EAP 버전 1.01 인증서 가이드

목차

소개

이 문서에서는 다양한 형태의 EAP(Extensible Authentication Protocol)와 관련된 다양한 인증서 유형, 형식 및 요구 사항과 관련된 몇 가지 혼동을 명확히 설명합니다. 이 문서에서 설명하는 EAP와 관련된 다섯 가지 인증서 유형은 서버, 루트 CA, 중간 CA, 클라이언트 및 시스템입니다. 이러한 인증서는 다양한 형식으로 발견되며 관련된 EAP 구현에 따라 각 인증서와 관련된 서로 다른 요구 사항이 있을 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

서버 인증서

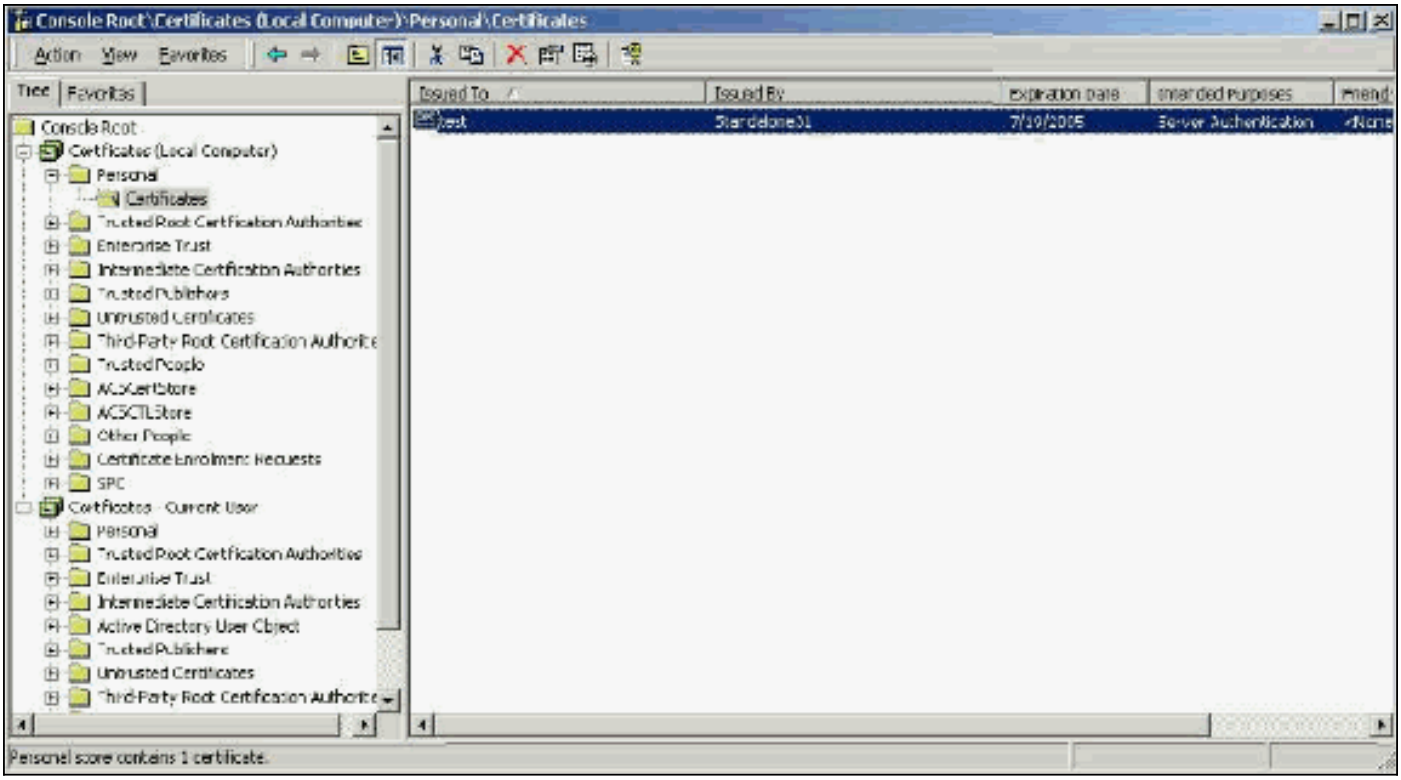
서버 인증서는 RADIUS 서버에 설치되며 EAP의 주 목적은 인증 정보를 보호하는 암호화된 TLS(전송 계층 보안) 터널을 만드는 것입니다. EAP-MSCHAPv2를 사용하는 경우 서버 인증서는 RADIUS 서버를 인증을 위한 신뢰할 수 있는 엔티티로 식별하는 보조 역할을 수행합니다. 이 보조 역할은 EKU(Enhanced Key Usage) 필드를 사용하여 수행됩니다. EKU 필드는 인증서를 유효한 서버 인증서로 식별하고 인증서를 발급한 루트 CA가 신뢰할 수 있는 루트 CA인지 확인합니다. 이를 위해서는 루트 CA 인증서가 있어야 합니다. Cisco Secure ACS에서는 인증서가 Base64 인코딩 또는 DER 인코딩 이진 X.509 v3 형식이어야 합니다.

CA에 제출되는 ACS에서 CSR(Certificate Signing Request)을 사용하여 이 인증서를 생성할 수 있습니다. 또는 사내 CA(예: Microsoft 인증서 서비스) 인증서 생성 양식을 사용하여 인증서를 잘라낼 수도 있습니다. 키 크기가 1024보다 큰 서버 인증서를 만들 수 있지만 1024보다 큰 키는 PEAP에서 작동하지 않습니다. 인증이 통과하더라도 클라이언트가 중단됩니다.

CSR을 사용하여 인증서를 생성하면 .cer, .pem 또는 .txt 형식으로 생성됩니다. 드문 경우지만 확장이 없는 상태로 생성됩니다. 인증서가 필요에 따라 변경할 수 있는 확장명을 가진 일반 텍스트 파일인지 확인합니다(ACS 어플라이언스는 .cer 또는 .pem 확장명을 사용). 또한 CSR을 사용하는 경우 인증서의 개인 키는 별도의 파일로 지정한 경로에 생성되며, 별도의 파일에는 확장자가 있을 수도 있고 없을 수도 있으며 비밀번호가 연결되어 있습니다(ACS에 설치하는 데 비밀번호가 필요함). 확장명과 상관없이 필요에 따라 변경할 수 있는 확장명이 있는 일반 텍스트 파일인지 확인합니다(ACS 어플라이언스는 .pvk 또는 .pem 확장명을 사용합니다). 개인 키에 대한 경로가 지정되지 않은 경우 ACS는 C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs 디렉토리에 키를 저장하고 인증서를 설치할 때 개인 키 파일에 대한 경로가 지정되지 않은 경우 이 디렉토리를 찾습니다.

Microsoft Certificate Services 인증서 전송 양식을 사용하여 인증서를 만든 경우 키를 내보낼 수 있는 것으로 표시해야 ACS에 인증서를 설치할 수 있습니다. 이러한 방식으로 인증서를 생성하면 설치 프로세스가 크게 간소화됩니다. 인증서 서비스 웹 인터페이스에서 적절한 Windows 저장소에 직접 설치한 다음 CN을 참조로 사용하여 저장소의 ACS에 설치할 수 있습니다. 로컬 컴퓨터 저장소에 설치된 인증서는 Windows 저장소에서 내보낼 수 있으며 쉽게 다른 컴퓨터에 설치할 수도 있습니다. 이 유형의 인증서를 내보내면 키를 내보낼 수 있는 것으로 표시하고 암호를 지정해야 합니다. 그런 다음 개인 키 및 서버 인증서를 포함하는 .pfx 형식으로 인증서가 나타납니다.

Windows 인증서 저장소에 올바르게 설치된 경우 서버 인증서가 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더에 나타나야 합니다(이 예제 창 참조).

