دليل شهادة EAP الإصدار 1.01

المحتويات

المقدمة

يوضح هذا المستند بعض التشويش الذي يصاحب مختلف أنواع الشهادات وتنسيقاتها ومتطلباتها المرتبطة بالأشكال المختلفة لبروتوكول المصادقة المتوسع (EAP). أنواع الشهادات الخمس المتعلقة ب EAP والتي يتناقش فيها هذا المستند هي الخادم والنسخة الأصلية والنسخة الوسيطة والعميل والجهاز. توجد هذه الشهادات في أشكال مختلفة ويمكن أن تكون هناك متطلبات مختلفة فيما يتعلق بكل منها استنادا إلى تنفيذ EAP المعني.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

شهادات الخادم

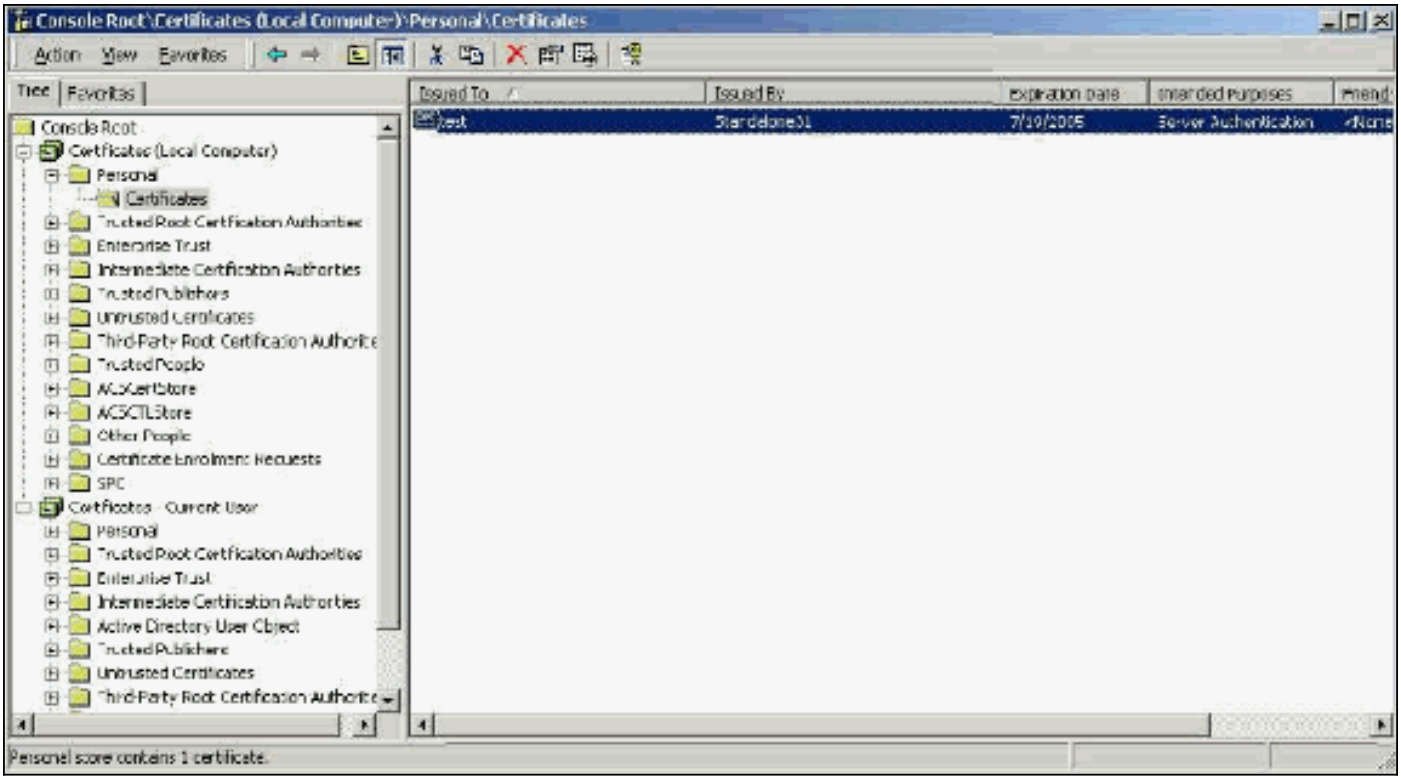
تثبت شهادة الخادم على خادم RADIUS والغرض الأساسي منها في EAP هو إنشاء نفق تأمين طبقة النقل المشفر (TLS) الذي يحمي معلومات المصادقة. عندما تستخدم EAP-MSCHAPv2، تأخذ شهادة الخادم دورا ثانويا وهو تعريف خادم RADIUS ككيان موثوق به للمصادقة. ويتم إنجاز هذا الدور الثانوي من خلال إستخدام حقل إستخدام المفتاح المحسن (EKU). يحدد حقل EKU الشهادة على أنها شهادة خادم صحيحة ويتحقق من أن المرجع المصدق الجذر الذي أصدر الشهادة هو مرجع مصدق مركزي موثوق به. وهذا يتطلب وجود شهادة المرجع المصدق الجذر. يتطلب ACS الآمن من Cisco أن تكون الشهادة إما بتنسيق X.509 v3 الثنائي المشفر أو Base64.

يمكنك إنشاء هذه الشهادة باستخدام طلب توقيع الشهادة (CSR) في ACS، والذي يتم إرساله إلى CA. أو، يمكنك أيضا قص الشهادة باستخدام نموذج إنشاء شهادة مرجع مصدق (مثل Microsoft Certificate Services) داخل الشركة. من المهم ملاحظة أنه في حين يمكنك إنشاء شهادة الخادم ذات أحجام المفاتيح الأكبر من 1024 فإن أي مفتاح أكبر من 1024 لا يعمل مع PEAP. يتم تعليق العميل حتى في حالة مرور المصادقة.

إذا قمت بإنشاء الترخيص باستخدام CSR، فإنه يتم إنشائه بتنسيق .pem، .cer، أو .txt. وفي حالات نادرة، ينشأ من دون أي تمديد. تأكد من أن ترخيصك ملف نص عادي بملحق يمكنك تغييره حسب الحاجة (يستخدم جهاز ACS ملحق .cer أو .pem). بالإضافة إلى ذلك، إذا كنت تستخدم CSR، فإن المفتاح الخاص للشهادة يتم إنشائه في المسار الذي تحدده كملف مستقل قد يحتوي أو لا يحتوي على ملحق والذي يحتوي على كلمة مرور مرتبطة به (كلمة المرور مطلوبة للتثبيت على ACS). بغض النظر عن الملحق، تأكد من أنه ملف نصي عادي بامتداد يمكنك تغييره حسب الحاجة (يستخدم جهاز ACS الامتداد .pvk أو .pem). في حالة عدم تحديد مسار للمفتاح الخاص، يقوم ACS بحفظ المفتاح في دليل Log\ CSAdmin\ CiscoSecure ACS vx.x\ Program Files\:C ويبحث في هذا الدليل في حالة عدم تحديد مسار لملف المفتاح الخاص عند تثبيت الشهادة.

إذا تم إنشاء الشهادة باستخدام النموذج الفرعي لشهادات Microsoft Certificate Services، تأكد من وضع علامة قابلة للتصدير على المفاتيح بحيث يمكنك تثبيت الشهادة في ACS. يؤدي إنشاء الشهادة بهذه الطريقة إلى تبسيط عملية التثبيت بشكل كبير. يمكنك تثبيته مباشرة في مخزن Windows المناسب من واجهة ويب "خدمات الشهادات" ثم تثبيته على ACS من التخزين باستخدام CN كمرجع. كما يمكن تصدير شهادة مثبتة في مخزن الكمبيوتر المحلي من وحدة تخزين Windows وتثبيتها على كمبيوتر آخر بسهولة. عندما يتم تصدير هذا النوع من الشهادات، يجب وضع علامة على المفاتيح كقابلة للتصدير وإعطائها كلمة مرور. تظهر الشهادة بعد ذلك بتنسيق .pfx الذي يتضمن المفتاح الخاص وشهادة الخادم.

عند تثبيته بشكل صحيح في مخزن تراخيص Windows، يجب أن تظهر شهادة الخادم في **مجلد الشهادات (الكمبيوتر المحلي) > شخصي > الشهادات** كما يظهر في نافذة المثال هذه.

