Guida ai certificati EAP versione 1.01

Sommario

Introduzione

Questo documento chiarisce alcune delle incertezze che accompagnano i vari tipi di certificati, formati e requisiti associati alle varie forme di EAP (Extensible Authentication Protocol). I cinque tipi di certificato relativi a EAP discussi in questo documento sono Server, CA radice, CA intermedia, Client e Computer. Questi certificati sono disponibili in vari formati e possono presentare requisiti diversi in relazione a ciascuno di essi, in base all'implementazione EAP interessata.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Certificati server

Il certificato server viene installato sul server RADIUS e il suo scopo principale in EAP è creare il tunnel TLS (Transport Layer Security) crittografato che protegge le informazioni di autenticazione. Quando si utilizza EAP-MSCHAPv2, il certificato server assume un ruolo secondario, ovvero identificare il server RADIUS come entità attendibile per l'autenticazione. Questo ruolo secondario viene eseguito tramite l'utilizzo del campo Utilizzo chiavi avanzato. Il campo EKU identifica il certificato come certificato server valido e verifica che la CA radice che ha rilasciato il certificato sia una CA radice attendibile. È necessaria la presenza del certificato CA radice. Cisco Secure ACS richiede che il certificato sia in formato binario con codifica Base64 o DER X.509 v3.

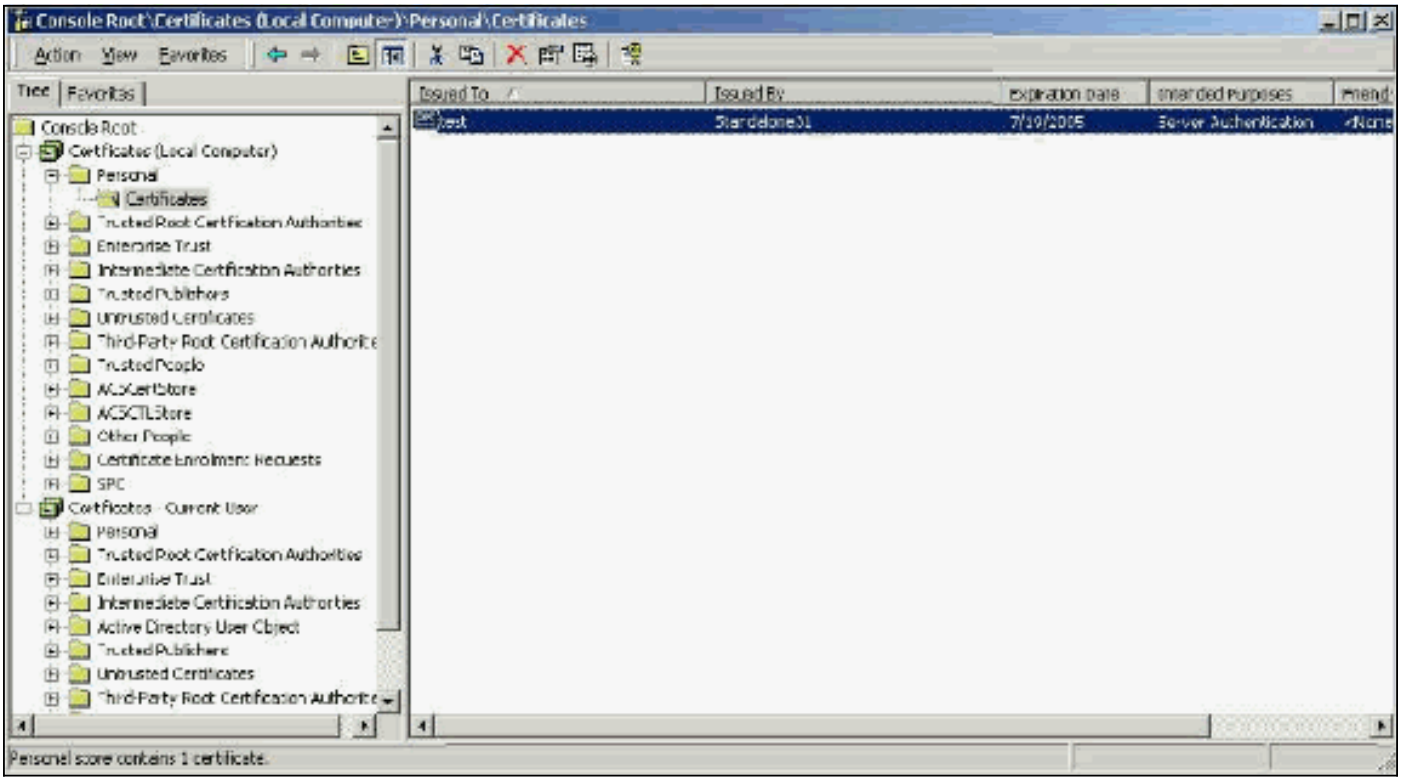
Èpossibile creare questo certificato utilizzando una richiesta di firma del certificato (CSR) in ACS, che viene inviata a una CA. In alternativa, è possibile tagliare il certificato utilizzando un modulo di creazione di certificati CA interno, ad esempio Servizi certificati Microsoft. È importante notare che, sebbene sia possibile creare il certificato server con chiavi di dimensioni superiori a 1024, le chiavi di dimensioni superiori a 1024 non funzionano con PEAP. Il client si blocca anche se l'autenticazione passa.

Se il certificato viene creato utilizzando un CSR, verrà creato in formato cer, pem o txt. In rare occasioni, viene creato senza estensione. Verificare che il certificato sia un file di testo normale con un'estensione che sia possibile modificare in base alle esigenze (l'accessorio ACS utilizza l'estensione cer o pem). Inoltre, se si utilizza un CSR, la chiave privata del certificato viene creata nel percorso specificato come file separato che può avere o meno un'estensione e a cui è associata una password (la password è necessaria per l'installazione su ACS). Indipendentemente dall'estensione, verificare che si tratti di un file di testo normale con un'estensione che può essere modificata in base alle esigenze (l'accessorio ACS utilizza l'estensione .pvk o .pem). Se non viene specificato alcun percorso per la chiave privata, ACS salva la chiave nella directory C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs e cerca in questa directory se non viene specificato alcun percorso per il file della chiave privata quando si installa il certificato.

Se il certificato viene creato utilizzando il modulo di invio certificati di Servizi certificati Microsoft, assicurarsi di contrassegnare le chiavi come esportabili in modo da poter installare il certificato in ACS. La creazione di un certificato in questo modo semplifica notevolmente il processo di installazione. È possibile installarlo direttamente nell'archivio Windows appropriato dall'interfaccia Web di Servizi certificati e quindi installarlo in ACS dall'archivio utilizzando la CN come riferimento. Un certificato installato nell'archivio del computer locale può inoltre essere esportato dall'archivio di Windows e installato in un altro computer con facilità. Quando si esporta questo tipo di

certificato, è necessario contrassegnare le chiavi come esportabili e specificare una password. Il certificato verrà quindi visualizzato in formato PFX che include la chiave privata e il certificato del server.

Se installato correttamente nell'archivio certificati di Windows, il certificato del server deve essere visualizzato nella cartella **Certificati (computer locale) > Personali > Certificati** come illustrato in questa finestra di esempio.



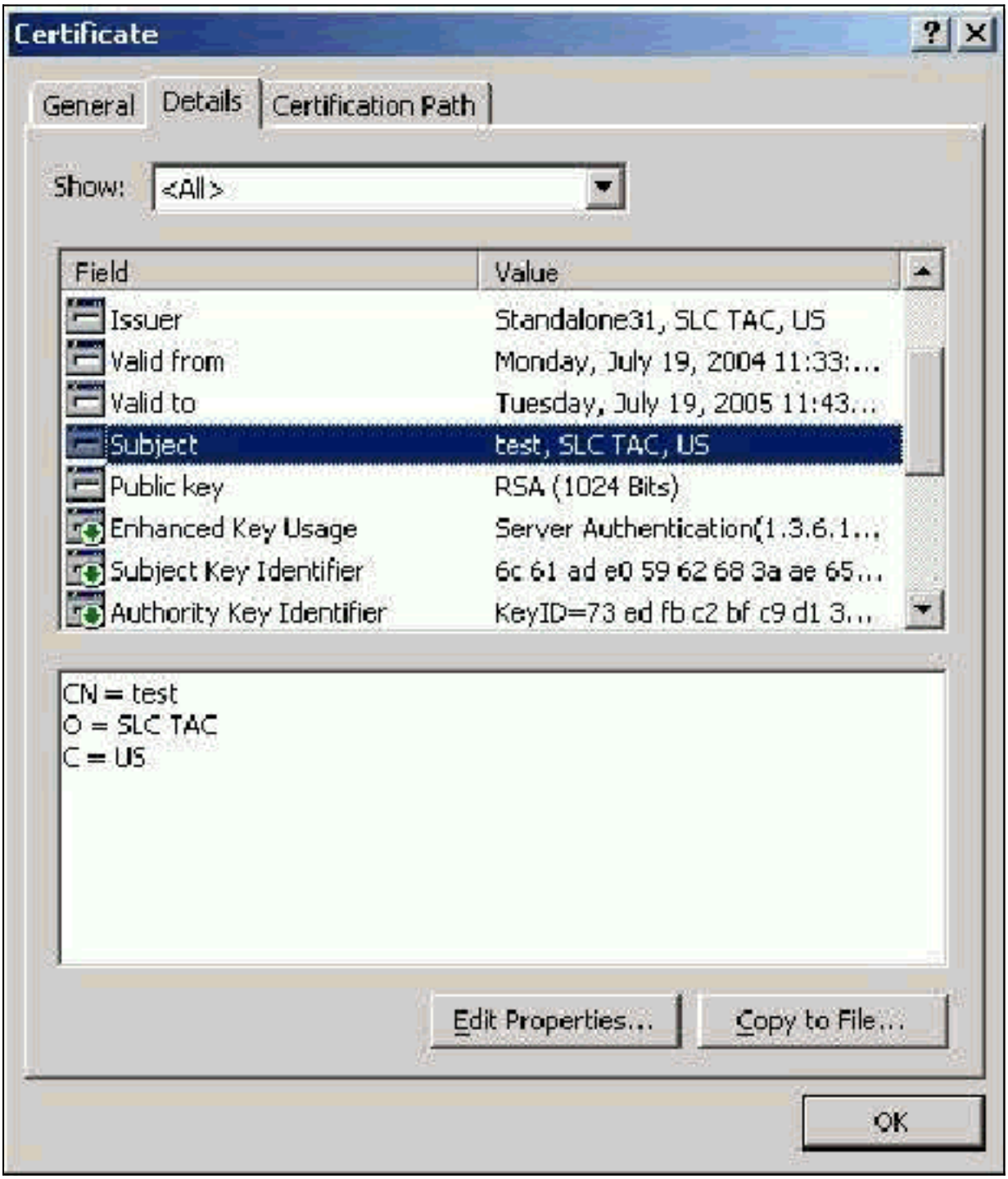
I certificati autofirmati sono certificati creati senza una radice o il coinvolgimento intermedio della CA. Hanno lo stesso valore sia nel campo dell'oggetto che in quello dell'autorità emittente, come un certificato CA radice. La maggior parte dei certificati autofirmati utilizza il formato X.509 v1. Pertanto, non funzionano con ACS. Tuttavia, a partire dalla versione 3.3, ACS può creare certificati autofirmati che possono essere utilizzati per EAP-TLS e PEAP. Non utilizzare una dimensione della chiave maggiore di 1024 per la compatibilità con PEAP e EAP-TLS. Se si utilizza un certificato autofirmato, il certificato funziona anche come certificato CA radice e deve essere installato nella cartella **Certificati (computer locale) > Autorità di certificazione radice attendibili > Certificati** del client quando si utilizza il supplicant Microsoft EAP. Viene installata automaticamente nell'archivio dei certificati radice attendibili nel server. Tuttavia, deve essere ancora considerato attendibile nell'elenco dei certificati attendibili in Installazione certificati ACS. Per ulteriori informazioni, vedere la sezione Certificati CA radice.

