Содержание

Введение

Этот документ разъясняет часть беспорядка, который сопровождает различные Типы сертификата, форматы и требования, привязанные к различным формам Протокола EAP. Этими пятью Типами сертификата, отнесенными к EAP, который обсуждает этот документ, является Сервер, Узел CA, Промежуточное звено CA, Клиент и Машина. Эти сертификаты найдены в различных форматах и там могут не соглашаться требования с отношением к каждому из них на основе включенной реализации EAP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Серверные сертификаты

Серверный сертификат установлен на сервере RADIUS, и его первичная цель в EAP должна создать зашифрованный туннель Transport Layer Security (TLS), который защищает информацию для аутентификации. При использовании EAP-MSCHAPv2 Серверный сертификат берет дополнительную роль, которая должна определить сервер RADIUS как надежный объект для аутентификации. Эта дополнительная роль выполнена с помощью поля Enhanced Key Usage (EKU). Поле EKU определяет сертификат как Сертификат допустимого сервера и проверяет, что узел CA, который выполнил сертификат, является CA. Trusted Root, Это требует присутствия Корневого сертификата CA. Cisco Secure ACS требует, чтобы сертификат был или закодирован Base64 или закодированный DER двоичный формат v3 X.509.

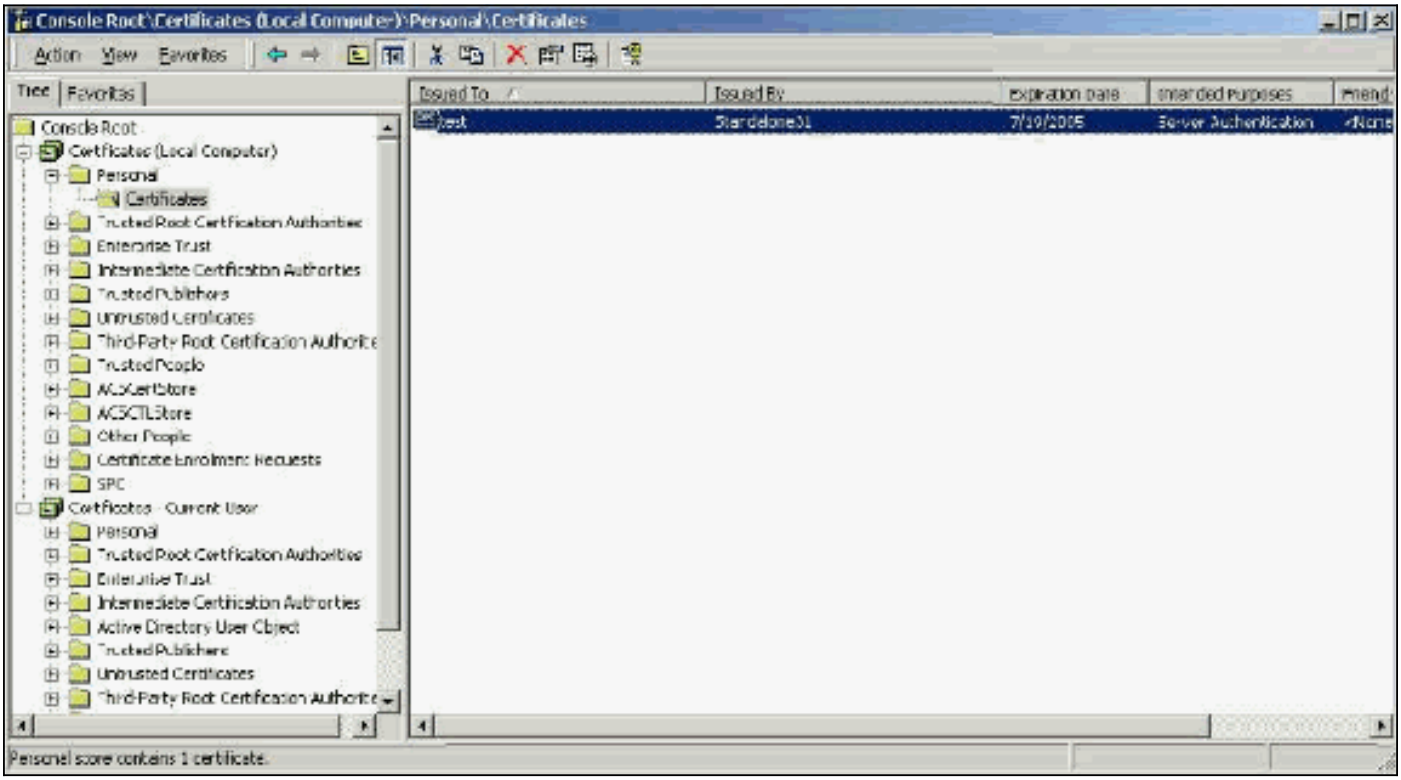
Можно создать этот сертификат или с использованием запроса подписи сертификата (CSR) в ACS, который отправлен CA. Или, можно также вырезать сертификат с использованием внутрифирменного CA (как службы Microsoft Certificate) форма создания сертификата. Следует отметить, что, в то время как можно создать серверный сертификат с размерами ключа, больше, чем 1024, любой ключ, больше, чем 1024, не работает с PEAP. Даже если аутентификация проходит, клиент "зависает".

При создании сертификата с использованием CSR это создано с .cer, .pem или форматом .txt. В редких случаях это создано без расширения. Гарантируйте, что ваш сертификат является файлом открытого текста с расширением, которое можно изменить по мере необходимости (прибор ACS использует .cer или расширение .pem). Кроме того, при использовании CSR секретный ключ сертификата создан в пути, который вы задаете как отдельный файл, который может или может не иметь расширения и которому привязали пароль к нему (пароль требуется для установки на ACS). Независимо от расширения гарантируйте, что это - файл открытого текста с расширением, которое можно изменить по мере необходимости (прибор ACS использует .pvk или расширение .pem). Если никакой путь не задан для секретного ключа, ACS сохраняет ключ в C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs каталог и взгляды в этом каталоге, если никакой путь не задан для файла закрытого ключа при установке сертификата.

Если сертификат создан с использованием формы подчиненного сертификата служб Microsoft Certificate, гарантируйте, что вы отмечаете ключи как экспортные так, чтобы можно было установить сертификат в ACS. Создание сертификата этим способом упрощает процесс установки значительно. Можно непосредственно установить его в надлежащее хранилище Windows от веб-интерфейса Сервисов сертификации и затем установить на ACS от хранилища с использованием CN как ссылка. Сертификат, установленный в хранилище локального компьютера, может также быть экспортирован от Хранилища windows и установлен на другом компьютере легко. Когда этот тип сертификата экспортируется, ключи

должны быть отмечены как экспортные и данные пароль. Сертификат тогда появляется в формате .pfx, который включает секретный ключ и серверный сертификат.

Когда правильно установлено в хранилище сертификата Windows, Серверный сертификат должен появиться в папке **Certificates (Local Computer)> Personal> Certificates**, как замечено в окне данного примера.



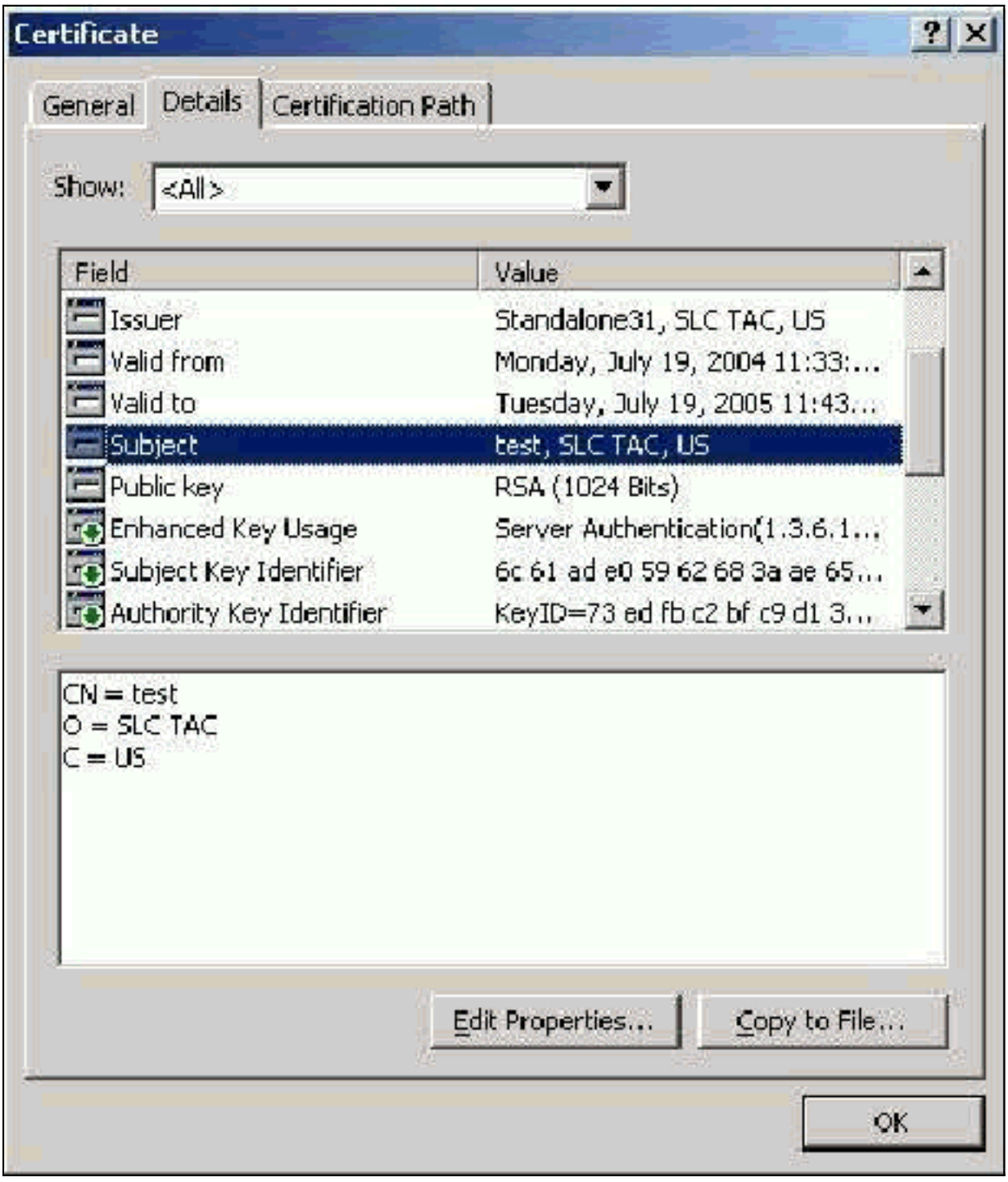
Подписанные сертификаты являются сертификатами, которые вы создаете без root или промежуточного вовлечения CA., у Них есть то же значение и в предмете и в полях отправителя как Корневой сертификат CA. Большинство подписанных сертификатов использует формат v1 X.509. Поэтому они не работают с ACS. Однако с версии 3.3, ACS имеет способность создать ее собственные подписанные сертификаты, которые можно использовать для EAP-TLS и PEAP. Не используйте размер ключа, больше, чем 1024 для совместимости с PEAP и EAP-TLS. При использовании подписанного сертификата сертификат также действует от лица Корневого сертификата CA и должен быть установлен в папке **Certificates (Local Computer)> Trusted Root Certification Authorities> Certificates** клиента при использовании Microsoft EAP supplicant. Это автоматически устанавливает в хранилище сертификатов доверенного корня на сервере. Однако этому нужно все еще доверять Списку надежных сертификатов в Установке сертификата ACS. Посмотрите раздел Корневых сертификатов CA для получения дополнительной информации.