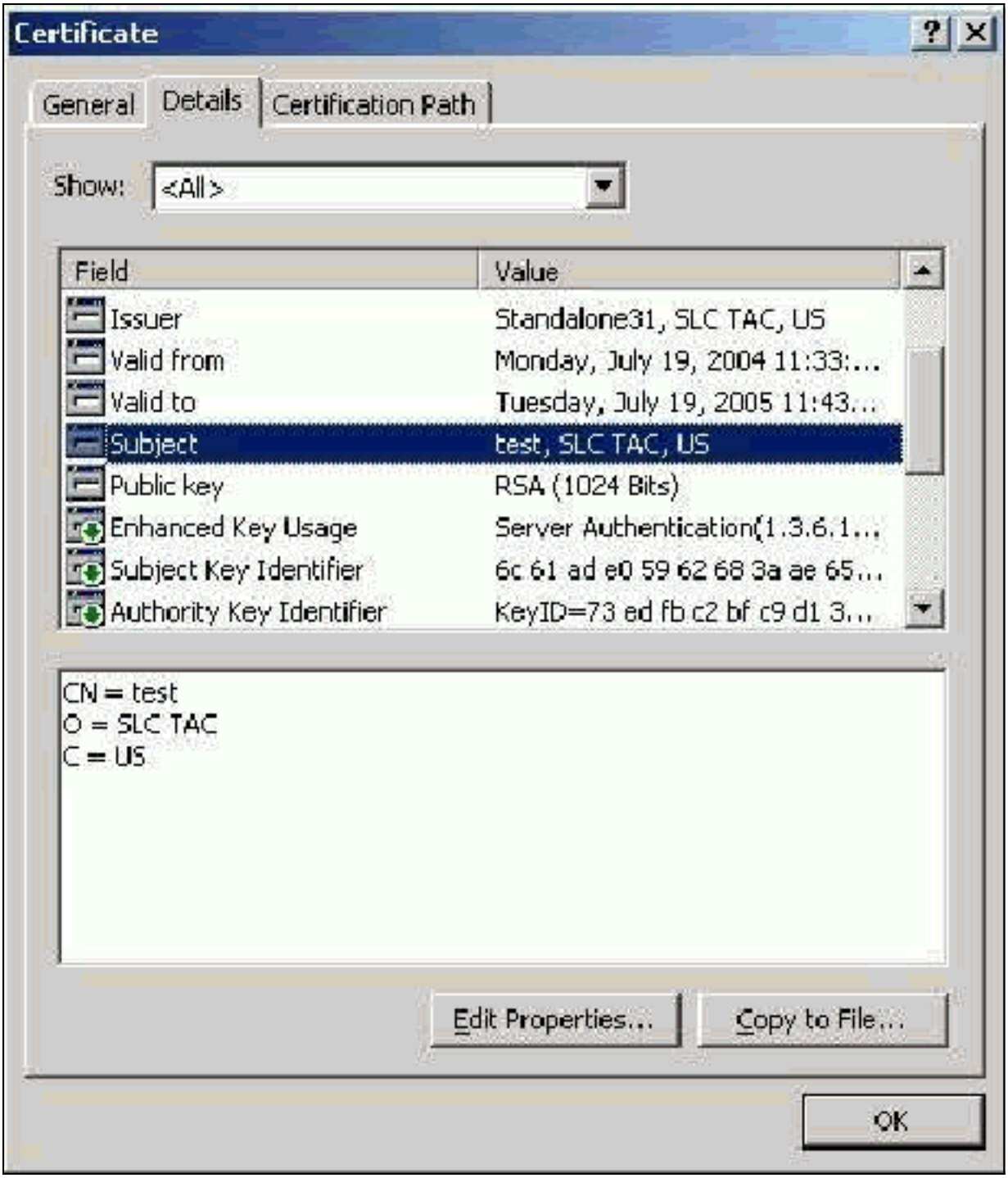


자체 서명 인증서는 루트 또는 CA의 중간 개입 없이 생성하는 인증서입니다. 루트 CA 인증서와 같은 주체 및 발급자 필드 모두에서 동일한 값을 가집니다. 대부분의 자체 서명 인증서는 X.509 v1 형식을 사용합니다. 따라서 ACS에서는 작동하지 않습니다. 그러나 버전 3.3부터 ACS는 EAP-TLS 및 PEAP에 사용할 수 있는 자체 서명 인증서를 만들 수 있습니다. PEAP 및 EAP-TLS와의 호환성을 위해 1024보다 큰 키 크기를 사용하지 마십시오. 자체 서명 인증서를 사용하는 경우 인증서는 루트 CA 인증서의 용량으로도 작동하며 Microsoft EAP 서 플리 컨 트를 사용할 때 클라이언트의 **인증서 (로컬 컴퓨터) > 신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더에 설치해야 합니다. 서버의 신뢰할 수 있는 루트 인증서 저장소에 자동으로 설치됩니다. 그러나 ACS 인증서 설정의 인증서 신뢰 목록에서 계속 신뢰할 수 있어야 합니다. 자세한 내용은 루트 CA 인증서 섹션을 참조하십시오.

자체 서명 인증서는 Microsoft EAP 신청자를 사용할 때 서버 인증서 검증을 위한 루트 CA 인증서로 사용되며, 유효 기간을 기본값인 1년에서 늘릴 수 없기 때문에, Cisco에서는 일반 CA를 사용할 수 있을 때까지 임시 측정으로 EAP에만 사용할 것을 권장합니다.

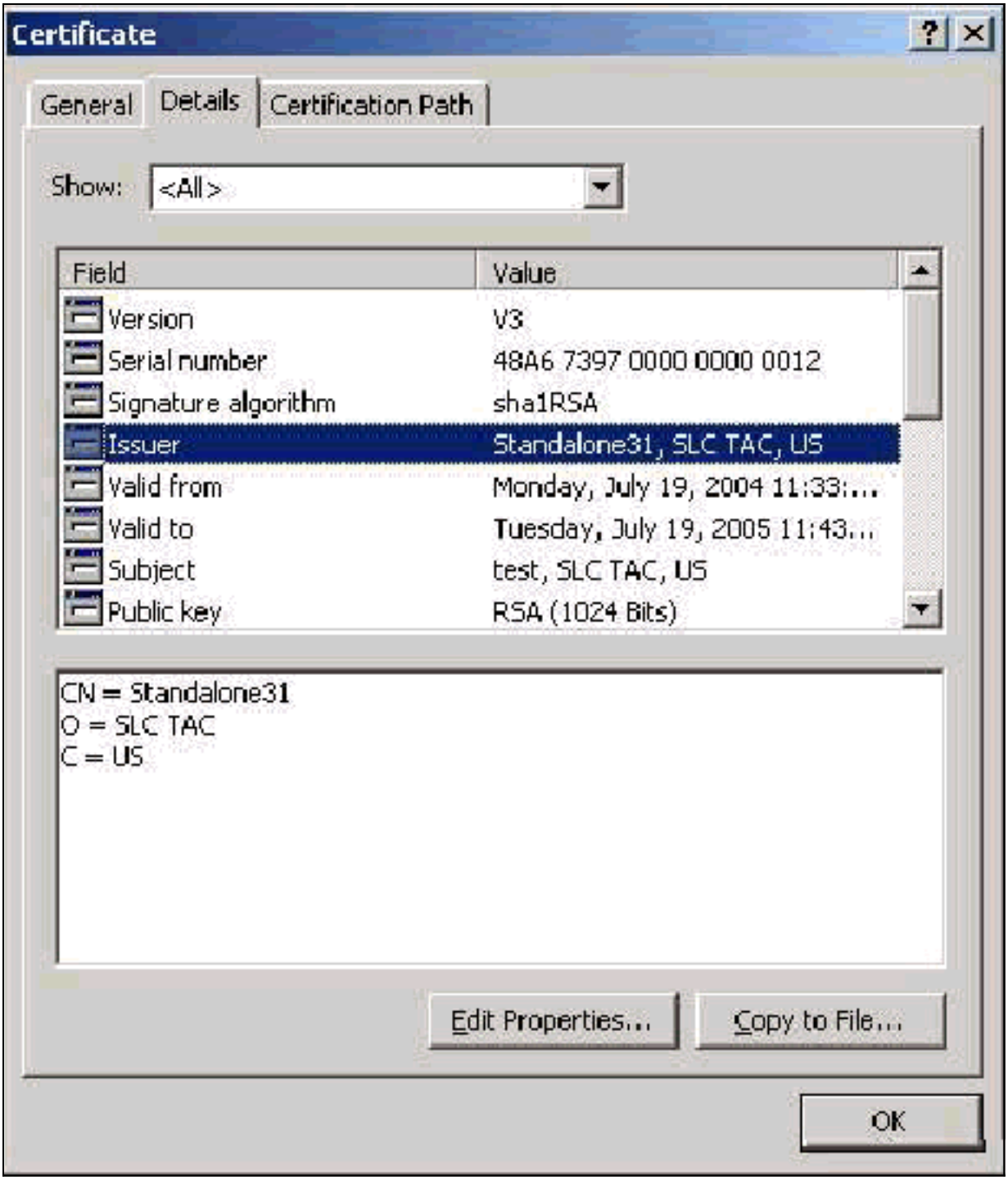
제목 필드

Subject(주체) 필드는 인증서를 식별합니다. CN 값은 인증서의 General(일반) 탭에서 Issued to(발급 대상) 필드를 결정하는 데 사용되며 ACS"CSR(CSR) 대화 상자의 Certificate subject(인증서 주체) 필드에 입력하는 정보나 Microsoft Certificate Services(Microsoft 인증서 서비스)의 Name(이름) 필드의 정보로 채워집니다. CN 값은 저장소에서 인증서를 설치하는 옵션이 사용되는 경우 로컬 컴퓨터 인증서 저장소에서 사용해야 하는 인증서를 ACS에 알려주는 데 사용됩니다.



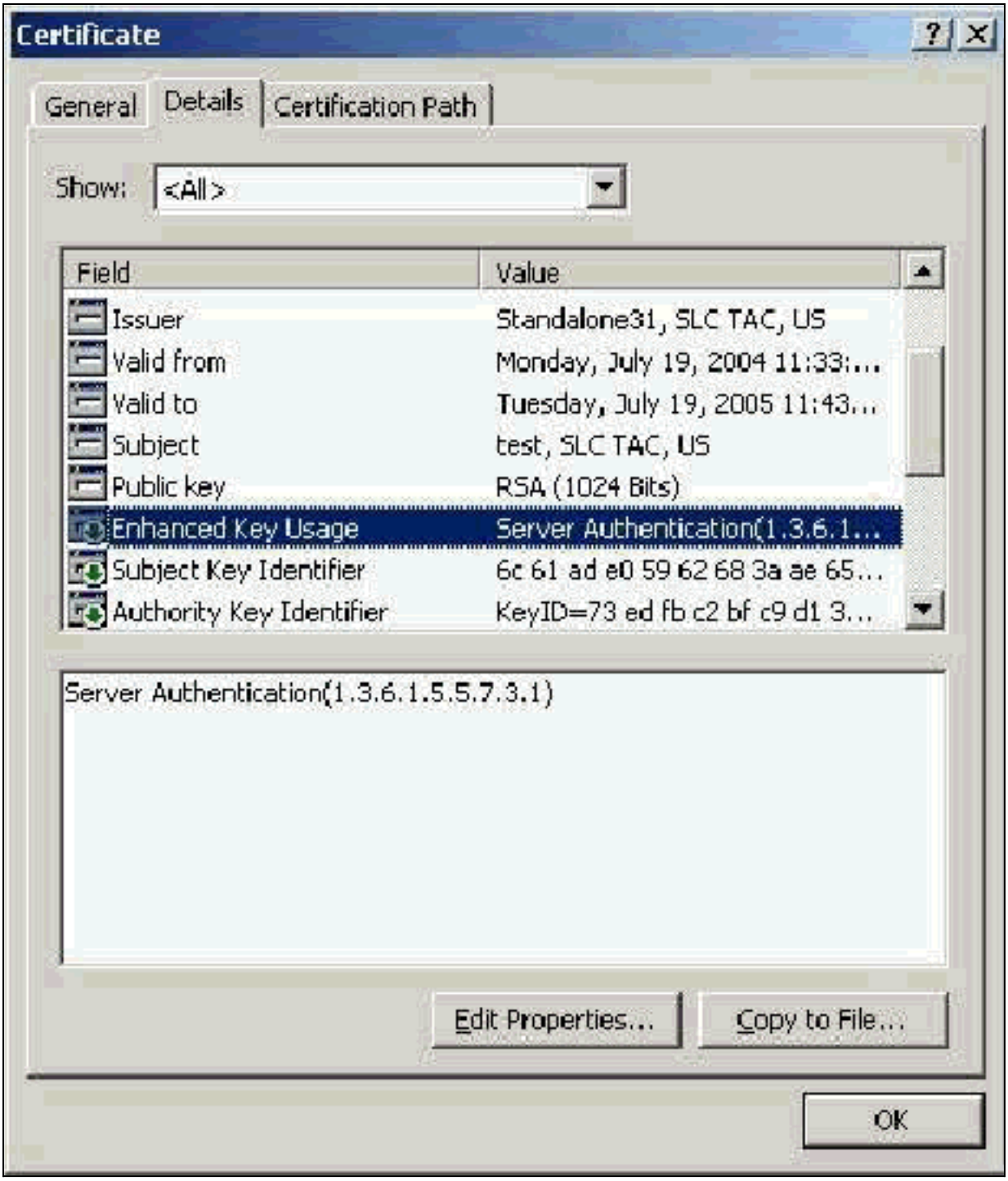
발급자 필드

Issuer 필드는 인증서를 잘라내는 CA를 식별합니다. 인증서의 General(일반) 탭에서 Issued by(발급자) 필드의 값을 확인하려면 이 값을 사용합니다. CA의 이름으로 채워집니다.