Poiché i certificati autofirmati vengono utilizzati come certificato CA radice per la convalida dei certificati server quando si utilizza il supplicant Microsoft EAP e poiché il periodo di validità non può essere aumentato rispetto all'anno predefinito, Cisco consiglia di utilizzarli solo per EAP come misura temporanea fino a quando non sarà possibile utilizzare una CA tradizionale.

Campo Oggetto

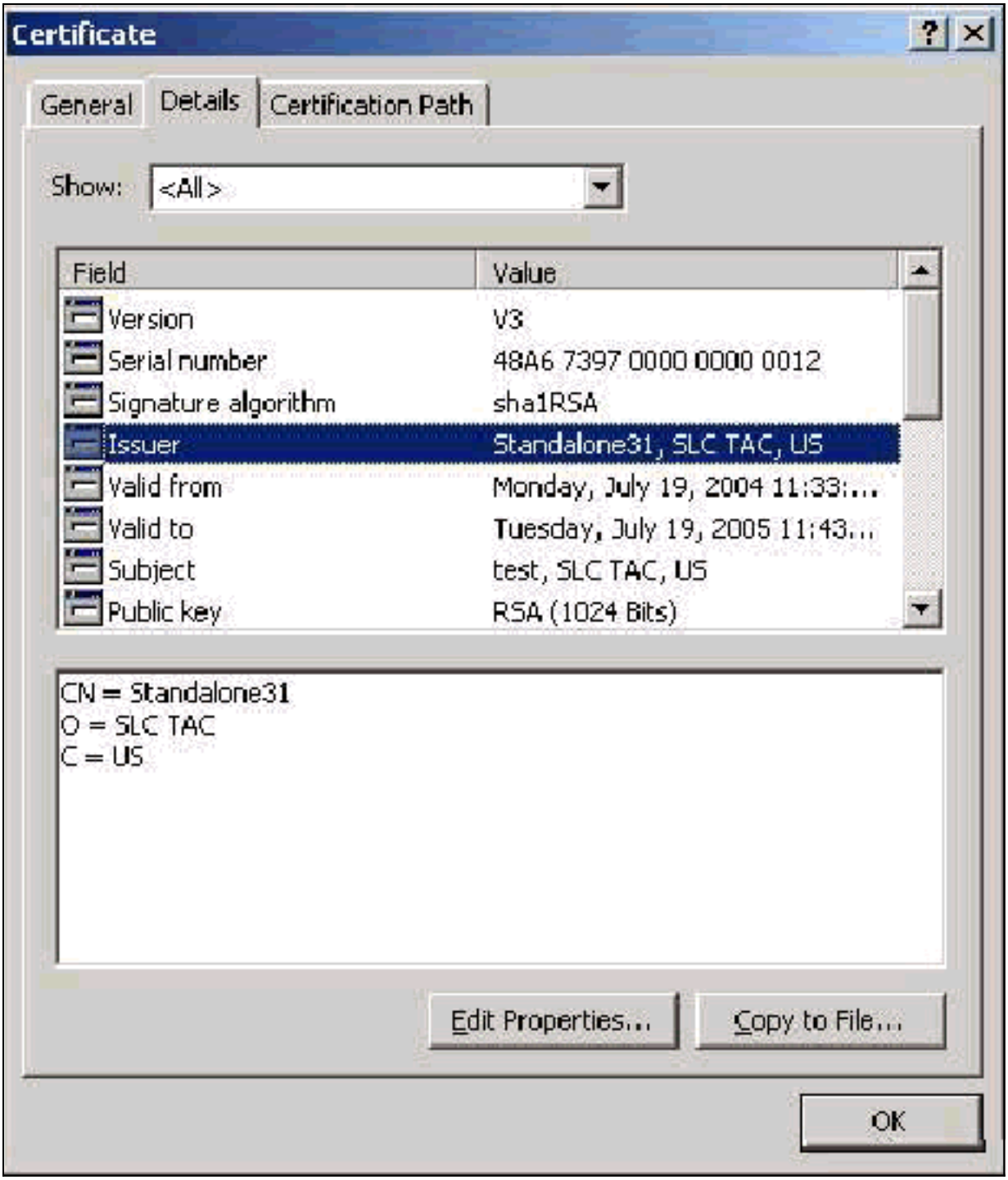
Il campo Oggetto identifica il certificato. Il valore CN viene utilizzato per determinare il campo Rilasciato a nella scheda Generale del certificato e viene popolato con le informazioni immesse nel campo Oggetto certificato della finestra di dialogo CSR di ACS o con le informazioni del campo Nome di Servizi certificati Microsoft. Il valore CN viene utilizzato per indicare ad ACS il

certificato che deve essere utilizzato dall'archivio certificati del computer locale se viene utilizzata l'opzione per installare il certificato dall'archivio.



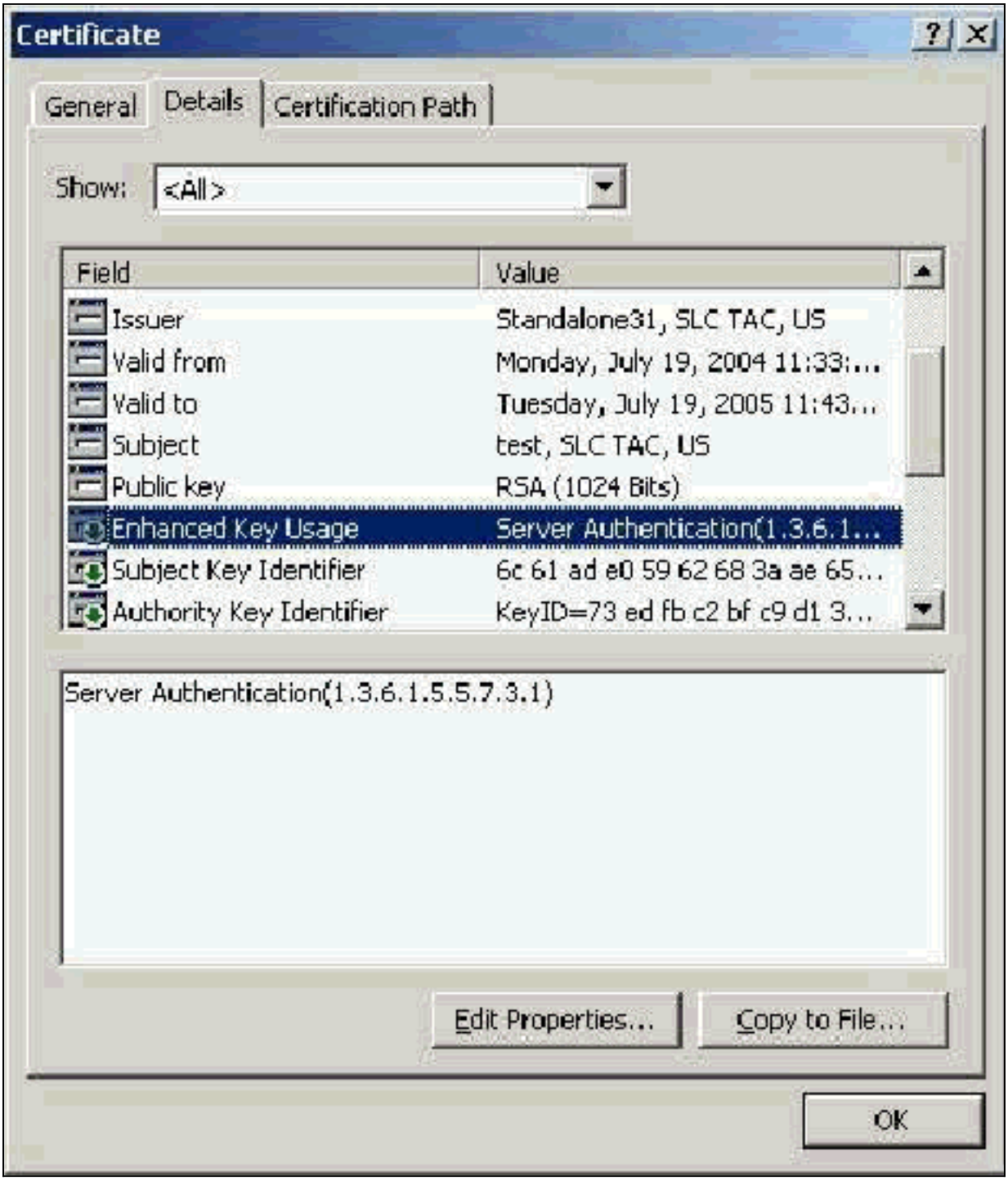
Campo Issuer

Il campo Issuer identifica la CA che ha tagliato il certificato. Utilizzare questo valore per determinare il valore del campo Rilasciato da nella scheda Generale del certificato. Viene popolato con il nome della CA.