Поскольку подписанные сертификаты используются в качестве Корневого сертификата CA для проверки Серверного сертификата при использовании Microsoft EAP supplicant, и потому что период достоверности не может быть увеличен с по умолчанию одного года, Cisco рекомендует только использовать их для EAP как временное измерение, пока вы не можете использовать традиционного CA.

Поле Тема

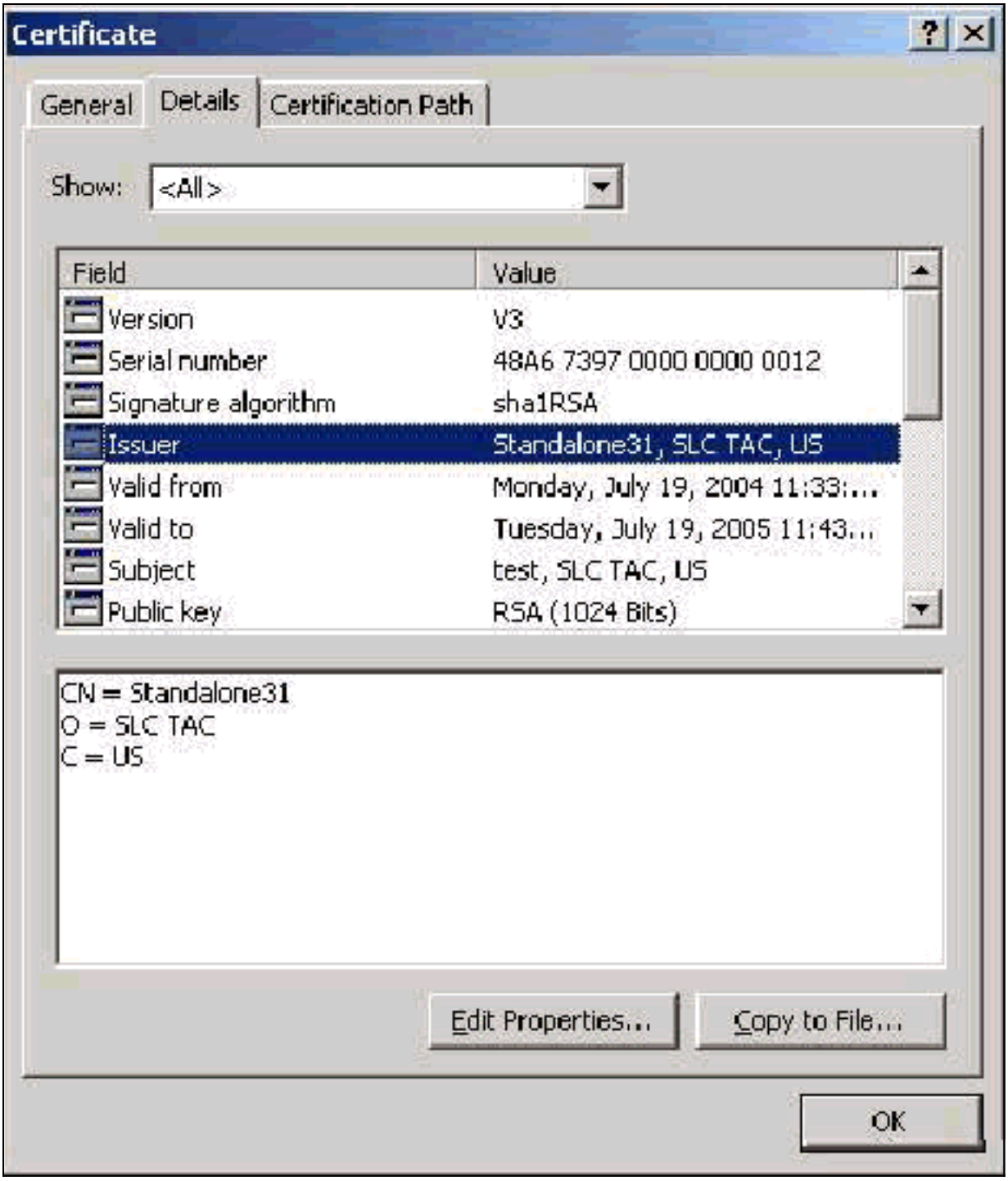
Поле Тема определяет сертификат. Значение CN используется для определения Выполненного к полю во Вкладке Общие сертификата и заполнено с информацией, что вы вводите в поле Тема Сертификата в ACS " диалог CSR или с информацией от Поля имени в

службах Microsoft Certificate. Значение CN используется для сообщения ACS, какой сертификат это должно использовать от хранилища сертификата локального компьютера, если используется опция для установки сертификата от хранилища.



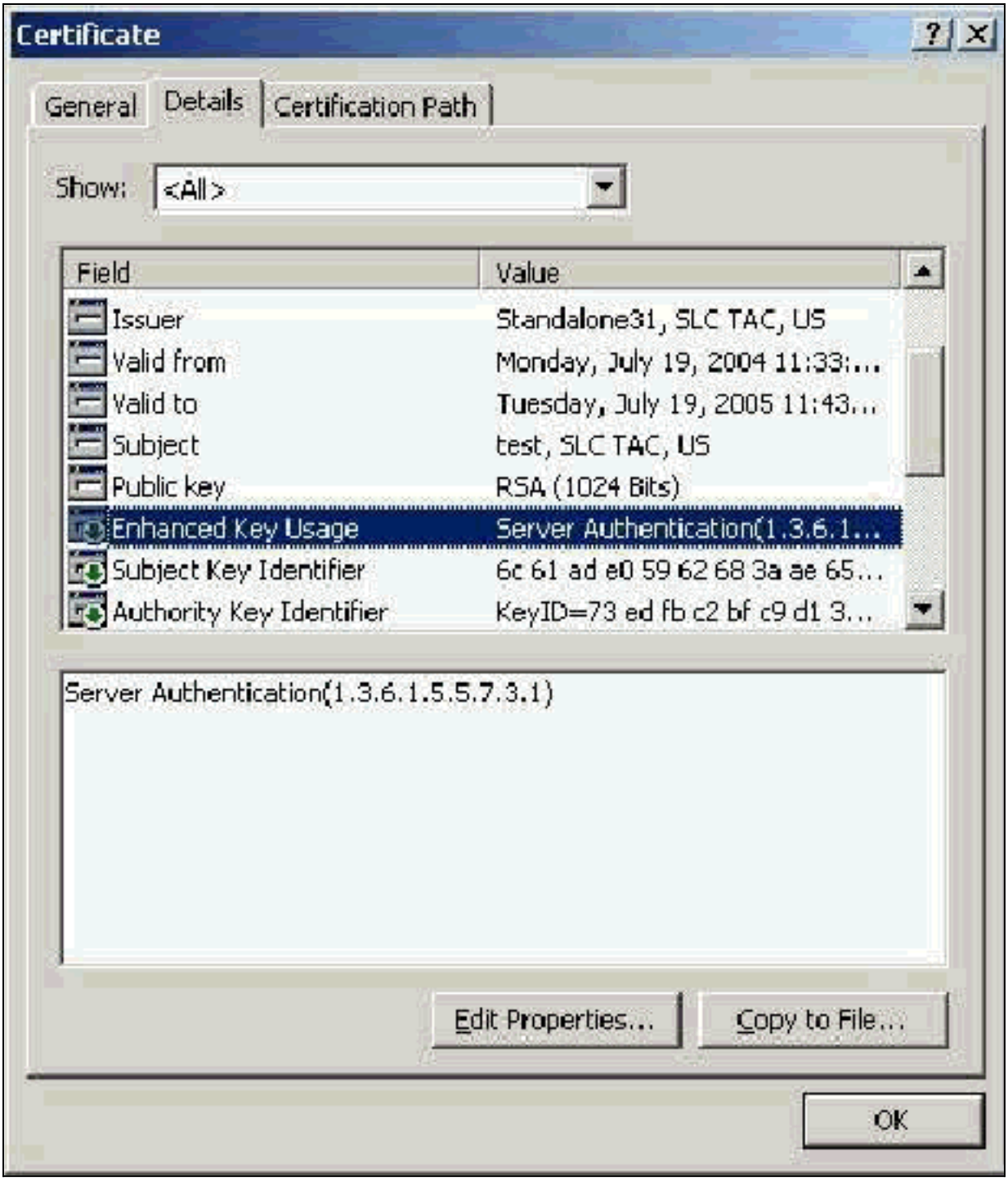
Поле отправителя

Поле Issuer определяет CA, которые вырезают сертификат. Используйте это значение для определения значения Выполненного полем во Вкладке Общие сертификата. Это заполнено с названием CA.