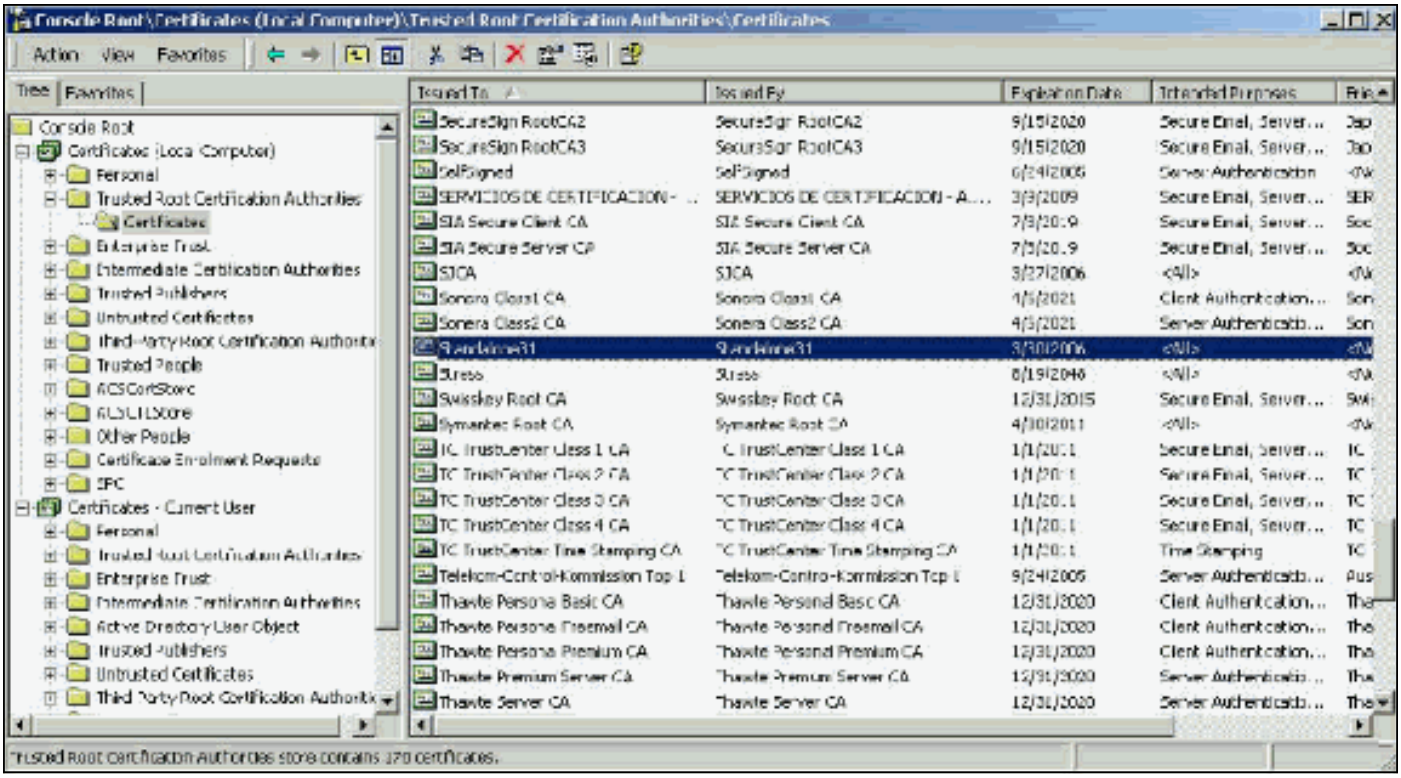
향상된 키 사용 필드

Enhanced Key Usage(고급 키 사용) 필드는 인증서의 용도를 식별하며 "서버 인증"으로 표시되어야 합니다. 이 필드는 PEAP 및 EAP-TLS에 Microsoft 서 플리 컨 트를 사용 할 때 필수 입력 합니다. Microsoft Certificate Services를 사용하는 경우 이는 Intended Purpose(용도) 드롭다운에서 **서버 인증 인증서**를 선택하여 독립형 CA에서 구성되고 Enterprise CA에서는 Certificate Template(인증서 템플릿) 드롭다운에서 **웹 서버**를 선택합니다. Microsoft Certificate Services에서 CSR을 사용하는 인증서를 요청할 경우 독립형 CA를 사용하여 Intended Purpose를 지정할 수 없습니다. 따라서 EKU 필드가 없습니다. Enterprise CA에서는 Intended Purpose(용도) 드롭다운이 있습니다. 일부 CA는 EKU 필드가 있는 인증서를 생성하지 않으므로 Microsoft EAP 신청자를 사용할 때 사용할 수 없습니다.



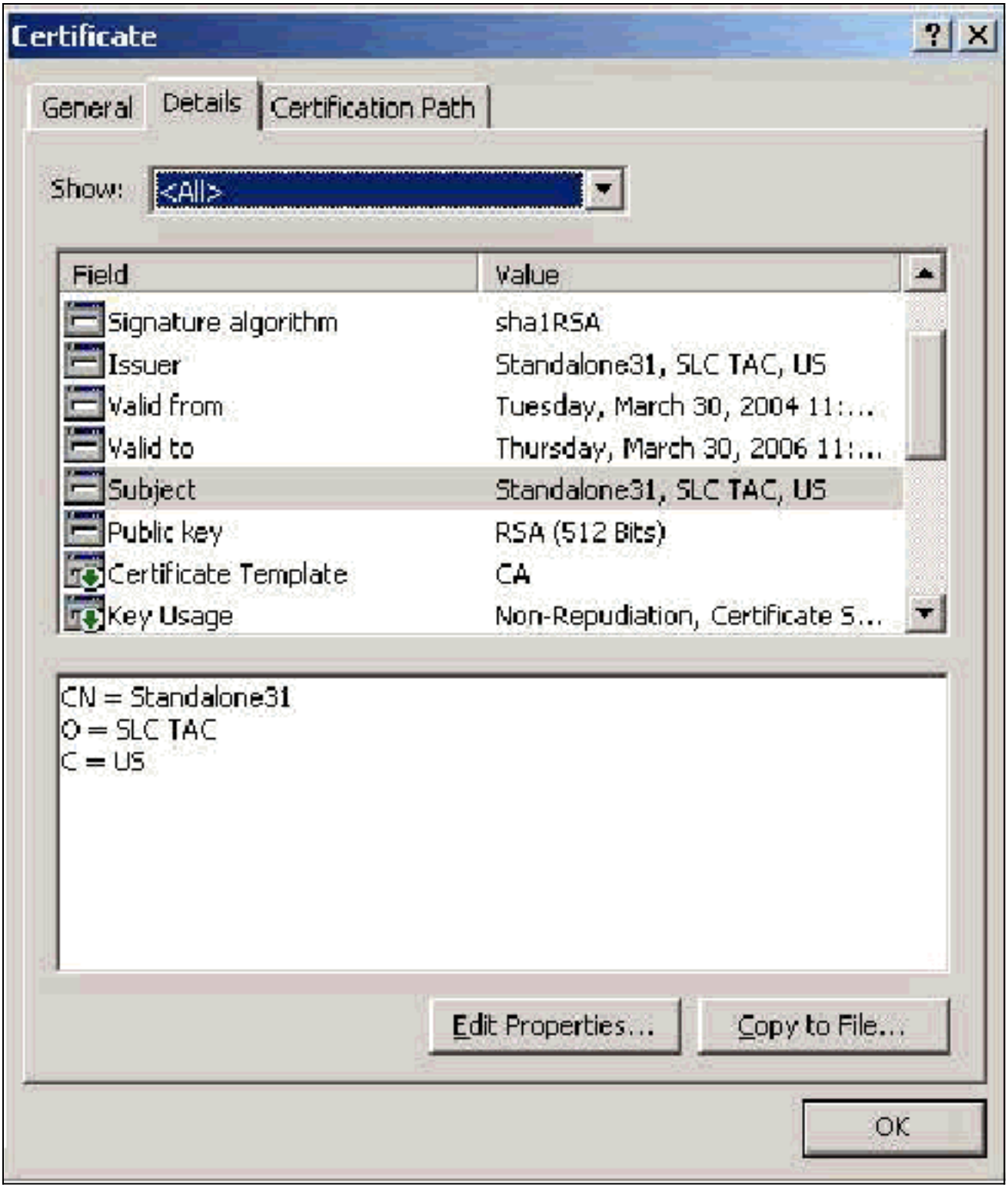
루트 CA 인증서

루트 CA 인증서의 한 가지 목적은 서버 인증서(및 해당하는 경우 중간 CA 인증서)를 ACS 및 Windows EAP-MSCHAPv2 신청자에 대한 신뢰할 수 있는 인증서로 식별하는 것입니다. ACS 서버 및 클라이언트 컴퓨터의 EAP-MSCHAPv2의 경우 Windows의 신뢰할 수 있는 루트 인증 기관 저장소에 있어야 합니다. 대부분의 서드파티 루트 CA 인증서는 Windows와 함께 설치되며, 이와 관련된 작업은 거의 없습니다. Microsoft Certificate Services가 사용되고 인증서 서버가 ACS와 동일한 시스템에 있으면 루트 CA 인증서가 자동으로 설치됩니다. Windows의 신뢰할 수 있는 루트 인증 기관 저장소에서 루트 CA 인증서를 찾을 수 없으면 CA에서 루트 CA 인증서를 취득하여 설치해야 합니다. Windows 인증서 저장소에 올바르게 설치된 경우 루트 CA 인증서가 **인증서(로컬 컴퓨터) > 신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더에 나타나야 합니다(이 예제 창 참조).



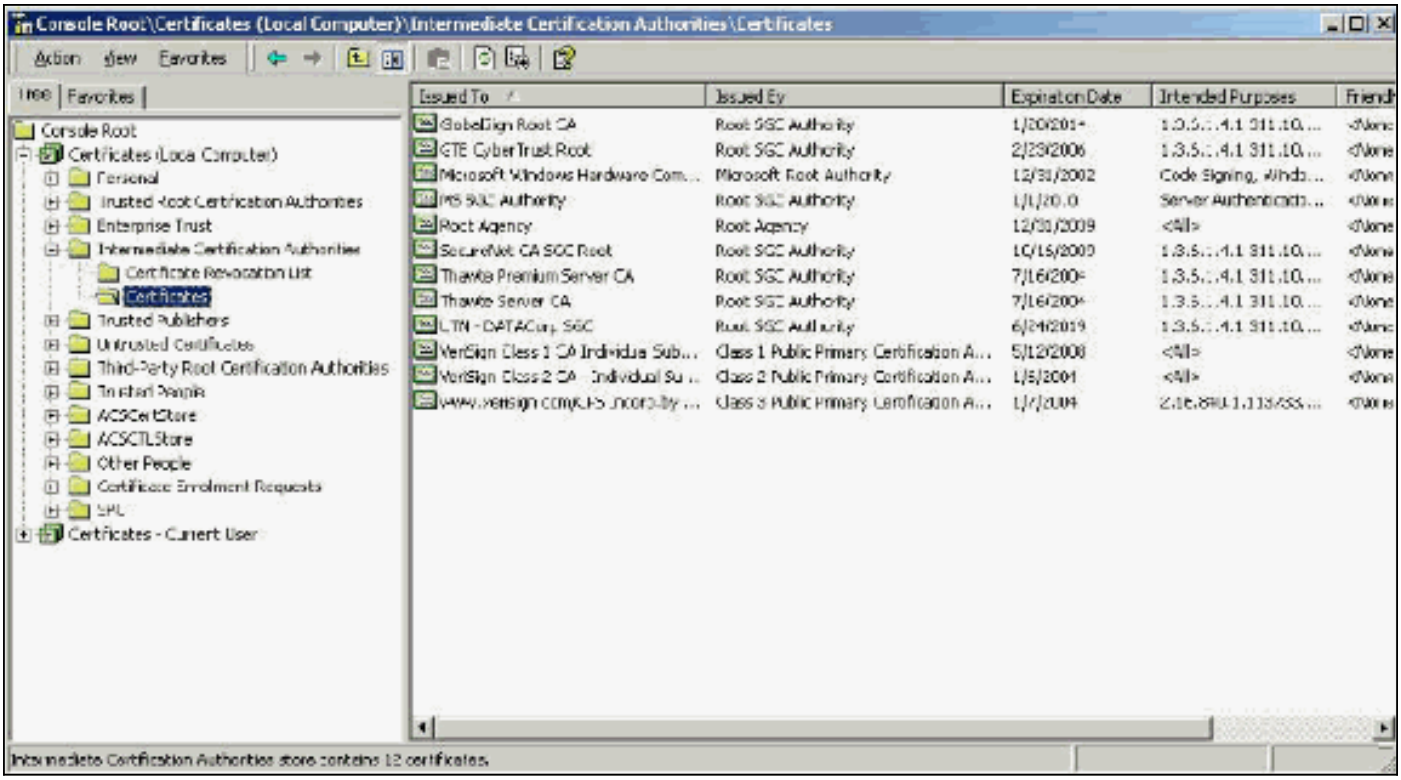
제목 및 발급자 필드

Subject(제목) 및 Issuer(발급자) 필드는 CA를 식별하며, 정확히 동일해야 합니다. 이 필드를 사용하여 인증서의 General(일반) 탭에 있는 Issued to(발급 대상) 및 Issued by(발급자) 필드를 채웁니다. 루트 CA의 이름으로 채워집니다.



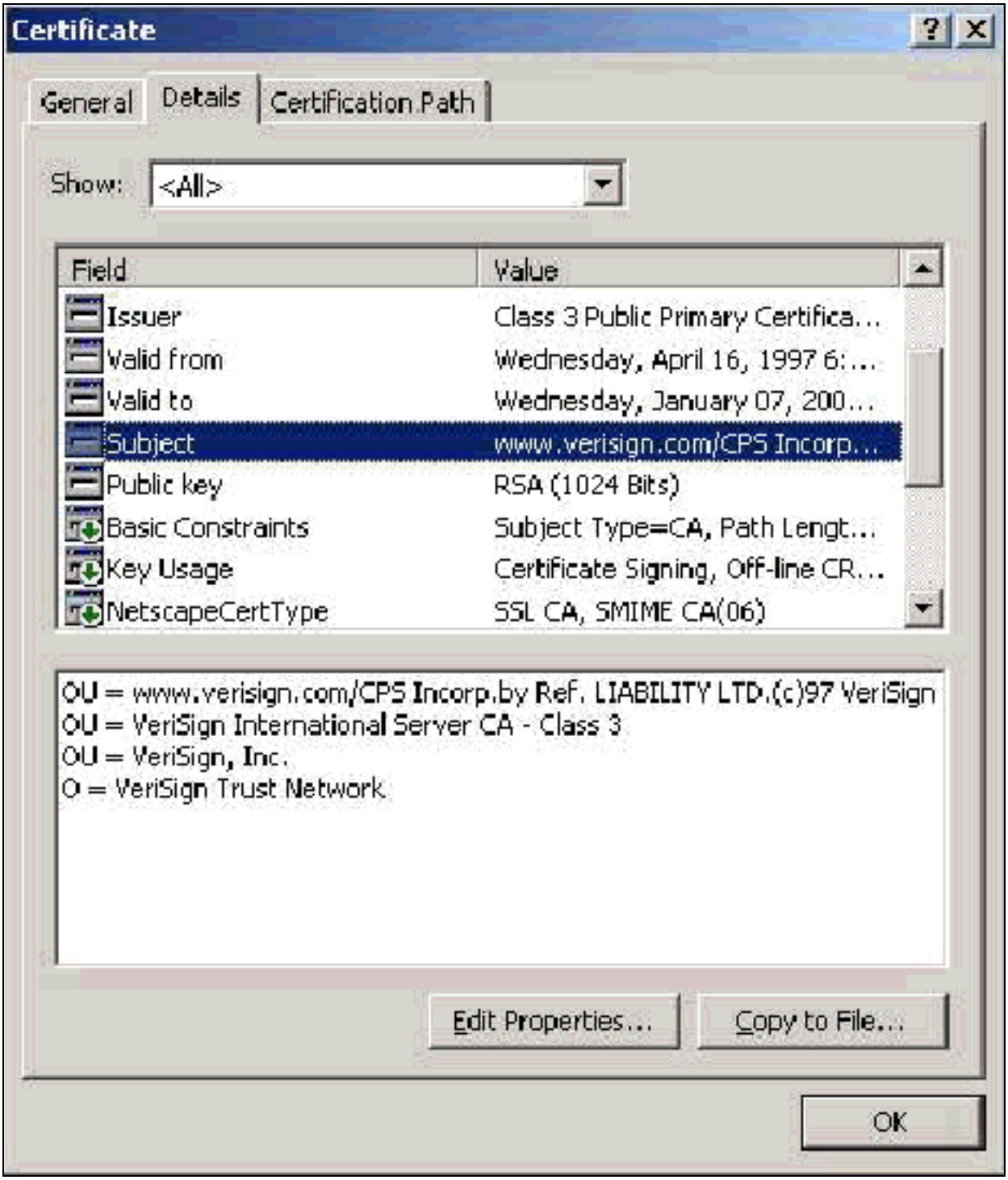
중간 CA 인증서

중간 CA 인증서는 루트 CA에 종속된 CA를 식별하는 데 사용하는 인증서입니다. 일부 서버 인증서(Verisign의 무선 인증서)는 중간 CA를 사용하여 생성됩니다. 중간 CA로 잘라낸 서버 인증서를 사용하는 경우 중간 CA 인증서는 ACS 서버에 있는 로컬 컴퓨터 저장소의 중간 인증 기관 영역에 설치해야 합니다. 또한 Microsoft EAP 서 플리 컨 트가 클라이언트에서 사용 된 경우 중간 CA 인증서를 생성 한 루트 CA의 루트 CA 인증서는 ACS 서버 및 클라이언트의 해당 저장소에 있어야 신뢰 체인을 설정 할 수 있습니다. 루트 CA 인증서와 중간 CA 인증서는 모두 ACS 및 클라이언트에서 신뢰된 것으로 표시되어야 합니다. 대부분의 중간 CA 인증서는 Windows와 함께 설치되지 않으므로 공급업체에서 얻어야 할 가능성이 높습니다. Windows 인증서 저장소에 올바르게 설치된 경우 중간 CA 인증서가 **인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서** 폴더에 나타납니다(이 예제 창 참조).



