Sie ein Serverzertifikat und den zugehörigen privaten Schlüssel und das Stammzertifizierungszertifikat in einer Datei bündeln und die Datei problemlos in den entsprechenden Windows-Zertifikatsspeicher importieren. Sie wird am häufigsten für Server- und Clientzertifikate verwendet. Wenn jedoch ein Zertifikat der Stammzertifizierungsstelle enthalten ist, wird das Zertifikat der Stammzertifizierungsstelle immer im Speicher des aktuellen Benutzers anstelle des lokalen Computerspeichers installiert, selbst wenn der lokale Computerspeicher für die Installation angegeben ist.

.p12: Dieses Format wird in der Regel nur mit einem Client-Zertifikat angezeigt. Sie können dieses Format in den Windows-Zertifikatsspeicher importieren.

.p7b: Dieses andere Format speichert mehrere Zertifikate in einer Datei. Sie können dieses Format in den Windows-Zertifikatsspeicher importieren.

Anhang B: Konvertierung des Zertifikatsformats

In den meisten Fällen erfolgt die Zertifikatskonvertierung, wenn Sie die Erweiterung (z. B. von .pem auf .cer) ändern, da die Zertifikate in der Regel im Textformat vorliegen. Manchmal ist ein

Zertifikat nicht im Klartextformat, und Sie müssen es mithilfe eines Tools wie OpenSSL konvertieren. Beispielsweise kann der ACS Solution Engine keine Zertifikate im PFX-Format installieren. Aus diesem Grund müssen Sie das Zertifikat und den privaten Schlüssel in ein verwendbares Format konvertieren. Dies ist die grundlegende Befehlssyntax für OpenSSL:

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

Sie werden zur Eingabe des Importpassworts und der PEM-Kennzeichenfolge aufgefordert. Diese Kennwörter müssen identisch sein und das private Schlüsselkennwort sein, das beim Exportieren der PFX-Datei angegeben wird. Die Ausgabe ist eine einzelne .pem-Datei, die alle Zertifikate und privaten Schlüssel in der PFX-Datei enthält. Diese Datei kann im ACS sowohl als Zertifikat als auch als private Schlüsseldatei bezeichnet werden und wird problemlos installiert.

Anhang C: Gültigkeitszeitraum der Bescheinigung

Ein Zertifikat kann nur während seiner Gültigkeitsdauer verwendet werden. Die Gültigkeitsdauer eines Zertifikats der Stammzertifizierungsstelle wird bestimmt, wenn die Stammzertifizierungsstelle eingerichtet ist und kann variieren. Die Gültigkeitsdauer eines Zertifikats der erweiterten Zertifizierungsstelle wird bestimmt, wenn die Zertifizierungsstelle errichtet wurde und die Gültigkeitsdauer der ihr unterstehenden Stammzertifizierungsstelle nicht überschreiten darf. Die Gültigkeitsdauer für Server-, Client- und Machine-Zertifikate wird bei Microsoft Certificate Services automatisch auf ein Jahr festgelegt. Dies kann nur geändert werden, wenn Sie die Windows-Registrierung gemäß dem Microsoft Knowledge Base-Artikel 254632 hacken und die Gültigkeitsdauer der Root-CA nicht überschreiten. Die Gültigkeitsdauer der selbstsignierten Zertifikate, die von ACS generiert werden, beträgt immer ein Jahr und kann in der aktuellen Version nicht geändert werden.

Zugehörige Informationen

- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support - Cisco Systems