Поле Enhanced Key Usage

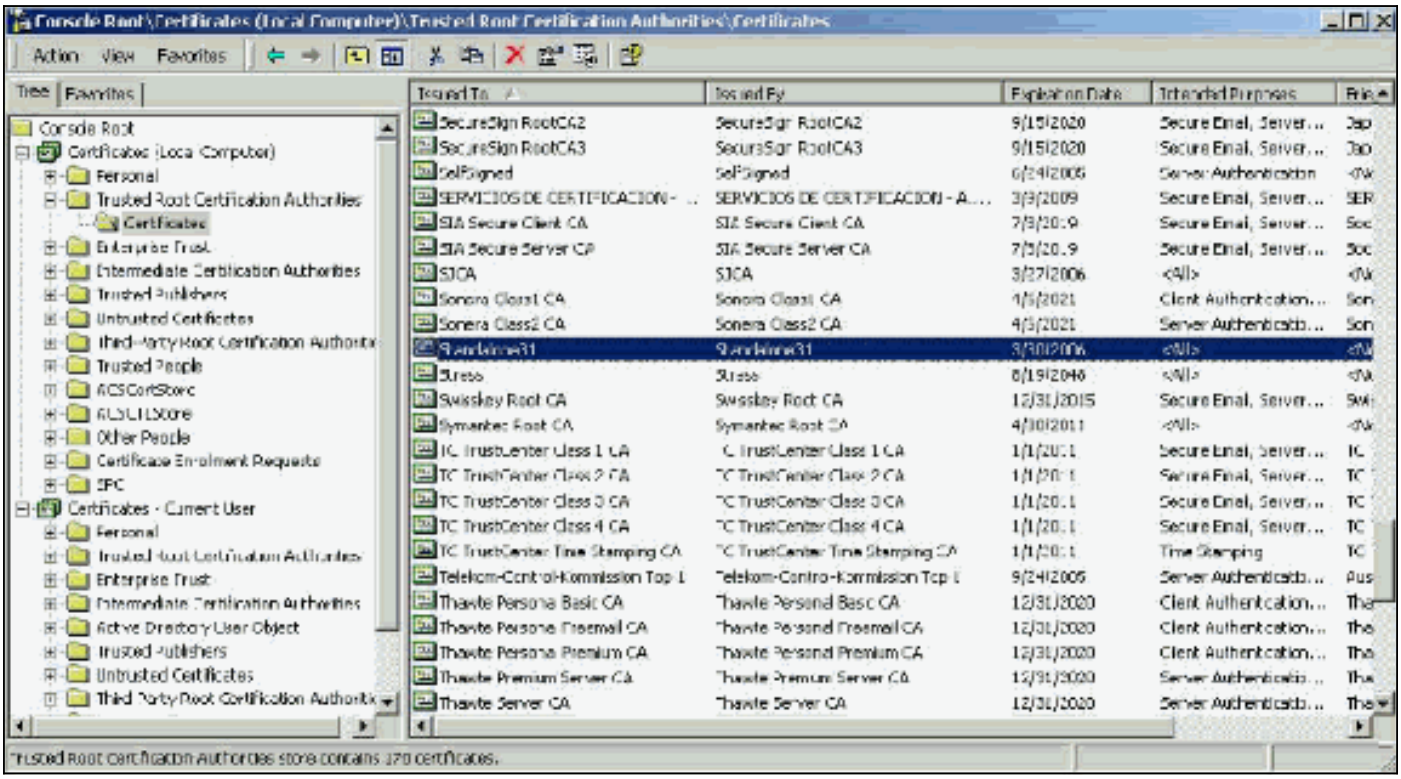
Поле Enhanced Key Usage определяет намеченную цель сертификата и должно быть перечислено как "Проверка подлинности сервера". Это поле является обязательным при использовании Microsoft supplicant для PEAP и EAP-TLS. При использовании служб Microsoft Certificate это настроено в Автономном CA с выбором **Сертификата проверки подлинности сервера** от Намеченной выпадающей Цели, и на Предприятии CA с выбором **Web-сервера** от Шаблона сертификата выпадают. При запросе сертификата с использованием CSR со службами Microsoft Certificate у вас нет опции для определения Намеченной Цели с Автономным CA. Поэтому, поле EKU отсутствует. С Предприятием CA, у вас есть Намеченная выпадающая Цель. Некоторые CAs не создают сертификаты с полем EKU, таким образом, они бесполезны, когда вы используете Microsoft EAP supplicant.



Корневые сертификаты CA

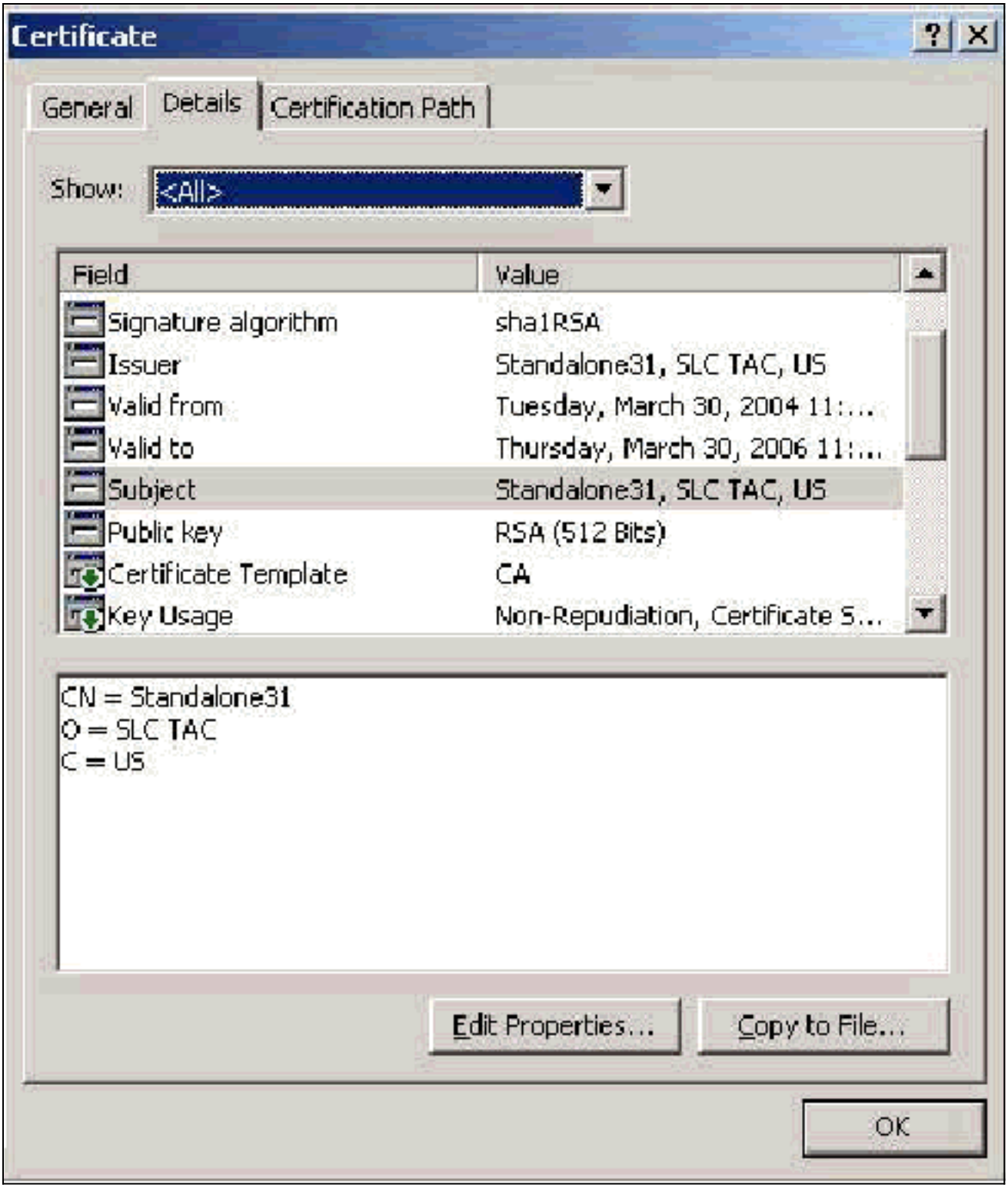
Одна цель Корневого сертификата CA состоит в том, чтобы определить Серверный сертификат (и Промежуточный сертификат CA если применимо) как надежный сертификат к ACS и соискателю Windows EAP-MSCHAPv2. Это должно быть расположенный в хранилище Доверенных корневых центров сертификации в Windows и на сервере ACS и на, в случае EAP-MSCHAPv2, на компьютере клиента. Большинство Корневых сертификатов CA третьей стороны установлено с Windows и существует мало усилия, связанного с этим. Если службы Microsoft Certificate используются, и сервер сертификатов находится на той же машине как ACS, то Корневой сертификат CA установлен автоматически. Если Корневой сертификат CA не найден в хранилище Доверенных корневых центров сертификации в Windows, то это должно быть полученный от вашего CA и установленный. Когда правильно установлено в хранилище сертификата Windows, Корневой сертификат CA должен появиться в папке **Certificates (Local Computer)> Trusted Root Certification Authorities> Certificates**, как замечено в

окне данного примера.