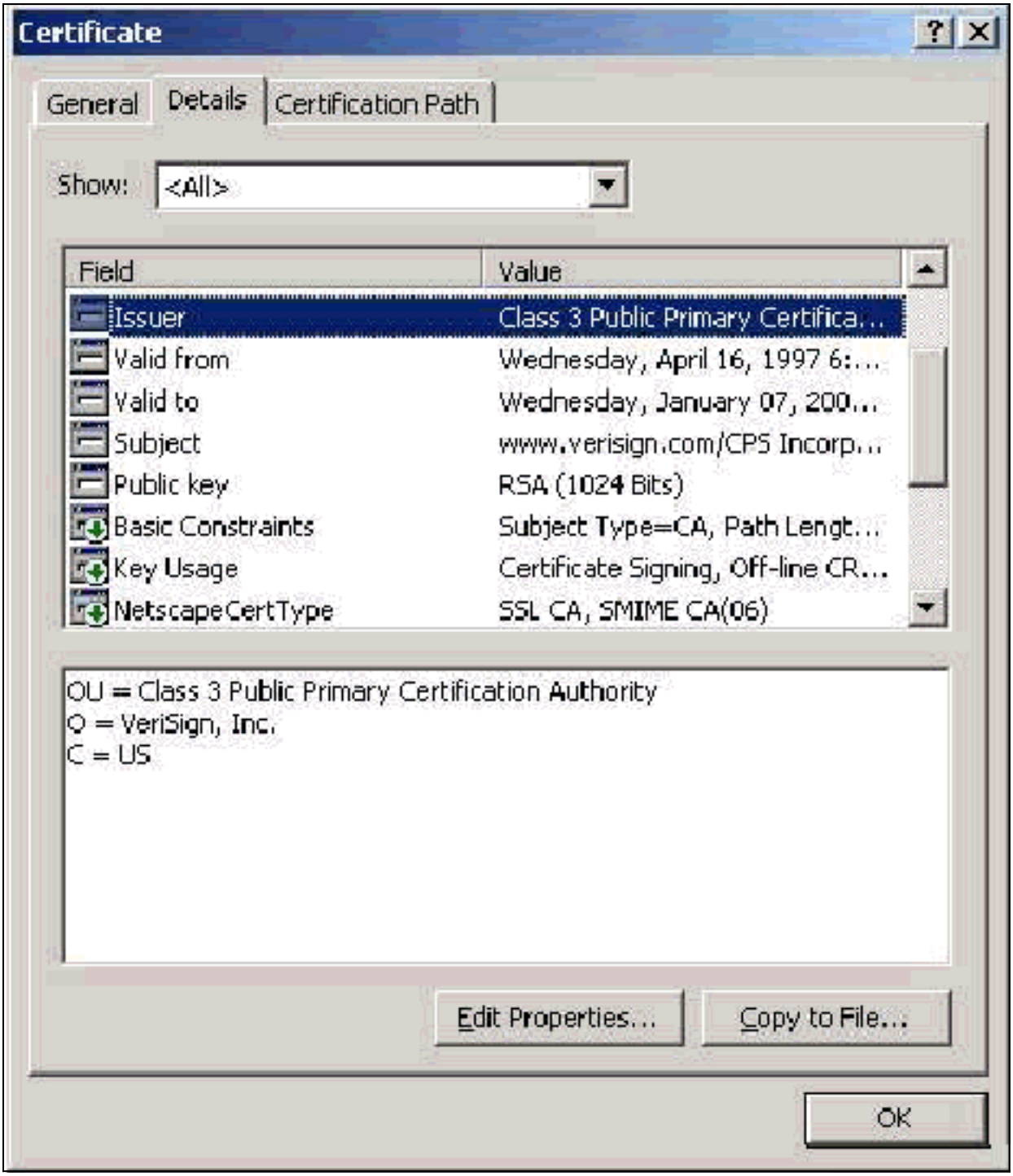
제목 필드

Subject(제목) 필드는 중간 CA를 식별합니다. 이 값은 인증서의 General(일반) 탭에서 Issued to(발급 대상) 필드를 결정하는 데 사용됩니다.



발급자 필드

Issuer 필드는 인증서를 잘라내는 CA를 식별합니다. 인증서의 General(일반) 탭에서 Issued by(발급자) 필드의 값을 확인하려면 이 값을 사용합니다. CA의 이름으로 채워집니다.



클라이언트 인증서

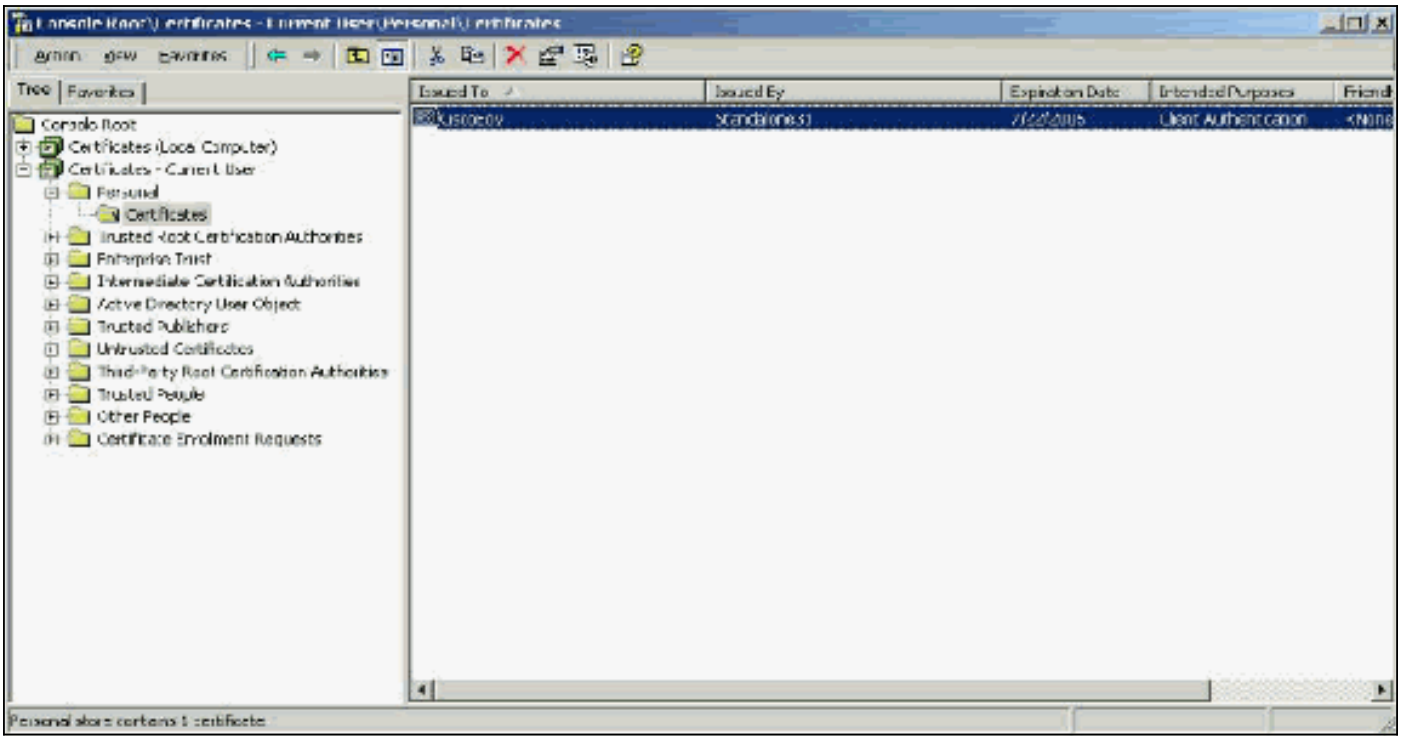
클라이언트 인증서는 EAP-TLS에서 사용자를 긍정적으로 식별하는 데 사용됩니다. TLS 터널을 구축하는 데 아무런 역할이 없으며 암호화에 사용되지 않습니다. 긍정적인 식별은 다음 세 가지 방법 중 하나로 이루어집니다.

- **CN(또는 이름)Comparison(**비교) - 인증서의 CN을 데이터베이스의 사용자 이름과 비교합니다. 이 비교 유형에 대한 자세한 내용은 인증서의 Subject(주체) 필드에 대한 설명에 포함되어 있습니다.
- **SAN Comparison(SAN 비교)** - 인증서의 SAN을 데이터베이스의 사용자 이름과 비교합니다. ACS 3.2부터 지원됩니다. 이 비교 유형에 대한 자세한 내용은 인증서의 Subject Alternative Name(주체 대체 이름) 필드에 대한 설명에 포함되어 있습니다.
- **Binary Comparison(이진 비교)** - 인증서를 데이터베이스에 저장된 인증서의 이진 복사본과 비

교합니다(AD 및 LDAP만 이 작업을 수행할 수 있음). 인증서 이진 비교를 사용하는 경우 사용자 인증서를 이진 형식으로 저장해야 합니다. 또한 일반 LDAP 및 Active Directory의 경우 인증서를 저장하는 특성은 "usercertificate"라는 표준 LDAP 특성이어야 합니다.

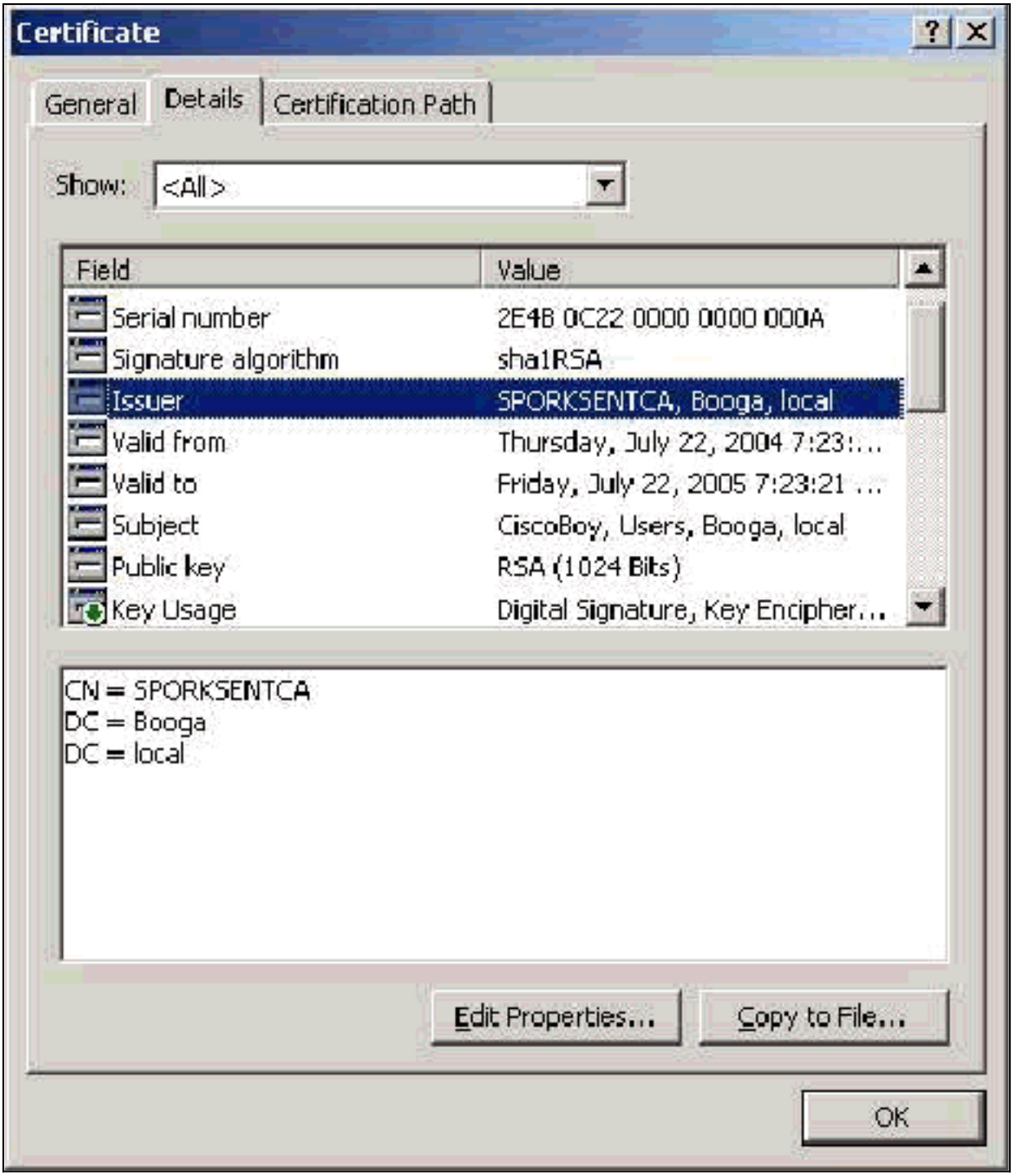
어떤 비교 방법을 사용하든 해당 필드(CN 또는 SAN)의 정보는 데이터베이스가 인증에 사용하는 이름과 일치해야 합니다. AD는 혼합 모드의 인증에 NetBios 이름을 사용하고 네이티브 모드의 UPN을 사용합니다.

이 섹션에서는 Microsoft 인증서 서비스를 사용하여 클라이언트 인증서 생성에 대해 설명합니다. EAP-TLS는 각 사용자를 인증하려면 고유한 클라이언트 인증서가 필요합니다. 인증서는 각 사용자에 대해 각 컴퓨터에 설치해야 합니다. 제대로 설치되면 인증서가 **Certificates -Current User > Personal > Certificates** 폴더에 있습니다(이 예제 창 참조).



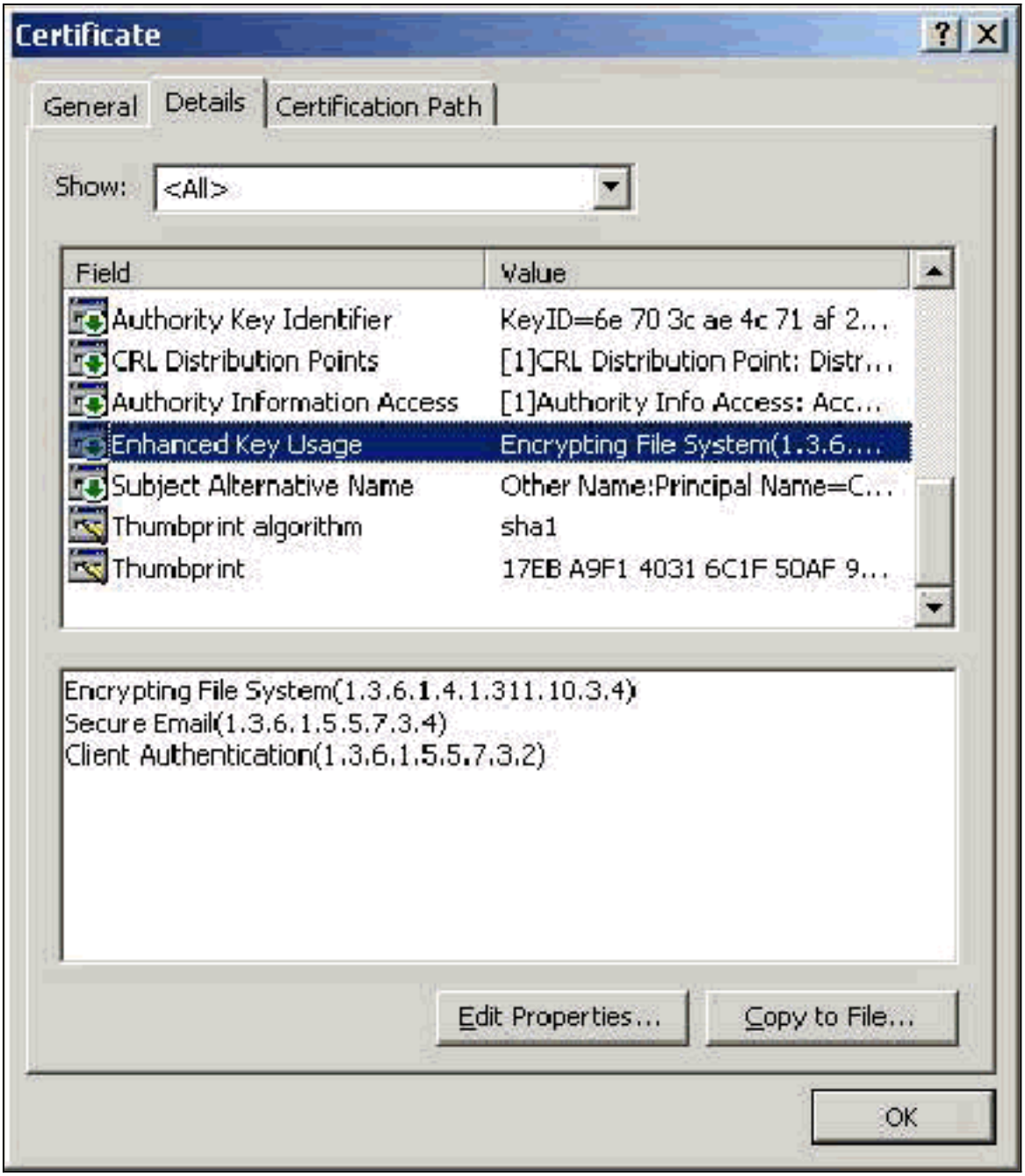
발급자 필드

Issuer 필드는 인증서를 잘라내는 CA를 식별합니다. 인증서의 General(일반) 탭에서 Issued by(발급자) 필드의 값을 확인하려면 이 값을 사용합니다. CA의 이름으로 채워집니다.



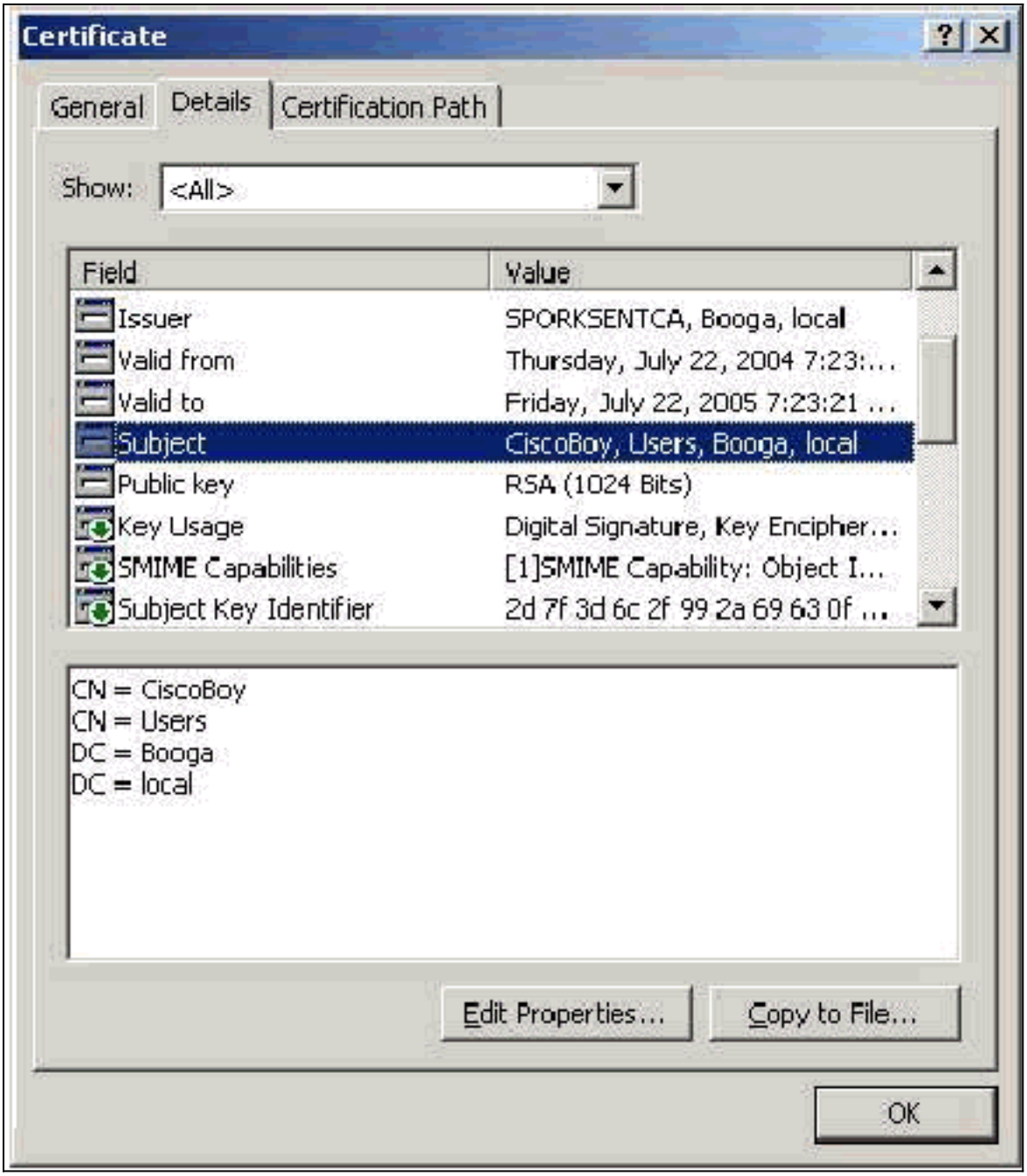
향상된 키 사용 필드

Enhanced Key Usage(고급 키 사용) 필드는 인증서의 용도를 식별하고 클라이언트 인증을 포함해야 합니다. 이 필드는 PEAP 및 EAP-TLS에 Microsoft 서 플리 컨 트를 사용 할 때 필수 입력 합니다. Microsoft Certificate Services를 사용하는 경우 Intended Purpose 드롭다운에서 **Client Authentication Certificate**를 선택하면 독립형 CA에서, Certificate Template(인증서 템플릿) 드롭다운에서 User(**사용자)**를 선택하면 Enterprise CA에서 구성됩니다. Microsoft Certificate Services에서 CSR을 사용하는 인증서를 요청할 경우 독립형 CA를 사용하여 Intended Purpose를 지정할 수 없습니다. 따라서 EKU 필드가 없습니다. Enterprise CA에서는 Intended Purpose(용도) 드롭다운이 있습니다. 일부 CA는 EKU 필드가 있는 인증서를 생성하지 않습니다. Microsoft EAP 서 플리 컨 트를 사용 할 때 사용 할 수 없습니다.



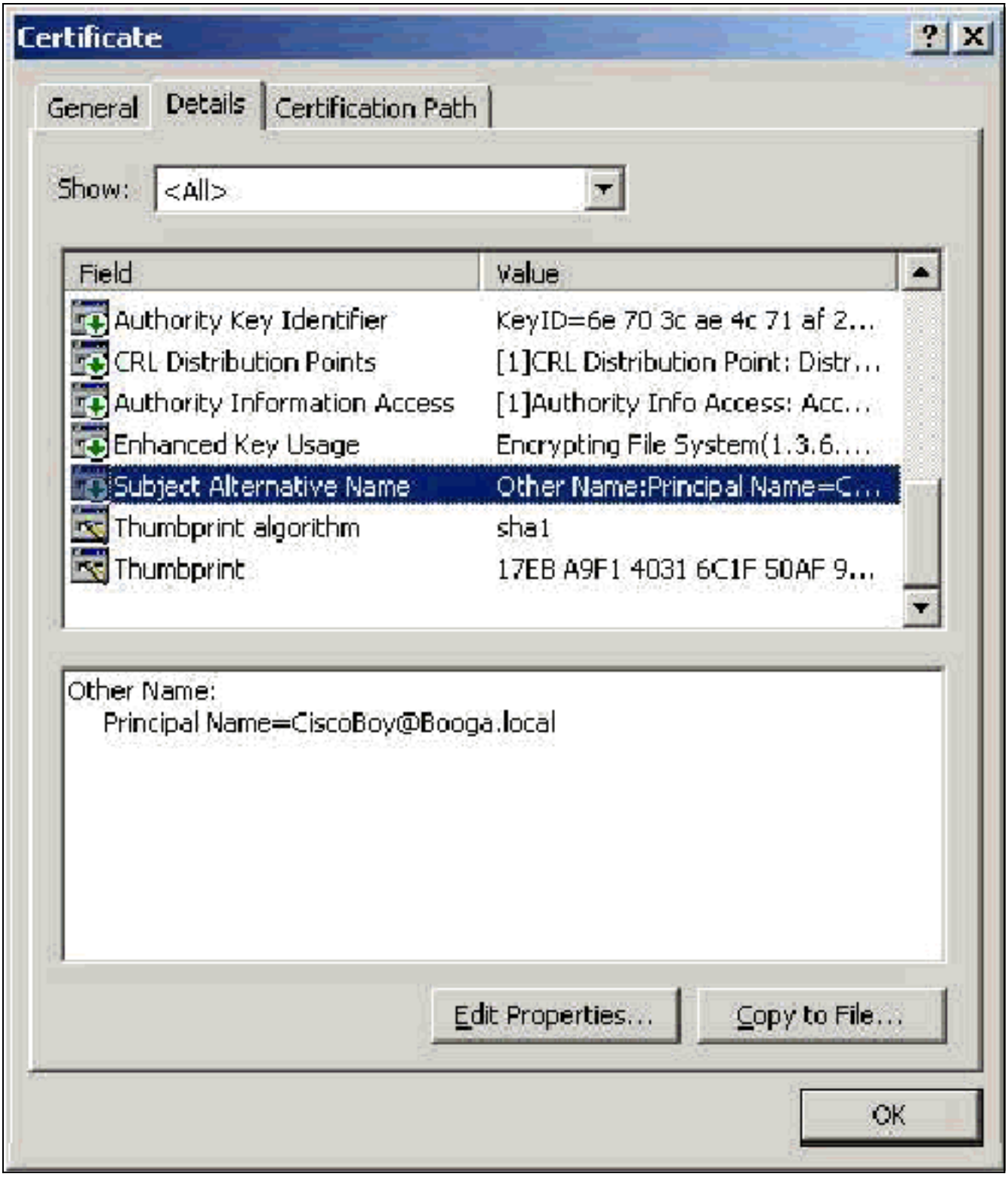
제목 필드

이 필드는 CN 비교에서 사용됩니다. 나열된 첫 번째 CN을 데이터베이스와 비교하여 일치하는 항목을 찾습니다. 일치하는 항목이 발견되면 인증이 성공합니다. 독립형 CA를 사용하는 경우 인증서 제출 양식의 Name 필드에 입력한 내용이 CN에 채워집니다. 엔터프라이즈 CA를 사용하는 경우 CN은 Active Directory 사용자 및 컴퓨터 콘솔에 나열된 계정 이름으로 자동으로 채워집니다(UPN 또는 NetBios 이름과 반드시 일치하지 않을 수도 있음).



제목 대체 이름 필드

Subject Alternative Name 필드는 SAN 비교에서 사용됩니다. 나열된 SAN을 데이터베이스와 비교하여 일치하는 항목을 찾습니다. 일치하는 항목이 발견되면 인증이 성공합니다. 엔터프라이즈 CA를 사용하는 경우 SAN은 UPN(Active Directory 로그온 이름 @domain)으로 자동으로 채워집니다. 독립형 CA는 SAN 필드를 포함하지 않으므로 SAN 비교를 사용할 수 없습니다.

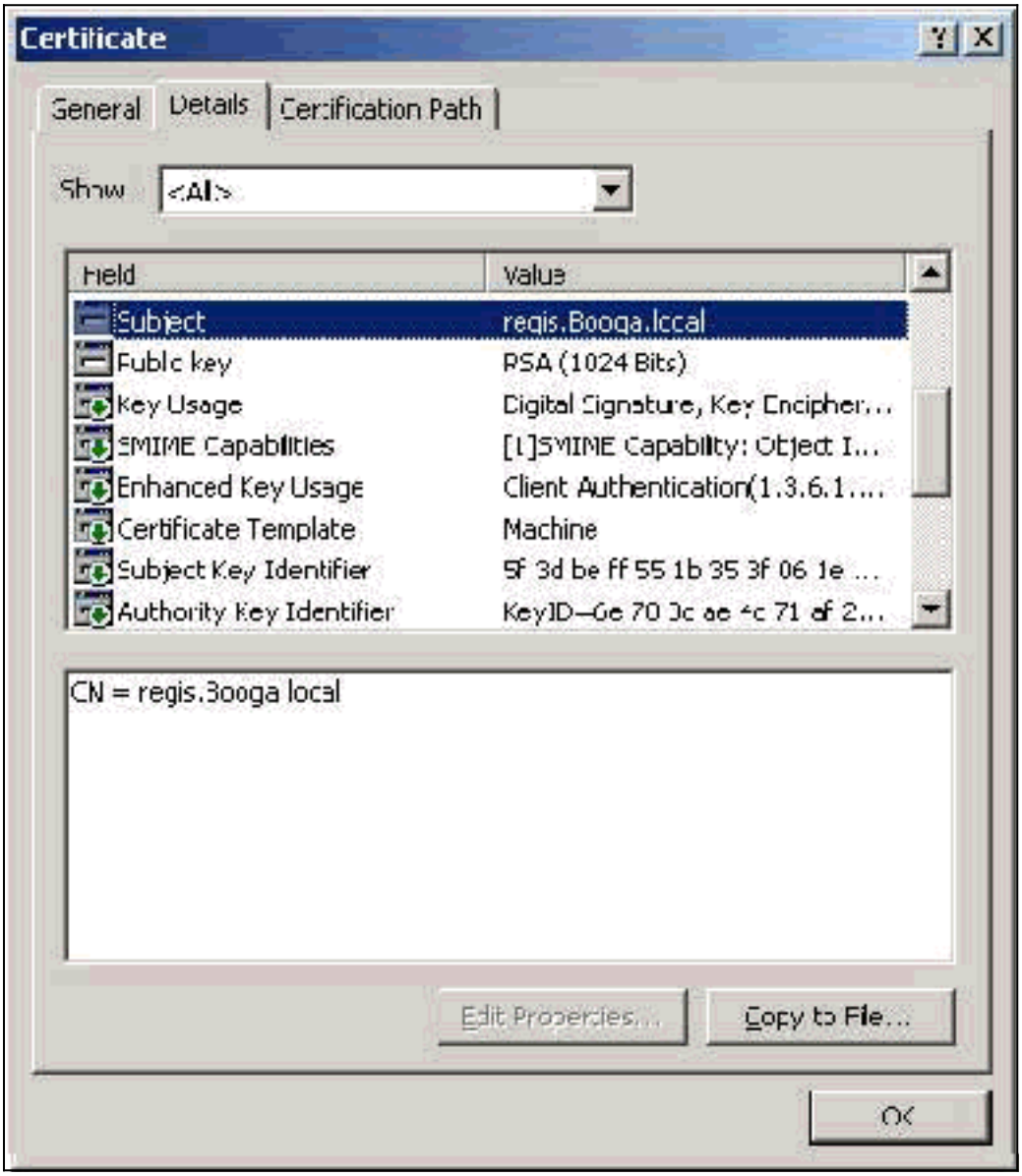


컴퓨터 인증서

머신 인증은 EAP-TLS에서 머신 인증을 사용할 때 컴퓨터를 긍정적으로 식별하는 데 사용됩니다. 인증서 자동 등록을 위해 Microsoft Enterprise CA를 구성하고 컴퓨터를 도메인에 조인하는 경우에만 이러한 인증서에 액세스할 수 있습니다. 컴퓨터의 Active Directory 자격 증명을 사용하여 로컬 컴퓨터 저장소에 설치하면 인증서가 자동으로 생성됩니다. 자동 등록을 구성하기 전에 이미 도메인의 구성원인 컴퓨터는 다음에 Windows를 다시 시작할 때 인증서를 받습니다. 컴퓨터 인증서는 서버 인증서와 마찬가지로 인증서(로컬 컴퓨터) > **개인** > **인증서**(로컬 컴퓨터) MMC 스냅인의 인증서 폴더에 설치됩니다. 개인 키를 내보낼 수 없으므로 다른 컴퓨터에 이 인증서를 설치할 수 없습니다.

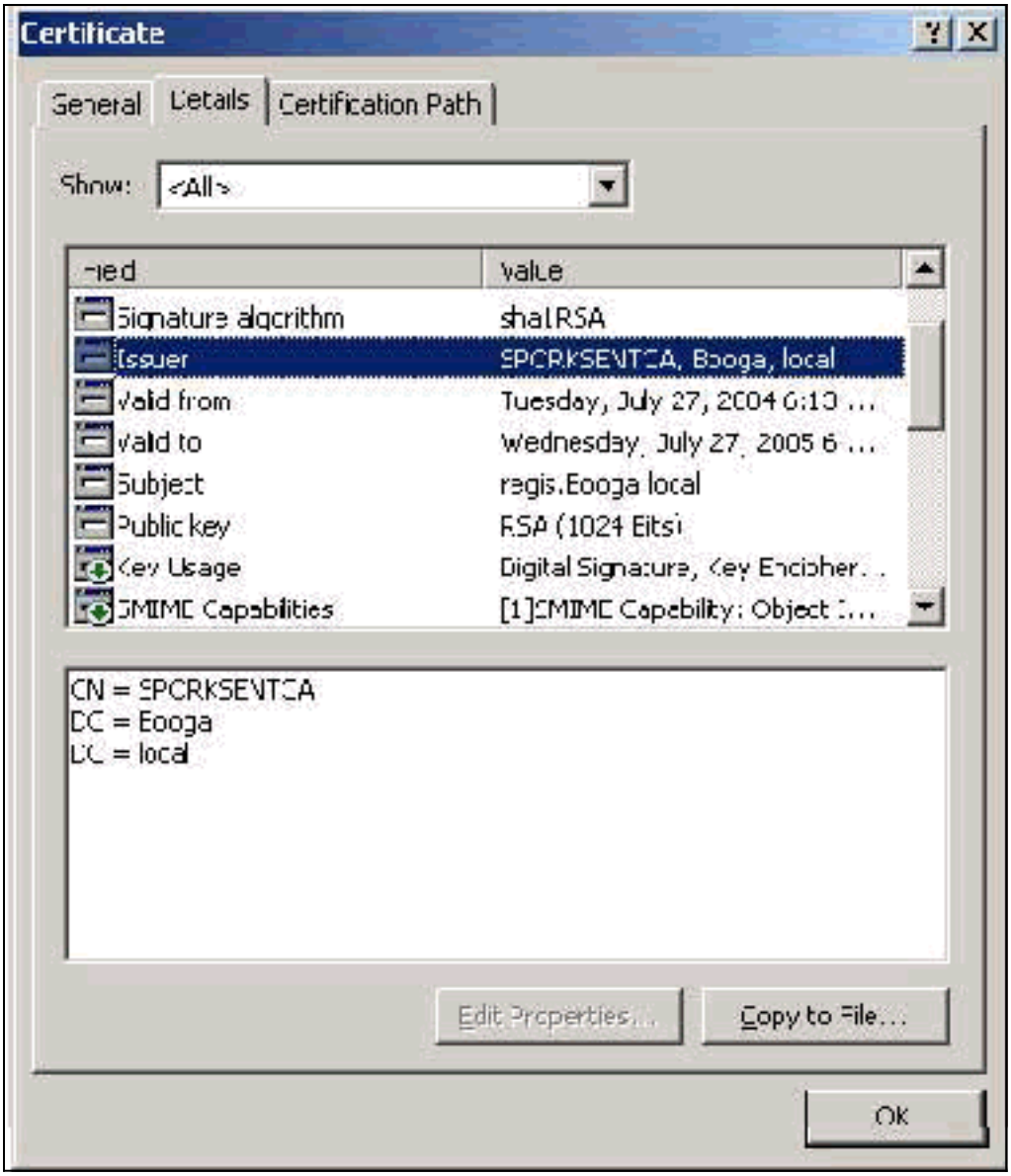
제목 및 SAN 필드

제목 및 SAN 필드는 컴퓨터를 식별합니다. 이 값은 컴퓨터의 정규화된 이름으로 채워지며 인증서의 General(일반) 탭에서 Issued to(발급 대상) 필드를 결정하는 데 사용되며 Subject(제목) 및 SAN(SAN) 필드 모두에 대해 동일합니다.



발급자 필드

Issuer 필드는 인증서를 잘라내는 CA를 식별합니다. 인증서의 General(일반) 탭에서 Issued by(발급자) 필드의 값을 확인하려면 이 값을 사용합니다. CA의 이름으로 채워집니다.



부록 A - 공통 인증서 확장

.csr—이는 실제 인증서가 아니라 인증서 서명 요청입니다. 다음과 같은 형식의 일반 텍스트 파일입니다.

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

.pvk - 이 확장은 개인 키를 나타내지만, 이 확장은 콘텐츠가 실제로 개인 키임을 보장하지는 않습니다. 내용은 다음 형식의 일반 텍스트여야 합니다.

```
-----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 - 인증서를 나타내는 일반 확장입니다. 서버, 루트 CA 및 중간 CA 인증서는 이 형식일 수 있습니다. 일반적으로 확장자가 필요한 경우 변경할 수 있는 일반 텍스트 파일이며 DER 또는 Base 64 형식일 수 있습니다. 이 형식을 Windows 인증서 저장소로 가져올 수 있습니다.

.pem - 이 확장은 프라이버시 향상 메일을 나타냅니다. 이 확장은 일반적으로 UNIX, Linux, BSD 등과 함께 사용됩니다. 일반적으로 서버 인증서 및 개인 키에 사용되며, Windows 인증서 저장소로 가져올 수 있도록 확장자가 .pem에서 .cer인 일반 텍스트 파일입니다.

.cer 및 .pem 파일의 내부 내용은 일반적으로 다음과 같습니다.

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

.pfx - 이 확장은 개인 정보 교환을 나타냅니다. 이 형식은 인증서를 단일 파일로 번들하는 데 사용할 수 있는 방법입니다. 예를 들어, 서버 인증서 및 관련 개인 키 및 루트 CA 인증서를 하나의 파일로 번들하고 파일을 적절한 Windows 인증서 저장소로 쉽게 가져올 수 있습니다. 서버 및 클라이언트 인증서에 가장 일반적으로 사용됩니다. 그러나 루트 CA 인증서가 포함된 경우 로컬 컴퓨터 저장소가 설치용으로 지정된 경우에도 루트 CA 인증서는 로컬 컴퓨터 저장소 대신 항상 현재 사용자 저장소에 설치됩니다.

.p12—이 형식은 일반적으로 클라이언트 인증서에서만 표시됩니다. 이 형식을 Windows 인증서 저장소로 가져올 수 있습니다.

.p7b—여러 인증서를 한 파일에 저장하는 또 다른 형식입니다. 이 형식을 Windows 인증서 저장소로 가져올 수 있습니다.

부록 B - 인증서 형식 변환

대부분의 경우 인증서가 일반 텍스트 형식으로 되어 있으므로 확장자를 변경할 때(예: .pem에서 .cer로) 인증서 변환이 발생합니다. 때때로 인증서가 일반 텍스트 형식이 아니므로 OpenSSL과 같은 도구를 사용하여 변환해야 합니다 . 예를 들어 ACS 솔루션 엔진은 .pfx 형식으로 인증서를 설치할 수 없습니다. 따라서 인증서 및 개인 키를 사용 가능한 형식으로 변환해야 합니다. 다음은 OpenSSL에 대한 기본 명령 구문입니다.

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

Import Password(비밀번호 가져오기) 및 PEM 암호문을 입력하라는 메시지가 표시됩니다. 이러한 암호는 동일해야 하며 .pfx를 내보낼 때 지정된 개인 키 암호여야 합니다. 출력은 .pfx의 모든 인증서 및 개인 키를 포함하는 단일 .pem 파일입니다. 이 파일은 ACS에서 인증서 및 개인 키 파일로 참조될 수 있으며 문제 없이 설치됩니다.

부록 C - 인증서 유효 기간

인증서는 유효 기간 동안에만 사용할 수 있습니다. 루트 CA 인증서의 유효 기간은 루트 CA가 설정될 때 결정되며 다를 수 있습니다. 중간 CA 인증서의 유효 기간은 CA가 설정될 때 결정되며 하위 CA가 속한 루트 CA의 유효 기간을 초과할 수 없습니다. 서버, 클라이언트 및 컴퓨터 인증서의 유효 기간은 Microsoft 인증서 서비스를 통해 자동으로 1년으로 설정됩니다. Microsoft 기술 자료 문서 254632 에 따라 Windows 레지스트리를 해킹할 때만 이를 변경할 수 있으며 루트 CA의 유효 기간을 초과할 수 없습니다. ACS에서 생성하는 자체 서명 인증서의 유효 기간은 항상 1년이며 현재 버전에서는 변경할 수 없습니다.

관련 정보

- RADIUS 지원 페이지
- RFC(Request for Comments)
- Technical Support - Cisco Systems