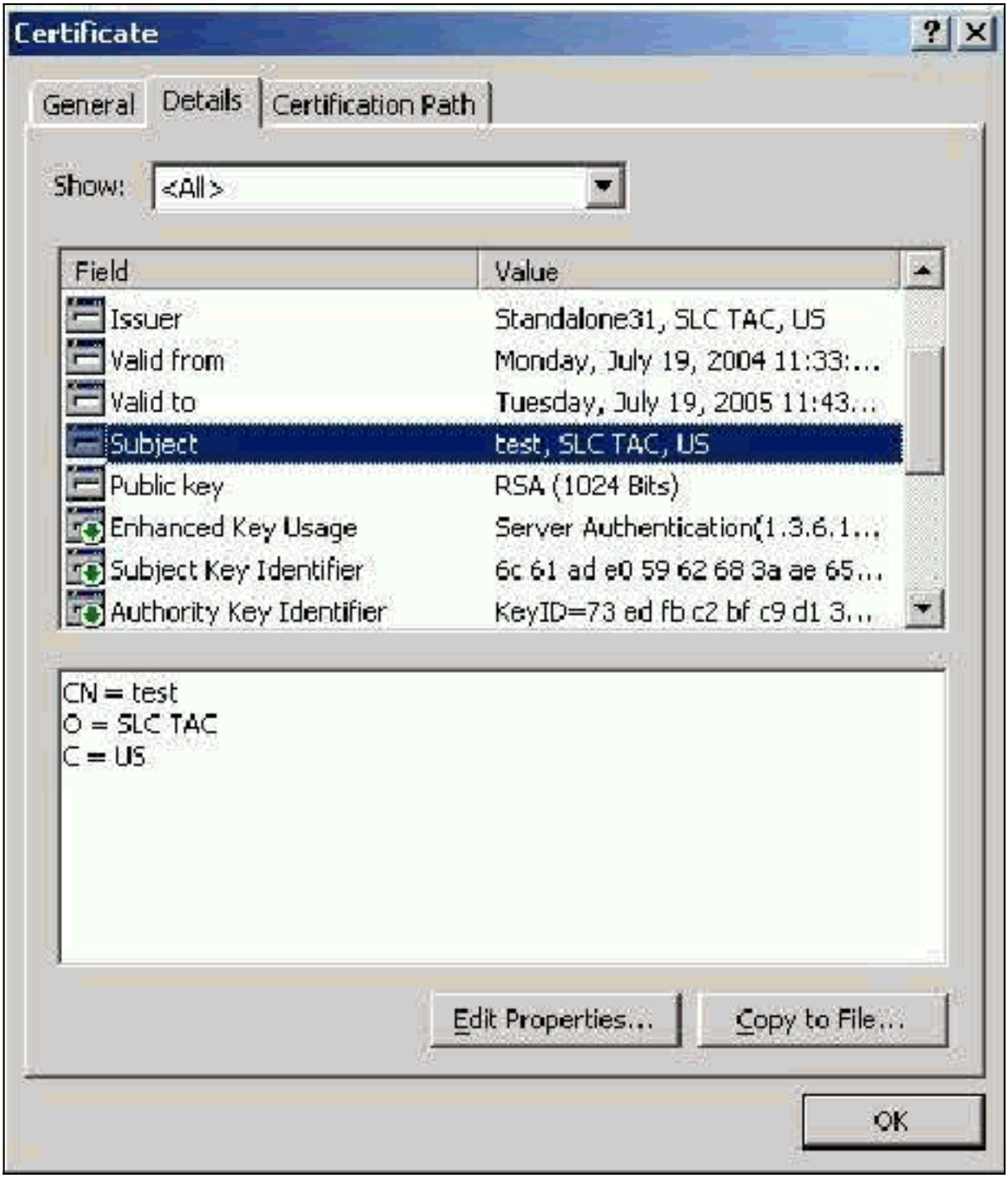


الشهادات الموقعة ذاتيا هي شهادات تقوم بإنشائها بدون جذر أو مشاركة وسيطة من المرجع المصدق. لهما نفس القيمة في كل من حقلي الموضوع والمصدر مثل شهادة مرجع مصدق جذري. تستخدم معظم الشهادات الموقعة ذاتيا تنسيق X.509 v1. لذلك، فهي لا تعمل مع ACS. ومع ذلك، فإنه بدءا من الإصدار 3.3، يكون ل ACS القدرة على إنشاء شهادته الموقعة ذاتيا والتي يمكنك إستخدامها مع EAP-TLS و PEAP. لا تستخدم حجم مفتاح أكبر من 1024 للتوافق مع PEAP و EAP-TLS. إذا كنت تستخدم شهادة موقعة ذاتيا، فإن الشهادة تعمل أيضا في سعة شهادة المرجع المصدق الجذر ويجب تثبيتها في **الشهادات (الكمبيوتر المحلي) > المراجع المصدقة الجذر الموثوق فيها >** مجلد **الشهادات** الخاص بالعميل عندما تستخدم طالب Microsoft EAP. يتم تثبيته تلقائيا في مخزن الشهادات الجذر الموثوق به على الخادم. ومع ذلك، يجب أن تظل هذه الثقة موثوق بها في "قائمة الشهادات الموثوق بها" في "إعداد شهادة ACS". راجع قسم شهادات المرجع المصدق الجذر للحصول على مزيد من المعلومات.

لأن الشهادات الموقعة ذاتيا يتم إستخدامها كشهادة مرجع مصدق جذري للتحقق من شهادة الخادم عندما تستخدم ملتمس Microsoft EAP، ولأن فترة الصلاحية لا يمكن زيادتها من الفترة الافتراضية من سنة واحدة، توصي Cisco باستخدام الشهادات ل EAP فقط كمقياس مؤقت حتى يمكنك إستخدام مرجع مصدق تقليدي.

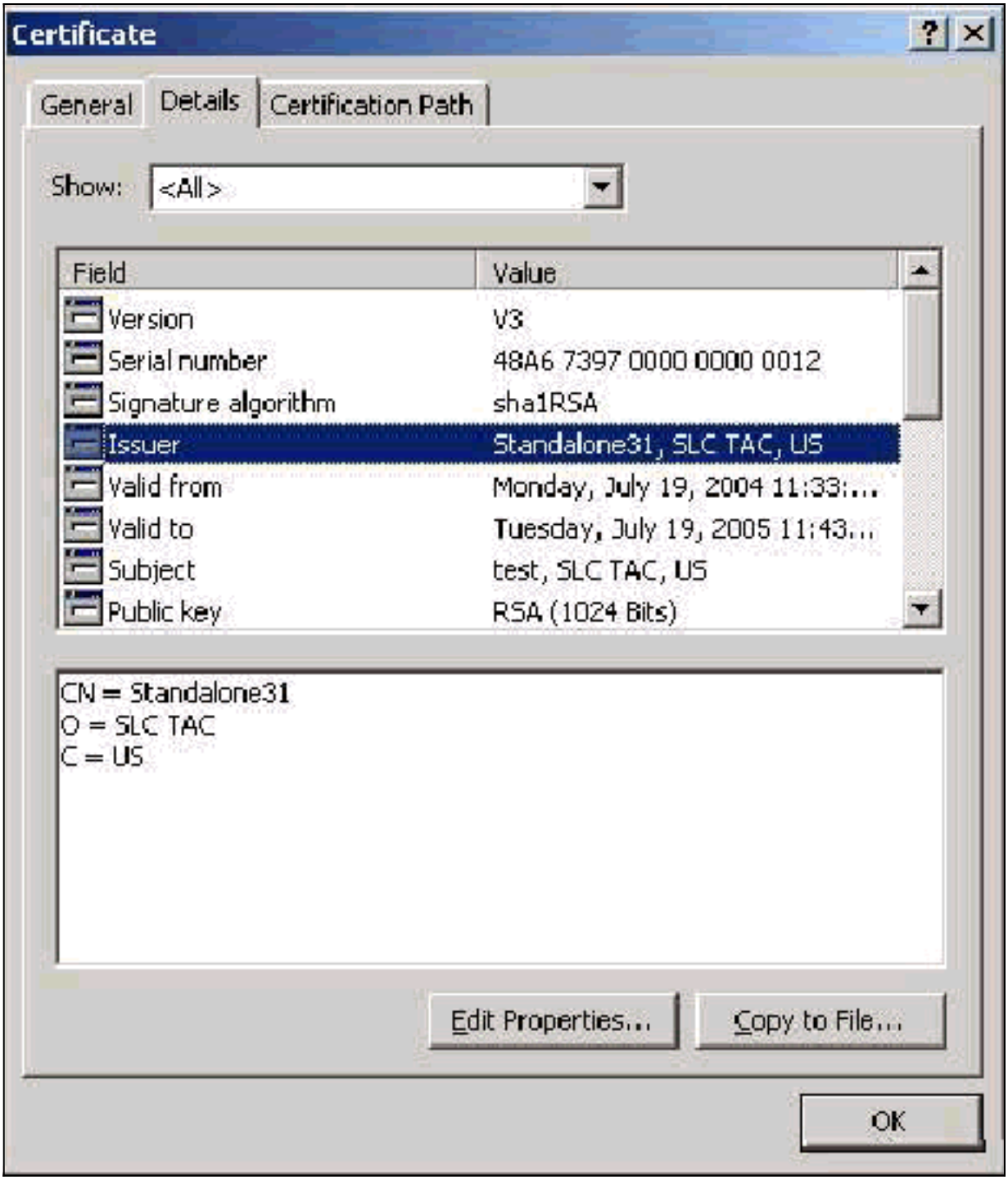
حقل الموضوع

يحدد حقل الموضوع الشهادة. يتم إستخدام قيمة CN لتحديد الحقل "تم إصداره إلى" في علامة التبويب "عام" الخاصة بالشهادة ويتم تعبئتها بالمعلومات التي تدخلها في حقل موضوع الشهادة في مربع حوار 'ACS 'CSR أو مع المعلومات الواردة من حقل "الاسم" في "خدمات شهادات Microsoft". يتم إستخدام قيمة CN لإخبار ACS بالشهادة التي تحتاج لاستخدامها من مخزن شهادات الجهاز المحلي إذا تم إستخدام خيار تثبيت الشهادة من التخزين.



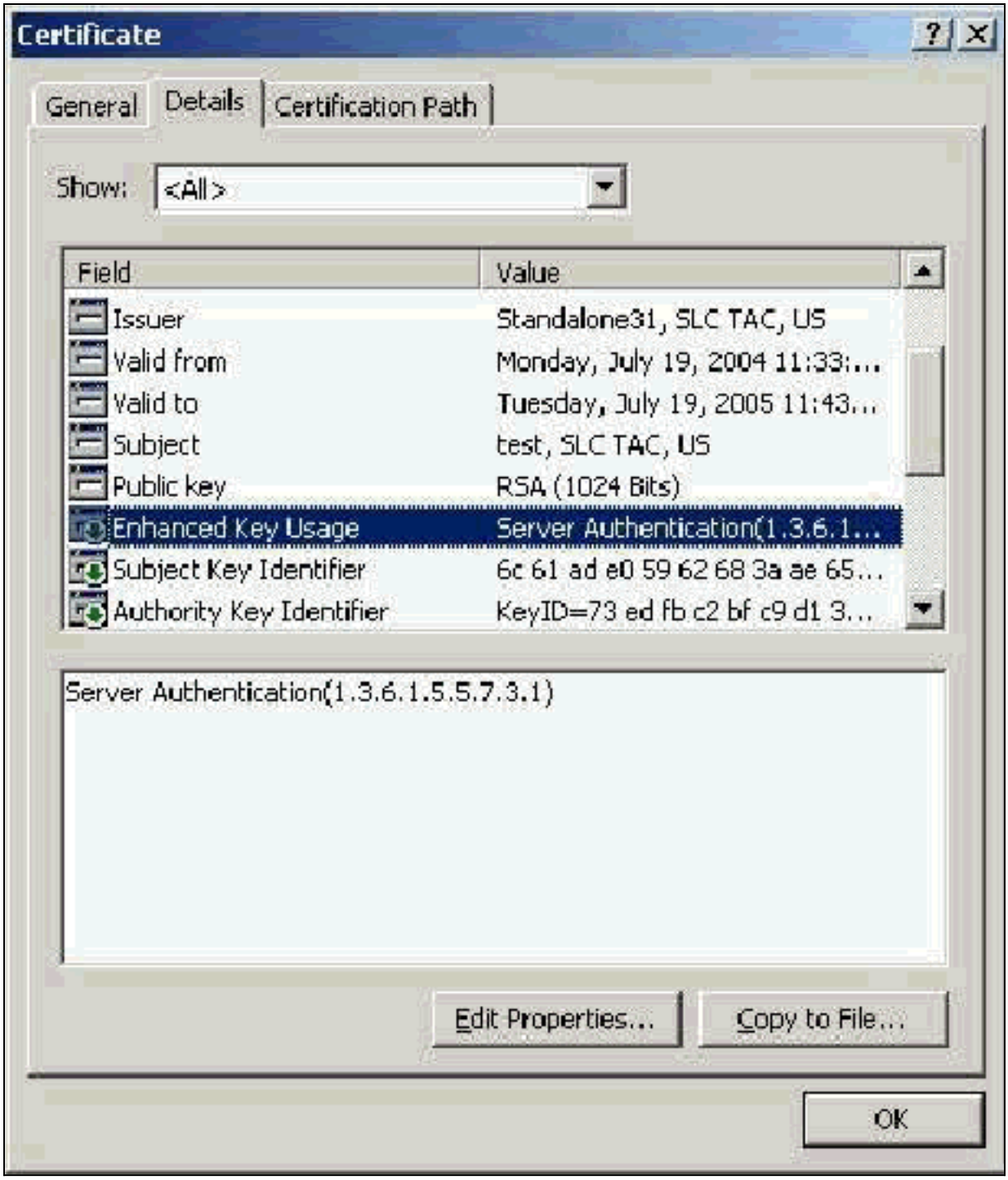
حقل المصدر

يحدد حقل المصدر المرجع المصدق الذي يقطع الشهادة. أستخدم هذه القيمة لتحديد قيمة الحقل الصادر حسب في علامة التبويب "عام" في الشهادة. إنه مملوء باسم المرجع المصدق.



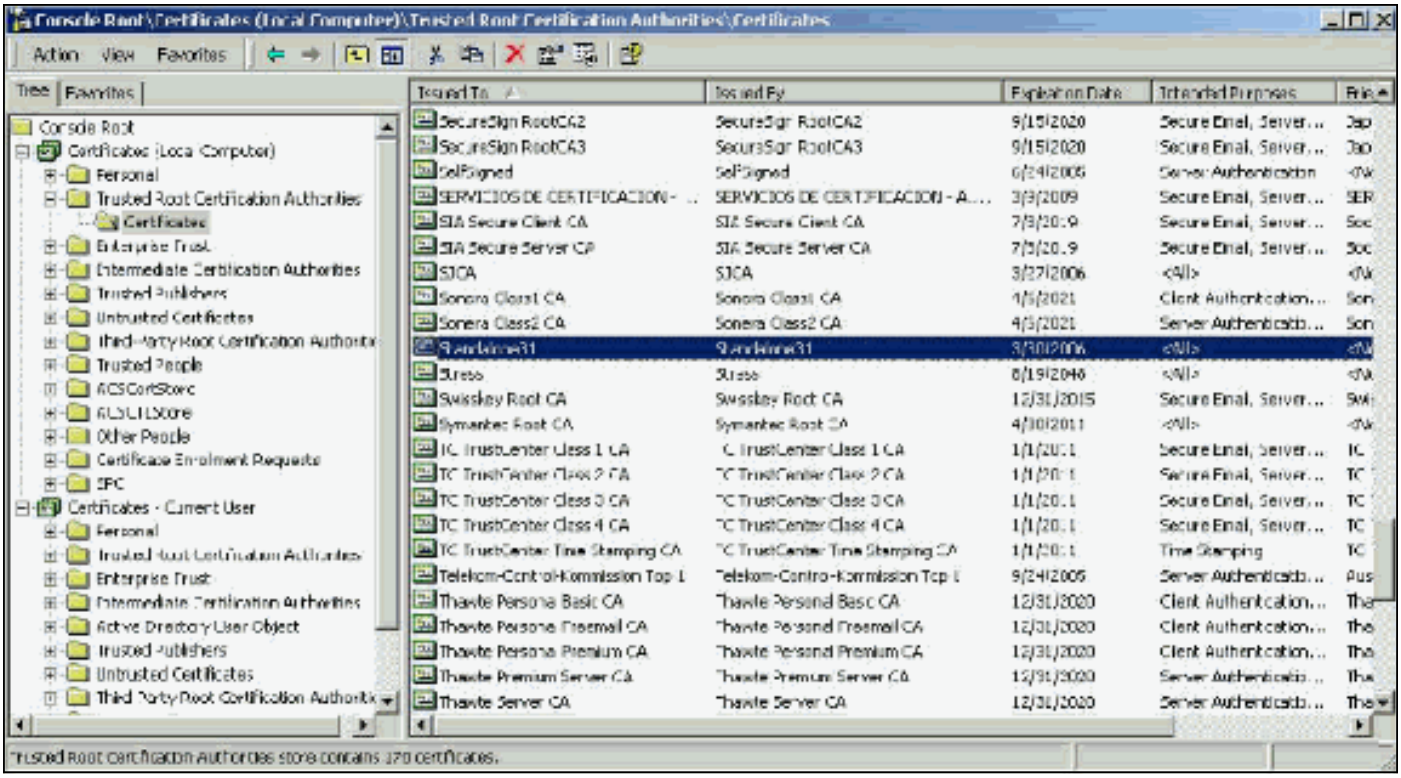
حقل إستخدام المفتاح المحسن

يحدد حقل "إستخدام المفتاح المحسن" الغرض المقصود من الشهادة ويلزم إدراجه ك "مصادقة الخادم". يكون هذا الحقل إلزاميا عندما تستخدم ملتمس Microsoft لكل من PEAP و EAP-TLS. عند إستخدام Microsoft Certificate Services، يتم تكوين ذلك في المرجع المصدق المستقل باستخدام تحديد **شهادة مصادقة الخادم** من القائمة المنسدلة الغرض المقصود وفي المرجع المصدق للمؤسسة مع تحديد **خادم الويب** من القائمة المنسدلة لقالب الشهادة. إذا طلبت شهادة باستخدام CSR مع خدمات شهادات Microsoft، فليس لديك الخيار لتحديد الغرض المقصود باستخدام CA المستقل. لذلك، لا يوجد حقل EKU. مع المرجع المصدق (CA) للمؤسسة، لديك القائمة المنسدلة الغرض المقصود. لا تقوم بعض المراجع المصدقة بإنشاء شهادات باستخدام حقل EKU، لذلك فإنها تكون غير مفيدة عند إستخدام ملتمس Microsoft EAP.



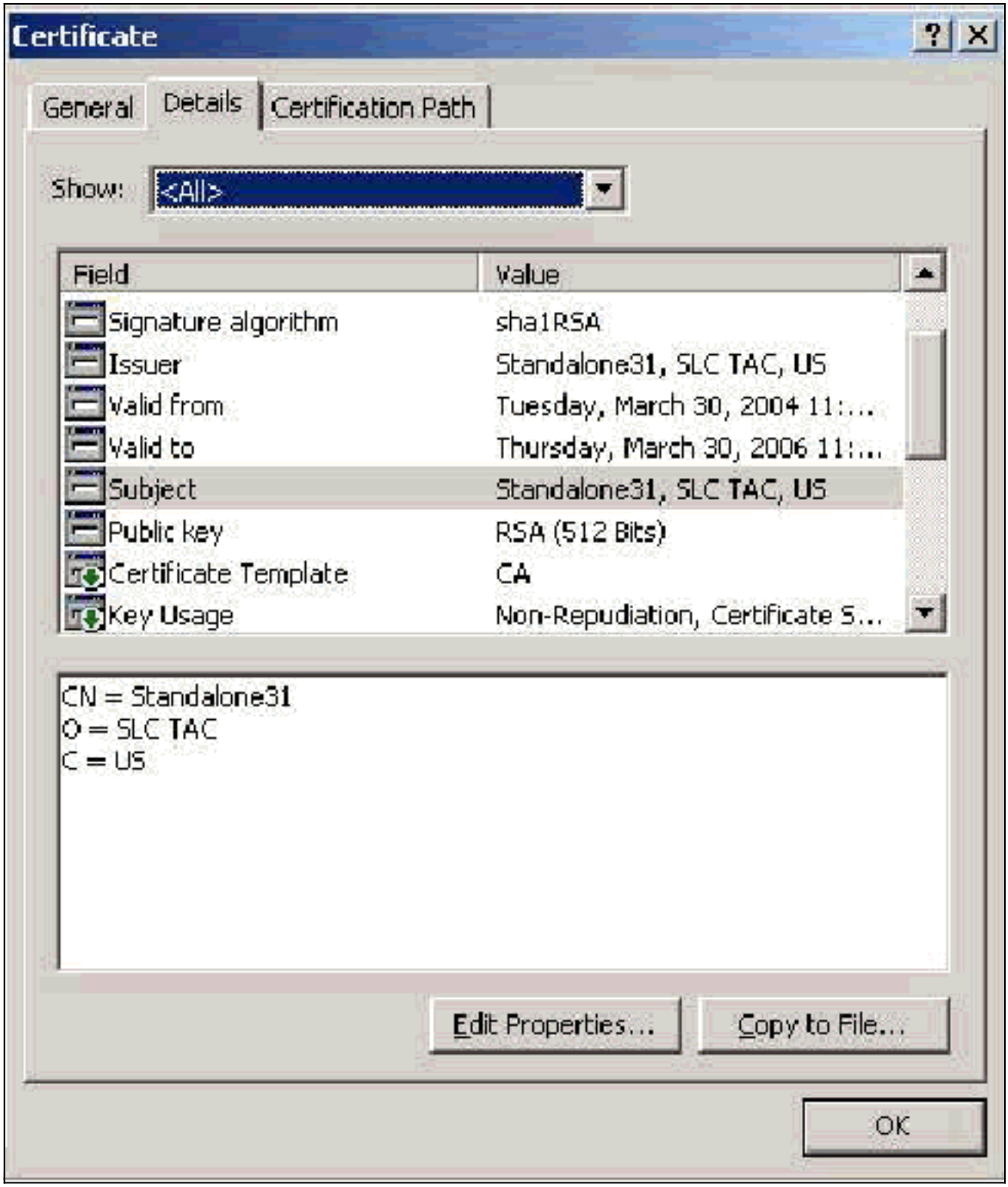
شهادات المرجع المصدق الجذر

الغرض الوحيد من شهادة المرجع المصدق الجذر هو تعريف شهادة الخادم (وشهادة المرجع المصدق الوسيطة إن أمكن) كشهادة موثوق بها إلى ACS وإلى متطلب Windows EAP-MSCHAPv2. ويجب أن يكون موجودا في مخزن مراجع التصديق الجذر الموثوق بها في Windows على كل من خادم ACS، وفي حالة EAP-MSCHAPv2، على كمبيوتر العميل. يتم تثبيت معظم شهادات المرجع المصدق (CA) التابعة لجهة خارجية مع Windows، ولا يتطلب هذا الأمر جهدا يذكر. في حالة إستخدام Microsoft Certificate Services ووجود خادم الشهادات على نفس الجهاز الذي يستخدم فيه ACS، يتم تثبيت شهادة المرجع المصدق الجذر تلقائيا. إذا لم يتم العثور على شهادة المرجع المصدق الجذر في مخزن مراجع التصديق الجذر الموثوق بها في Windows، فيجب الحصول عليها من المرجع المصدق وتثبيتها. عند تثبيتها بشكل صحيح في مخزن تراخيص Windows، يجب أن تظهر شهادة المرجع المصدق الجذر في **الشهادات (الكمبيوتر المحلي) > مراجع التصديق الجذر الموثوق بها >** مجلد **الشهادات** كما يظهر في نافذة المثال هذا.



حقول الموضوع والمصدر

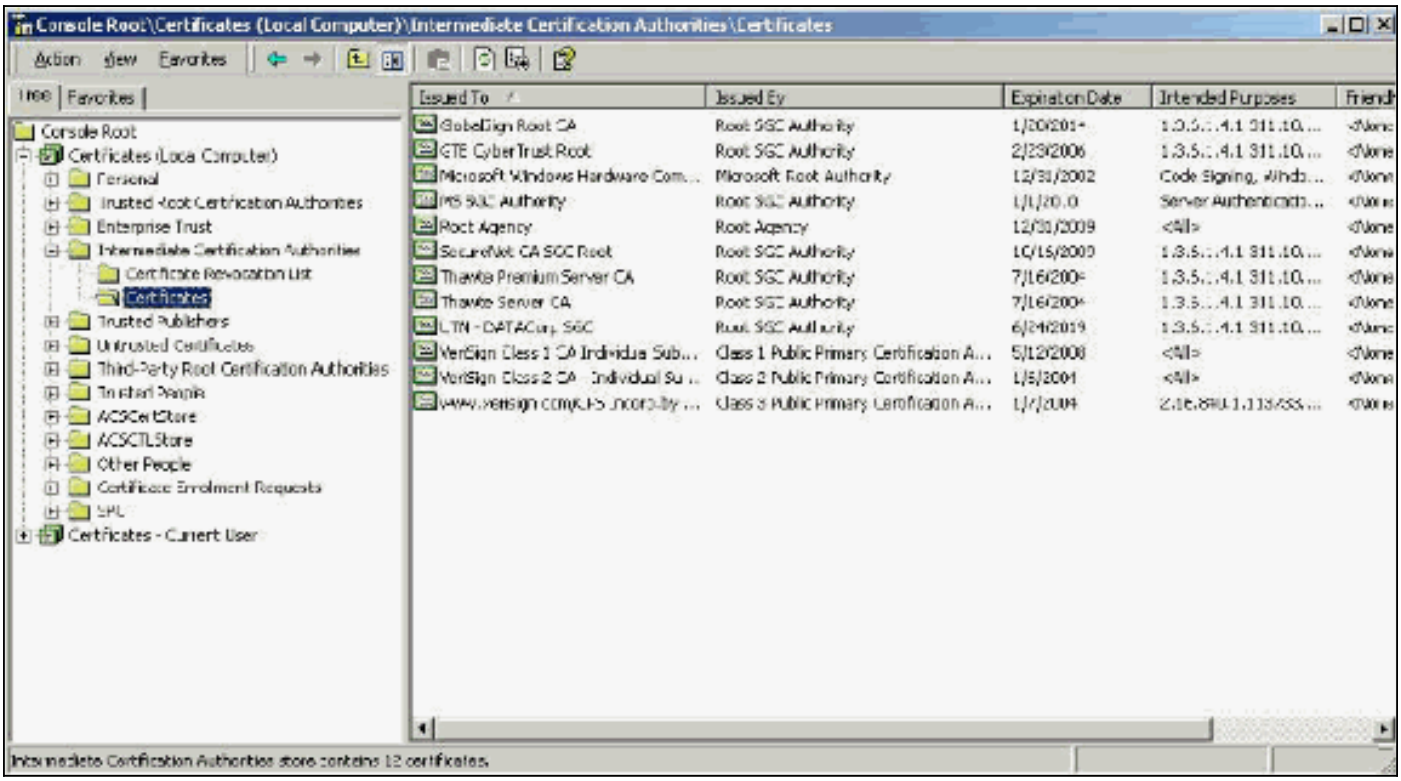
يحدد الحقلان "الموضوع" و"المصدر" المرجع المصدق ويجب أن يكونا متماثلين تماما. أستخدم هذه الحقول لملء الحقول "تم إصدارها إلى" و"تم إصدارها بواسطة" في علامة التبويب "عام" في الترخيص. يتم تعبئتها باسم الجذر الكيميائي.



شهادات CA الوسيطة

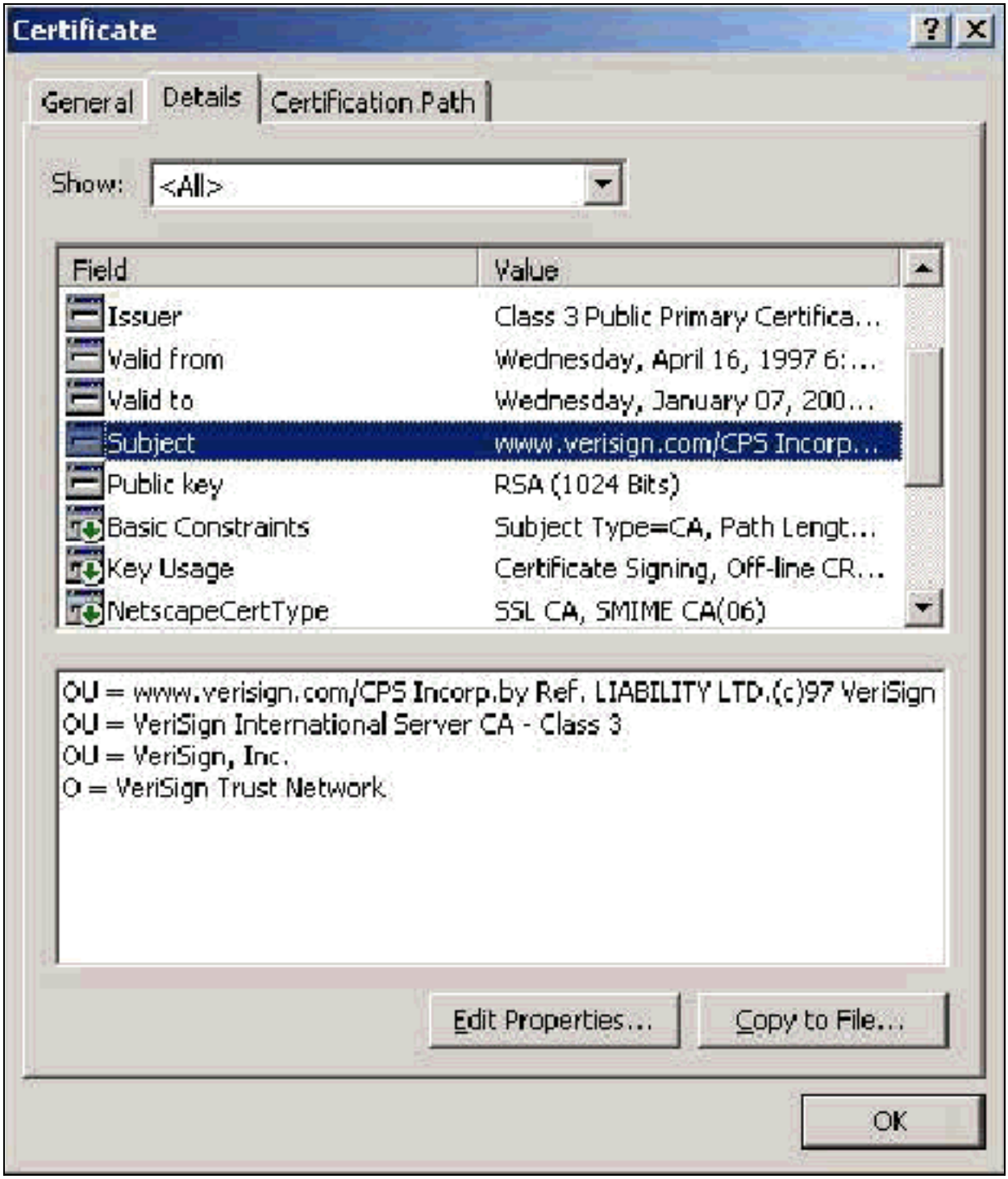
شهادات المرجع المصدق الوسيطة هي شهادات تستخدمها لتعريف مرجع مصدق تابع لأحد المراجع المصدقة الجذر. يتم إنشاء بعض شهادات الخادم (شهادات Verising اللاسلكية) باستخدام CA متوسط. في حالة إستخدام شهادة خادم مقطوعة بواسطة المرجع المصدق الوسيط، يجب تثبيت شهادة المرجع المصدق الوسيط في منطقة "المراجع المصدقة الوسيطة" في مخزن الجهاز المحلي على خادم ACS. وفي حالة إستخدام ملتمس Microsoft EAP على العميل، فإن شهادة المرجع المصدق الجذر الخاصة ب CA الجذر التي أنشأت شهادة المرجع المصدق الوسيط يجب أن تكون أيضا في المخزن المناسب على خادم ACS والعميل حتى يمكن إنشاء سلسلة الثقة. يجب وضع علامة "شهادة المرجع المصدق الجذر" و"شهادة المرجع المصدق الوسيطة" كشهادة موثوق بها في ACS وعلى العميل. لم يتم تثبيت معظم شهادات CA الوسيطة مع Windows لذلك من المحتمل أن تحتاج إلى الحصول عليها من المورد. عندما يتم تثبيتها بشكل صحيح في مخزن تراخيص Windows، تظهر شهادة CA الوسيطة في **الشهادات (الكمبيوتر**

المحلي) > مراجع التصديق الوسيطة > مجلد **الشهادات** كما يظهر في نافذة المثال هذه.



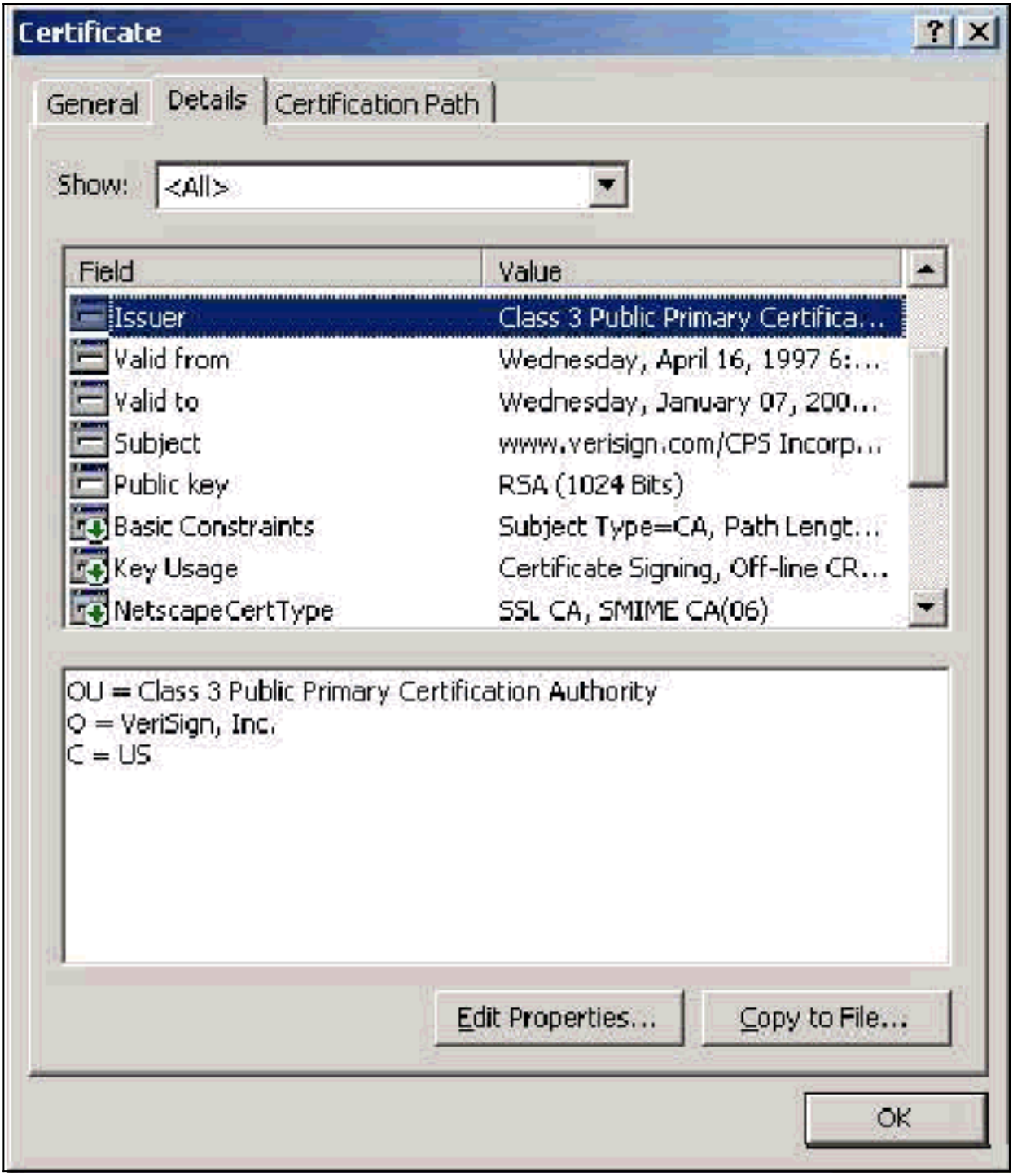
حقل الموضوع

يحدد حقل الموضوع المرجع المصدق الوسيط. تستخدم هذه القيمة لتحديد الحقل "تم إصداره إلى" في علامة التبويب "عام" في الشهادة.



حقل المصدر

يحدد حقل المصدر المرجع المصدق الذي يقطع الشهادة. أستخدم هذه القيمة لتحديد قيمة الحقل الصادر حسب في علامة التبويب "عام" في الشهادة. إنه مملوء باسم المرجع المصدق.



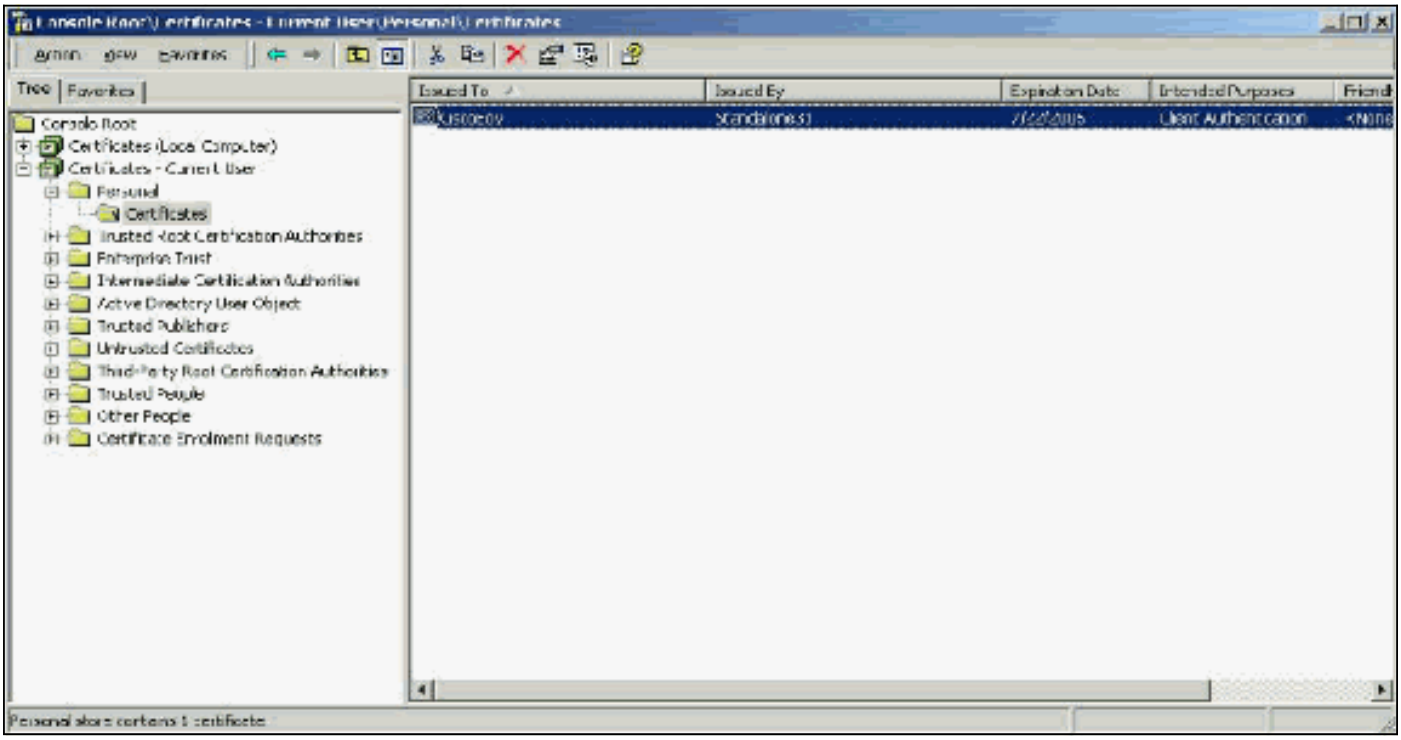
شهادات العميل

تستخدم شهادات العميل لتعريف المستخدم في EAP-TLS بشكل إيجابي. وليس لها دور في بناء نفق TLS ولا تستخدم للتشفير. ويتم التوصل إلى تحديد الهوية بشكل إيجابي من خلال واحدة من ثلاث وسائل:

- **مقارنة CN (أو الاسم)**—يقارن ال CN في الشهادة باسم المستخدم في قاعدة البيانات. يتم تضمين مزيد من المعلومات حول نوع المقارنة هذا في وصف حقل الموضوع للشهادة.
- **مقارنة شبكة منطقة التخزين (SAN)** — مقارنة شبكة منطقة التخزين (SAN) في الشهادة باسم المستخدم في قاعدة البيانات. وهذا مدعوم فقط اعتبارا من ACS 3.2. يتم تضمين مزيد من المعلومات حول نوع المقارنة هذا في وصف حقل "الاسم البديل للموضوع" للشهادة.
- **مقارنة ثنائية**- تقارن الشهادة بنسخة ثنائية من الشهادة المخزنة في قاعدة البيانات (يمكن فقط ل AD و LDAP القيام بذلك). إذا كنت تستخدم مقارنة ثنائية للشهادة، فيجب عليك تخزين شهادة المستخدم بتنسيق ثنائي. أيضا، بالنسبة ل LDAP العام و Active Directory، يجب أن تكون السمة التي تخزن الشهادة هي سمة LDAP

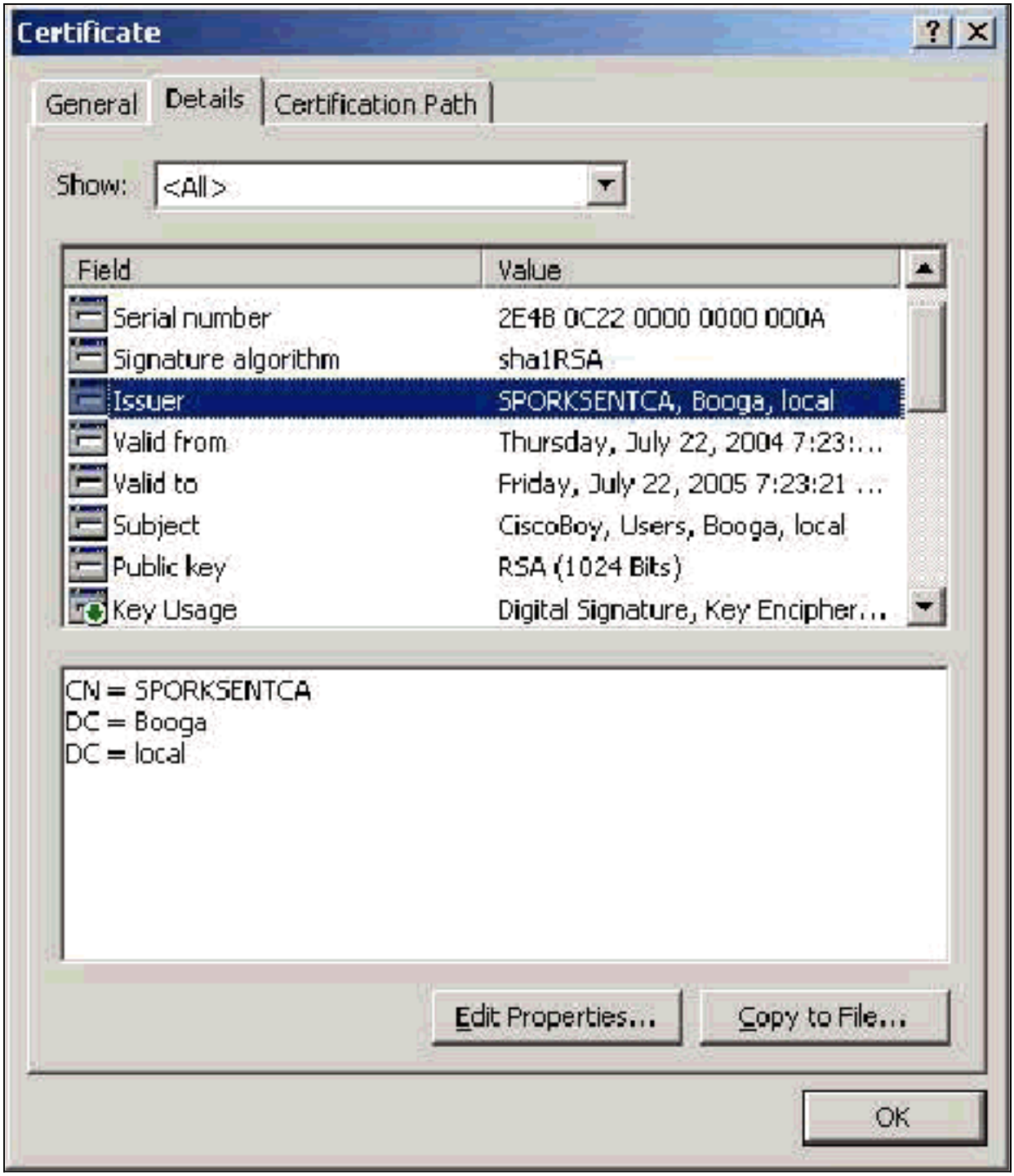
القياسية المسماة "userCertificate".
أيا كانت طريقة المقارنة المستخدمة، يجب أن تتطابق المعلومات الموجودة في الحقل المناسب (CN أو SAN) مع الاسم الذي تستخدمه قاعدة البيانات للمصادقة. يستخدم AD اسم NetBios للمصادقة في الوضع المختلط و UPN في الوضع الأصلي.

يناقش هذا القسم إنشاء شهادة العميل باستخدام Microsoft Certificate Services. يتطلب EAP-TLS شهادة عميل فريدة لمصادقة كل مستخدم. يجب تثبيت الشهادة على كل كمبيوتر لكل مستخدم. عند التثبيت بشكل صحيح، تكون الشهادة موجودة في **مجلد الشهادات - المستخدم الحالي > شخصي > الشهادات** كما يظهر في نافذة المثال هذه.



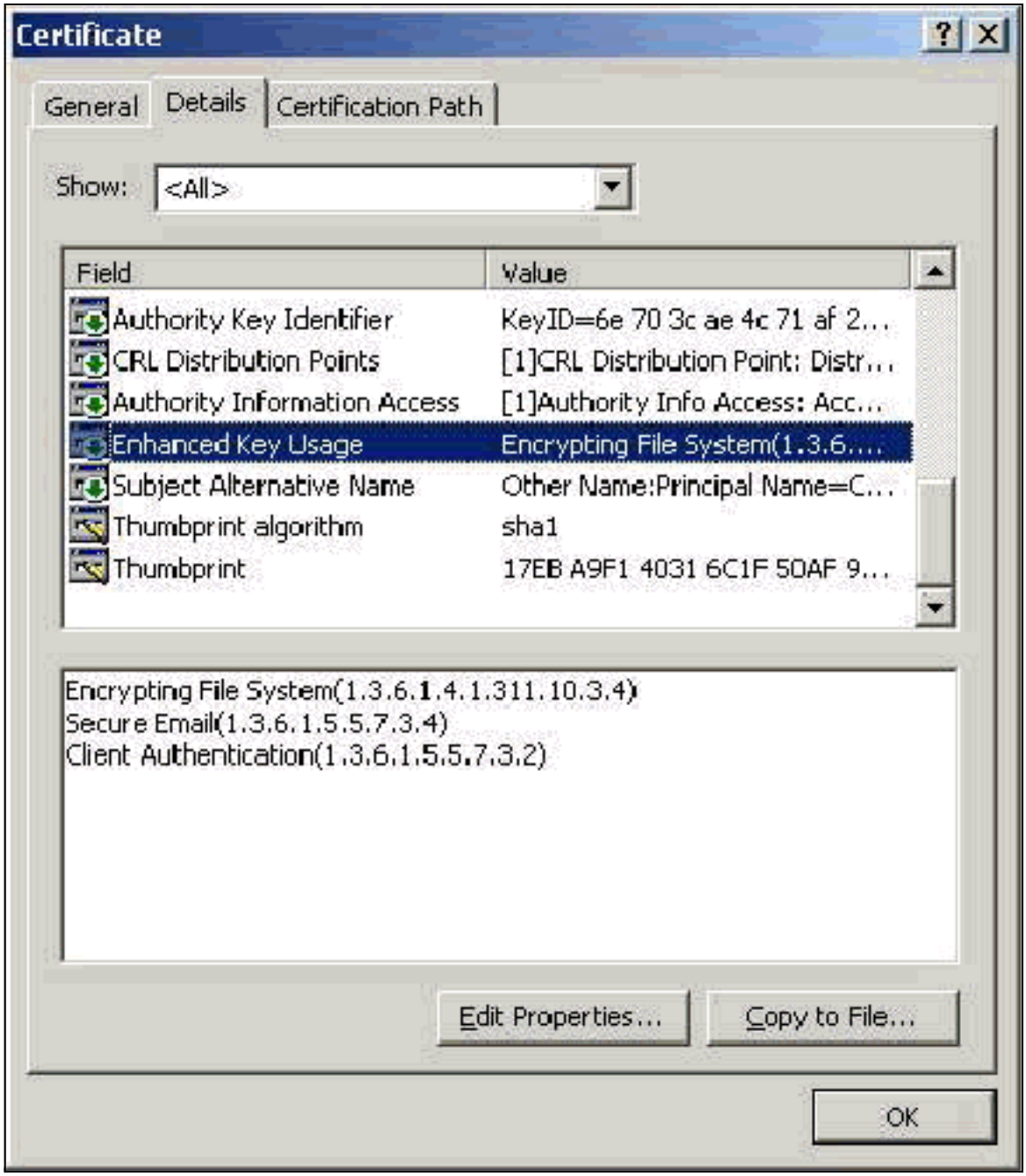
حقل المصدر

يحدد حقل المصدر المرجع المصدق الذي يقطع الشهادة. أستخدم هذه القيمة لتحديد قيمة الحقل الصادر حسب في علامة التبويب "عام" في الشهادة. هذا مملوء باسم المرجع المصدق.



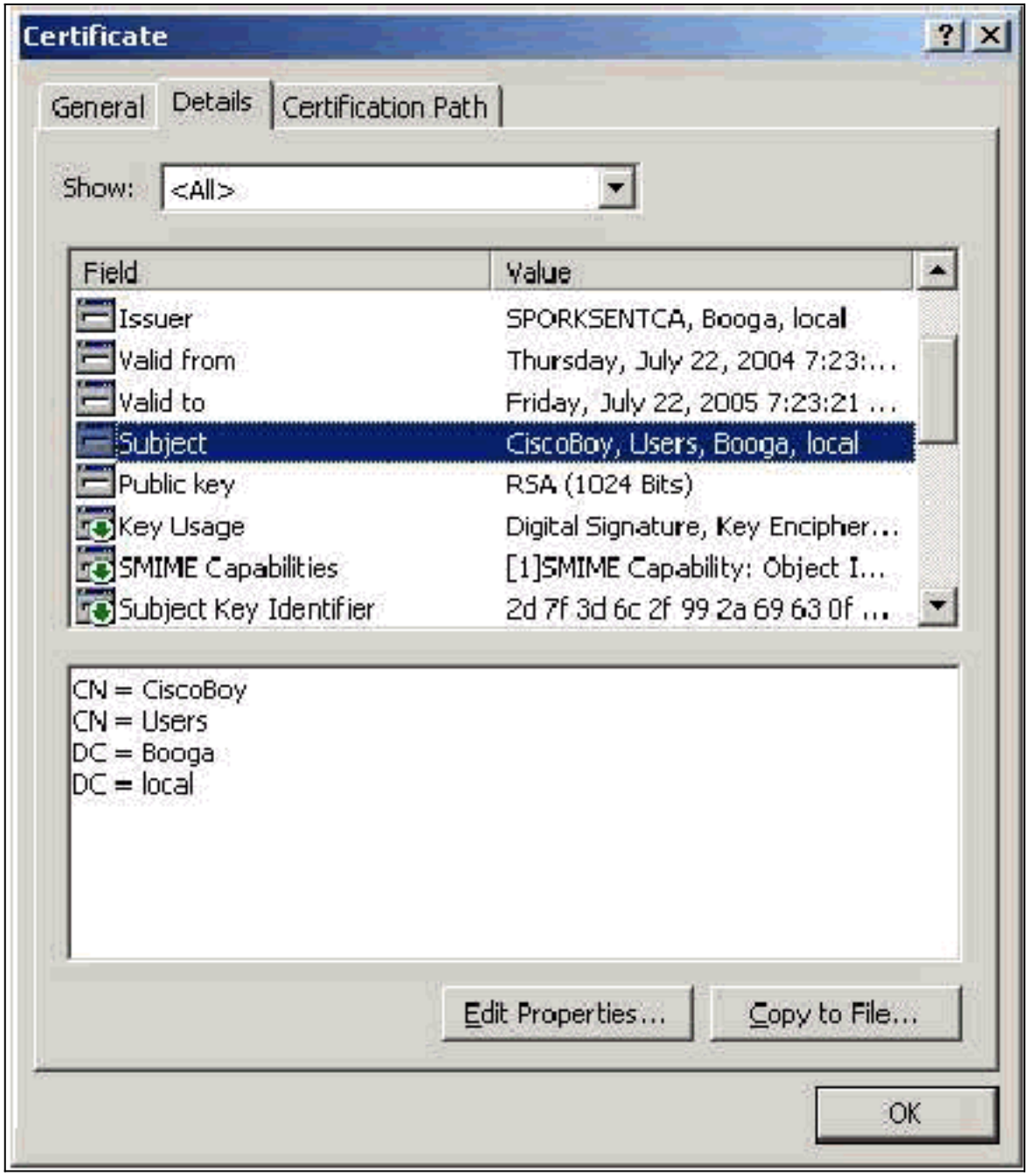
حقل إستخدام المفتاح المحسن

يحدد حقل "إستخدام المفتاح المحسن" الغرض المقصود من الشهادة ويلزم أن يحتوي على مصادقة العميل. يكون هذا الحقل إلزاميا عندما تستخدم ملتمس Microsoft لكل من PEAP و EAP-TLS. عند إستخدام Microsoft Certificate Services، يتم تكوين ذلك في المرجع المصدق المستقل عند تحديد **شهادة مصادقة العميل** من القائمة المنسدلة الغرض المقصود وفي المرجع المصدق للمؤسسة عند تحديد **المستخدم** من القائمة المنسدلة لقالب الشهادة. إذا طلبت شهادة باستخدام CSR مع خدمات شهادات Microsoft، فليس لديك الخيار لتحديد الغرض المقصود باستخدام CA المستقل. لذلك، لا يوجد حقل EKU. مع المرجع المصدق (CA) للمؤسسة، لديك القائمة المنسدلة الغرض المقصود. لا تقوم بعض المراجع المصدقة بإنشاء شهادات باستخدام حقل EKU. ولا فائدة منها عندما تستخدم متطلب Microsoft EAP.



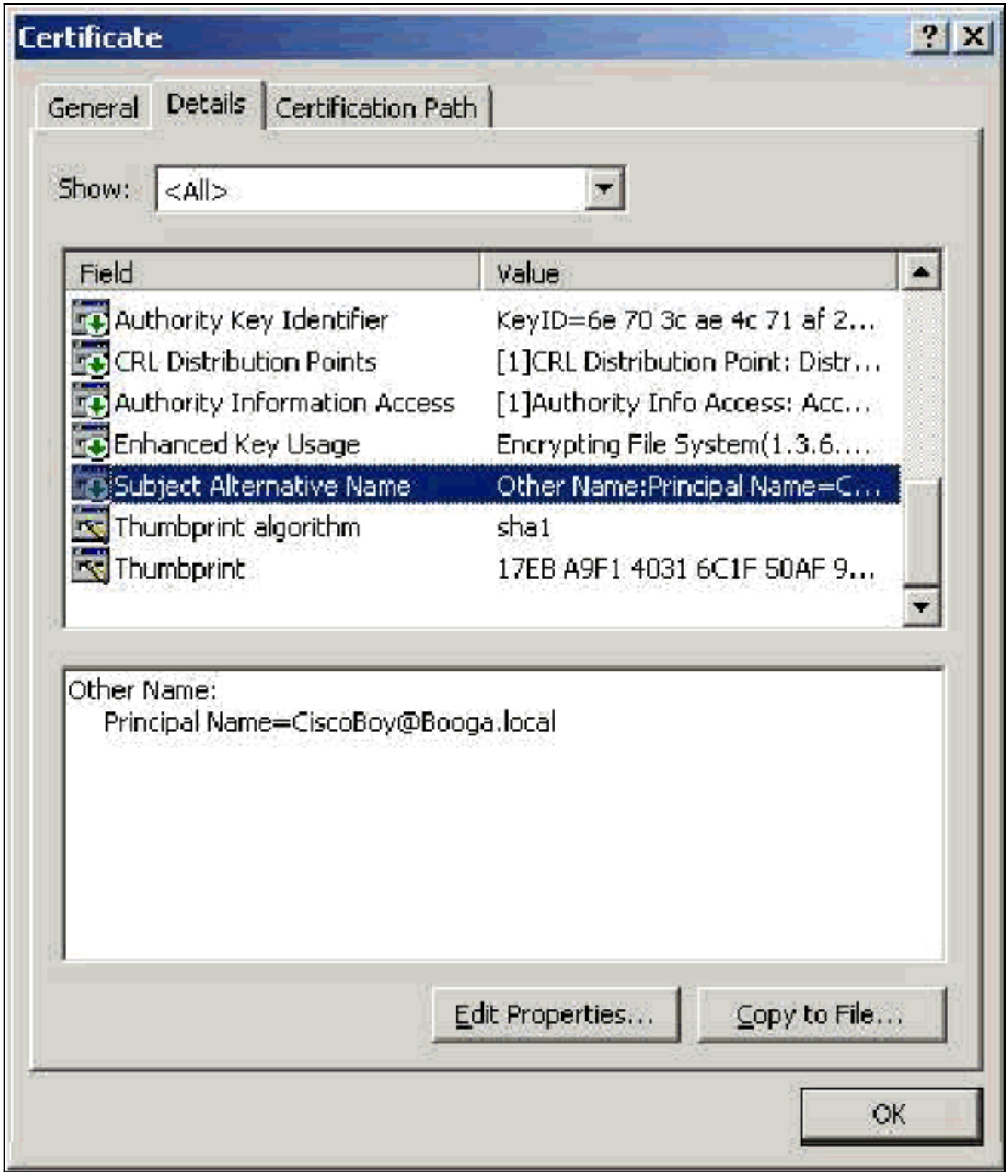
حقل الموضوع

يستخدم هذا الحقل في مقارنة CN. تتم مقارنة CN الأول المدرج مع قاعدة البيانات للعثور على تطابق. إذا تم العثور على تطابق، تنجح المصادقة. إذا كنت تستخدم المرجع المصدق المستقل، فإن CN يتم تعبئته بأي شيء تضعه في حقل الاسم في نموذج الشهادة المقدم. إذا كنت تستخدم المرجع المصدق (CA) الخاص بالمؤسسة، يتم ملء CN تلقائيا باسم الحساب كما هو مدرج في وحدة تحكم مستخدمي وأجهزة الكمبيوتر في Active Directory (لا يتطابق هذا بالضرورة مع UPN أو اسم NetBios).



حقل الاسم البديل للموضوع

يتم إستخدام حقل "الاسم البديل للموضوع" في مقارنة SAN. تتم مقارنة شبكة التخزين (SAN) المدرجة بقاعدة البيانات للعثور على تطابق. إذا تم العثور على تطابق، تنجح المصادقة. إذا كنت تستخدم المرجع المصدق للمؤسسة، يتم تعبئة شبكة التخزين (SAN) تلقائيا باسم تسجيل الدخول إلى (UPN @domain) Active Directory). لا يتضمن المرجع المصدق المستقل حقل SAN، لذلك لا يمكنك إستخدام مقارنة SAN.

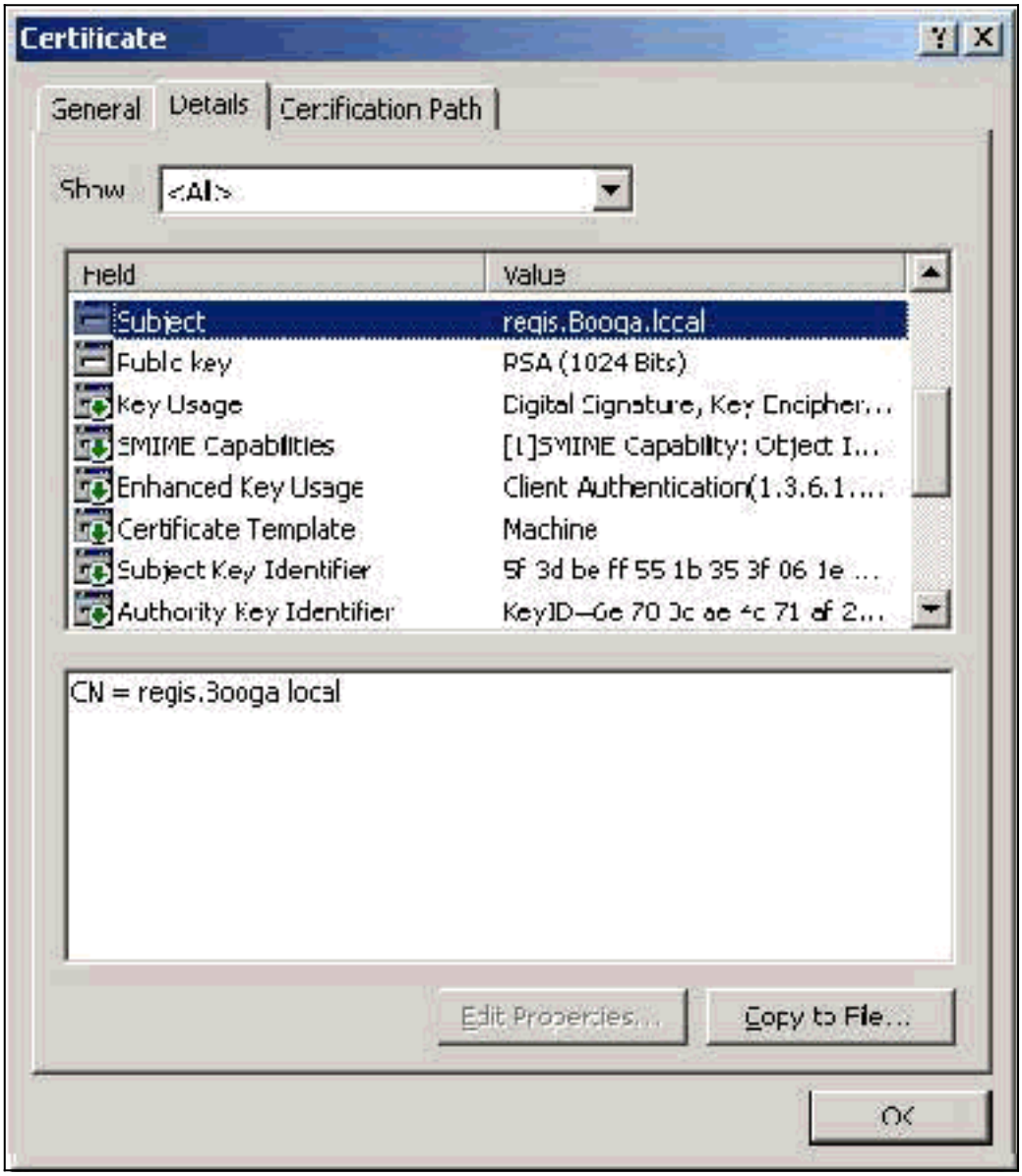


شهادات الجهاز

تستخدم شهادات الجهاز في EAP-TLS لتعريف الكمبيوتر بشكل إيجابي عند إستخدام مصادقة الجهاز. يمكنك الوصول إلى هذه الشهادات فقط عند تكوين المرجع المصدق ل Microsoft Enterprise للتسجيل التلقائي للشهادة والانضمام إلى الكمبيوتر في المجال. يتم إنشاء الشهادة تلقائيا عند إستخدام بيانات اعتماد Active Directory الخاصة بالكمبيوتر وتثبيتها في مخزن الكمبيوتر المحلي. تتلقى أجهزة الكمبيوتر التي تكون أعضاء بالفعل في المجال قبل تكوين التسجيل التلقائي شهادة في المرة التالية التي يتم فيها إعادة تشغيل Windows. يتم تثبيت "شهادة الجهاز" في مجلد **الشهادات (الكمبيوتر المحلي) > شخصي > شهادات** الشهادات الخاص ب "الشهادات" (الكمبيوتر المحلي) MMC مثل "شهادات الخادم". لا يمكنك تثبيت هذه الشهادات على أي جهاز آخر لأنه لا يمكنك تصدير المفتاح الخاص.

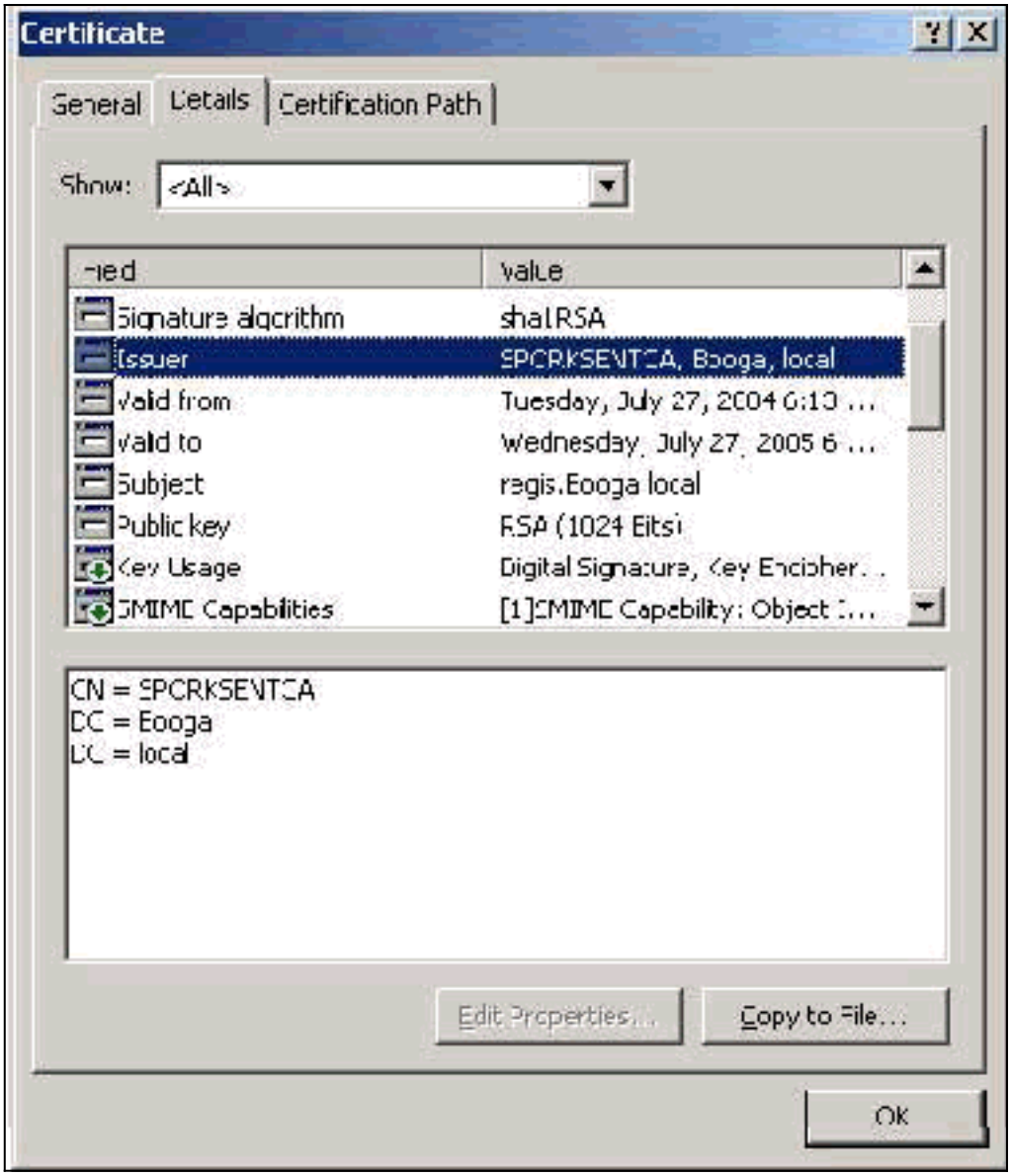
الموضوع وحقول شبكة منطقة التخزين (SAN)

يعرف حقلا الموضوع وشبكة منطقة التخزين (SAN) الكمبيوتر. يتم ملء القيمة باسم الكمبيوتر المؤهل بالكامل ويتم إستخدامها لتحديد الحقل "تم الإصدار إلى" في علامة التبويب "عام" في الشهادة وهي نفسها لكل من حقلي "الموضوع" و"شبكة منطقة التخزين (SAN)".



حقل المصدر

يحدد حقل المصدر المرجع المصدق الذي يقطع الشهادة. أستخدم هذه القيمة لتحديد قيمة الحقل الصادر حسب في علامة التبويب "عام" في الشهادة. إنه مملوء باسم المرجع المصدق.



الملحق أ - امتدادات الشهادات العامة

csr.—هذه ليست في الواقع شهادة ولكن بالأحرى طلب توقيع شهادة. هو ملف نص عادي بهذا التنسيق:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBtDCCAR0CAQIwDzENMAsGA1UEAxMETW9yazCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAu3duNPToM711jadL1hMWTMTl2yzDn2btVQsWHjdS9FARBOpVIuQe
BAMCBkAwDQYJKoZIhvcNAQEFBQADgYEAkvHoMkTY0mhHwavsDey8IN7DsN0Io6vP
tyjWnoKzHycO6NHt3k7f55Ch/nQ6ONSGBs02uYpjUUPJPqlhGBY4VEcV39zdPNs8
uPCuex/LZ4sOqgmd6WOxup3rEI01fJnqjpd7fwbX9Jr3Awc1gFsXS0Kg3WnjJD4i
ILII9Vhw89s=
-----END CERTIFICATE REQUEST-----
```

pvk.—يشير هذا الملحق إلى مفتاح خاص على الرغم من أن الملحق لا يضمن أن المحتوى هو في الواقع مفتاح خاص. يجب أن يكون المحتوى نصا عاديا بهذا التنسيق:

```
-----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.—هذا ملحق عام يشير إلى شهادة. يمكن أن يكون الخادم وشهادات المرجع المصدق الجذر والشهادات المصدقة الوسيطة بهذا التنسيق. عادة ما يكون ملف نص عادي بامتداد يمكنك تغييره حسب حاجتك ويمكن أن يكون إما بتنسيق DER أو Base 64. يمكنك إستيراد هذا التنسيق إلى مخزن تراخيص Windows.

pem.—هذا الملحق يمثل البريد المحسن للخصوصية. يشيع إستخدام هذا الملحق مع UNIX و Linux و BSD وهكذا دواليك. يستخدم بشكل عام لشهادات الخادم والمفاتيح الخاصة، وهو عادة ملف نص عادي بامتداد يمكنك تغييره كما تريد من .pem إلى .cer حتى يمكنك إستيراده إلى مخزن شهادات Windows.

المحتوى الداخلي لملفات .cer و .pem بشكل عام يشبه هذا المخرج:

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

pfx.—هذا الملحق يمثل تبادل المعلومات الشخصية. هذا التنسيق هو طريقة يمكنك إستخدامها لتجميع الشهادات في ملف واحد. على سبيل المثال، يمكنك تجميع شهادة خادم والمفتاح الخاص المرتبط بها وشهادة المرجع المصدق الجذر في ملف واحد واستيراد الملف بسهولة إلى مخزن تراخيص Windows المناسب. يستخدم هذا الخيار عادة لشهادات الخادم والعميل. للأسف، إذا تم تضمين شهادة مرجع مصدق جذري، فإن شهادة المرجع المصدق الجذر تكون مثبتة دائما في مخزن المستخدم الحالي بدلا من مخزن الكمبيوتر المحلي حتى إذا تم تحديد مخزن الكمبيوتر المحلي للتثبيت.

p12.—لا يظهر هذا التنسيق بشكل عام إلا مع شهادة العميل. يمكنك إستيراد هذا التنسيق إلى مخزن تراخيص Windows.

p7b.- هذا تنسيق آخر يقوم بتخزين شهادات متعددة في ملف واحد. يمكنك إستيراد هذا التنسيق إلى مخزن تراخيص Windows.

الملحق ب - تحويل تنسيق الشهادة

في معظم الحالات، يحدث تحويل الشهادة عندما تقوم بتغيير الامتداد (على سبيل المثال، من .pem إلى .cer) لأن الشهادات تكون عادة بتنسيق نص عادي. في بعض الأحيان، لا تكون الشهادة بتنسيق نص عادي ويجب عليك تحويلها باستخدام أداة مثل OpenSSL . على سبيل المثال، يتعذر على "محرك حلول ACS" تثبيت الشهادات بتنسيق .pfx. لذلك، يجب تحويل الشهادة والمفتاح الخاص إلى تنسيق قابل للاستخدام. هذه هي صياغة الأمر الأساسية ل OpenSSL:

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

أنت حضضت على الإدراج كلمة وعبارة مرور PEM. يجب أن تكون كلمات المرور هذه هي نفسها وتكون كلمة مرور المفتاح الخاص التي يتم تحديدها عند تصدير .pfx. الإنتاج هو ملف .pem مفرد الذي يتضمن كل التراخيص والمفاتيح الخاصة في .pfx. يمكن الإشارة إلى هذا الملف في ACS على أنه كل من الشهادة والملف المفتاح الخاص ويتم تثبيته بدون مشاكل.

الملحق ج - فترة صلاحية الشهادة

لا يمكن إستخدام الشهادة إلا أثناء فترة صلاحيتها. تحدد فترة صلاحية شهادة المرجع المصدق الجذر عند تأسيس المرجع المصدق الجذر وقد تختلف. تحدد فترة صلاحية شهادة المرجع المصدق الوسيط عند تأسيس المرجع المصدق ولا يمكن أن تتجاوز فترة صلاحية المرجع المصدق الجذر الذي تتبعه. يتم تعيين فترة الصلاحية لشهادات الخادم والعميل والآلة تلقائيا على سنة واحدة مع خدمات شهادات Microsoft. لا يمكن تغيير هذا إلا عند أختراق سجل Windows وفقا لمقالة قاعدة معارف Microsoft 254632 ولا يمكن أن يتجاوز فترة الصلاحية للمرجع المصدق الجذر. تكون فترة صلاحية الشهادات الموقعة ذاتيا التي يقوم ACS بتوليدها سنة واحدة دائما ولا يمكن تغييرها في الإصدارات الحالية.

معلومات ذات صلة

- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).