[Предмет и поля отправителя]

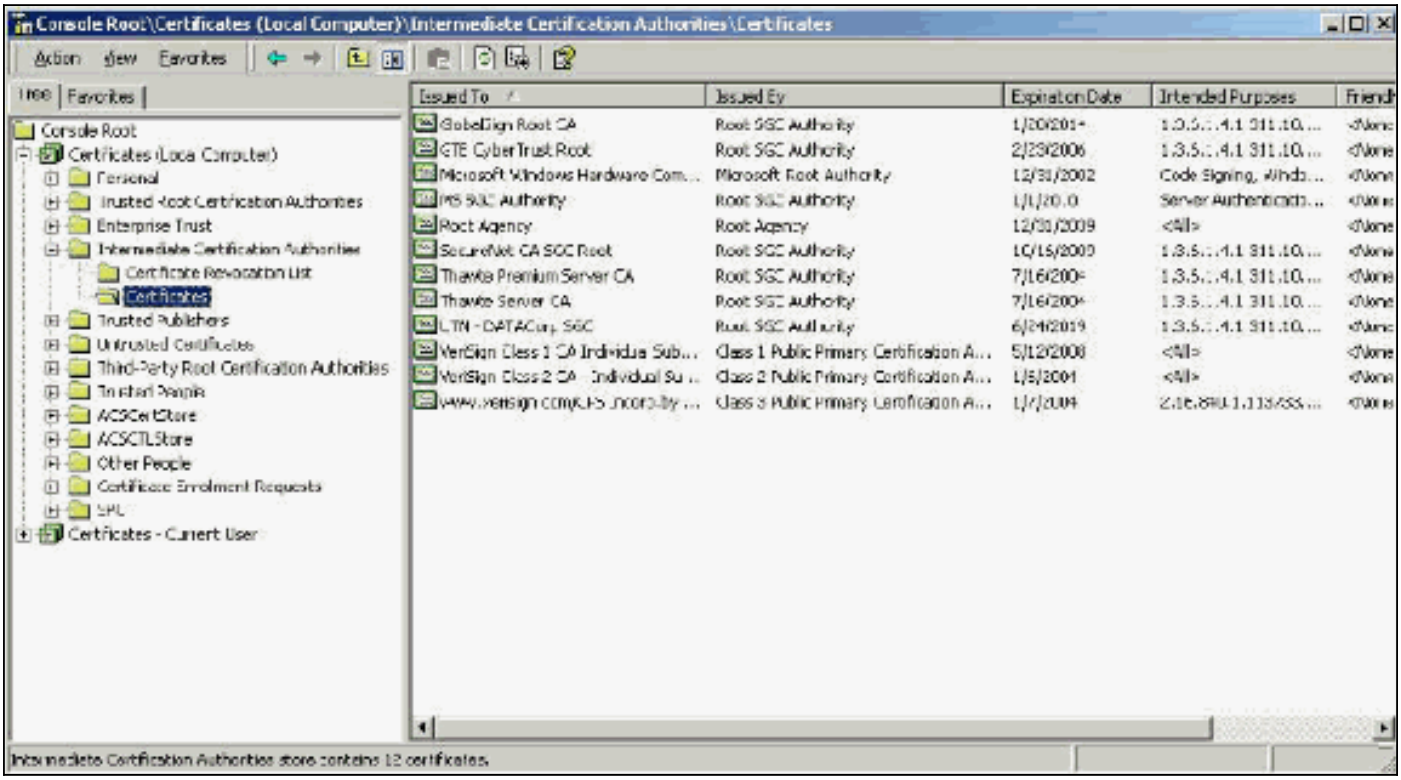
Поля Subject и Issuer определяют CA и должны быть точно тем же. Используйте эти поля для начальной загрузки Выполненного к и Выполненный полями во Вкладке Общие сертификата. Они заполнены с названием узла CA.



Промежуточные сертификаты CA

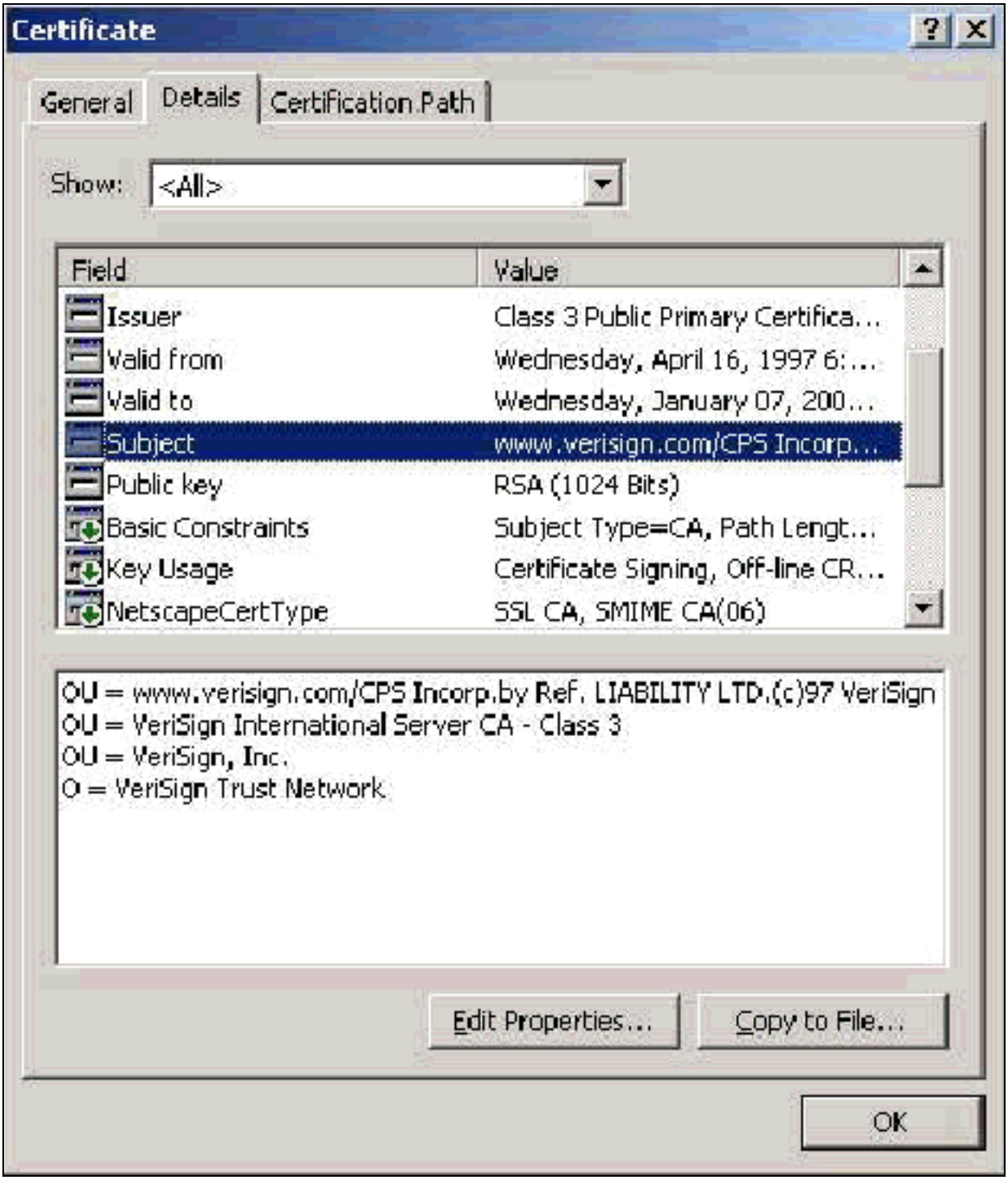
Промежуточные сертификаты CA являются сертификатами, которые вы используете для определения CA, который зависим от узла CA. Некоторые Серверные сертификаты (беспроводные сертификаты Verisign) созданы с использованием промежуточного CA., Если Серверный сертификат, который вырезан Промежуточным звеном CA, используется, Промежуточный сертификат CA должен быть установлен в области Intermediate Certification Authorities памяти локального компьютера на сервере ACS. Кроме того, если Microsoft EAP supplicant используется на клиенте, Корневой сертификат CA узла CA, который создал Промежуточный сертификат CA, должен также быть в соответствующем хранилище на сервере ACS и клиенте так, чтобы могла быть установлена цепочка доверия. И Корневой

сертификат CA и Промежуточный сертификат CA должны быть отмечены, как доверяется ACS и на клиенте. Большинство Промежуточных сертификатов CA не установлено с Windows, таким образом, скорее всего, необходимо получить их от поставщика. Когда правильно установлено в хранилище сертификата Windows, Промежуточный сертификат CA появляется в папке **Certificates (Local Computer)> Intermediate Certification Authorities> Certificates**, как замечено в окне данного примера.