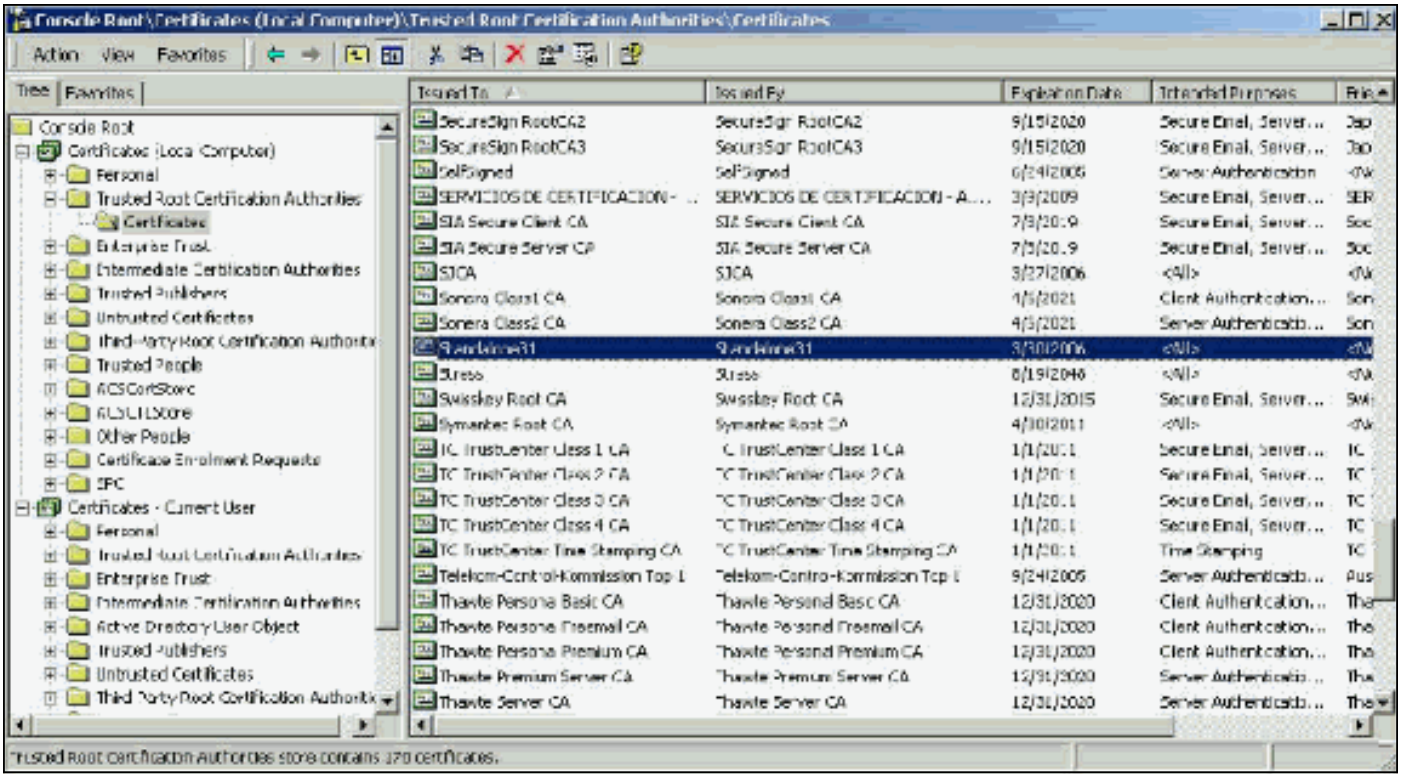
Campo Utilizzo chiavi avanzato

Il campo Utilizzo chiave avanzato identifica lo scopo previsto del certificato e deve essere elencato come "Autenticazione server". Questo campo è obbligatorio quando si utilizza il supplicant Microsoft per PEAP e EAP-TLS. Quando si utilizza Servizi certificati Microsoft, questo viene configurato nella CA autonoma (Standalone) con la selezione di **Certificato di autenticazione server** dall'elenco a discesa Scopo designato (Intended Purpose) e nella CA dell'organizzazione (Enterprise) con la selezione di **Server Web** dall'elenco a discesa Modello di certificato (Certificate Template). Se si richiede un certificato con l'utilizzo di un CSR con Servizi certificati Microsoft, non è possibile specificare lo scopo previsto con la CA autonoma (Standalone). Il campo EKU è quindi assente. Nella CA Enterprise è disponibile l'elenco a discesa Scopo designato. Alcune CA non creano certificati con un campo EKU, pertanto sono inutili quando si utilizza il supplicant Microsoft EAP.



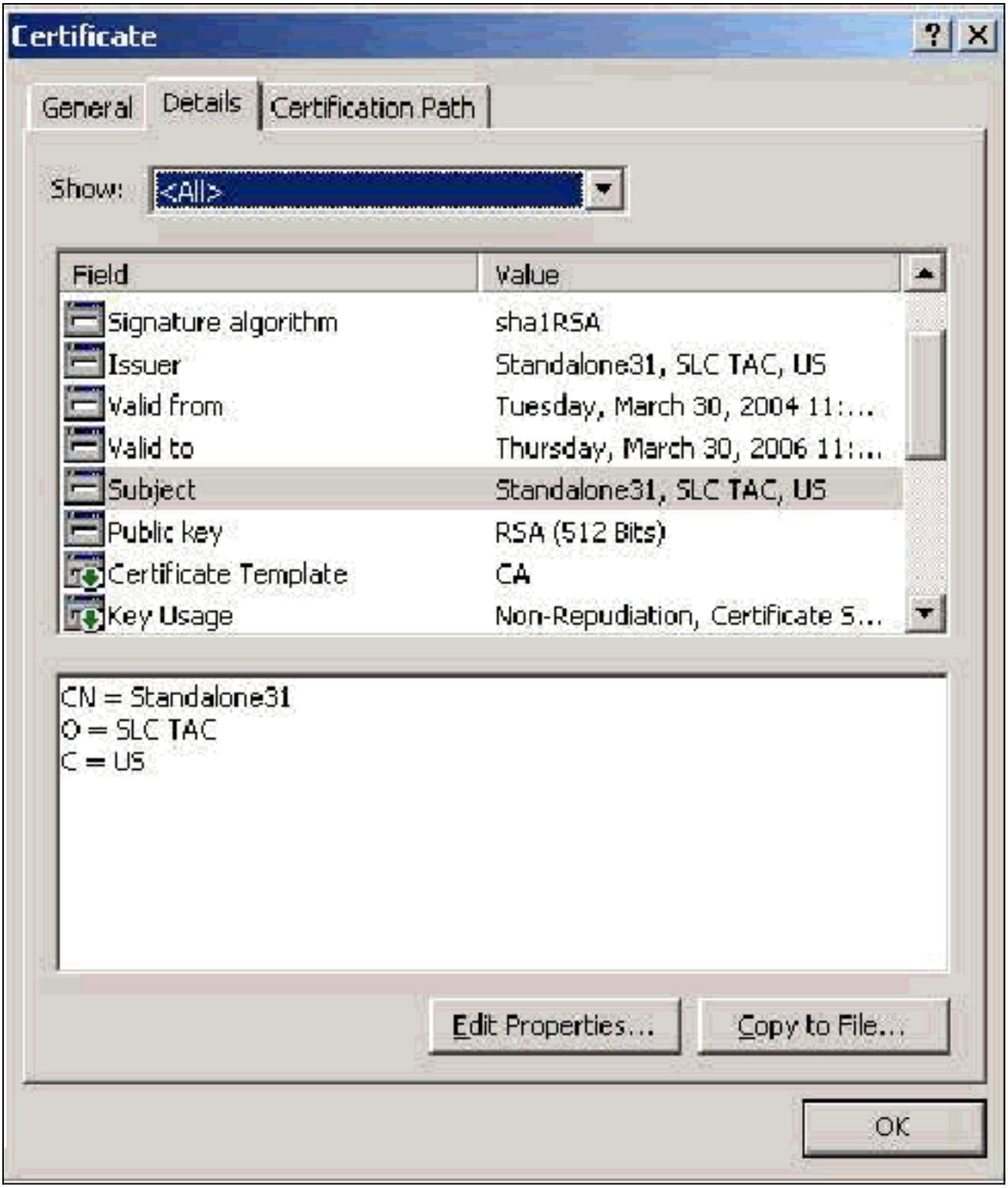
Certificati CA radice

Lo scopo del certificato CA radice è quello di identificare il certificato del server (e il certificato CA intermedio, se applicabile) come certificato attendibile per ACS e per il supplicant Windows EAP-MSCHAPv2. Deve trovarsi nell'archivio Autorità di certificazione radice attendibili in Windows sia sul server ACS che, nel caso di EAP-MSCHAPv2, sul computer client. La maggior parte dei certificati CA radice di terze parti viene installata con Windows e non è necessario eseguire alcuna operazione. Se si utilizza Servizi certificati Microsoft e il server dei certificati si trova nello stesso computer di ACS, il certificato CA radice viene installato automaticamente. Se il certificato CA radice non viene trovato nell'archivio Autorità di certificazione radice attendibili di Windows, è necessario acquisirlo dalla CA e installarlo. Se installato correttamente nell'archivio certificati di Windows, il certificato CA radice deve essere visualizzato nella cartella **Certificati (computer locale) > Autorità di certificazione radice attendibili >** Certificati come illustrato in questa finestra di esempio.



Campi Oggetto ed Emittente

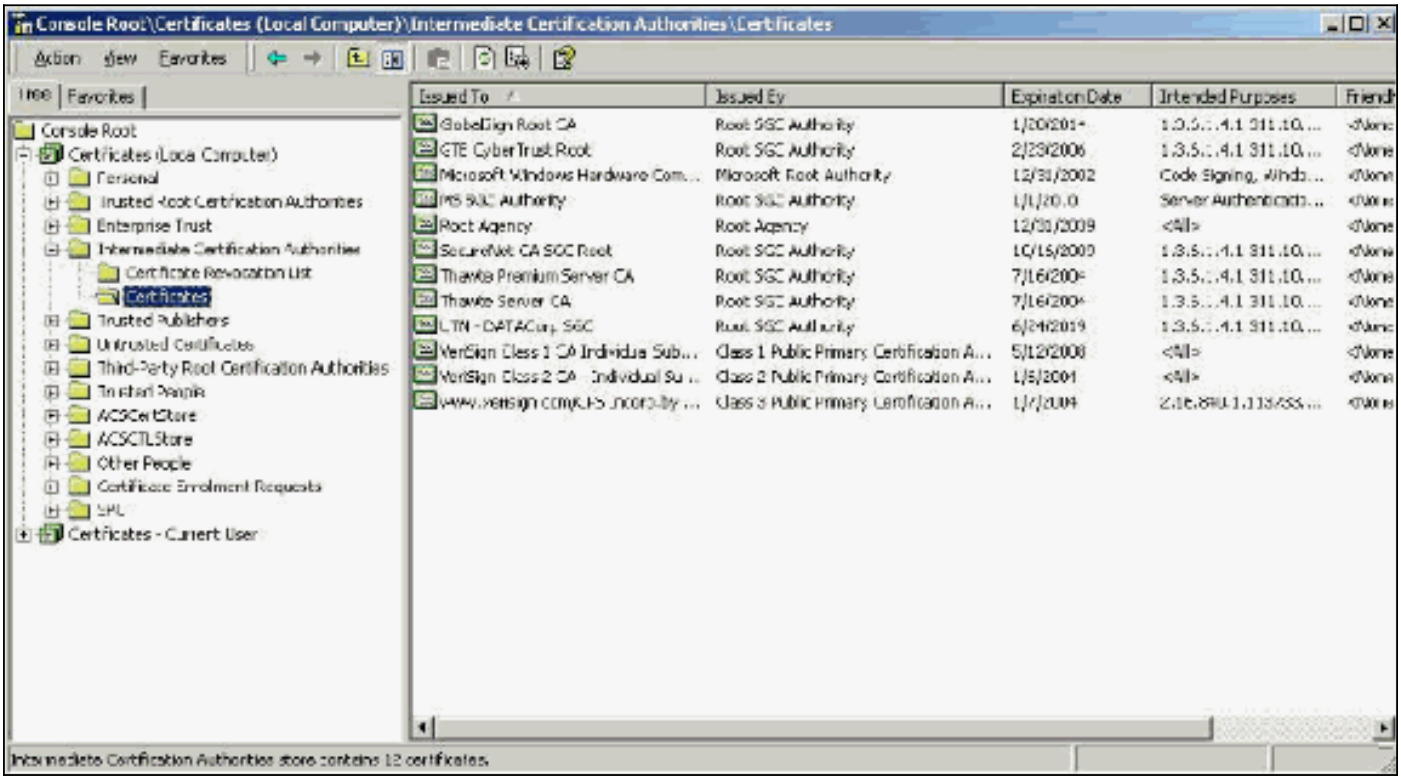
I campi Oggetto ed Emittente identificano la CA e devono essere esattamente gli stessi. Utilizzare questi campi per compilare i campi Rilasciato a e Rilasciato da nella scheda Generale del certificato. Vengono popolati con il nome della CA radice.



Certificati CA intermedi

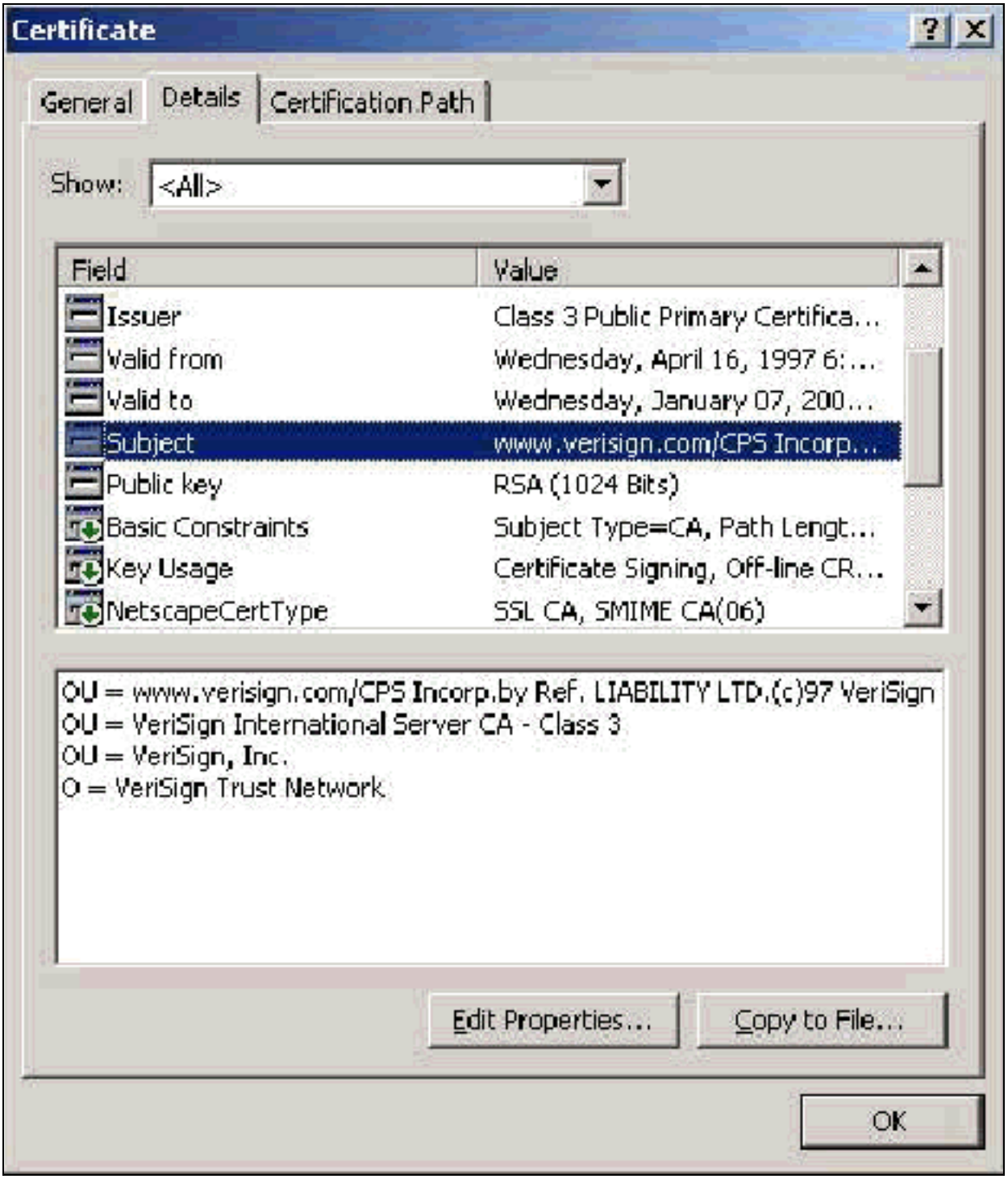
I certificati CA intermedi sono certificati utilizzati per identificare una CA subordinata a una CA radice. Alcuni certificati server (certificati wireless di Verisign) vengono creati con l'utilizzo di una CA intermedia. Se si utilizza un certificato server tagliato da una CA intermedia, il certificato CA intermedio deve essere installato nell'area Autorità di certificazione intermedie dell'archivio del computer locale sul server ACS. Inoltre, se sul client viene utilizzato il supplicant Microsoft EAP, anche il certificato CA radice della CA radice che ha creato il certificato CA intermedio deve trovarsi nell'archivio appropriato sul server e sul client ACS, in modo da poter stabilire la catena di attendibilità. Sia il certificato CA radice che il certificato CA intermedio devono essere contrassegnati come attendibili in ACS e nel client. La maggior parte dei certificati CA intermedi

non è installata con Windows, pertanto è molto probabile che sia necessario acquisirli dal fornitore. Se correttamente installato nell'archivio certificati di Windows, il certificato CA intermedio viene visualizzato nella cartella **Certificati (computer locale) > Autorità di certificazione intermedie >** Certificati come illustrato in questa finestra di esempio.



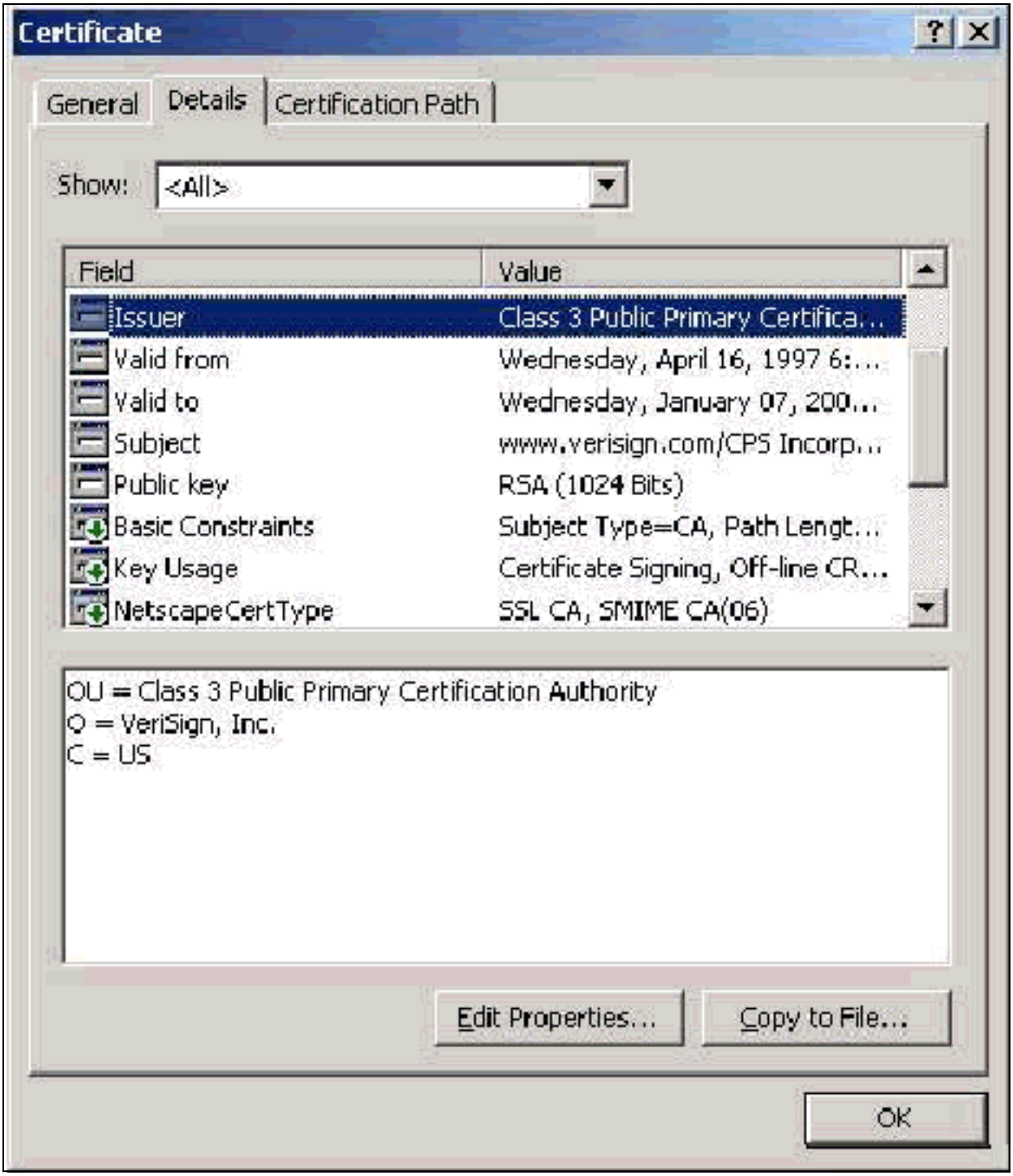
Campo Oggetto

Il campo Oggetto identifica la CA intermedia. Questo valore viene utilizzato per determinare il campo Rilasciato a nella scheda Generale del certificato.



Campo Issuer

Il campo Issuer identifica la CA che ha tagliato il certificato. Utilizzare questo valore per determinare il valore del campo Rilasciato da nella scheda Generale del certificato. Viene popolato con il nome della CA.



Certificati client

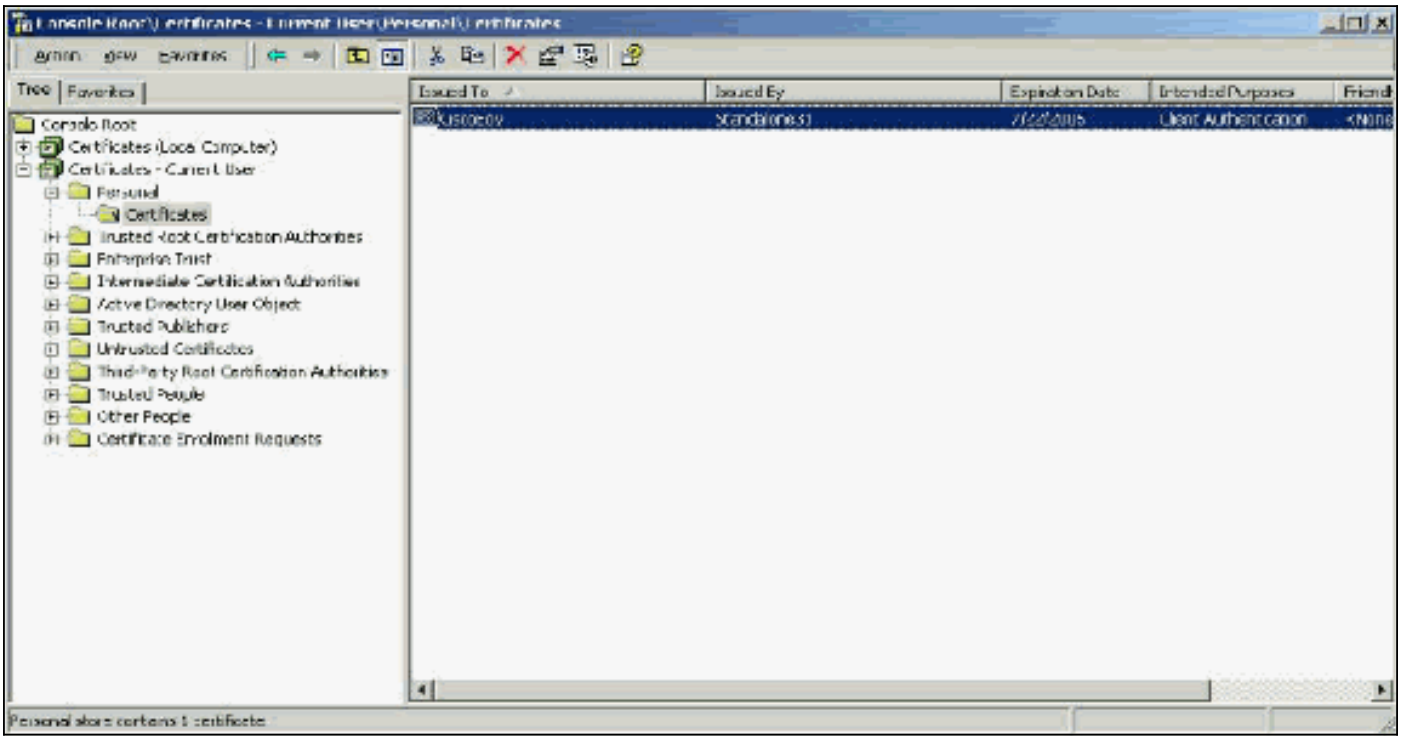
I certificati client vengono utilizzati per identificare l'utente in EAP-TLS. Non hanno alcun ruolo nella creazione del tunnel TLS e non sono utilizzate per la crittografia. L'identificazione positiva avviene in uno dei tre modi seguenti:

- **Confronto CN (o Nome)**: confronta il CN nel certificato con il nome utente nel database. Ulteriori informazioni su questo tipo di confronto sono incluse nella descrizione del campo Oggetto del certificato.
- **Confronto SAN**: confronta la SAN nel certificato con il nome utente nel database. Questa condizione è supportata solo a partire da ACS 3.2. Ulteriori informazioni su questo tipo di confronto sono incluse nella descrizione del campo Nome alternativo soggetto del certificato.
- **Confronto binario**: confronta il certificato con una copia binaria del certificato memorizzata nel

database (solo AD e LDAP possono eseguire questa operazione). Se si utilizza il confronto binario dei certificati, è necessario archiviare il certificato utente in formato binario. Inoltre, per LDAP generico e Active Directory, l'attributo che memorizza il certificato deve essere l'attributo LDAP standard denominato "usercertificate".

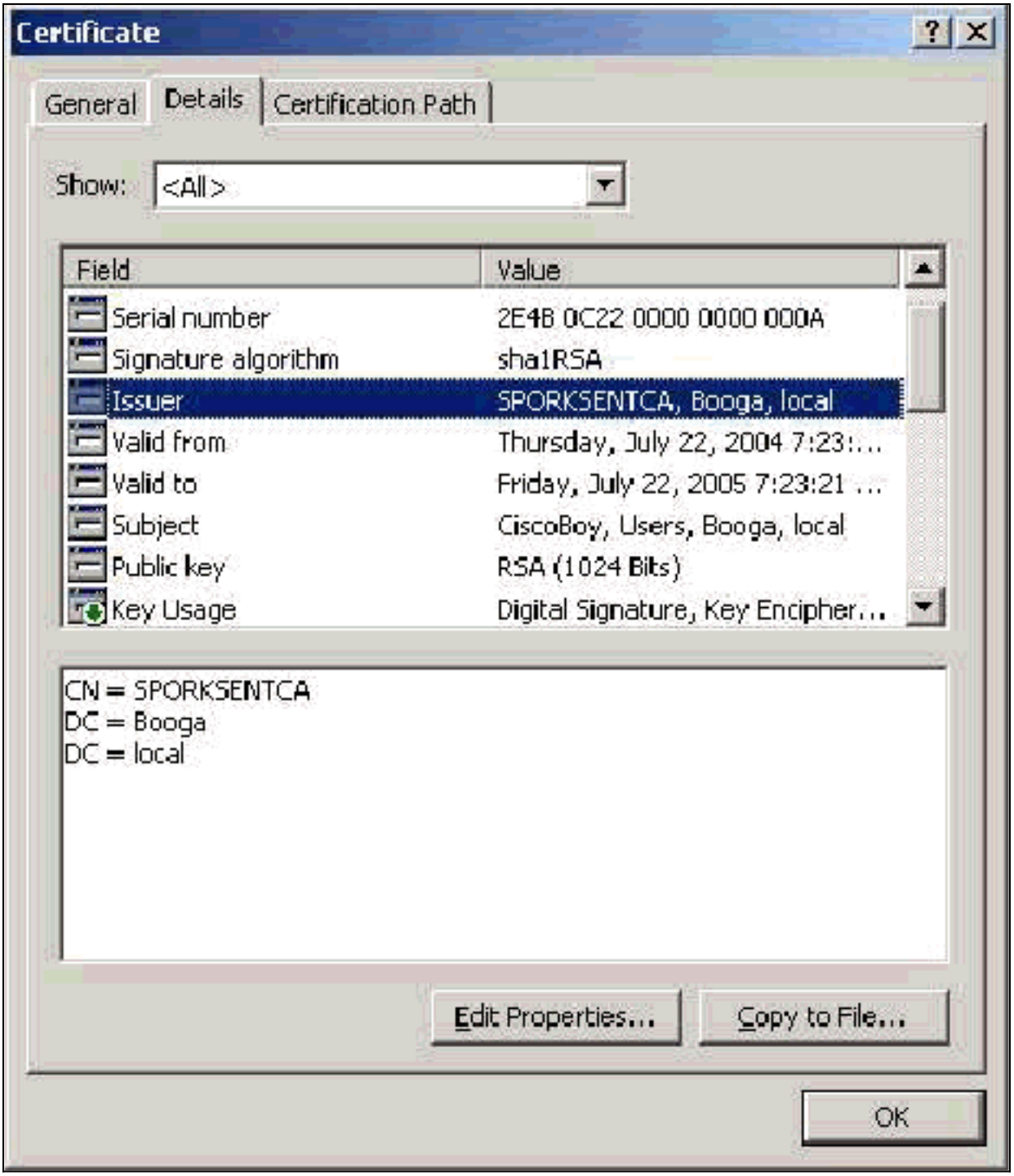
Indipendentemente dal metodo di confronto utilizzato, le informazioni nel campo appropriato (CN o SAN) devono corrispondere al nome utilizzato dal database per l'autenticazione. AD utilizza il nome NetBios per l'autenticazione in modalità mista e l'UPN in modalità nativa.

In questa sezione viene illustrata la generazione di certificati client tramite Servizi certificati Microsoft. EAP-TLS richiede un certificato client univoco per l'autenticazione di ogni utente. Il certificato deve essere installato in ogni computer per ogni utente. Se installato correttamente, il certificato si trova nella cartella **Certificati -Utente corrente > Personale > Certificati** come mostrato in questa finestra di esempio.



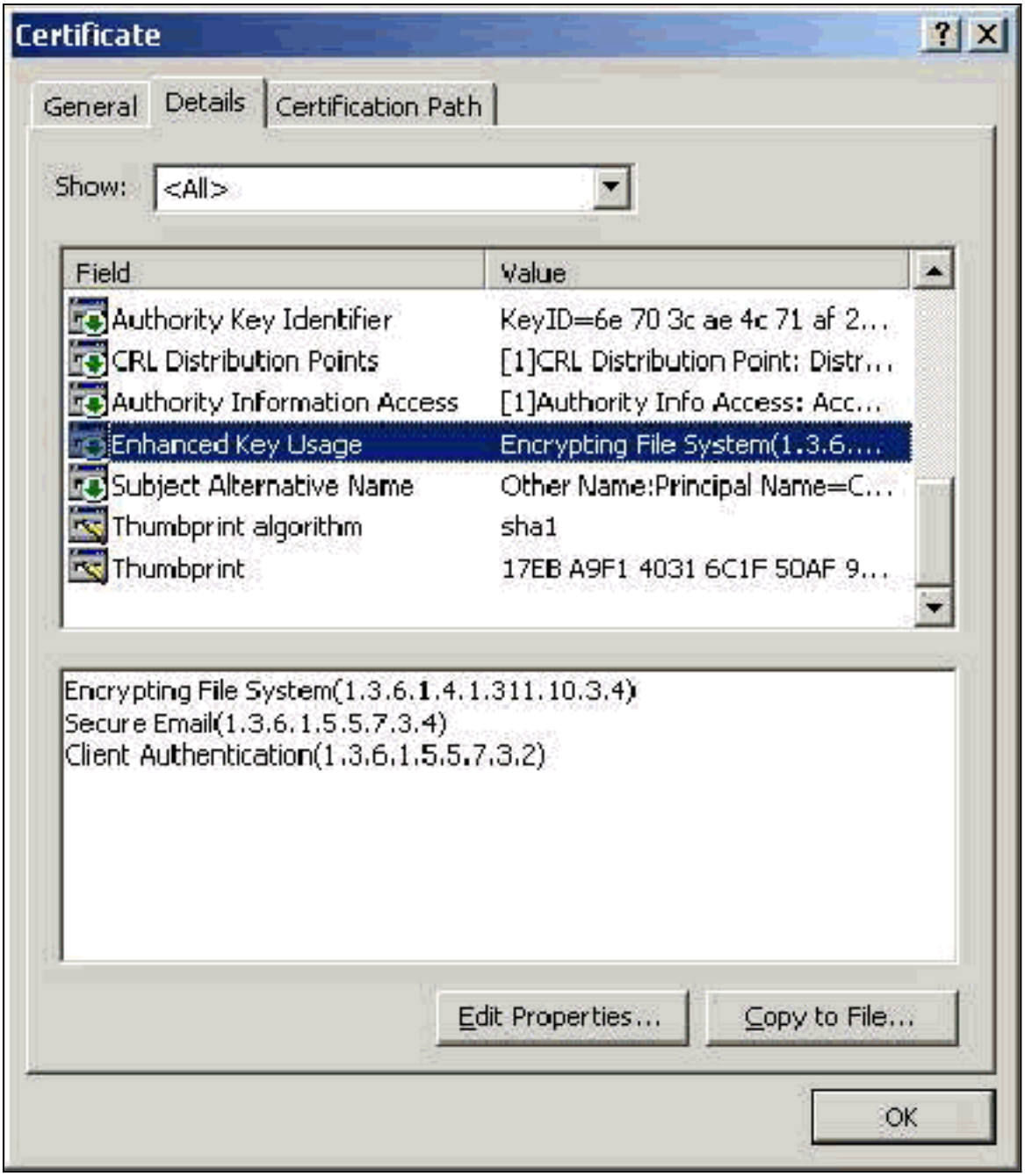
Campo Issuer

Il campo Issuer identifica la CA che taglia il certificato. Utilizzare questo valore per determinare il valore del campo Rilasciato da nella scheda Generale del certificato. Viene compilato con il nome della CA.



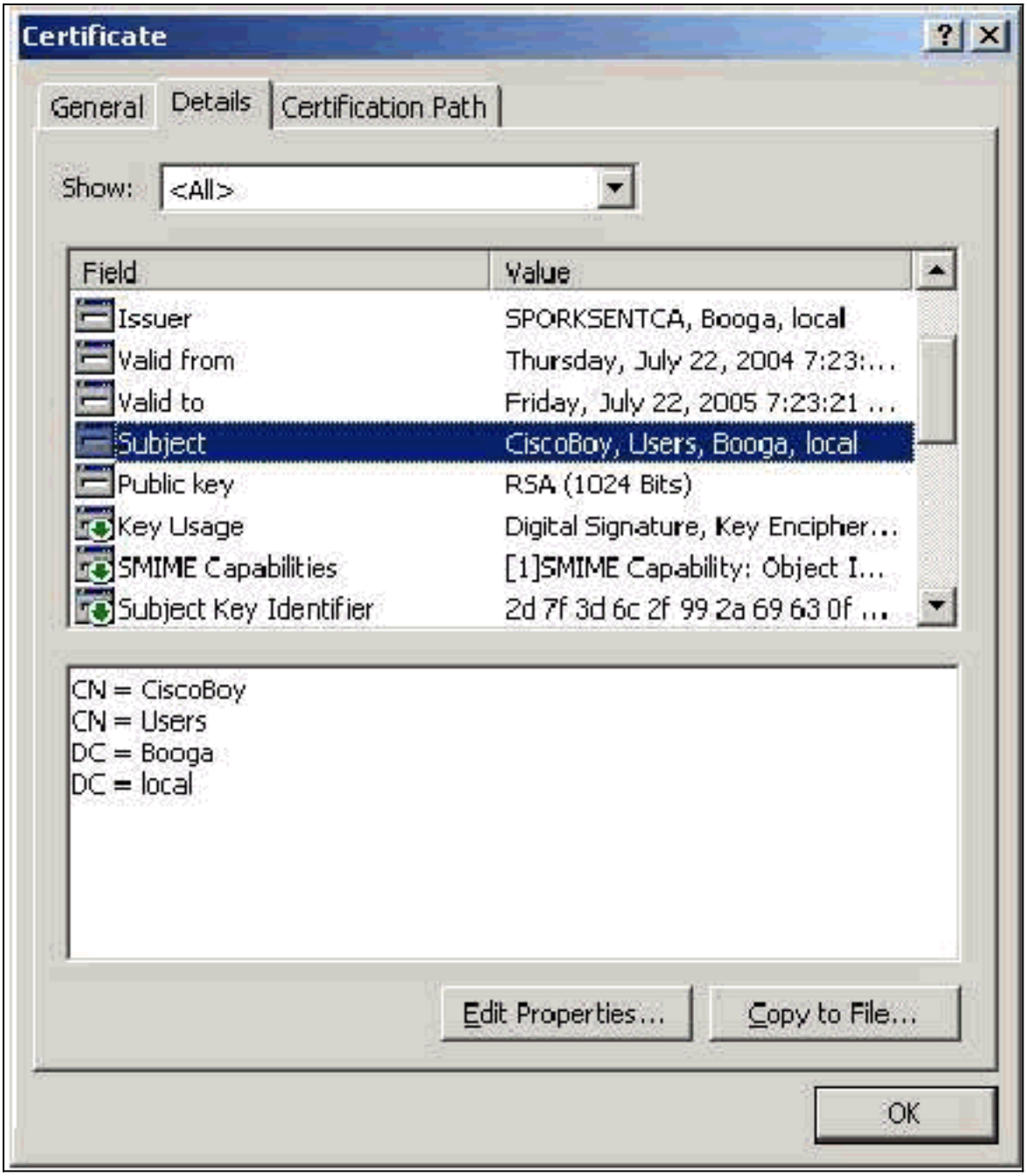
Campo Utilizzo chiavi avanzato

Il campo Utilizzo chiave avanzato identifica lo scopo previsto del certificato e deve contenere Autenticazione client. Questo campo è obbligatorio quando si utilizza il supplicant Microsoft per PEAP e EAP-TLS. Quando si utilizza Servizi certificati Microsoft, questa impostazione viene configurata nella CA autonoma (Standalone) quando si seleziona **Certificato di autenticazione client** dall'elenco a discesa Scopo designato e nella CA dell'organizzazione (Enterprise) quando si seleziona **Utente** dall'elenco a discesa Modello di certificato. Se si richiede un certificato con l'utilizzo di un CSR con Servizi certificati Microsoft, non è possibile specificare lo scopo previsto con la CA autonoma (Standalone). Il campo EKU è quindi assente. Nella CA Enterprise è disponibile l'elenco a discesa Scopo designato. Alcune CA non creano certificati con un campo EKU. Sono inutili quando si utilizza il supplicant Microsoft EAP.



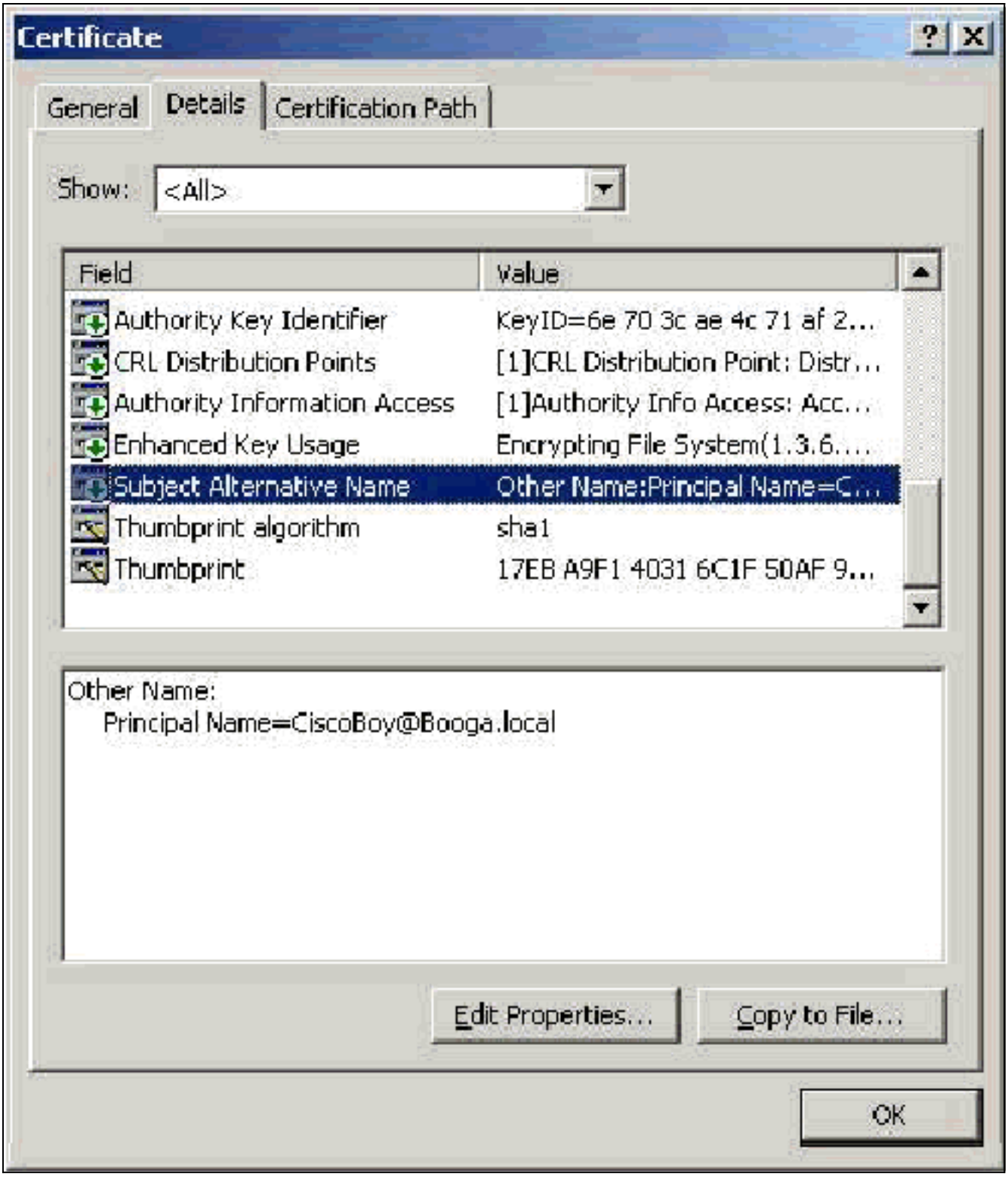
Campo Oggetto

Questo campo viene utilizzato nel confronto CN. Il primo CN elencato viene confrontato con il database per trovare una corrispondenza. Se viene trovata una corrispondenza, l'autenticazione ha esito positivo. Se si utilizza una CA autonoma (Standalone), la CN viene popolata con qualsiasi elemento inserito nel campo Nome del modulo di invio del certificato. Se si utilizza l'autorità di certificazione dell'organizzazione (enterprise), nella CN viene automaticamente inserito il nome dell'account elencato nella console Utenti e computer di Active Directory. Tale nome non corrisponde necessariamente al nome UPN o NetBios.



Campo Nome alternativo soggetto

Il campo Nome alternativo soggetto viene utilizzato nel confronto SAN. La SAN elencata viene confrontata con il database per trovare una corrispondenza. Se viene trovata una corrispondenza, l'autenticazione ha esito positivo. Se si utilizza la CA dell'organizzazione (Enterprise), nella SAN viene automaticamente inserito il nome di accesso ad Active Directory @domain (UPN). La CA autonoma (Standalone) non include un campo SAN, pertanto non è possibile utilizzare il confronto SAN.



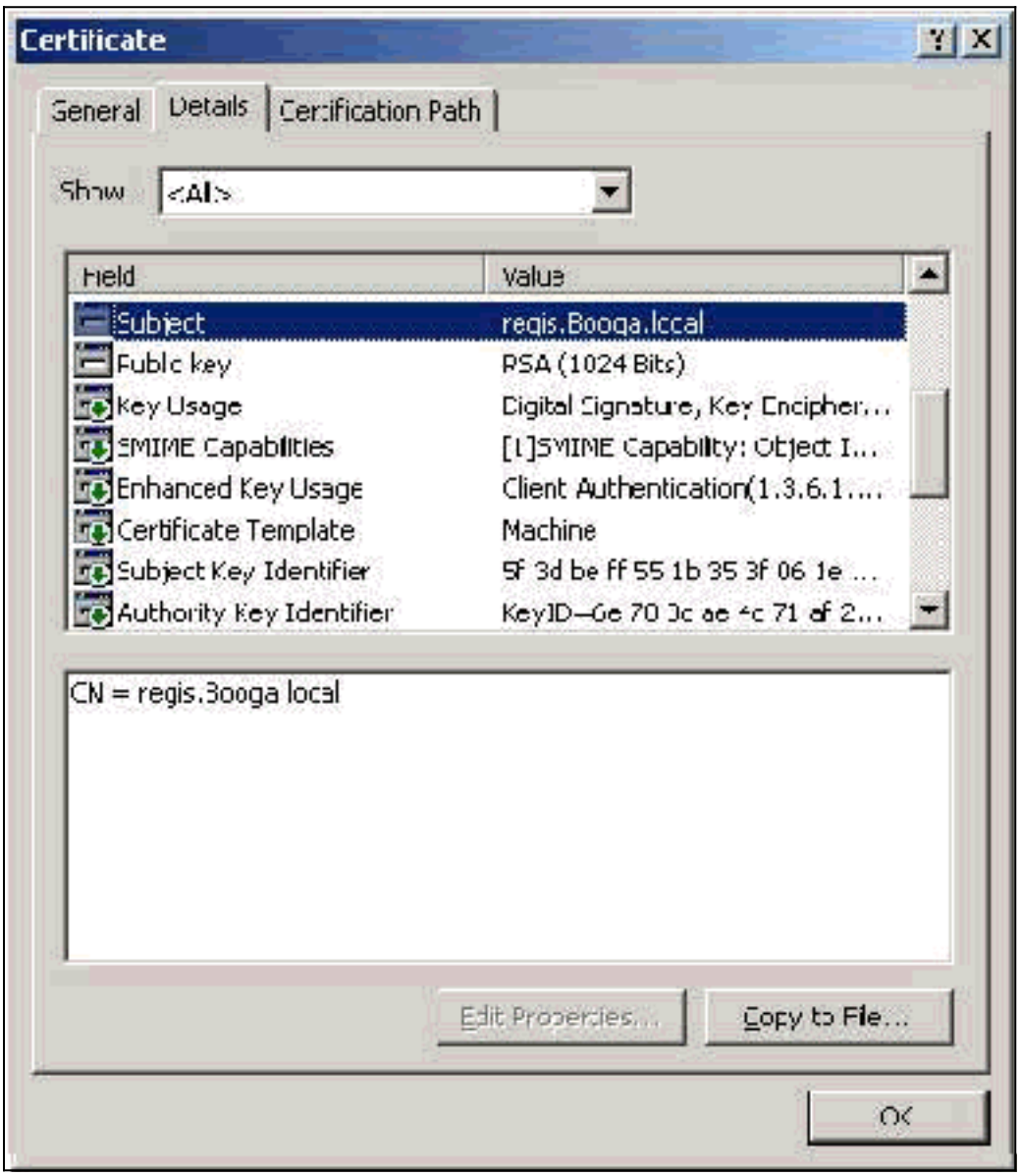
Certificati computer

I certificati del computer vengono utilizzati in EAP-TLS per identificare in modo positivo il computer quando si utilizza l'autenticazione del computer. È possibile accedere a questi certificati solo quando si configura la CA dell'organizzazione (enterprise) Microsoft per la registrazione automatica dei certificati e si aggiunge il computer al dominio. Il certificato viene creato automaticamente quando si utilizzano le credenziali di Active Directory del computer e le si installa nell'archivio del computer locale. I computer che sono già membri del dominio prima della configurazione della registrazione automatica ricevono un certificato al successivo riavvio di Windows. Il certificato del computer viene installato nella cartella **Certificati (computer locale) > Personali > Certificati** dello snap-in MMC Certificati (computer locale) come nei certificati del

server. Non è possibile installare questi certificati in altri computer poiché non è possibile esportare la chiave privata.

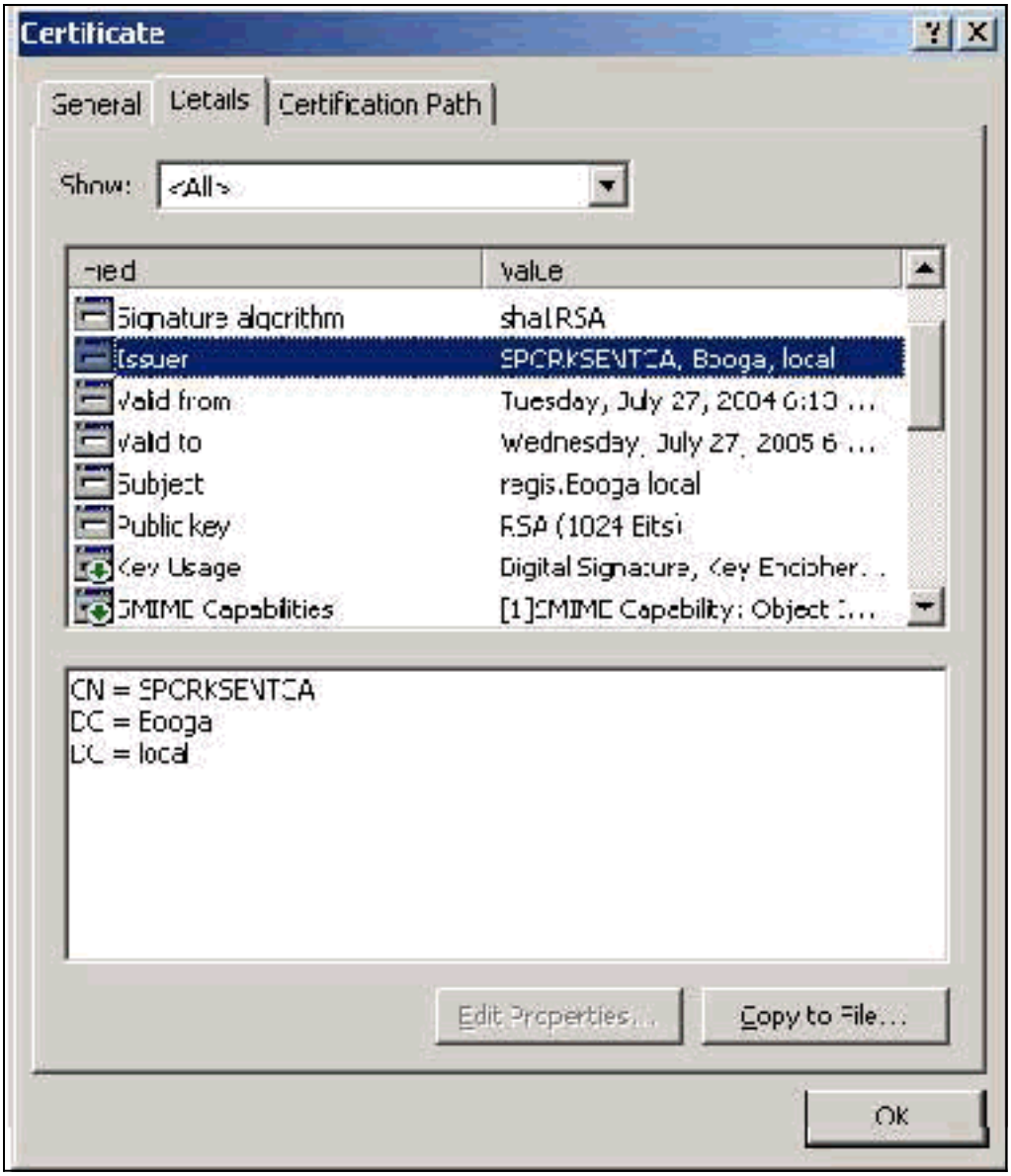
Campi soggetto e SAN

I campi Oggetto e SAN identificano il computer. Il valore è popolato dal nome completo del computer e viene utilizzato per determinare il campo Rilasciato a nella scheda Generale del certificato ed è lo stesso per entrambi i campi Soggetto e SAN.



Campo Issuer

Il campo Issuer identifica la CA che ha tagliato il certificato. Utilizzare questo valore per determinare il valore del campo Rilasciato da nella scheda Generale del certificato. Viene popolato con il nome della CA.



Appendice A - Estensioni comuni dei certificati

.csr: in realtà non si tratta di un certificato, ma di una richiesta di firma del certificato. Si tratta di un file di testo normale con il seguente formato:

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

.pvk - Questa estensione indica una chiave privata, ma non garantisce che il contenuto sia effettivamente una chiave privata. Il contenuto deve essere in testo normale con questo formato:

```
-----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 - Estensione generica che indica un certificato. I certificati del server, della CA radice e della CA intermedia possono essere in questo formato. Si tratta in genere di un file di testo normale con un'estensione che può essere modificata in base alle esigenze e può essere in formato DER o Base 64. È possibile importare questo formato nell'archivio certificati di Windows.

.pem: questa estensione indica Privacy Enhanced Mail. Questa estensione viene comunemente utilizzata con UNIX, Linux, BSD e così via. Viene in genere utilizzato per i certificati server e le chiavi private e in genere è un file di testo normale con un'estensione che è possibile modificare in base alle esigenze, da .pem a .cer, in modo da poterlo importare nell'archivio certificati di Windows.

Il contenuto interno dei file con estensione cer e pem ha in genere l'aspetto seguente:

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

.pfx: questa estensione è l'acronimo di Personal Information Exchange. Questo formato è un metodo che consente di raggruppare i certificati in un singolo file. È ad esempio possibile raggruppare in un unico file un certificato server e la chiave privata e il certificato CA radice associati e importare facilmente il file nell'archivio certificati di Windows appropriato. Viene in genere utilizzato per i certificati server e client. Sfortunatamente, se è incluso un certificato CA radice, il certificato CA radice viene sempre installato nell'archivio dell'utente corrente anziché in quello del computer locale, anche se per l'installazione è specificato l'archivio del computer locale.

.p12 - Questo formato viene in genere visualizzato solo con un certificato client. È possibile importare questo formato nell'archivio certificati di Windows.

.p7b - Si tratta di un altro formato che consente di memorizzare più certificati in un unico file. È possibile importare questo formato nell'archivio certificati di Windows.

Appendice B - Conversione del formato del certificato

Nella maggior parte dei casi, la conversione dei certificati viene eseguita quando si modifica l'estensione, ad esempio da .pem a .cer, poiché i certificati sono in genere in formato testo normale. A volte un certificato non è in formato testo normale ed è necessario convertirlo utilizzando uno strumento quale OpenSSL . Ad esempio, il motore della soluzione ACS non è in

grado di installare certificati in formato PFX. È pertanto necessario convertire il certificato e la chiave privata in un formato utilizzabile. Questa è la sintassi del comando di base per OpenSSL:

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

Vengono richieste la password di importazione e la passphrase PEM. Tali password devono essere identiche e corrispondono alla password della chiave privata specificata al momento dell'esportazione del file con estensione pfx. L'output è un singolo file con estensione pem che include tutti i certificati e le chiavi private nel file con estensione pfx. In ACS è possibile fare riferimento a questo file come certificato e file di chiave privata e l'installazione viene eseguita senza problemi.

Appendice C - Periodo di validità del certificato

Un certificato è utilizzabile solo durante il relativo periodo di validità. Il periodo di validità di un certificato CA radice viene determinato quando la CA radice viene stabilita e può variare. Il periodo di validità di un certificato CA intermedio viene determinato quando la CA viene stabilita e non può superare il periodo di validità della CA radice a cui è subordinata. Il periodo di validità per i certificati server, client e computer viene impostato automaticamente su un anno con Servizi certificati Microsoft. È possibile modificare questa impostazione solo se si esegue l'hack del Registro di sistema di Windows in base all'articolo 254632 della Microsoft Knowledge Base e non è possibile superare il periodo di validità della CA radice. Il periodo di validità dei certificati autofirmati generati da ACS è sempre un anno e non può essere modificato nelle versioni correnti.

Informazioni correlate

- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems