EAP, versie 1.01-certificaatgids

Inhoud

Inleiding

Dit document verduidelijkt een deel van de verwarring die gepaard gaat met de verschillende certificatypen, formaten en vereisten die aan de verschillende vormen van het Extensible Authentication Protocol (EAP) zijn gekoppeld. De vijf certificatypen die betrekking hebben op EAP zijn Server, Root CA, Intermediate CA, Client, en Machine. Deze certificaten zijn in verschillende formaten te vinden en er kunnen verschillende eisen worden gesteld aan elk van deze certificaten op basis van de betrokken MAP-implementatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Server-certificaten

Het servercertificaat is geïnstalleerd op de RADIUS-server en het belangrijkste doel ervan is in EAP de gecodeerde TLS-tunnel (Transport Layer Security) te creëren die de verificatieinformatie beschermt. Wanneer u EAP-MSCHAPv2 gebruikt, krijgt het servercertificaat een secundaire rol, namelijk om de RADIUS-server te identificeren als een vertrouwde entiteit voor verificatie. Deze secundaire rol wordt vervuld door gebruik te maken van het veld Uitgebreide Key Gebruik (EKU). Het EKU-veld identificeert het certificaat als een geldig servercertificaat en verifieert dat de basisCA die het certificaat heeft afgegeven, een betrouwbaar basiscertificaat is. Dit vereist de aanwezigheid van het Root CA-certificaat. Cisco Secure ACS vereist dat het certificaat hetzij Base64-gecodeerd is, hetzij DER-gecodeerd binair X.509 v3-formaat.

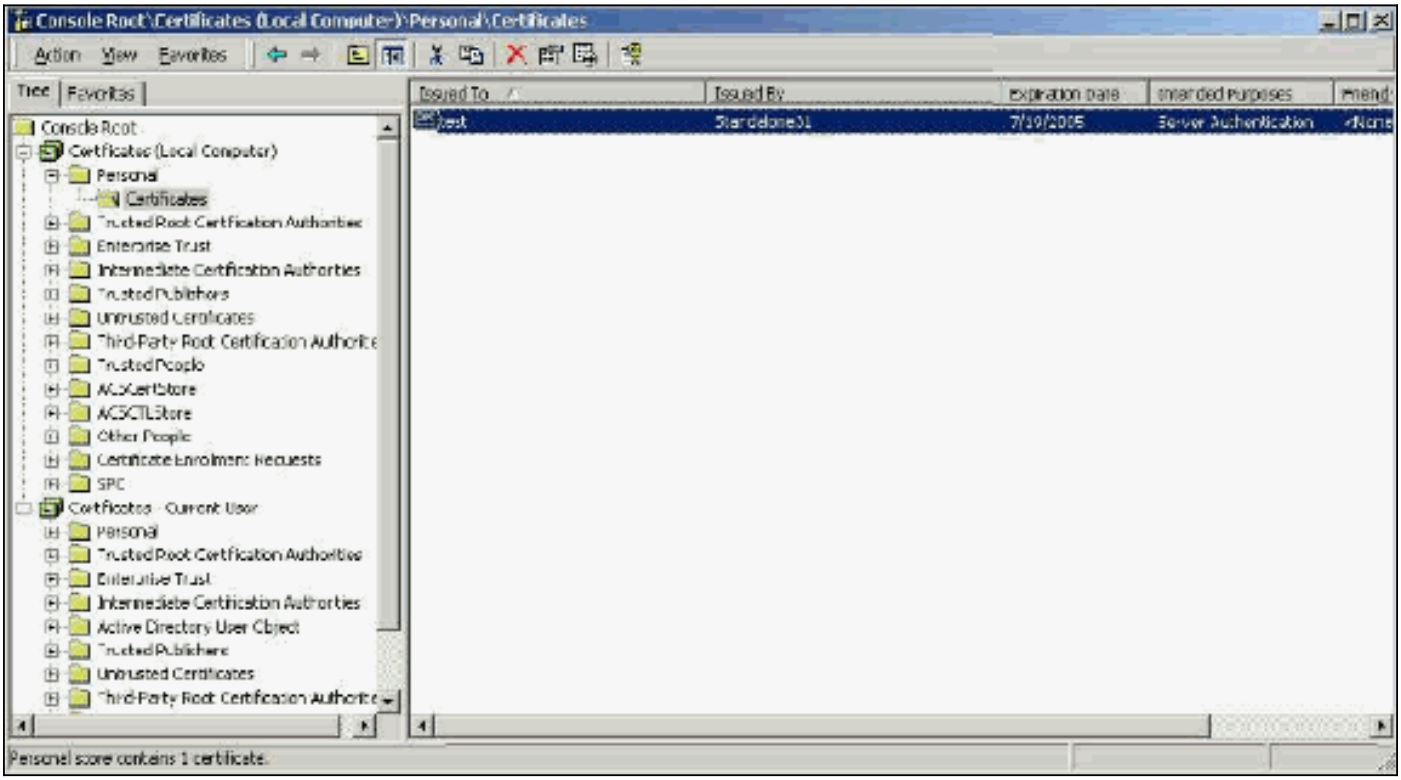
U kunt dit certificaat maken met behulp van een CSR (certificaatsignaalaanvraag) bij ACS, dat aan een CA wordt verzonden. U kunt het certificaat ook snijden met behulp van een interne CA (zoals Microsoft certificaatservices)-formulier. Het is belangrijk om op te merken dat, terwijl u het servercertificaat kunt maken met een belangrijke grootte groter dan 1024, elke sleutel groter dan 1024 niet werkt met PEAP. De cliënt blijft zelfs staan als de authenticatie passeert.

Als u het certificaat maakt met gebruik van een CSR, wordt het gemaakt met een .cer, .pem of .txt formaat. In zeldzame gevallen wordt het zonder verlenging gemaakt. Zorg ervoor dat uw certificaat een eenvoudig tekstbestand is met een uitbreiding die u naar wens kunt wijzigen (het ACS-apparaat gebruikt de bestandsextensie .cer of .pem). Als u een CSR gebruikt, wordt de privé-toets van het certificaat bovendien aangemaakt in het pad dat u specificeert als een afzonderlijk bestand dat al dan niet een extensie heeft en waaraan een wachtwoord is gekoppeld (het wachtwoord is vereist voor installatie op ACS). Ongeacht de verlenging, zorg er dan voor dat het een gewoon tekstbestand is met een extensie die u naar wens kunt wijzigen (het ACS-apparaat gebruikt de bestandsextensie .pvk of .pem). Als geen pad wordt opgegeven voor de privé-toets, slaat ACS de toets op in de C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs folder en kijkt in deze folder als geen pad is opgegeven voor het privé-sleutelbestand wanneer u het certificaat installeert.

Als het certificaat is gemaakt met behulp van het formulier voor het indienen van het Microsoft certificaatcertificaat, zorg er dan voor dat u de sleutels als exporteerbaar aanduidt, zodat u het certificaat in ACS kunt installeren. De invoering van een certificaat vereenvoudigt het installatieproces aanzienlijk. U kunt deze rechtstreeks in de juiste Windows-winkel installeren vanuit de webinterface certificaatservices en vervolgens op ACS-opslag installeren met behulp van de GN als referentie. Een certificaat dat in de lokale computerwinkel is geïnstalleerd, kan ook vanuit Windows-opslagindeling worden geëxporteerd en met gemak op een andere computer worden geïnstalleerd. Bij uitvoer van dit soort certificaat moeten de sleutels worden gemarkeerd

als uitvoerbaar en met een wachtwoord worden ingevuld. Het certificaat verschijnt dan in .pfx-formaat, dat de privétoets en het servercertificaat bevat.

Als u het programma correct in de Windows-certificeringswinkel hebt geïnstalleerd, moet het servercertificaat worden weergegeven in de map **Certificaten (lokale computer) > Persoonlijk > Certificaten** zoals in dit voorbeeldvenster wordt weergegeven.



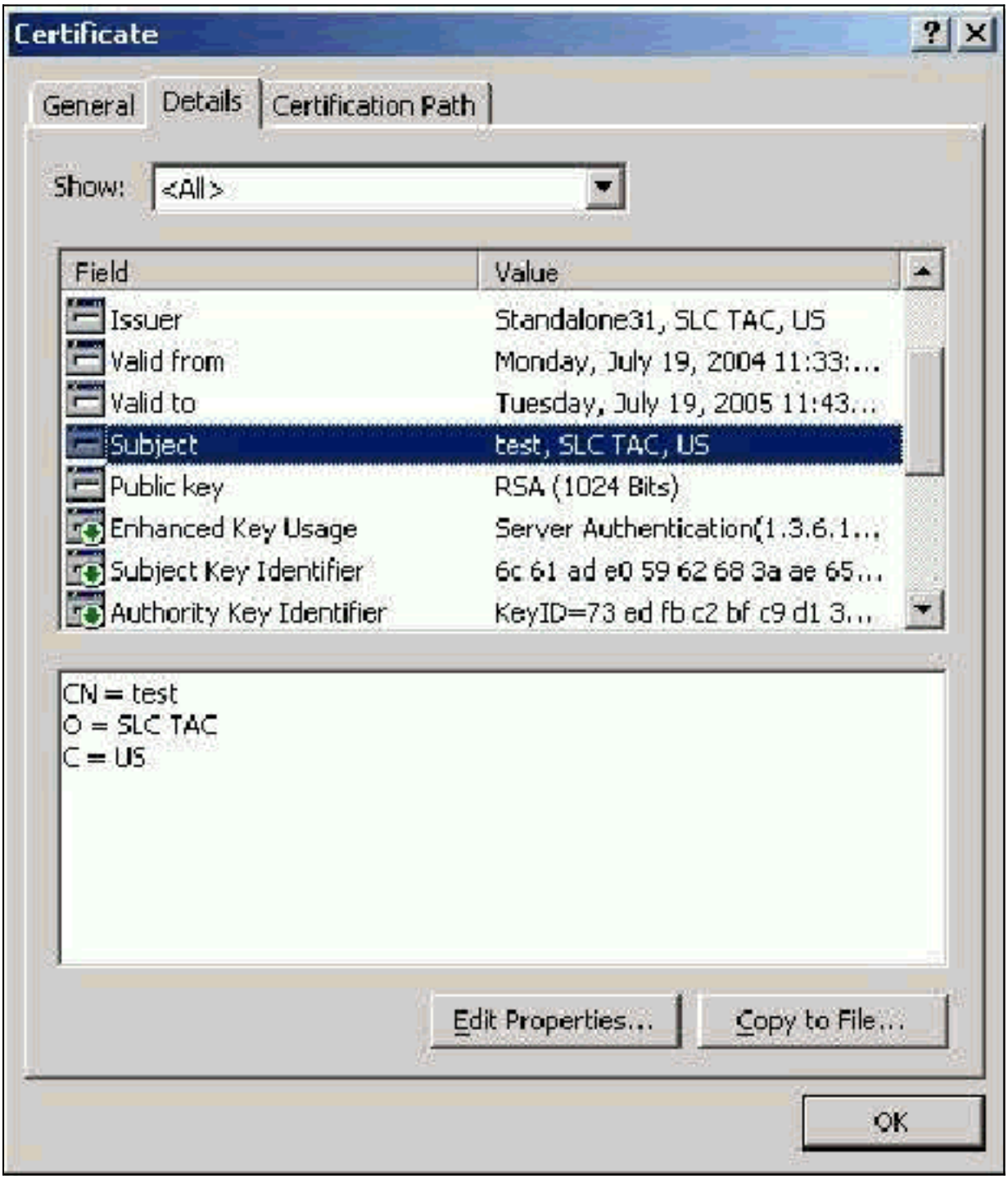
Zelfgetekende certificaten zijn certificaten die u maakt zonder wortel of tussenkomst van de CA. Ze hebben dezelfde waarde in zowel de onderwerpregel- als de emittentenvelden als een Root CA-certificaat. De meeste zelfgetekende certificaten gebruiken X.509 v1-formaat. Daarom werken ze niet met ACS. Vanaf versie 3.3 kunnen ACS echter zelf certificaten creëren die u voor EAP-TLS en PEAP kunt gebruiken. Gebruik geen sleutelgrootte van meer dan 1024 voor compatibiliteit met PEAP en EAP-TLS. Als u een zelf-ondertekend certificaat gebruikt, werkt het certificaat ook in de hoedanigheid van het Root CA-certificaat en moet het worden geïnstalleerd in de **certificeringsinstanties (Local Computer) > Trusted Root Certified** Automation **Services > de** map **Certificates** van de client wanneer u de Microsoft EAP-aanvraag gebruikt. Het installeert automatisch in de vertrouwde wortelcertificatenopslag op de server. Het moet echter nog steeds worden vertrouwd in de certificaatlijst in de ACS-certificaatinstelling. Zie de sectie Root CA Certificates voor meer informatie.

Omdat zelfgetekende certificaten worden gebruikt als de Root CA-certificering voor servercertificatie wanneer u de Microsoft EAP-smeekbede gebruikt en omdat de geldigheidsperiode niet kan worden verlengd vanaf de standaard van één jaar, raadt Cisco u aan deze alleen voor EAP als tijdelijke maatregel te gebruiken totdat u een traditionele CA kunt gebruiken.

Onderwerp

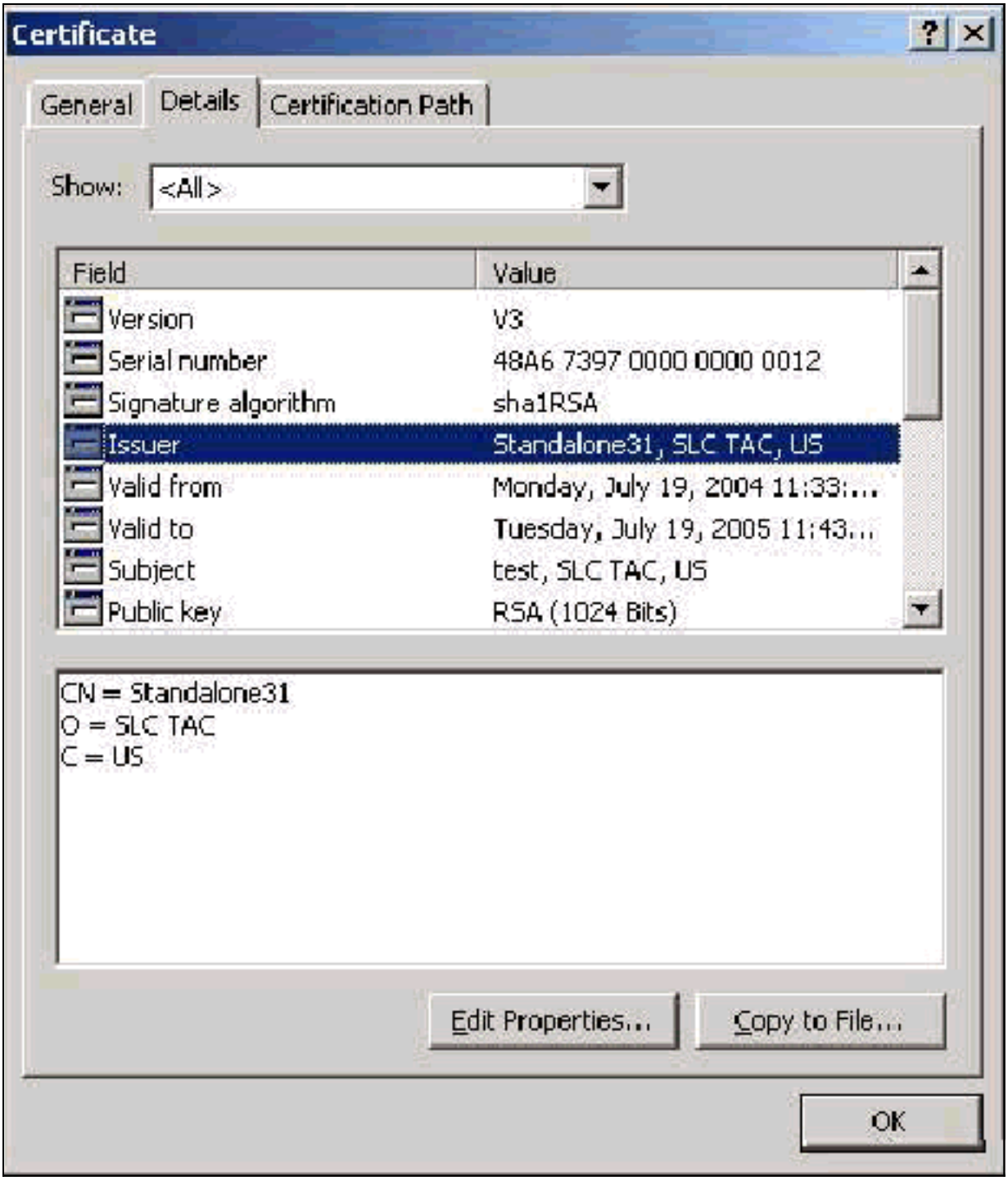
Het veld Onderwerp identificeert het certificaat. De GN-waarde wordt gebruikt om de Opgegeven te bepalen in het veld Algemeen op het certificaat en is ingevuld met de informatie die u in het veld certificaatonderwerp invoert in het CSR-dialoogvenster van ACS of met de informatie uit het veld Naam in Microsoft certificaatservices. De GN-waarde wordt gebruikt om ACS te vertellen welk

certificaat het van de opslagplaats van het plaatselijke machinecertificaat moet gebruiken indien gebruik wordt gemaakt van de mogelijkheid om het opslagcertificaat te installeren.



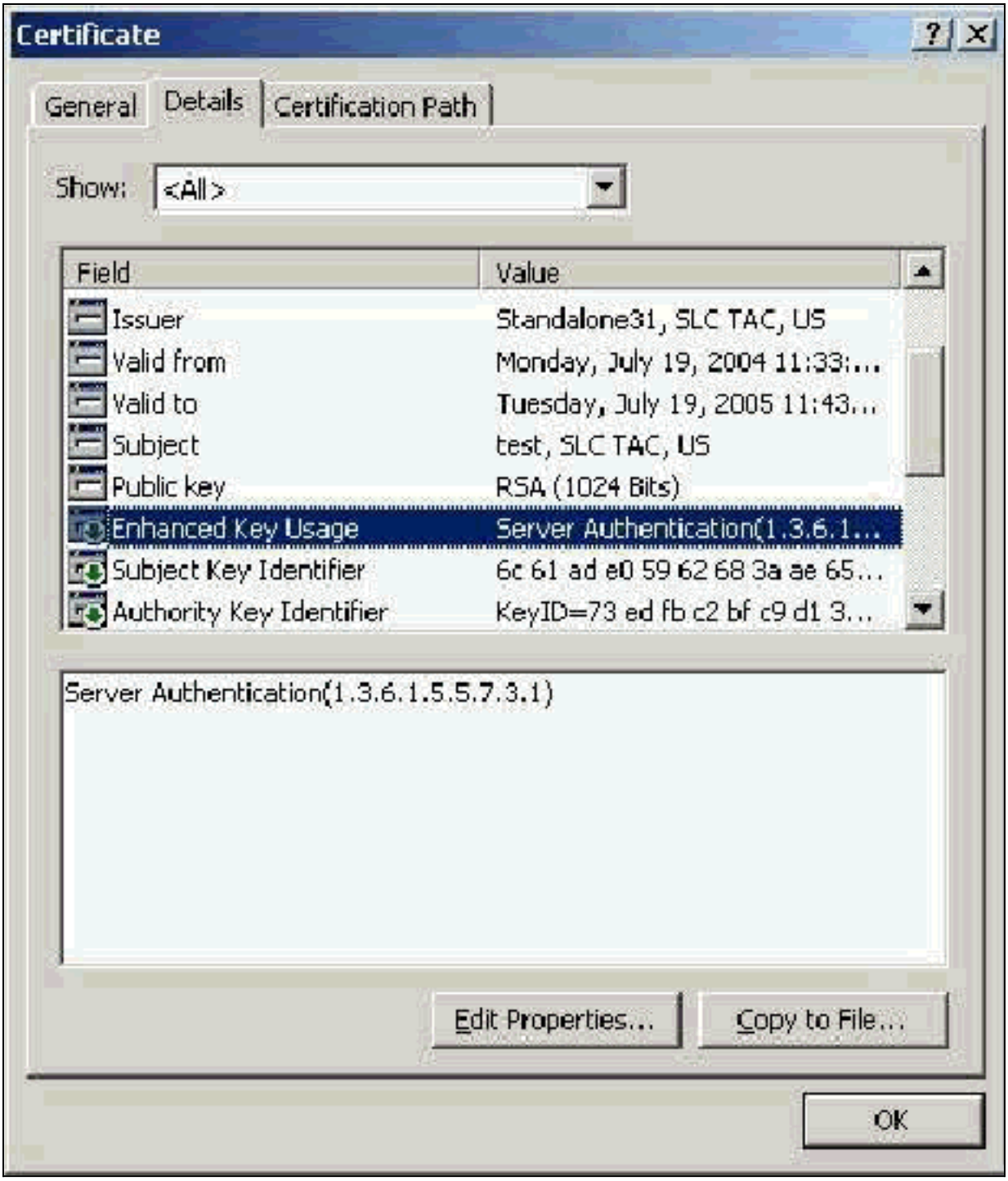
Uitgifteveld

Het veld Uitgever identificeert de CA die het certificaat heeft gesneden. Gebruik deze waarde om de waarde te bepalen van de uitgifte door veld in het tabblad Algemeen van het certificaat. Het is bevolkt met de naam van de CA.



Uitgebreid veld voor gebruik

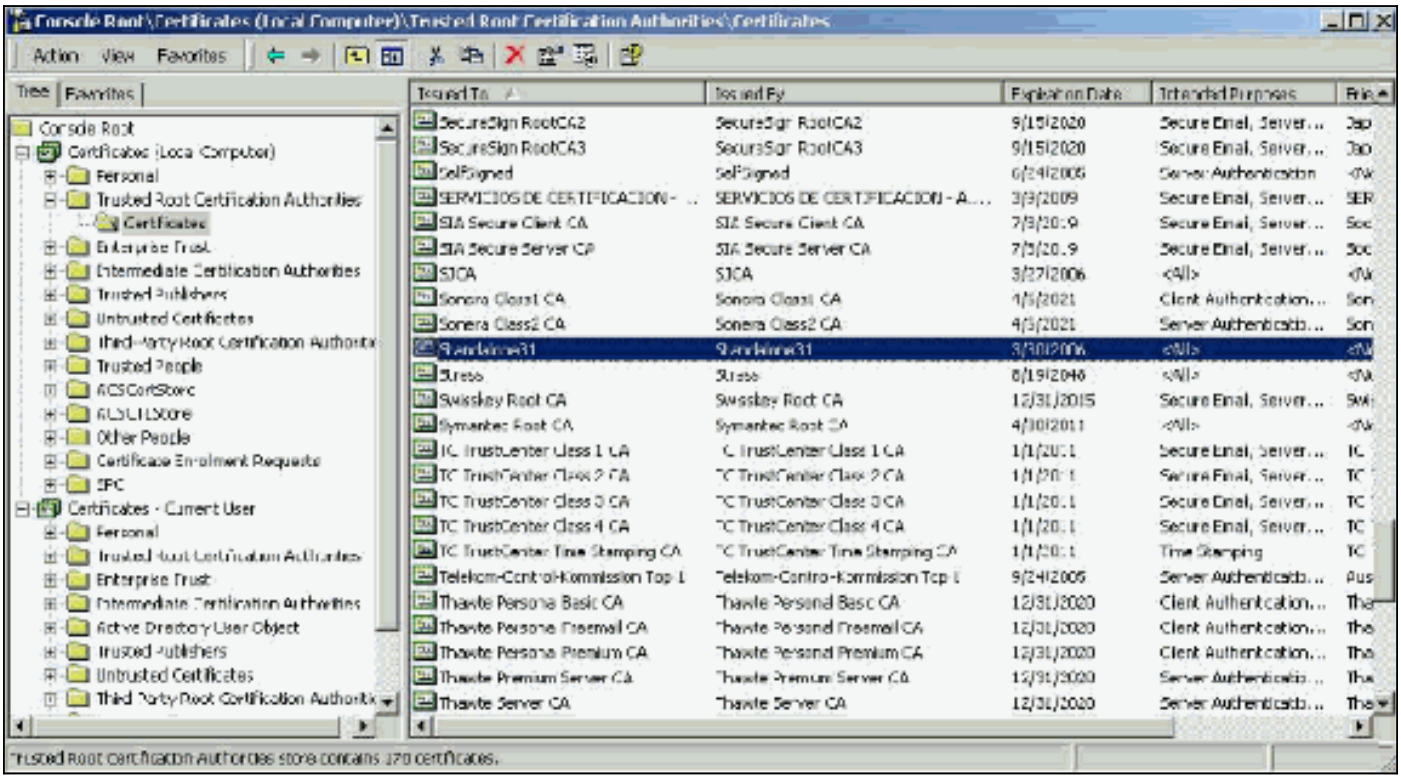
Het veld Uitgebreide sleutel voor gebruik identificeert het beoogde doel van het certificaat en moet worden vermeld als "serververificatie". Dit veld is verplicht als u de Microsoft Suppliciet voor PEAP en EAP-TLS gebruikt. Wanneer u Microsoft certificaatservices gebruikt, wordt dit ingesteld in de standalone CA met de selectie van **serververificatiecertificaat** uit de vervolgkeuzelijst Doelstelling en in de optie Enterprise CA met de selectie van **webserver** uit de vervolgkeuzelijst certificaatsjabloon. Als u een certificaat vraagt met het gebruik van een CSR met Microsoft certificaatservices, hebt u niet de optie om het beoogde doel te specificeren met de standalone CA. Daarom is het EKU-veld afwezig. Met de Enterprise CA, heb je de bedoelde doeloptie. Sommige CA's maken geen certificaten met een EKU-veld, dus ze zijn nutteloos wanneer u de Microsoft EAP-smeekbede gebruikt.



Root CA-certificaten

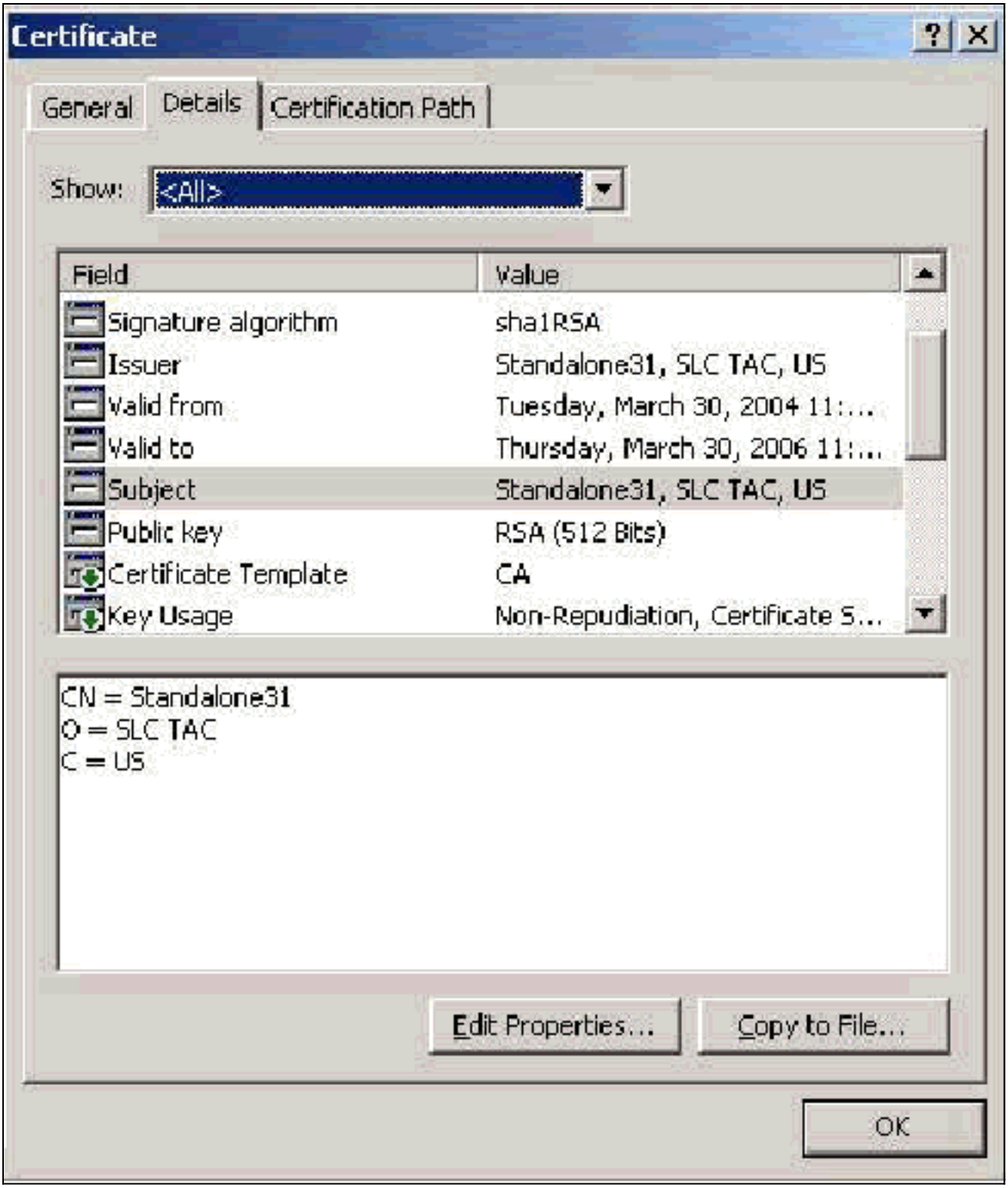
Het enige doel van het Root CA-certificaat is de identificatie van het servercertificaat (en, indien van toepassing, het Intermediate CA-certificaat) als een betrouwbaar certificaat voor ACS en de Windows EAP-MSCHAPv2-aanvrager. Het moet zich bevinden in de winkel Trusted Root-certificeringsinstanties in Windows op zowel de ACS-server als, in het geval van EAP-MSCHAPv2, op de clientcomputer. De meeste CA-certificaten van derden zijn geïnstalleerd bij Windows en er is weinig moeite mee. Als Microsoft certificaatservices wordt gebruikt en de certificaatserver op dezelfde machine staat als ACS, wordt het certificaat van hoofdlettertype automatisch geïnstalleerd. Als het Root CA-certificaat niet is gevonden in de winkel Trusted Root certificeringsinstanties in Windows, dan moet dit aan uw CA zijn aangeschaft en zijn geïnstalleerd. Als u het programma correct in de Windows-certificeringswinkel hebt geïnstalleerd, moet het Root CA-certificaat worden weergegeven in de map Certificaten **(Local Computer) > Trusted Root Certified** Certified **Certified** Certified **Automation** Services **>** zoals in dit voorbeeldvenster wordt

weergegeven.



Betreft: Uitgiftevelden

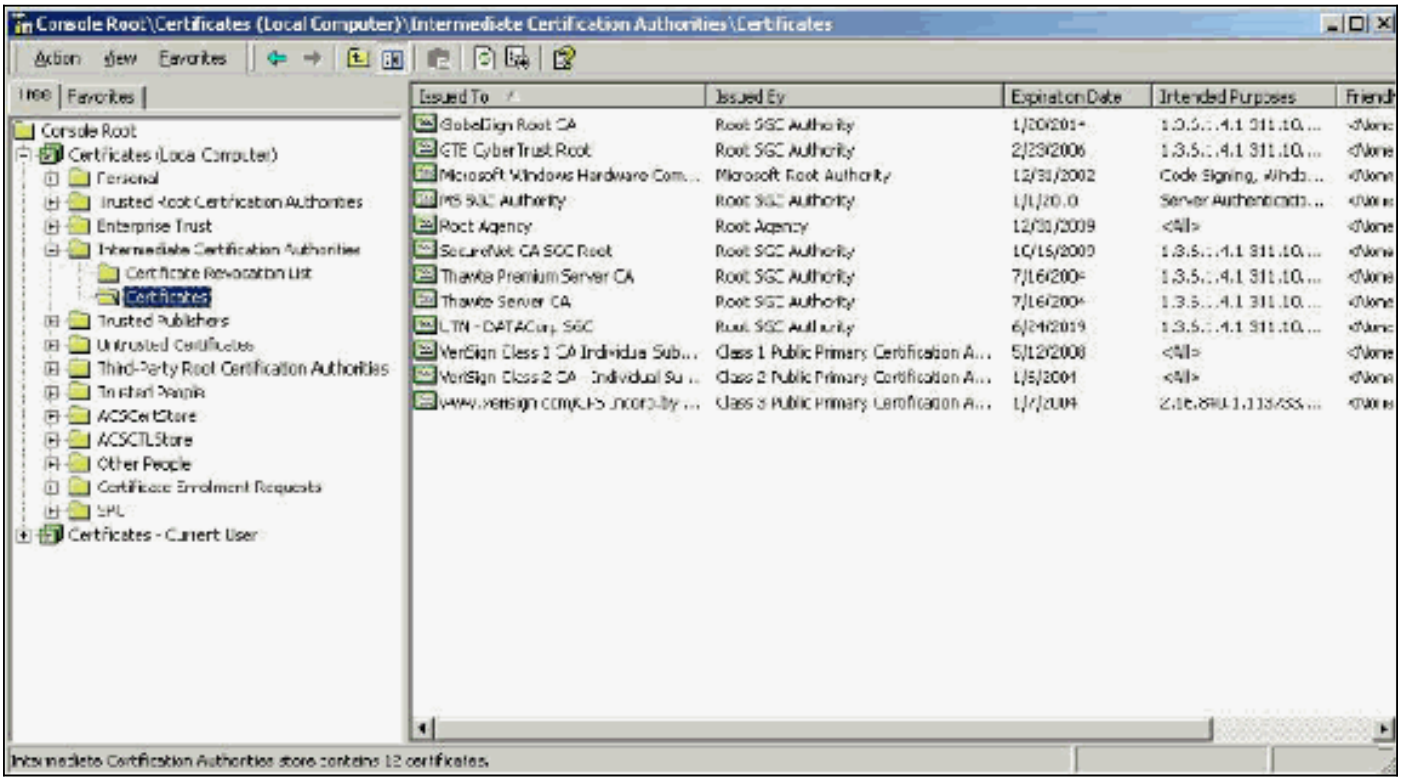
In de velden Onderwerp en Uitgifte wordt de CA geïdentificeerd en moet deze exact hetzelfde zijn. Gebruik deze velden om de Opgegeven tekst aan en uitgegeven door velden in het tabblad Algemeen van het certificaat te vullen. Ze zijn bevolkt met de naam van de wortel CA.



Intermediate CA-certificaten

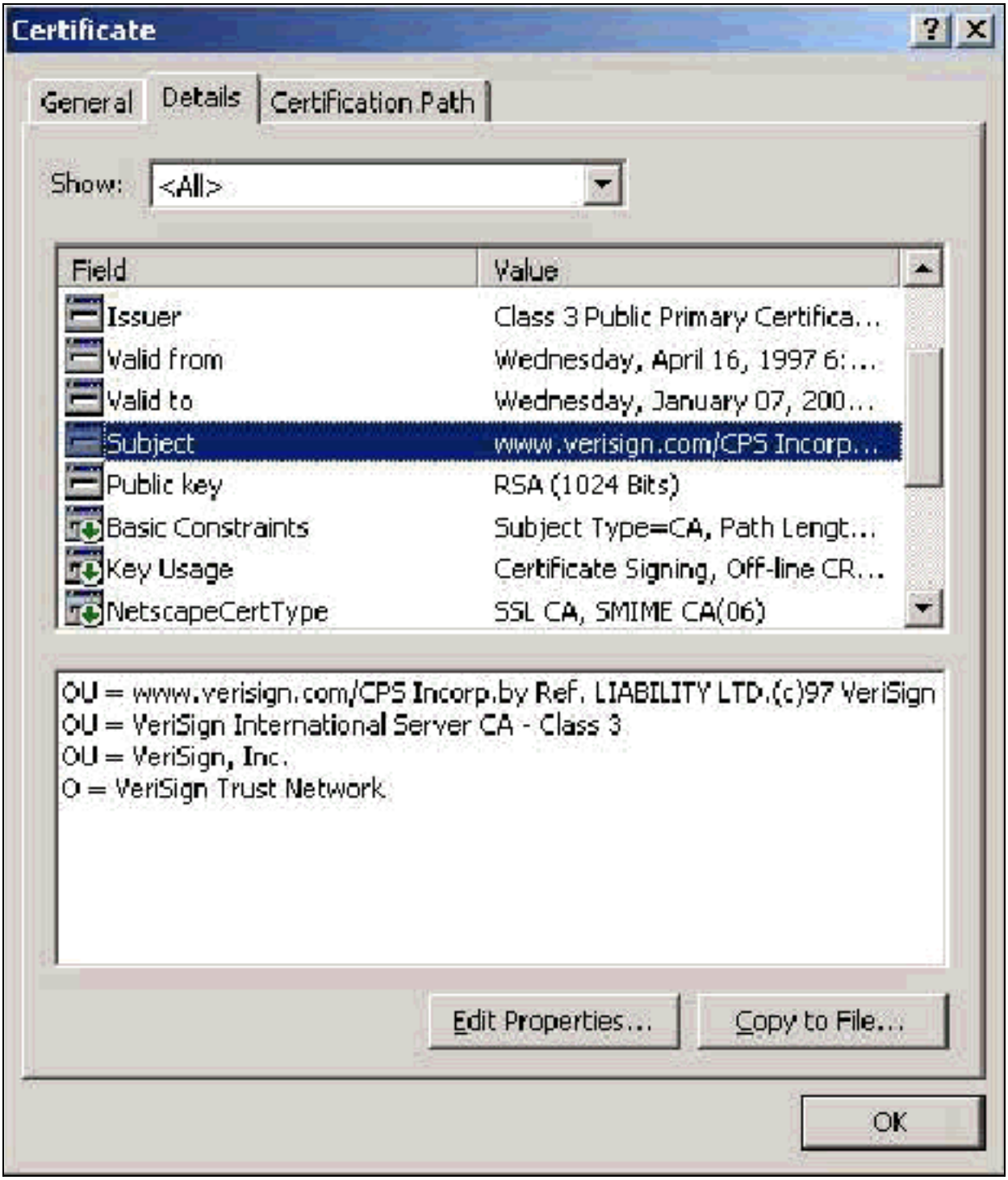
Intermediate CA Certificaten zijn certificaten die u gebruikt om CA te identificeren die aan een wortel CA ondergeschikt is. Sommige servercertificaten (de draadloze certificaten van Versizing) worden gemaakt met het gebruik van een intermediaire CA. Als een servercertificaat wordt gebruikt dat is gesneden door een midden CA, moet het middelste CA-certificaat worden geïnstalleerd in het gebied Intermediate Certified Autorité van de lokale machinewinkel op de ACS-server. Als de Microsoft EAP-smeekbede op de client wordt gebruikt, moet het Root CA-certificaat van de wortel CA dat het Intermediate CA-certificaat heeft gemaakt ook in de juiste winkel op de ACS-server en de client zijn, zodat de vertrouwensketen kan worden vastgesteld. Zowel het Root CA-certificaat als het Intermediate CA-certificaat moeten worden gemarkeerd als

vertrouwd in ACS en op de client. Meest middelste CA-certificaten zijn niet bij Windows geïnstalleerd, zodat u deze waarschijnlijk bij de verkoper moet kopen. Als u het product op de juiste manier in de Windows-certificaatwinkel hebt geïnstalleerd, verschijnt het CA-certificaat via de **certificaten (lokale computer) > Intermediate certificeringsinstanties >** map **certificaten** zoals in dit voorbeeldvenster wordt weergegeven.



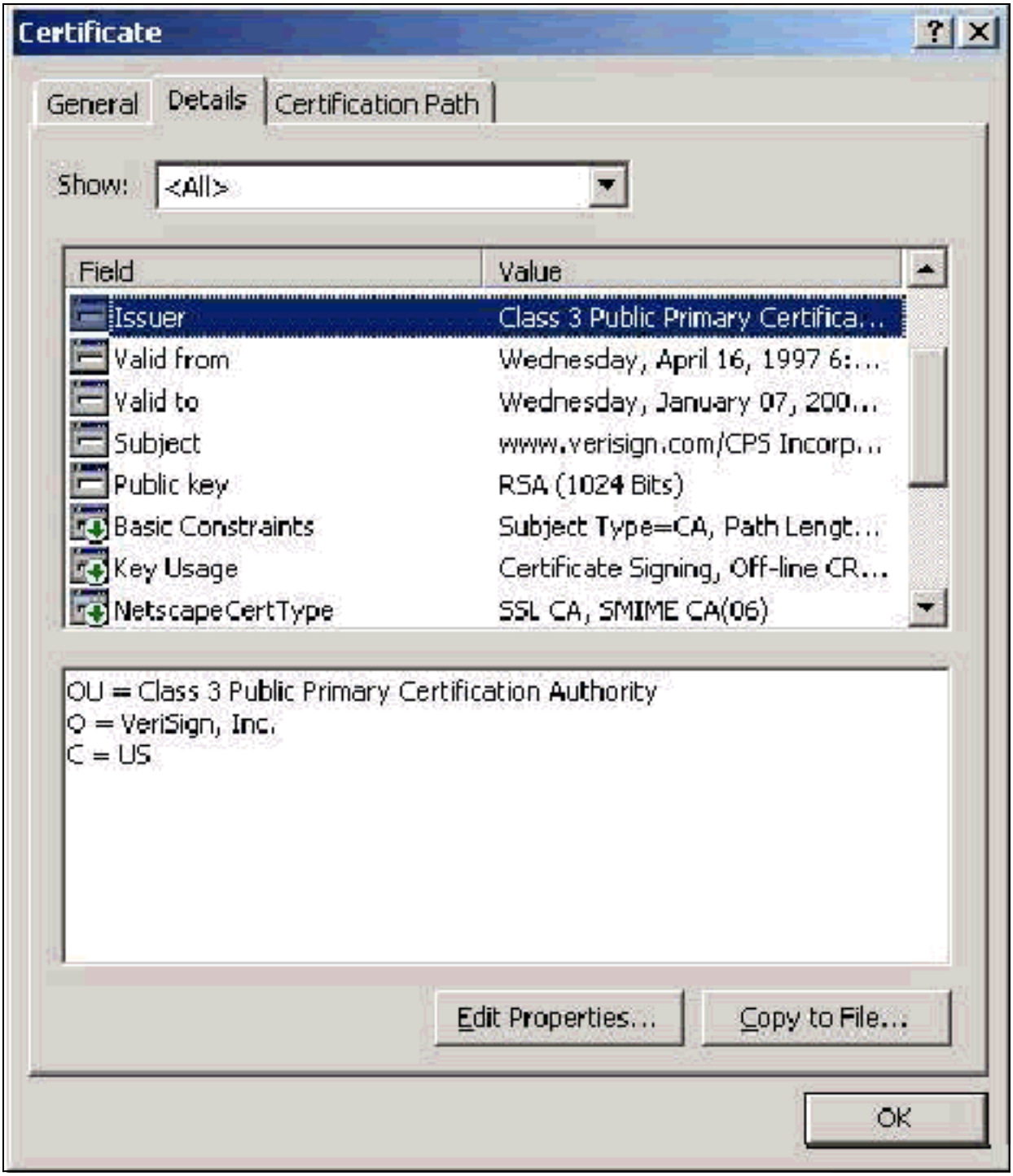
Onderwerp

Het veld Onderwerp identificeert de tussenliggende CA. Deze waarde wordt gebruikt om de Opgegeven tekst te bepalen in het veld Algemeen op het certificaat.



Uitgifteveld

Het veld Uitgever identificeert de CA die het certificaat heeft gesneden. Gebruik deze waarde om de waarde te bepalen van de uitgifte door veld in het tabblad Algemeen van het certificaat. Het is bevolkt met de naam van de CA.



Clientcertificaten

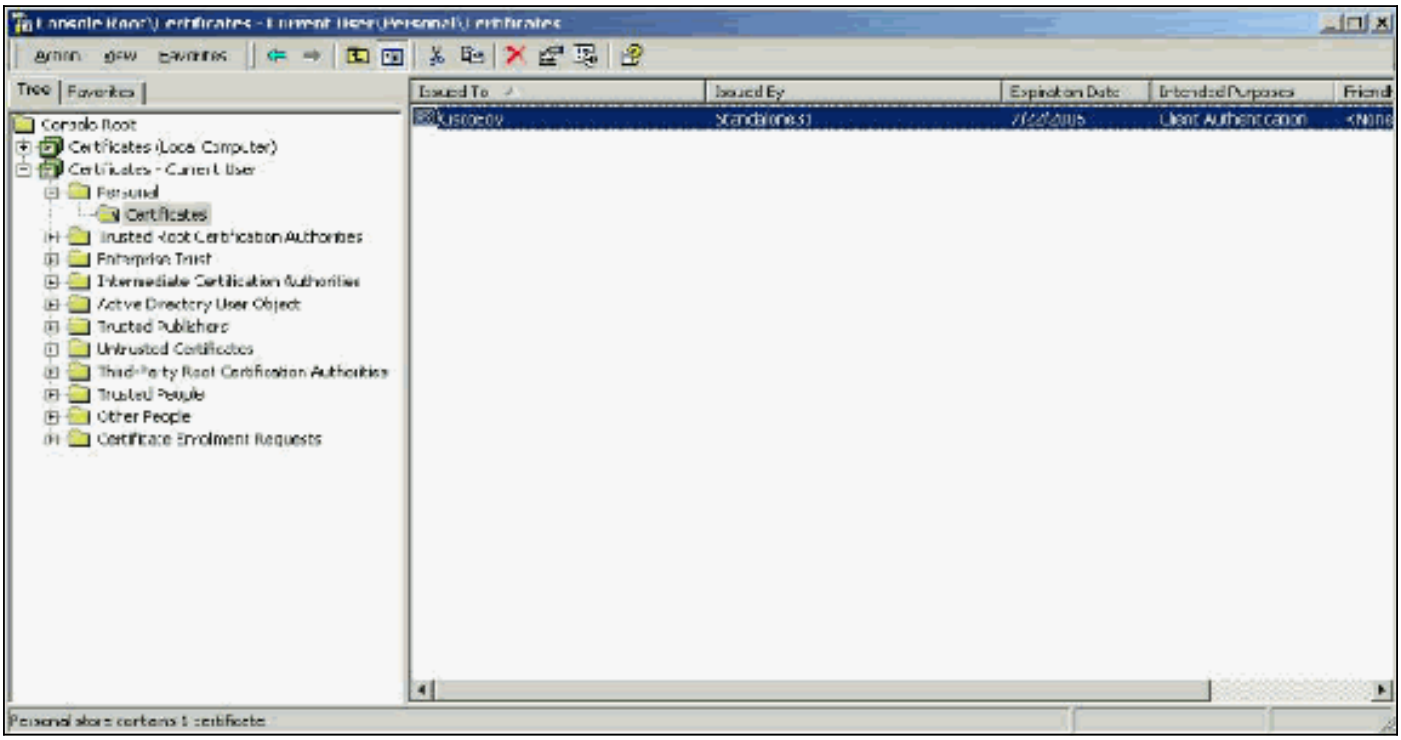
Clientcertificaten worden gebruikt om de gebruiker in het MAP-TLS positief te identificeren. Zij spelen geen rol bij de bouw van de TLS-tunnel en worden niet gebruikt voor encryptie. Positieve identificatie wordt op drie manieren bereikt:

- **GN (of naam)Vergelijking**—Vergelijk de GN in het certificaat met de gebruikersnaam in het gegevensbestand. Meer informatie over dit vergelijkingstype is opgenomen in de beschrijving van het onderwerpveld van het certificaat.
- **SAN Vergelijking**—Vergelijk de SAN in het certificaat met de gebruikersnaam in de database. Dit wordt alleen ondersteund vanaf ACS 3.2. Meer informatie over dit vergelijkingstype is opgenomen in de beschrijving van het veld Onderwerp Alternatieve Naam van het certificaat.
- **Binaire vergelijking**—vergelijkt het certificaat met een binair exemplaar van het certificaat dat

in de database is opgeslagen (dit kan alleen voor AD en LDAP worden gedaan). Als u certificaat binaire vergelijking gebruikt, moet u het gebruikerscertificaat in een binair formaat opslaan. Voor generieke LDAP en Actieve Map moet de eigenschap die het certificaat opslaat, ook de standaard LDAP-eigenschap zijn die "gebruikerscertificaat" wordt genoemd.

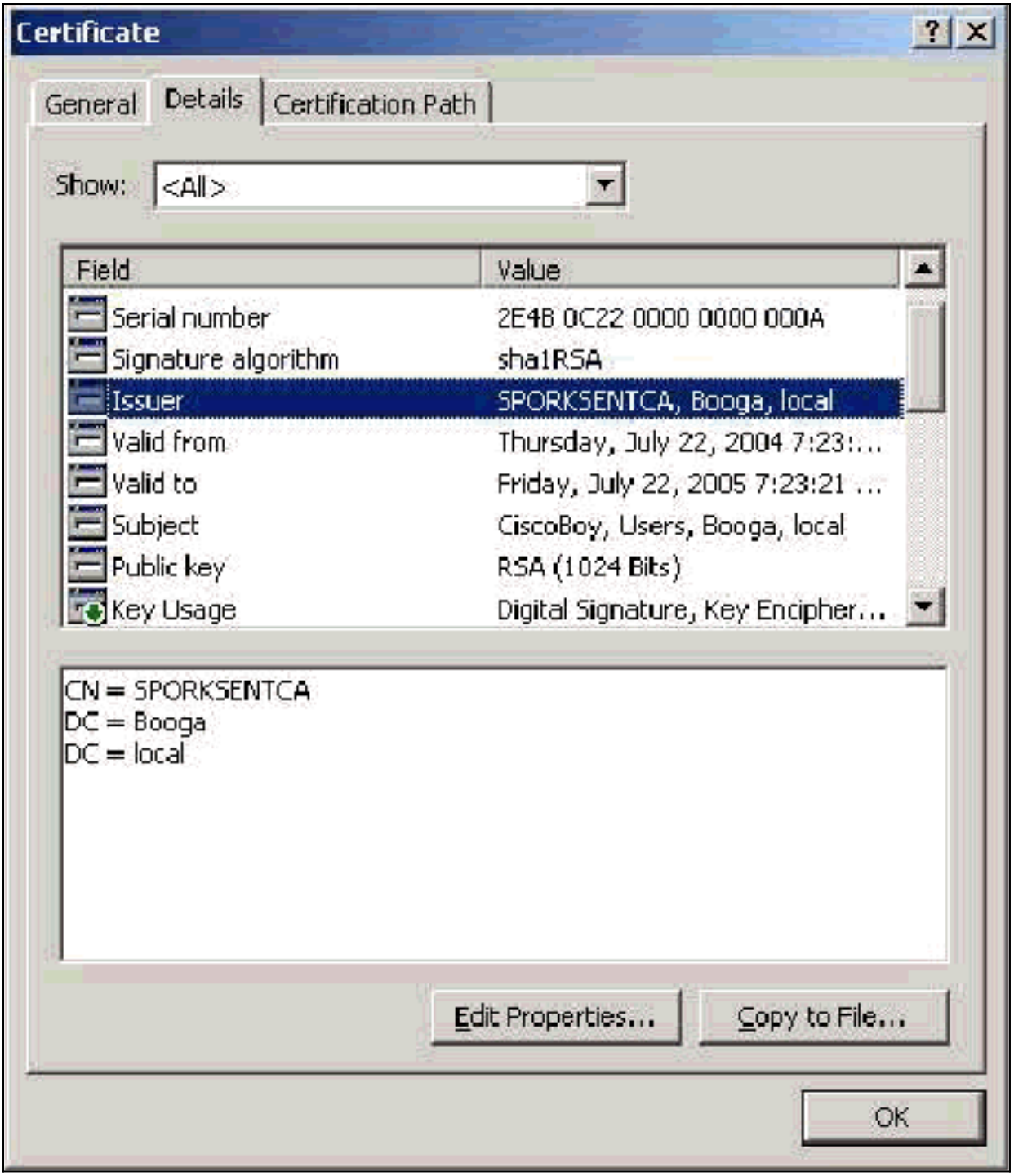
Welke vergelijkingsmethode ook wordt gebruikt, de informatie in het betreffende veld (CN of SAN) moet overeenkomen met de naam die uw database voor authenticatie gebruikt. AD gebruikt de NetBios naam voor authenticatie in gemengde modus en het UPN in de oorspronkelijke modus.

In deze sectie wordt de productie van Clientcertificaten besproken met het gebruik van Microsoft certificaatservices. Voor het MAP-TLS is een uniek clientcertificaat vereist, zodat elke gebruiker kan worden geauthentificeerd. Het certificaat moet voor elke gebruiker op elke computer zijn geïnstalleerd. Indien correct geïnstalleerd, bevindt het certificaat zich in de map **Certificaten - Huidige gebruiker > Persoonlijk > Certificaten** zoals in dit voorbeeldvenster weergegeven.



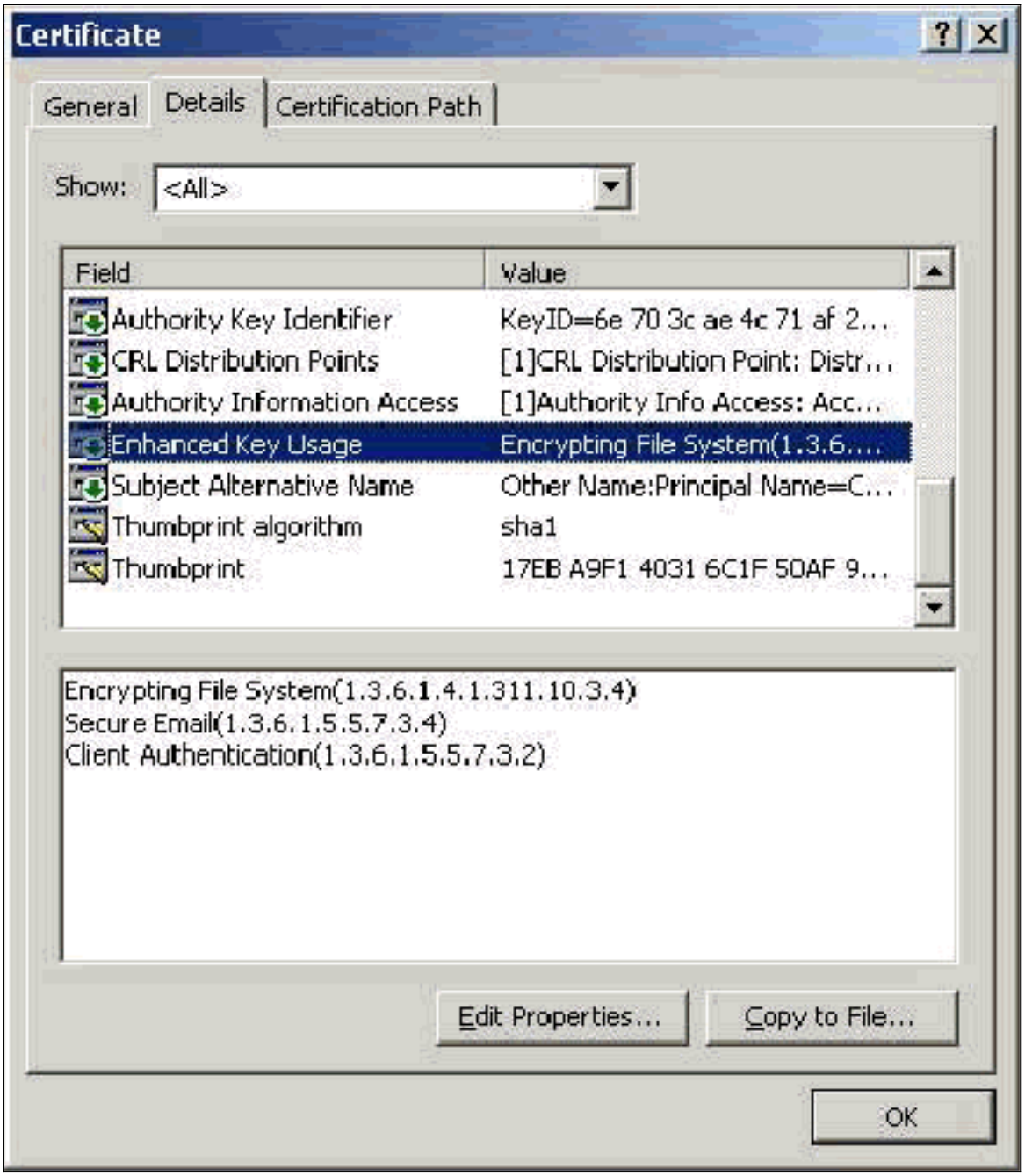
Uitgifteveld

Het veld Uitgever identificeert de CA die het certificaat snijdt. Gebruik deze waarde om de waarde te bepalen van de uitgifte door veld in het tabblad Algemeen van het certificaat. Dit is bevolkt met de naam van de CA.



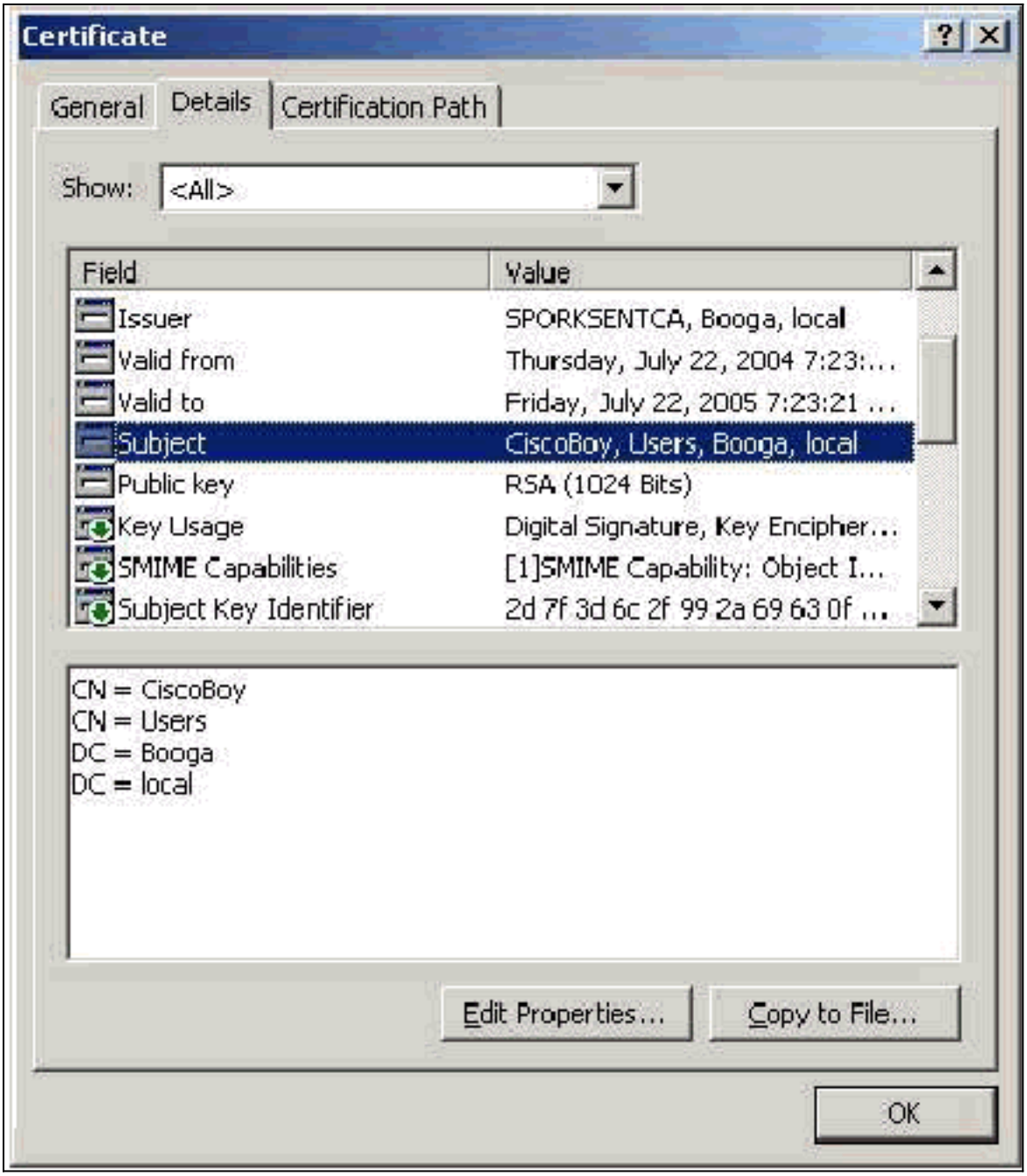
Uitgebreid veld voor gebruik

Het veld Uitgebreide sleutel voor gebruik identificeert het beoogde doel van het certificaat en moet clientverificatie bevatten. Dit veld is verplicht als u de Microsoft Suppliciet voor PEAP en EAP-TLS gebruikt. Wanneer u Microsoft certificaatservices gebruikt, wordt dit ingesteld in de standalone CA wanneer u **clientverificatiecertificaat** selecteert uit de vervolgkeuzelijst Doelstelling en in de optie Enterprise CA wanneer u **Gebruiker** uit de vervolgkeuzelijst **certificaatsjabloon** selecteert. Als u een certificaat vraagt met het gebruik van een CSR met Microsoft certificaatservices, hebt u niet de optie om het beoogde doel te specificeren met de standalone CA. Daarom is het EKU-veld afwezig. Met de Enterprise CA, heb je de bedoelde doeloptie. Sommige CA's maken geen certificaten met een EKU-veld. Ze zijn nutteloos als u de MAP-applicatie van Microsoft gebruikt.



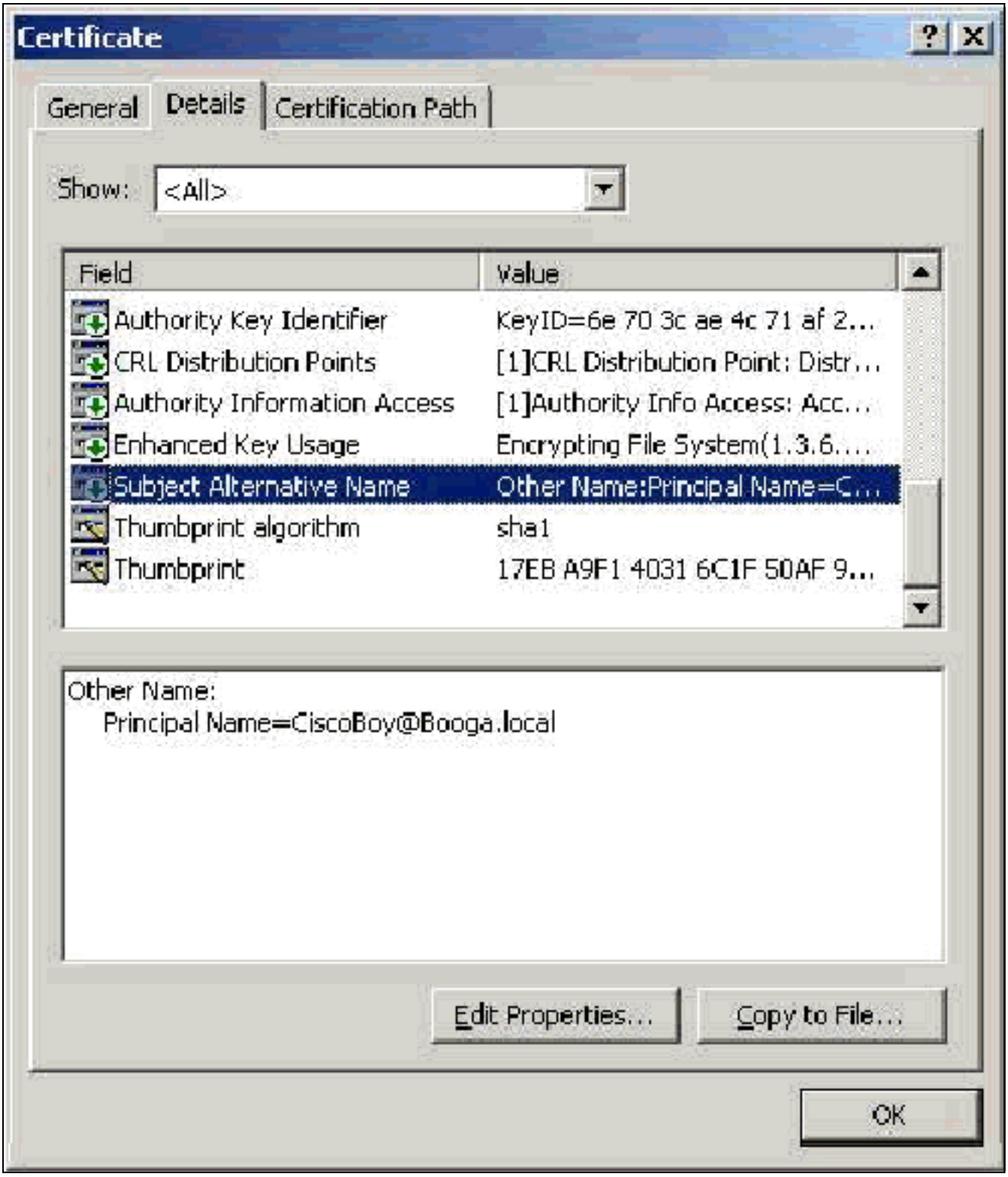
Onderwerp

Dit veld wordt gebruikt bij GN-vergelijking. De eerste GN-lijst wordt vergeleken met de database om een match te vinden. Als een overeenkomst wordt gevonden, slaagt de authenticiteit in. Als u een standalone CA gebruikt, wordt de GN ingevuld met wat u in het veld Naam in het formulier voor certificaatindiening plaatst. Als u de Enterprise CA gebruikt, wordt de CN automatisch bevolkt met de naam van de rekening zoals vermeld in de console van de Gebruikers en Computers van de Actieve Map (dit komt niet noodzakelijk overeen met UPN of de naam NetBios).



Veld met alternatieve naam

Het veld Alternatieve naam onderwerp wordt in SAN-vergelijking gebruikt. De SAN-lijst wordt vergeleken met de database om een match te vinden. Als een overeenkomst wordt gevonden, slaagt de authenticiteit in. Als u de Enterprise CA gebruikt, wordt SAN automatisch ingevuld met de naam van de Actieve Map-aanmelding @domein (UPN). De standalone CA omvat geen SAN gebied zodat u geen SAN vergelijking kunt gebruiken.



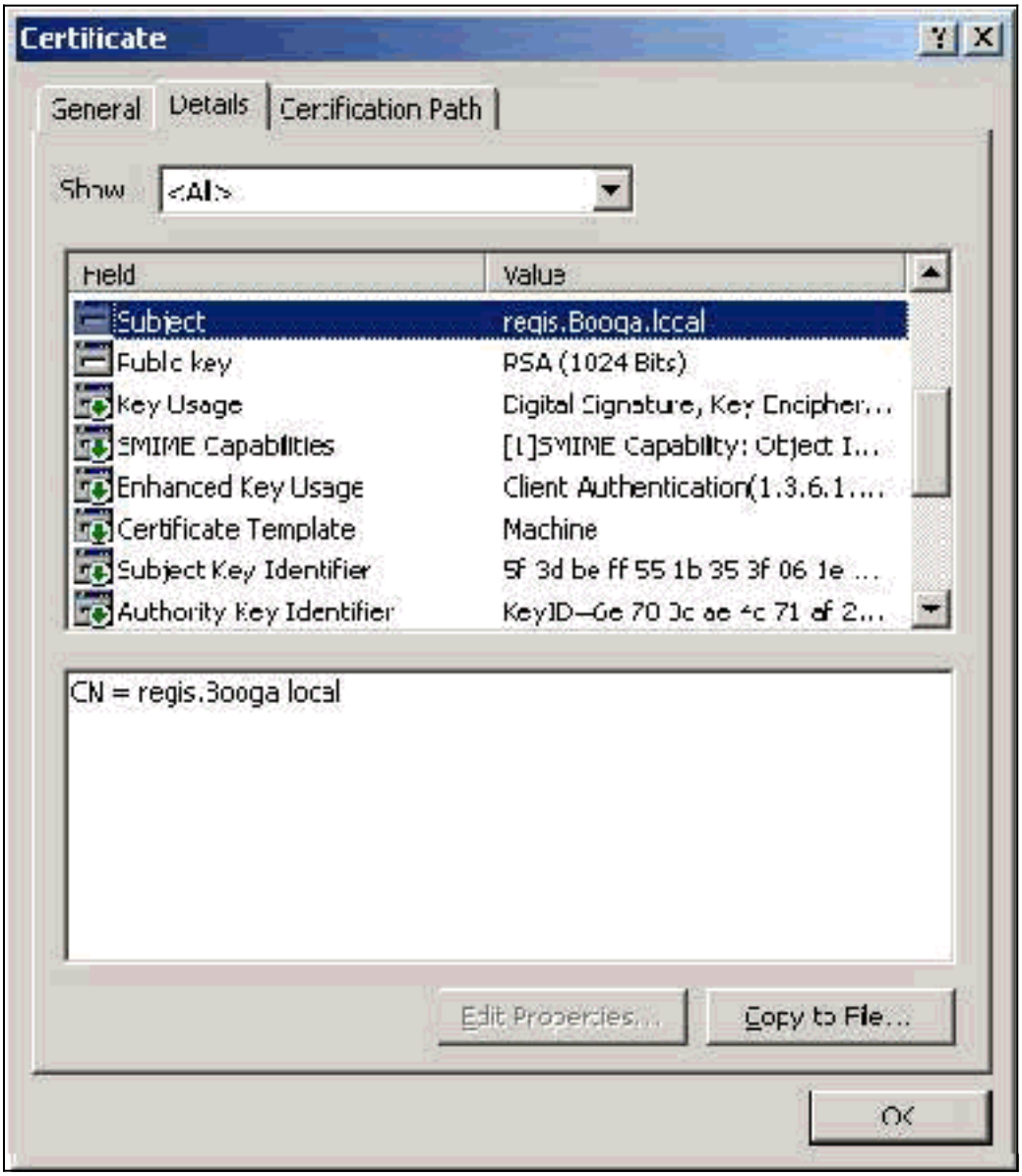
Machinecertificaten

Machinecertificaten worden in EAP-TLS gebruikt om de computer positief te identificeren wanneer u de echtheidscontrole van de machine gebruikt. U hebt alleen toegang tot deze certificaten wanneer u uw Microsoft Enterprise CA voor de automatische inschrijving van certificaten configureren en de computer aan het domein toevoegen. Het certificaat wordt automatisch aangemaakt wanneer u de actieve directory-referenties van de computer gebruikt en in de lokale computerwinkel installeert. Computers die al lid zijn van het domein voordat u de automatische inschrijving configureren ontvangen een certificaat de volgende keer dat Windows opnieuw start. Het machinecertificaat is geïnstalleerd in de **certificaten (lokale computer) > Persoonlijk > Certificaten** in map van de certificaten (lokale computer) MMC, net zoals servercertificaten. U kunt

deze certificaten niet op een andere machine installeren omdat u de privétoets niet kunt exporteren.

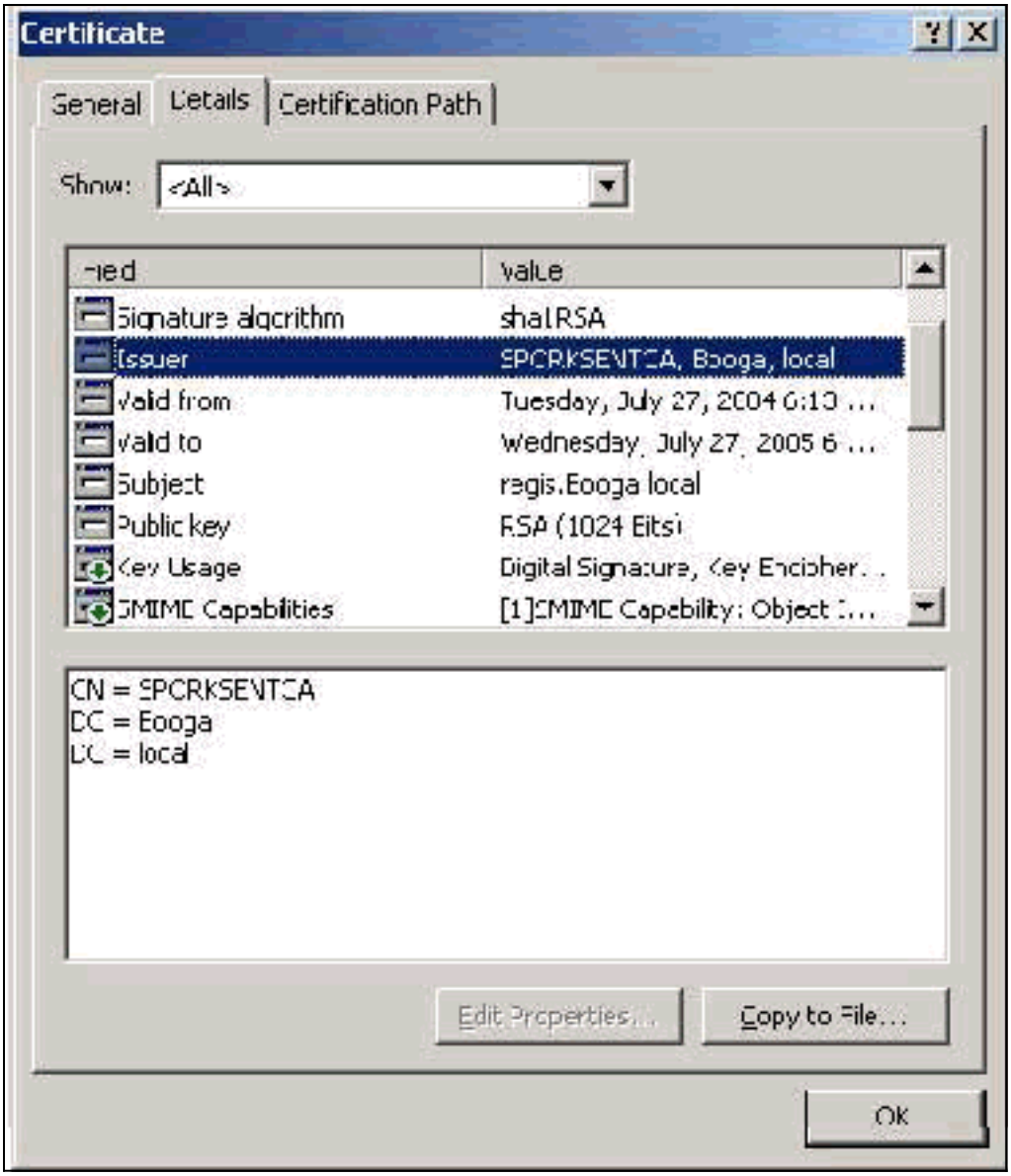
Onderwerp en SAN-velden

Onderwerp en SAN velden identificeren de computer. De waarde wordt ingevuld met de volledig gekwalificeerde naam van de computer en wordt gebruikt om het veld Uitgegeven in het tabblad Algemeen van het certificaat te bepalen en is hetzelfde voor zowel de onderwerpregel- als de SAN-velden.



Uitgifteveld

Het veld Uitgever identificeert de CA die het certificaat heeft gesneden. Gebruik deze waarde om de waarde te bepalen van de uitgifte door veld in het tabblad Algemeen van het certificaat. Het is bevolkt met de naam van de CA.



Bijlage A - Gemeenschappelijke certificaatuitbreidingen

.csr - Dit is geen certificaat maar een Aanvraag voor certificaatondertekening. Dit is een duidelijk tekstbestand met deze indeling:

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

.pvk—Deze extensie duidt op een particuliere toets hoewel de extensie niet garandeert dat de inhoud daadwerkelijk een privésleutel is. De inhoud moet onbewerkte tekst met deze indeling zijn:

```
-----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—Dit is een generieke extensie die een certificaat aangeeft. Server, Root CA, en Intermediate CA certificaten kunnen in deze indeling zijn. Het is meestal een onbewerkte tekstbestand met een extensie die u zo nodig kunt wijzigen en die op DER of Base64-indeling kan worden ingesteld. U kunt deze indeling importeren in de Windows-certificaatwinkel.

.pem-Deze extensie staat voor Privacy Enhanced Mail. Deze extensie wordt meestal gebruikt met UNIX, Linux, BSD, enzovoort. Het wordt over het algemeen gebruikt voor servercertificaten en privé toetsen en het is meestal een onbewerkte tekstbestand met een extensie die u kunt wijzigen zoals u wilt, van .pem naar .cer, zodat u het kunt importeren naar de Windows certificatenwinkel.

De interne inhoud van .cer en .pem bestanden ziet er over het algemeen als deze uitvoer uit:

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

.pfx—Deze extensie staat voor Mobile Information Exchange. Deze indeling is een methode die u kunt gebruiken om certificaten in één bestand te bundelen. U kunt bijvoorbeeld een servercertificaat en de bijbehorende privé-sleutel en CA-certificering in één bestand bundelen en het bestand eenvoudig in de juiste Windows-certificaatwinkel importeren. Het wordt het meest gebruikt voor server- en clientcertificaten. Helaas, als een CA-certificaat van Opstarten is inbegrepen, wordt het CA-certificaat van Opstarten altijd geïnstalleerd in de Huidige gebruikerswinkel in plaats van de lokale computerwinkel, zelfs als de Local Computer Store is gespecificeerd voor installatie.

.p12-Deze indeling wordt in het algemeen alleen gezien bij een clientcertificaat. U kunt deze indeling importeren in de Windows-certificaatwinkel.

.p7b-Dit is een ander formaat waarin meerdere certificaten in één bestand zijn opgeslagen. U kunt deze indeling importeren in de Windows-certificaatwinkel.

Bijlage B - Conversie van het certificaat

In de meeste gevallen vindt de conversie van het certificaat plaats wanneer u de extensie (bijvoorbeeld van .pem naar .cer) wijzigt, aangezien de certificaten algemeen in onbewerkte tekstindeling zijn. Soms is een certificaat niet in bestandsindeling en moet u het converteren met een gereedschap zoals OpenSSL . Bijvoorbeeld, kan de ACS Engine van de Oplossing geen

certificaten in het .pfx formaat installeren. Daarom moet u het certificaat en de privé-toets converteren naar een bruikbare indeling. Dit is de basale syntaxis van OpenSSL:

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

U wordt gevraagd het wachtwoord voor invoer in te voeren en de PEM-code. Deze wachtwoorden moeten hetzelfde zijn en het defaultwachtwoord (de privé-toets) zijn dat is gespecificeerd wanneer de .pfx wordt geëxporteerd. De uitvoer is één .pem-bestand dat alle certificaten en privé-toetsen in de .pfx bevat. Dit bestand kan in ACS als het certificaat en het privé-sleutelbestand worden aangeduid en het kan zonder problemen worden geïnstalleerd.

Bijlage C - geldigheidsduur van het certificaat

Een certificaat is slechts bruikbaar tijdens de geldigheidsduur ervan. De geldigheidsperiode voor een CA-certificaat van wortel wordt bepaald wanneer de CA van de wortel is vastgesteld en kan variëren. De geldigheidstermijn voor een middelgroot CA-certificaat wordt bepaald wanneer de CA wordt vastgesteld en mag niet langer zijn dan de geldigheidsperiode van de basisCA waarop zij is achtergesteld. De geldigheidsperiode voor Server-, client- en machinecertificaten wordt automatisch op één jaar ingesteld met Microsoft certificaatservices. Dit kan alleen worden gewijzigd wanneer u de Windows-registratie hackt zoals in artikel 254632 van de Microsoft Kennis Base-basis en de geldigheidsperiode van de bron CA niet overschrijdt. De geldigheidsperiode van de zelfondertekende certificaten die ACS genereert, is altijd één jaar en kan niet worden gewijzigd in de huidige versies.

Gerelateerde informatie

- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning - Cisco-systemen