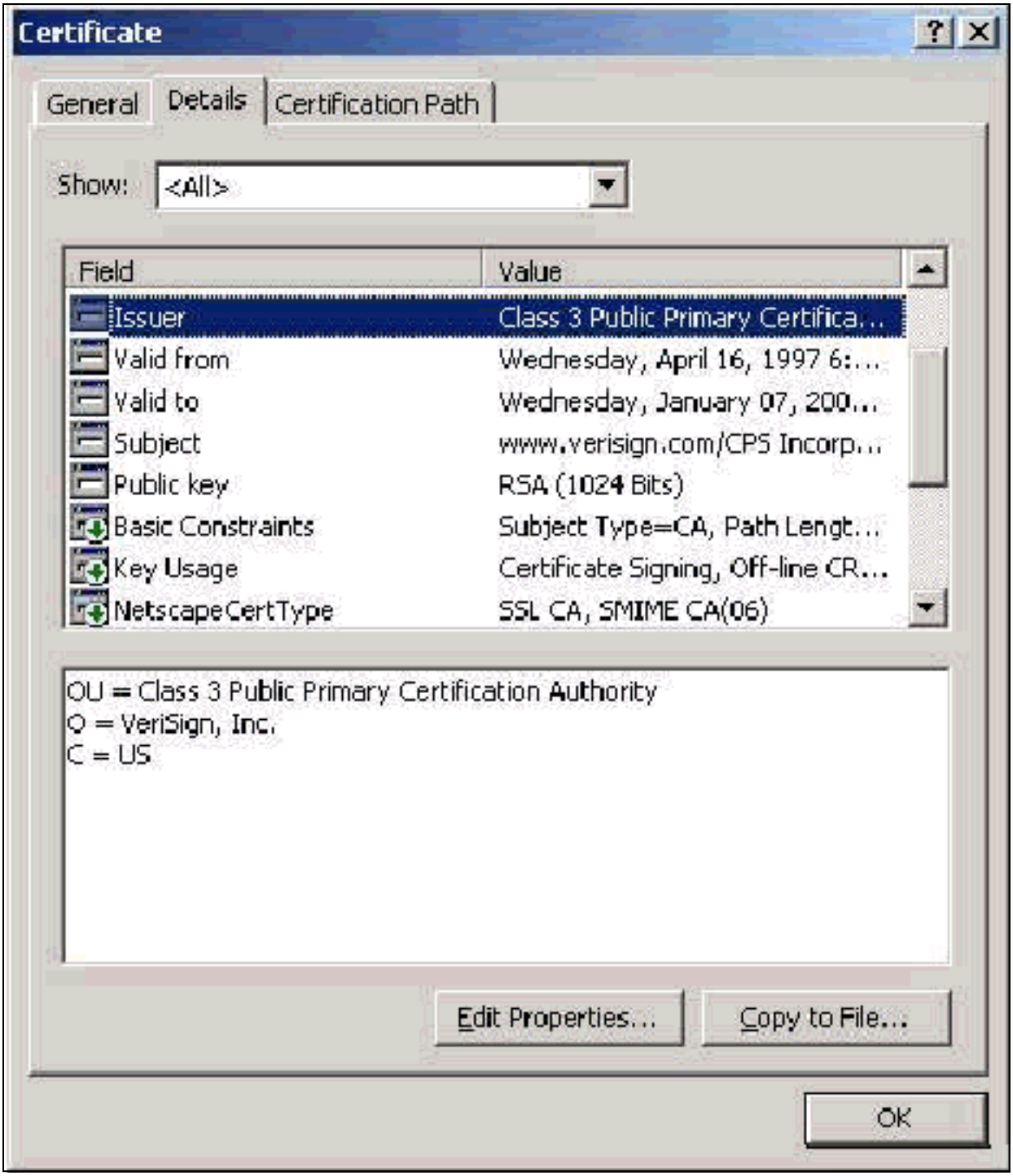
Поле Тема

Поле Тема определяет Промежуточного CA., Это значение используется для определения Выполненного к полю во Вкладке Общие сертификата.



Поле отправителя

Поле Issuer определяет CA, которые вырезают сертификат. Используйте это значение для определения значения Выполненного полем во Вкладке Общие сертификата. Это заполнено с названием CA.



Сертификаты клиента

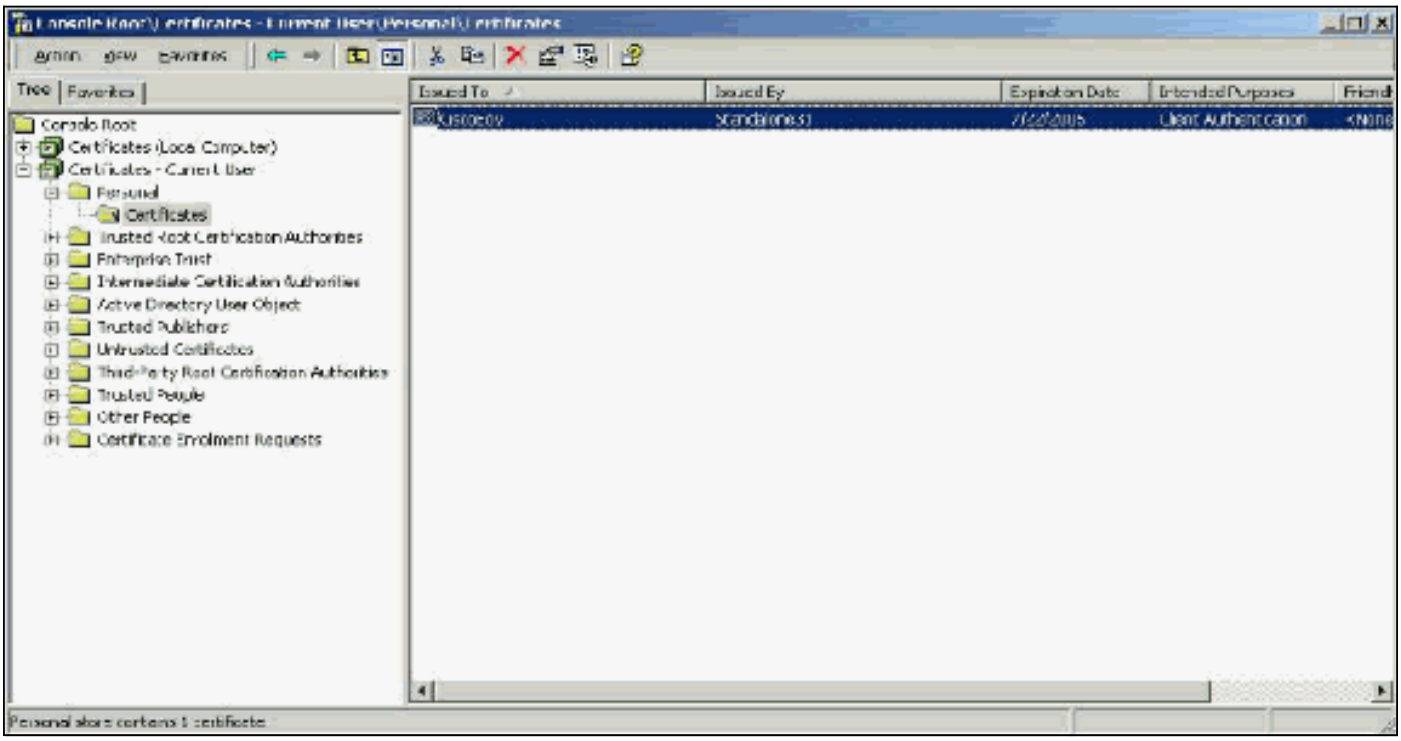
Сертификаты клиента используются для положительного определения пользователя в EAP-TLS. Они не имеют никакой роли в построении туннеля TLS и не используются для шифрования. Идентификация подтверждением выполнена одним из трех средств:

- **CN (или Название) Сравнение**? Сравнивает CN в сертификате с именем пользователя в базе данных. Дополнительные сведения об этом типе сравнения включены в описание Поля Тема сертификата.
- **Сравнение SAN**? Сравнивает SAN в сертификате с именем пользователя в базе данных. Это только поддерживается с ACS 3.2. Дополнительные сведения об этом типе сравнения включены в описание поля Subject Alternative Name сертификата.
- **Двоичное сравнение**? Сравнивает сертификат с двоичной копией сертификата,

сохраненного в базе данных (только AD и LDAP могут сделать это). При использовании сравнения двоичных файлов сертификата необходимо сохранить сертификат пользователя в двоичном формате. Кроме того, для LDAP общего назначения и Active Directory, атрибут, который хранит сертификат, должен быть стандартным атрибутом LDAP, названным "usercertificate".

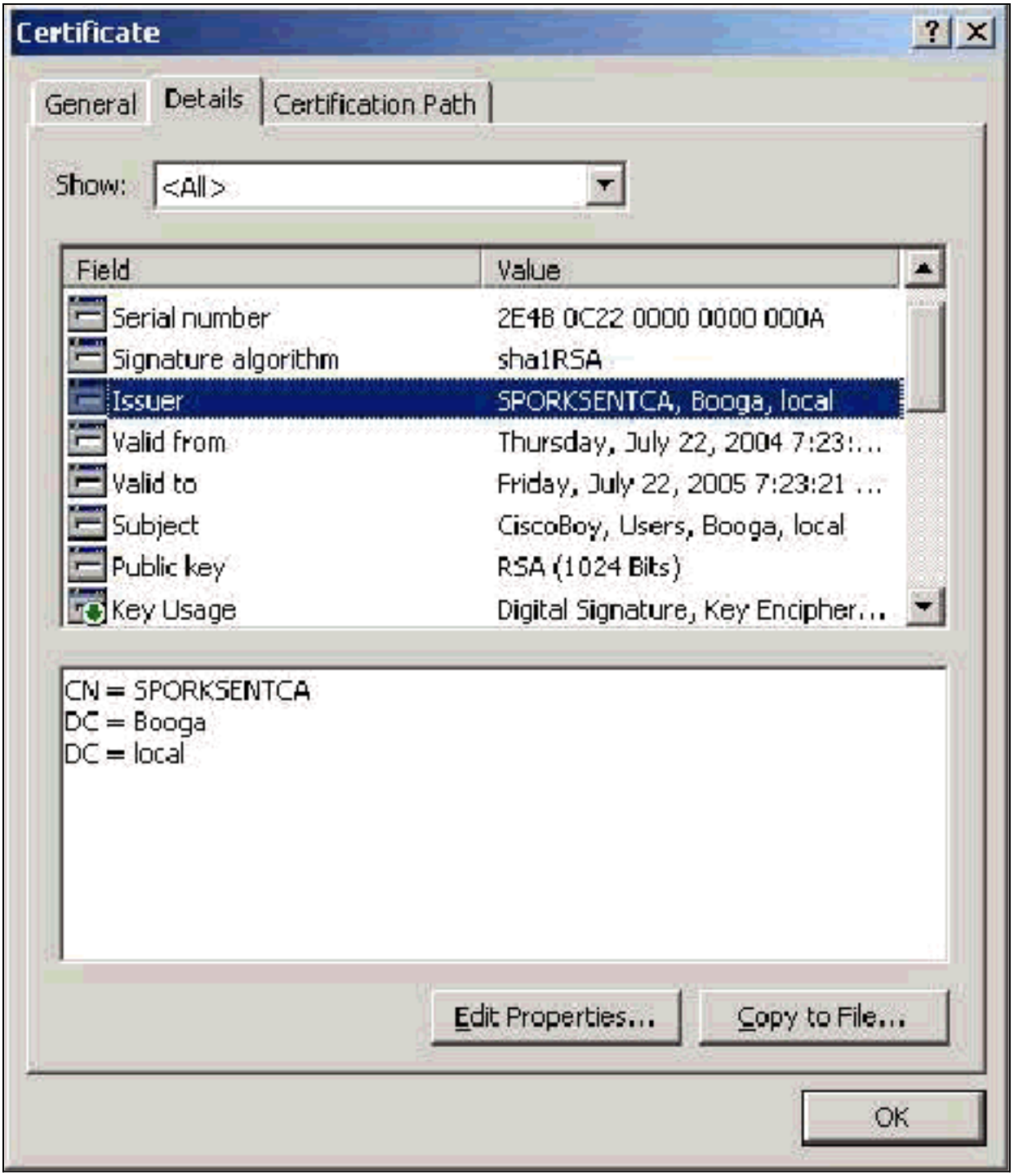
Независимо от того, что метод сравнения используется, информация в соответствующем поле (CN или SAN) должна совпасть с названием, которое ваша база данных использует для аутентификации. AD использует Имя NETBIOS для аутентификации в смешанном режиме и UPN в режиме работы в собственной системе команд.

В этом разделе рассматриваются генерацию Сертификата клиента с использованием служб Microsoft Certificate. EAP-TLS требует, чтобы аутентифицировался уникальный Сертификат клиента для каждого пользователя. Сертификат должен быть установлен на каждом компьютере для каждого пользователя. Когда должным образом установлено, сертификат расположен в **Сертификатах - Текущий пользователь>** папка **Personal> Certificates**, как замечено в окне данного примера.



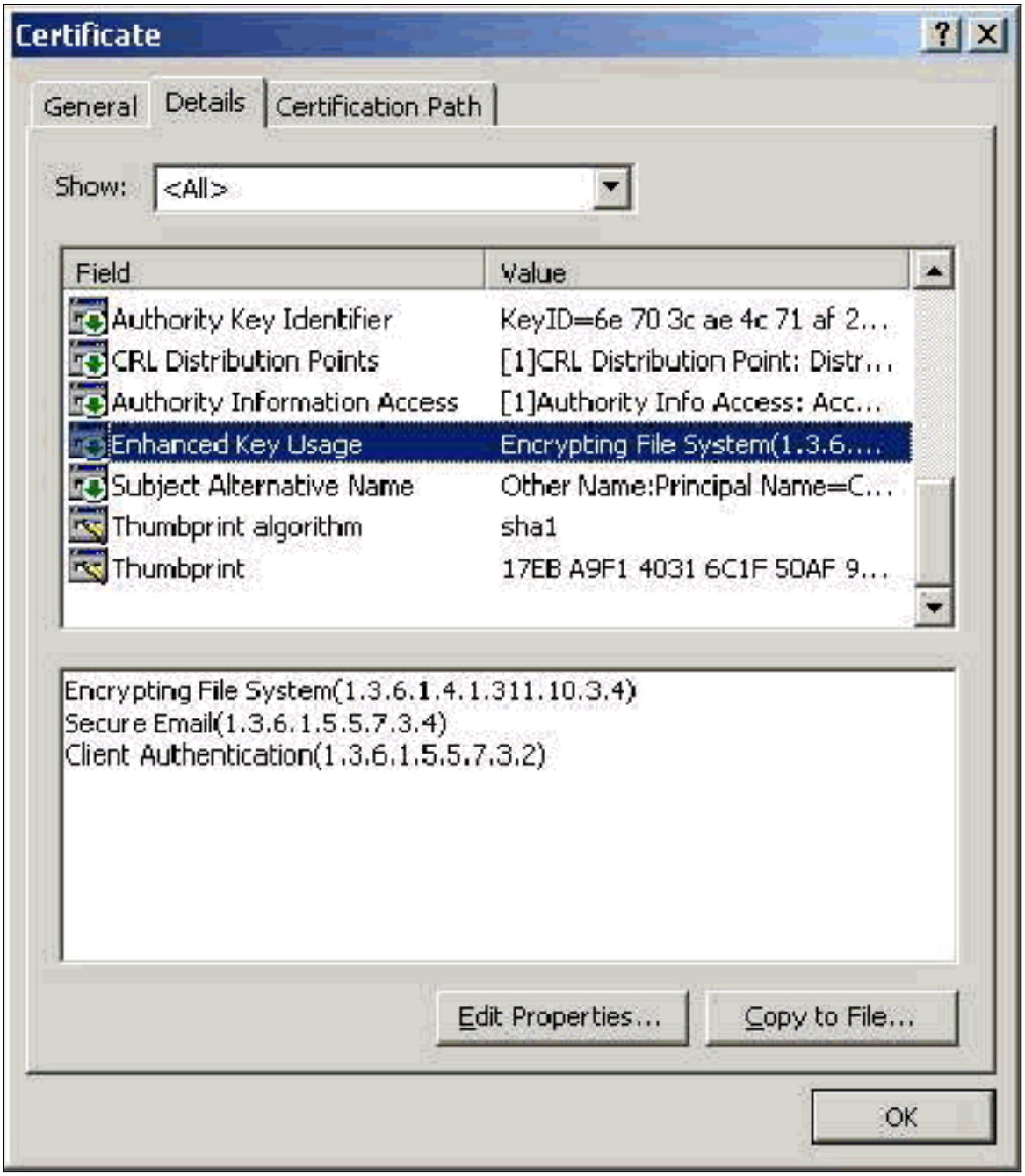
Поле отправителя

Поле Issuer определяет CA, который вырезает сертификат. Используйте это значение для определения значения Выполненного полем во Вкладке Общие сертификата. Это заполнено с названием CA.



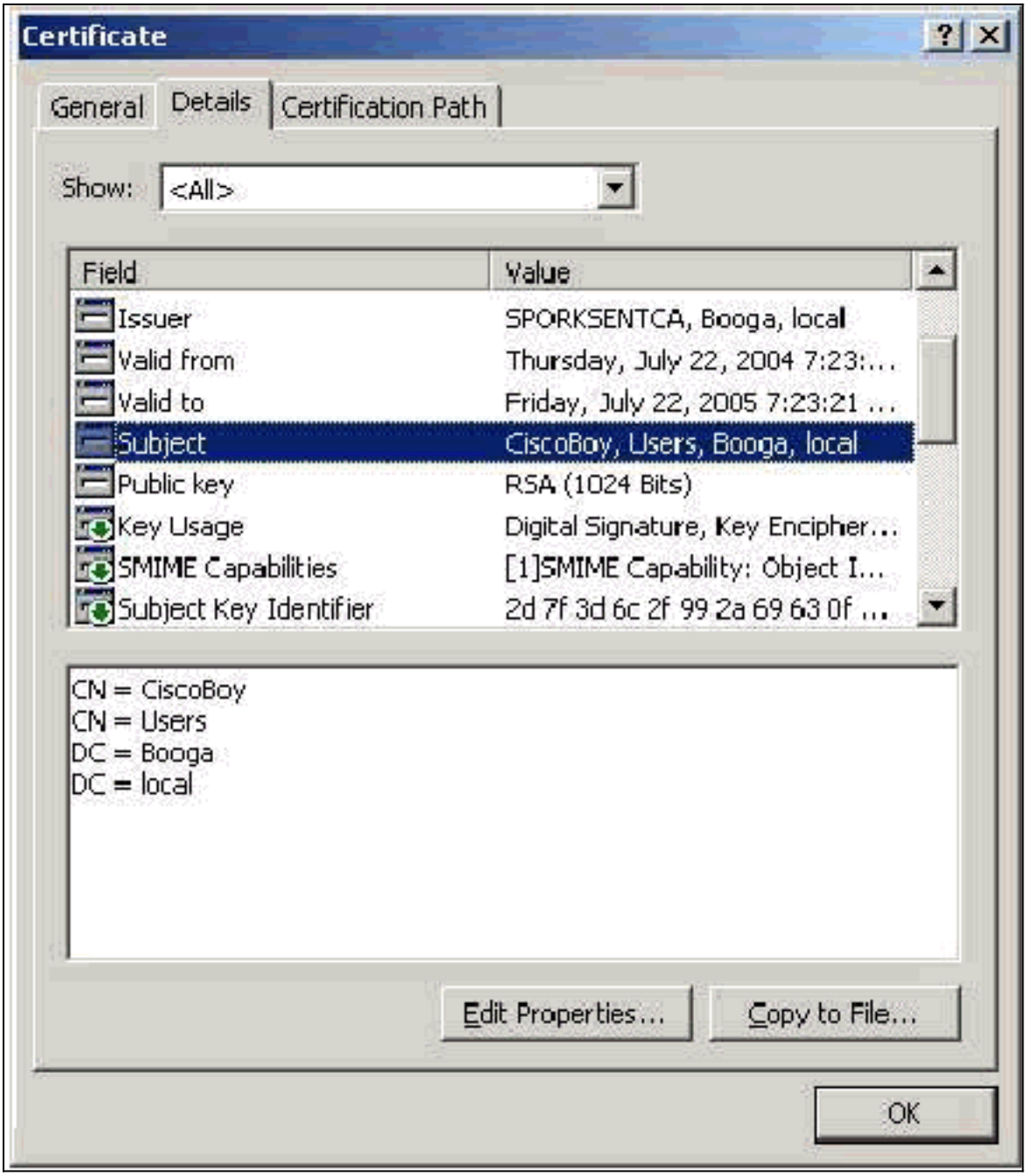
Поле Enhanced Key Usage

Поле Enhanced Key Usage определяет намеченную цель сертификата и должно содержать Аутентификацию клиента. Это поле является обязательным при использовании Microsoft supplicant для PEAP и EAP-TLS. При использовании служб Microsoft Certificate это настроено в Автономном CA при выборе **Client Authentication Certificate** от Намеченной выпадающей Цели и на Предприятии CA при выборе **User** от выпадающего Шаблона сертификата. При запросе сертификата с использованием CSR со службами Microsoft Certificate у вас нет опции для определения Намеченной Цели с Автономным CA. Поэтому, поле EKU отсутствует. С Предприятием CA, у вас есть Намеченная выпадающая Цель. Некоторые CAs не создают сертификаты с полем EKU. Когда вы используете Microsoft EAP supplicant, они бесполезны.



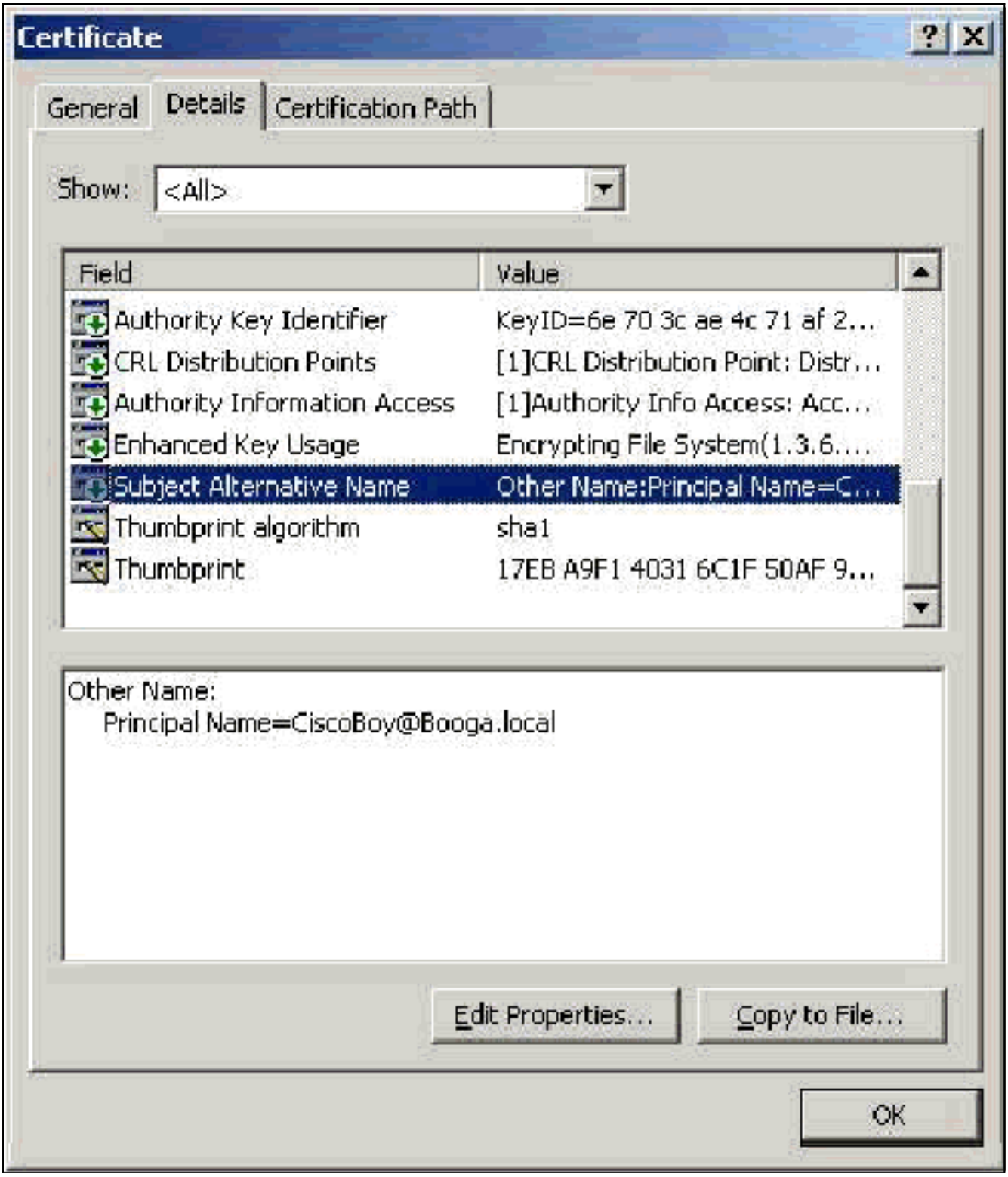
Поле Тема

Это поле используется в сравнении CN. Первый перечисленный CN сравнен с базой данных для обнаружения соответствия. Если соответствие найдено, аутентификация успешно выполняется. При использовании Автономного CA CN заполнен с тем, что вы вставляете Поле имени в форме подчиненного сертификата. При использовании Предприятия CA CN автоматически заполнен с названием учетной записи, как перечислено в консоли Пользователей и компьютеров Active Directory (это не обязательно совпадает с UPN или Именем NETBIOS).



Поле альтернативного имени субъекта

Поле Subject Alternative Name используется в сравнении SAN. Перечисленный SAN сравнен с базой данных для обнаружения соответствия. Если соответствие найдено, аутентификация успешно выполняется. При использовании Предприятия CA SAN автоматически заполнен с именем пользователя Active Directory @domain (UPN). Автономный CA не включает поле SAN, таким образом, вы не можете использовать сравнение SAN.



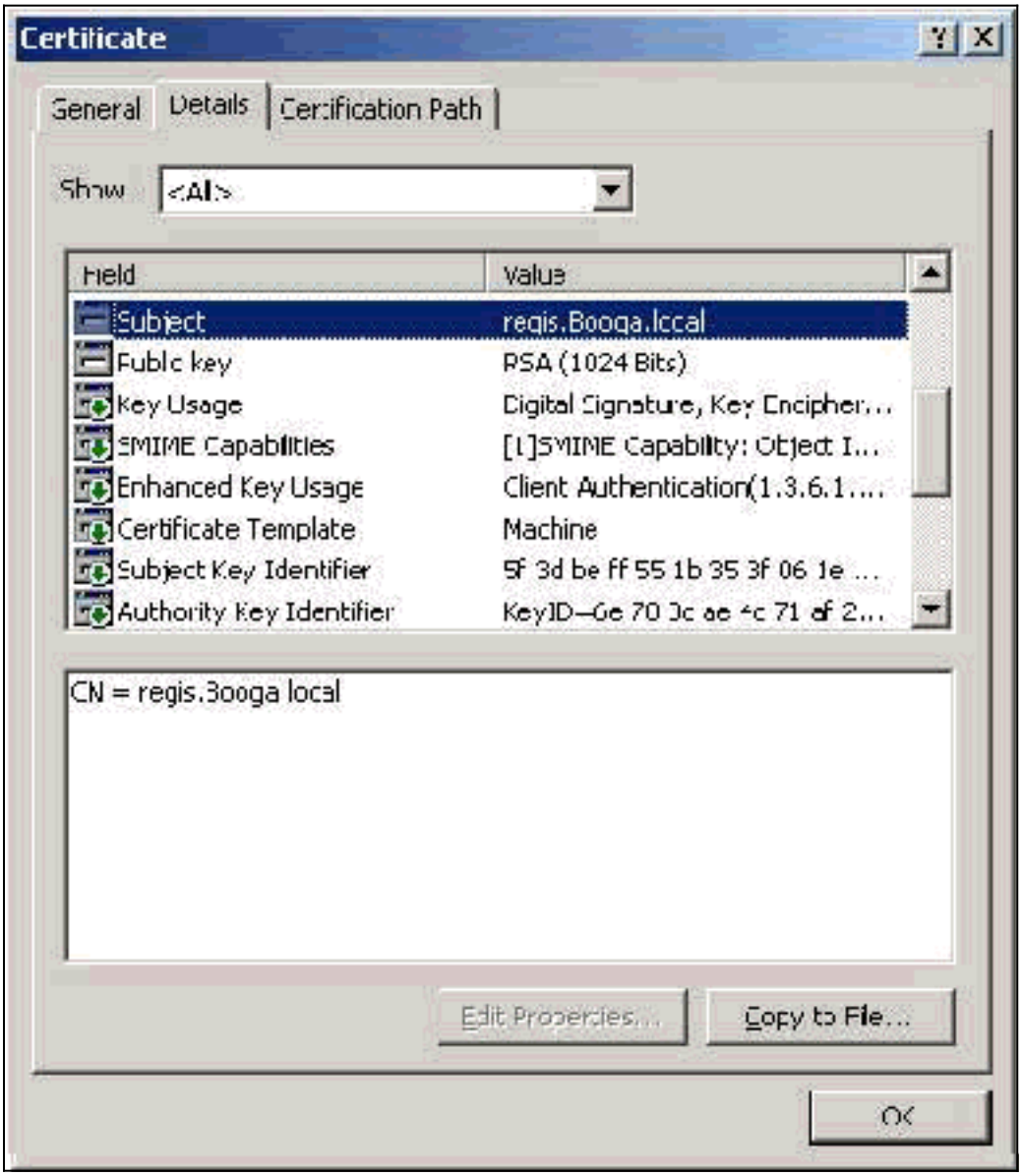
Сертификаты компьютера

Сертификаты компьютера используются в EAP-TLS для положительного определения компьютера при использовании аутентификации компьютера. Когда вы настраиваете свою Microsoft Enterprise CA для автоматической подачи заявок сертификата и соединяете компьютер с доменом, можно только обратиться к этим сертификатам. Сертификат автоматически создан, когда вы используете учетные данные Active Directory компьютера и устанавливаете их в хранилище локального компьютера. Компьютеры, которые уже являются участниками домена перед настройкой автоматической подачи заявок получают сертификат в следующий раз, когда Windows перезапускает. Сертификат компьютера установлен в папке **Certificates (Local Computer)> Personal> Certificates** Сертификатов

(Локальный компьютер) моментальный снимок MMC - в точно так же, как Серверные сертификаты. Вы не можете установить эти сертификаты ни на какой другой машине, так как вы не можете экспортировать секретный ключ.

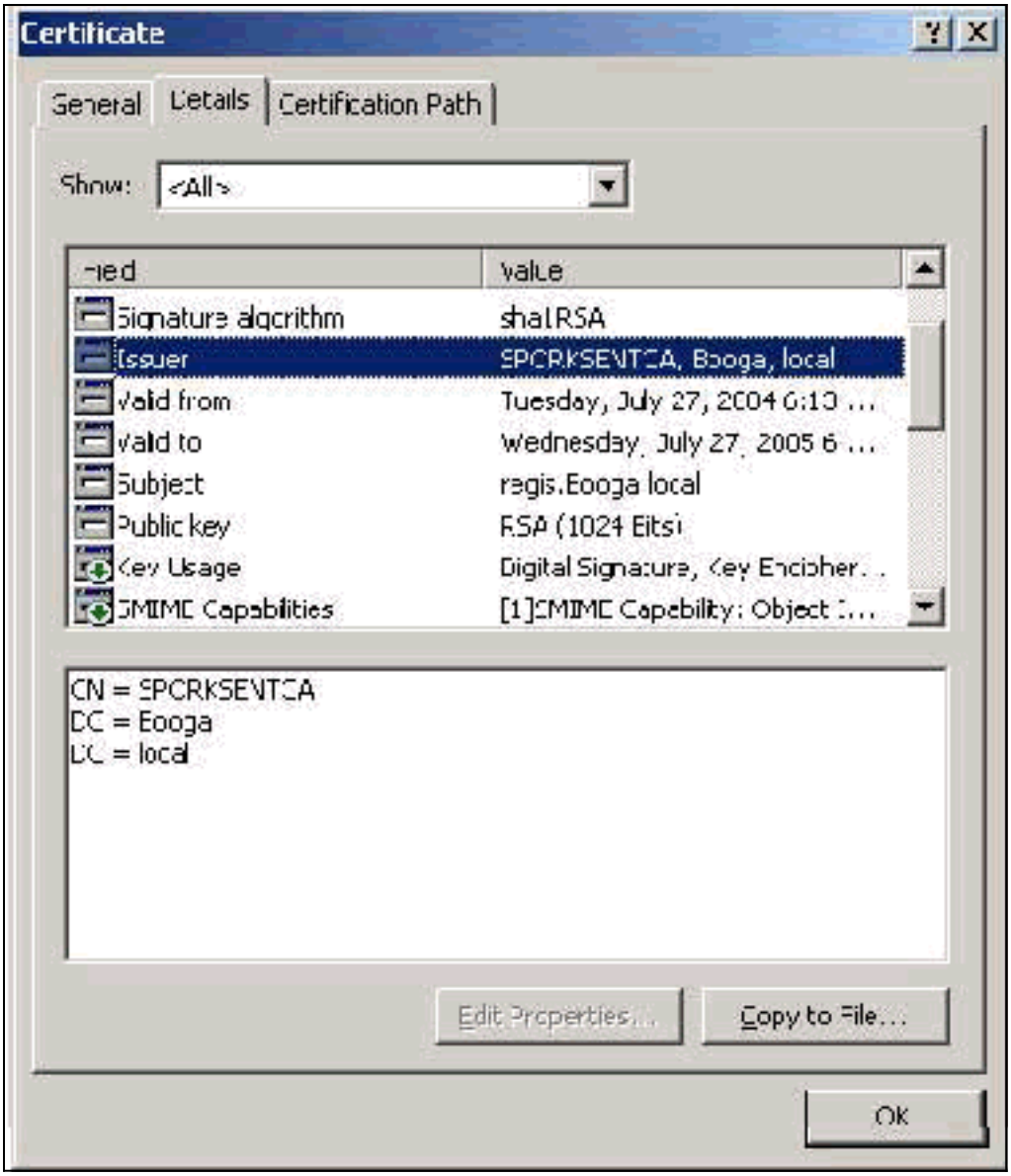
Подчиненные и SAN поля

Поля Subject и SAN определяют компьютер. Значение заполнено полностью определенным названием компьютера и используется, чтобы определить Выполненный к полю во Вкладке Общие сертификата и является тем же для обоих полей Subject и SAN.



Поле отправителя

Поле Issuer определяет CA, которые вырезают сертификат. Используйте это значение для определения значения Выполненного полем во Вкладке Общие сертификата. Это заполнено с названием CA.



Приложение A - общие расширения сертификата

.csr? Это не фактически сертификат, а скорее Запрос подписи сертификата. Это - файл открытого текста с этим форматом:

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

.pvk? Это расширение обозначает секретный ключ, хотя расширение не гарантирует, что содержание является фактически секретным ключом. Потребность содержания быть открытым текстом с этим форматом:

```
-----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? Это - общее расширение, которое обозначает сертификат. Сервер, Узел CA и Промежуточные сертификаты CA могут быть в этом формате. Это обычно - файл открытого текста с расширением, которое можно изменить, как вы нуждаетесь и можете быть или DER или Ядром 64 формата. Можно импортировать этот формат в хранилище сертификата Windows.

.pem? Это расширение обозначает Privacy Enhanced Mail. Это расширение обычно используется с UNIX, Linux, BSD, и т.д. Это обычно используется для серверных сертификатов и секретных ключей, и обычно является файлом открытого текста с расширением, которое можно изменить, поскольку вам нужно от .pem до .cer так, чтобы можно было импортировать его к хранилищу сертификата Windows.

Внутреннее содержание .cer и файлов .pem обычно похоже на эти выходные данные:

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

.pfx? Это расширение обозначает Exchange Личных данных. Этот формат является методом, который можно использовать для связывания сертификатов в отдельный файл. Например, можно связать Серверный сертификат и его связанный секретный ключ и Корневой сертификат CA в один файл и легко импортировать файл в соответствующее хранилище сертификата Windows. Это обычно используется для Сервера и Сертификатов клиента. К сожалению, если Корневой сертификат CA включен, Корневой сертификат CA всегда устанавливается в хранилище Текущего пользователя вместо хранилища Локального компьютера, даже если хранилище Локального компьютера задано для установки.

.p12? Этот формат обычно только замечен с Сертификатом клиента. Можно импортировать этот формат в хранилище сертификата Windows.

.p7b? Это - другой формат, который хранит несколька серверов сертификатов в одном файле. Можно импортировать этот формат в хранилище сертификата Windows.

Приложение B - преобразование формата сертификата

В большинстве случаев преобразование сертификата происходит при изменении

расширения (например, от .pem до .cer), так как сертификаты обычно находятся в открытом текстовом формате. Иногда, сертификат не находится в формате простого текста, и необходимо преобразовать его с использованием программного средства, такого как OpenSSL. Например, Прикладное устройство управления услугами Solution Engine ACS не может установить сертификаты в формате .pfx. Поэтому необходимо преобразовать сертификат и секретный ключ в применимый формат. Это - синтаксис основной команды для OpenSSL:

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

Вам предлагают для Пароля Импорта и Фраза - пропуск PEM. Эти пароли должны быть тем же и являются паролем с закрытым ключом, который задан, когда экспортируется .pfx. Выходные данные являются одиночным файлом .pem, который включает все сертификаты и секретные ключи в .pfx. Этот файл может быть упомянут в ACS и как сертификат и как файл закрытого ключа, и это устанавливает без проблем.

Приложение C - период Достоверности сертификата

Сертификат только применим во время своего периода достоверности. Когда узел CA установлен и может варьироваться, период достоверности для Корневого сертификата CA определен. Период достоверности для Промежуточного сертификата CA определен, когда CA установлен и не может превысить период достоверности узла CA, от которого это зависимо. Период достоверности для Сервера, Клиента и Сертификатов компьютера автоматически установлен в один год со службами Microsoft Certificate. Когда вы взламываете Реестр Windows согласно Статье базы знаний Microsoft 254632 и не можете превысить период достоверности узла CA, это может только быть изменено. Период достоверности подписанных сертификатов, которые генерирует ACS, всегда является одним годом и не может быть изменен в текущих версиях.

Дополнительные сведения

- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems