Guide de certificat pour EAP version 1.01

Contenu

Introduction

Ce document clarifie une partie de la confusion qui accompagne les différents types de certificats, formats et exigences associés aux différentes formes de protocole EAP (Extensible Authentication Protocol). Les cinq types de certificat liés au protocole EAP dont traite ce document sont Server, Root CA, Intermediate CA, Client et Machine. Ces certificats sont présentés sous différents formats et il peut y avoir des exigences différentes en ce qui concerne chacun d'entre eux en fonction de la mise en oeuvre du PAE en question.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Certificats serveur

Le certificat de serveur est installé sur le serveur RADIUS et son principal objectif dans EAP est de créer le tunnel TLS (Transport Layer Security) crypté qui protège les informations d'authentification. Lorsque vous utilisez EAP-MSCHAPv2, le certificat de serveur joue un rôle secondaire qui consiste à identifier le serveur RADIUS comme entité de confiance pour l'authentification. Ce rôle secondaire est accompli à l'aide du champ Utilisation de clé améliorée (EKU). Le champ EKU identifie le certificat en tant que certificat de serveur valide et vérifie que l'autorité de certification racine qui a émis le certificat est une autorité de certification racine de confiance. Cela nécessite la présence du certificat d'autorité de certification racine. Cisco Secure ACS exige que le certificat soit au format binaire X.509 v3 codé en base64 ou en DER.

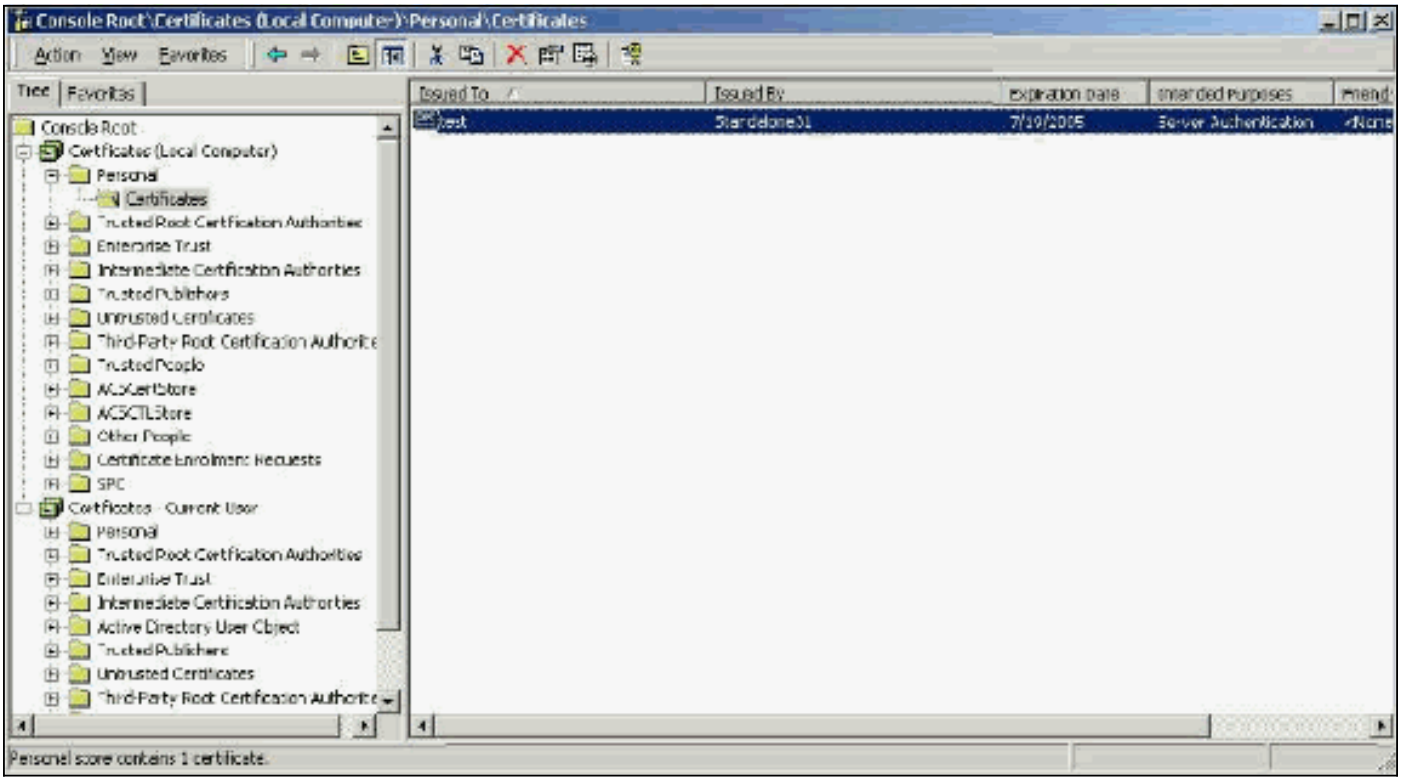
Vous pouvez créer ce certificat avec l'utilisation d'une demande de signature de certificat (CSR) dans ACS, qui est soumise à une autorité de certification. Vous pouvez également couper le certificat à l'aide d'un formulaire de création de certificat CA interne (comme Microsoft Certificate Services). Il est important de noter que, bien que vous puissiez créer le certificat de serveur avec des tailles de clé supérieures à 1024, toute clé supérieure à 1024 ne fonctionne pas avec PEAP. Le client est suspendu même si l'authentification réussit.

Si vous créez le certificat à l'aide d'un CSR, il est créé au format .cer, .pem ou .txt. En de rares occasions, il est créé sans extension. Assurez-vous que votre certificat est un fichier texte brut avec une extension que vous pouvez modifier si nécessaire (l'appliance ACS utilise l'extension .cer ou .pem). En outre, si vous utilisez un CSR, la clé privée du certificat est créée dans le chemin d'accès que vous spécifiez en tant que fichier distinct qui peut ou non avoir une extension et qui a un mot de passe associé à celle-ci (le mot de passe est requis pour l'installation sur ACS). Quelle que soit l'extension, assurez-vous qu'il s'agit d'un fichier texte brut avec une extension que vous pouvez modifier si nécessaire (l'appliance ACS utilise l'extension .pvk ou .pem). Si aucun chemin n'est spécifié pour la clé privée, ACS enregistre la clé dans le répertoire C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs et recherche dans ce répertoire si aucun chemin n'est spécifié pour le fichier de clé privée lors de l'installation du certificat.

Si le certificat est créé à l'aide du formulaire de soumission du certificat des services de certificats Microsoft, assurez-vous que vous marquez les clés comme exportables afin que vous puissiez installer le certificat dans ACS. La création d'un certificat de cette manière simplifie considérablement le processus d'installation. Vous pouvez l'installer directement dans le magasin Windows approprié à partir de l'interface Web des Services de certificats, puis l'installer sur ACS à partir du stockage avec l'utilisation du CN comme référence. Un certificat installé dans le magasin d'ordinateurs local peut également être exporté à partir du stockage Windows et installé facilement

sur un autre ordinateur. Lorsque ce type de certificat est exporté, les clés doivent être marquées comme exportables et un mot de passe doit leur être attribué. Le certificat apparaît ensuite au format .pfx qui inclut la clé privée et le certificat du serveur.

Une fois installé correctement dans le magasin de certificats Windows, le certificat serveur doit apparaître dans le dossier **Certificats (Ordinateur local) > Personnel > Certificats** comme indiqué dans cet exemple de fenêtre.



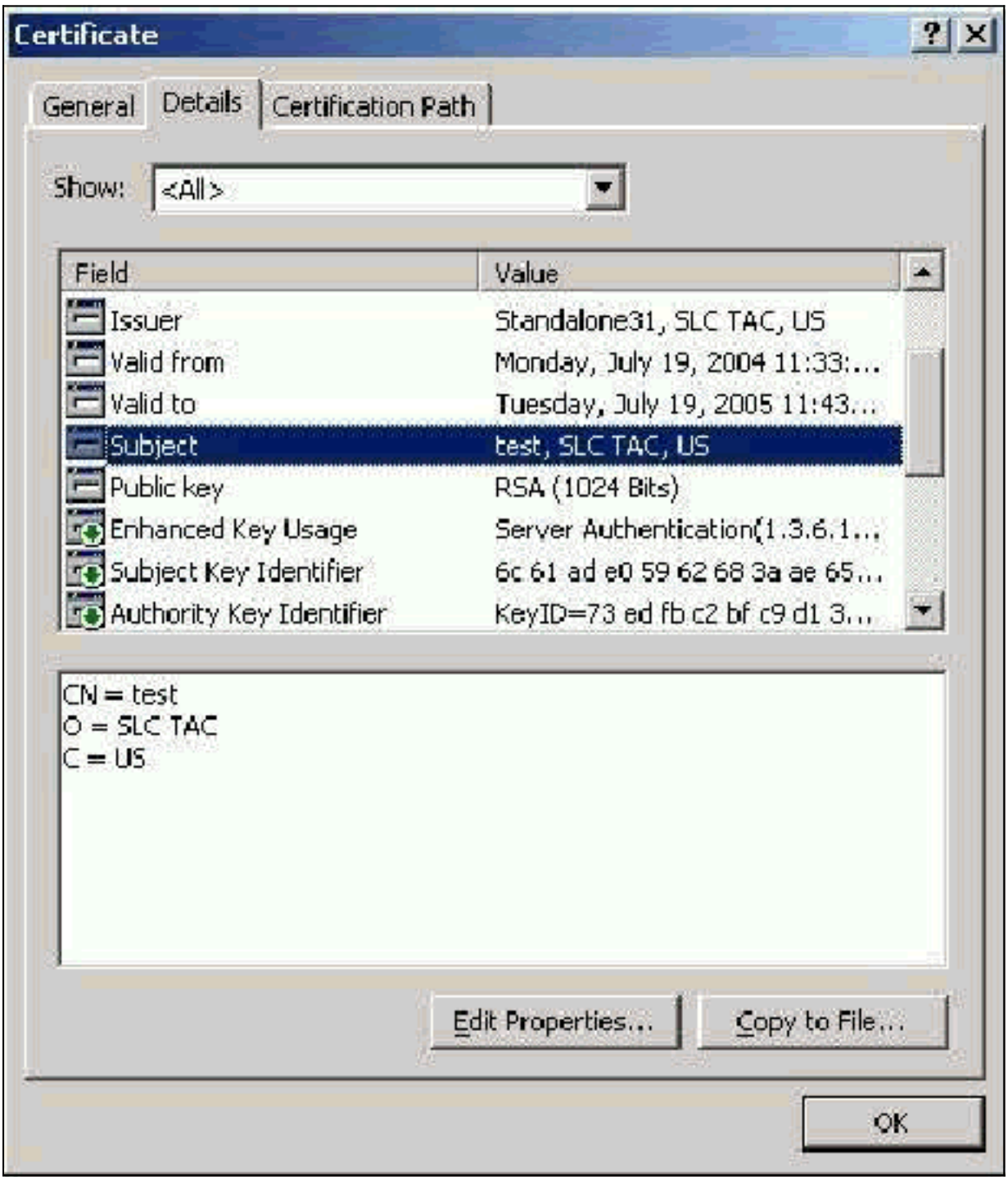
Les certificats auto-signés sont des certificats que vous créez sans l'implication racine ou intermédiaire de l'autorité de certification. Ils ont la même valeur dans les champs Objet et Émetteur, comme un certificat de CA racine. La plupart des certificats auto-signés utilisent le format X.509 v1. Par conséquent, ils ne fonctionnent pas avec ACS. Cependant, depuis la version 3.3, ACS a la possibilité de créer ses propres certificats auto-signés que vous pouvez utiliser pour EAP-TLS et PEAP. N'utilisez pas une taille de clé supérieure à 1024 pour la compatibilité avec PEAP et EAP-TLS. Si vous utilisez un certificat auto-signé, le certificat agit également en tant que certificat d'autorité de certification racine et doit être installé dans le dossier **Certificats (Ordinateur local) > Autorités de certification racine de confiance > Certificats** du client lorsque vous utilisez le demandeur Microsoft EAP. Il s'installe automatiquement dans le magasin de certificats racine approuvés sur le serveur. Cependant, il doit toujours être approuvé dans la liste des certificats de confiance dans la configuration des certificats ACS. Consultez la section Certificats d'autorité de certification racine pour plus d'informations.

Étant donné que les certificats auto-signés sont utilisés comme certificat d'autorité de certification racine pour la validation de certificat de serveur lorsque vous utilisez le demandeur Microsoft EAP et que la période de validité ne peut pas être augmentée à partir de la valeur par défaut d'un an, Cisco vous recommande de ne les utiliser que pour EAP comme mesure temporaire jusqu'à ce que vous puissiez utiliser une autorité de certification traditionnelle.

Champ Objet

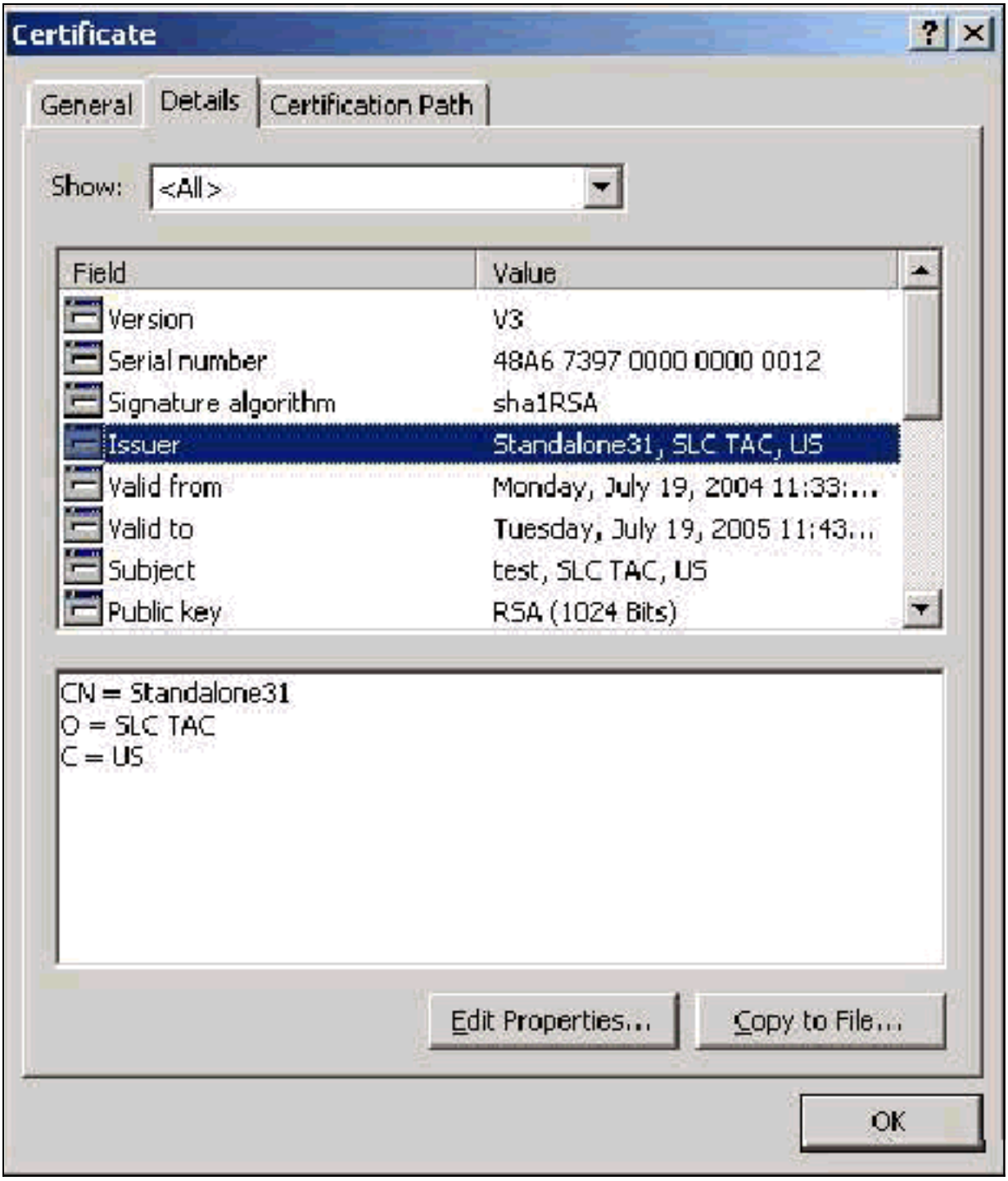
Le champ Objet identifie le certificat. La valeur CN est utilisée pour déterminer le champ Émis à dans l'onglet Général du certificat et est renseignée avec les informations que vous entrez dans le

champ Objet du certificat dans la boîte de dialogue CSR d'ACS ou avec les informations du champ Nom dans Microsoft Certificate Services. La valeur CN est utilisée pour indiquer à ACS quel certificat il doit utiliser à partir du magasin de certificats de l'ordinateur local si l'option d'installation du certificat à partir du stockage est utilisée.



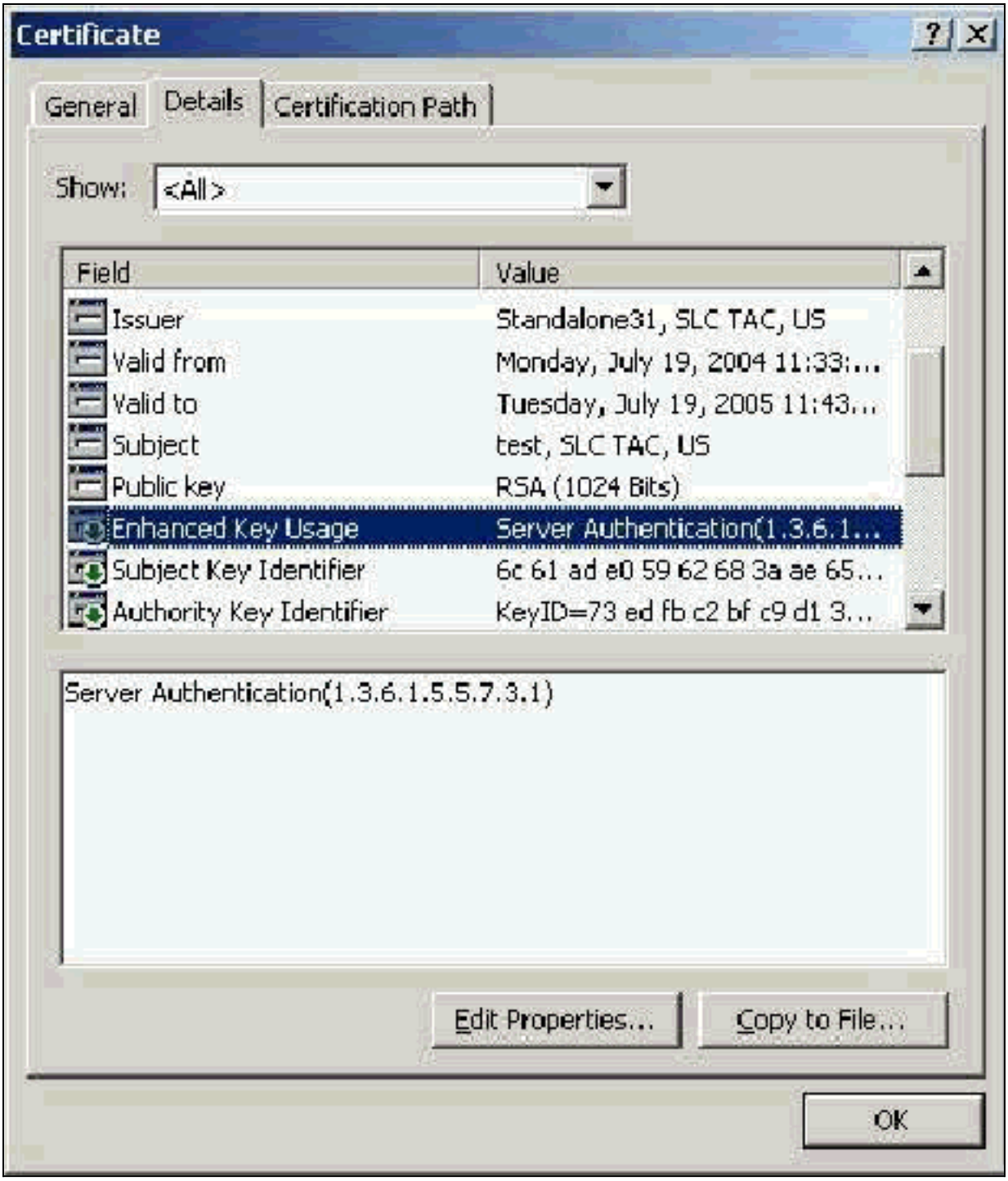
Champ Émetteur

Le champ Émetteur identifie l'autorité de certification qui a supprimé le certificat. Utilisez cette valeur afin de déterminer la valeur du champ Émis par dans l'onglet Général du certificat. Il est renseigné avec le nom de l'autorité de certification.



Champ Utilisation de clé améliorée

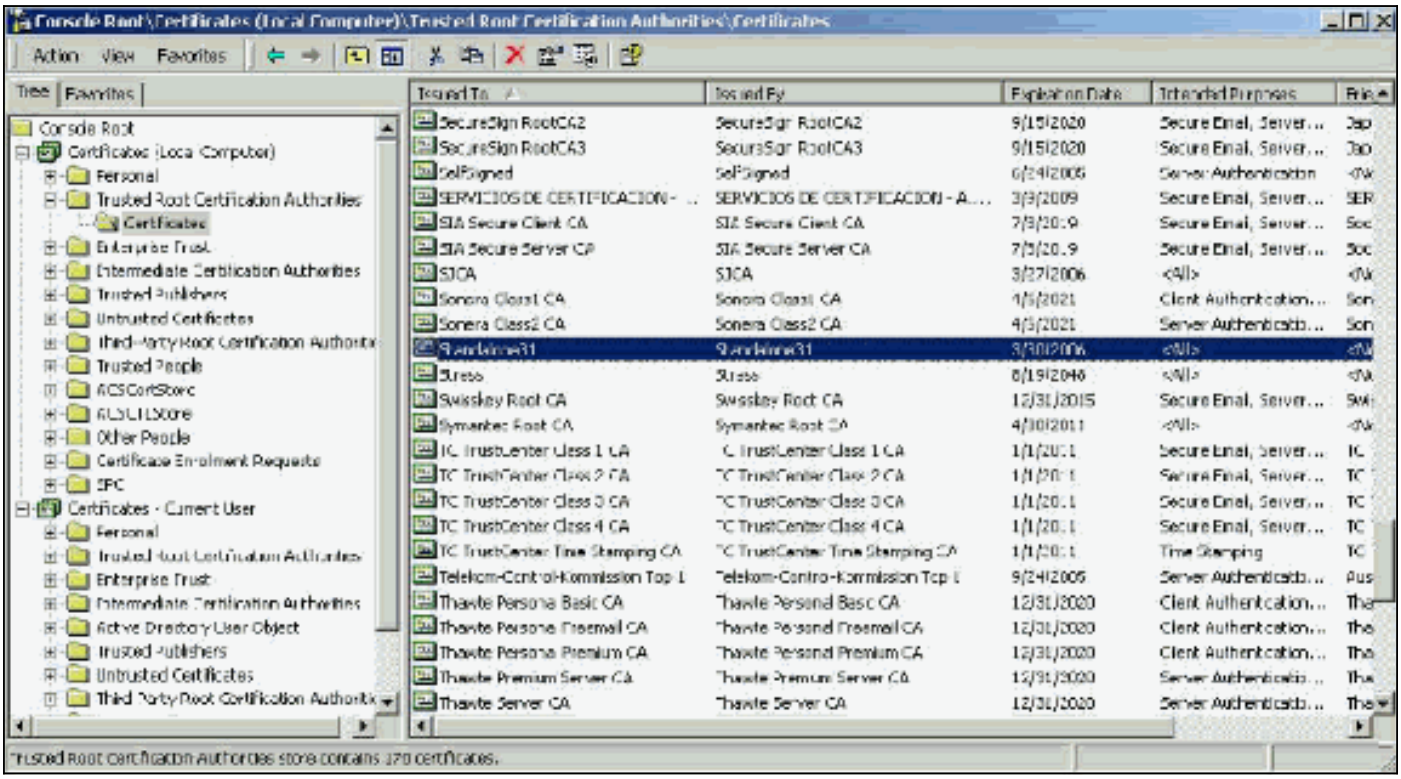
Le champ Utilisation améliorée de la clé identifie l'objectif prévu du certificat et doit être répertorié comme « Authentification du serveur ». Ce champ est obligatoire lorsque vous utilisez le demandeur Microsoft pour PEAP et EAP-TLS. Lorsque vous utilisez les services de certificats Microsoft, ceci est configuré dans l'autorité de certification autonome avec la sélection du **certificat d'authentification du serveur** dans la liste déroulante Fonction prévue et dans l'autorité de certification d'entreprise avec la sélection du **serveur Web** dans la liste déroulante Modèle de certificat. Si vous demandez un certificat avec l'utilisation d'un CSR avec Microsoft Certificate Services, vous n'avez pas la possibilité de spécifier l'objectif prévu avec l'autorité de certification autonome. Par conséquent, le champ EKU est absent. Avec l'Autorité de certification d'entreprise, vous disposez de la liste déroulante Fonction prévue. Certaines autorités de certification ne créent pas de certificats avec un champ EKU. Elles sont donc inutiles lorsque vous utilisez le demandeur Microsoft EAP.



Certificats CA racine

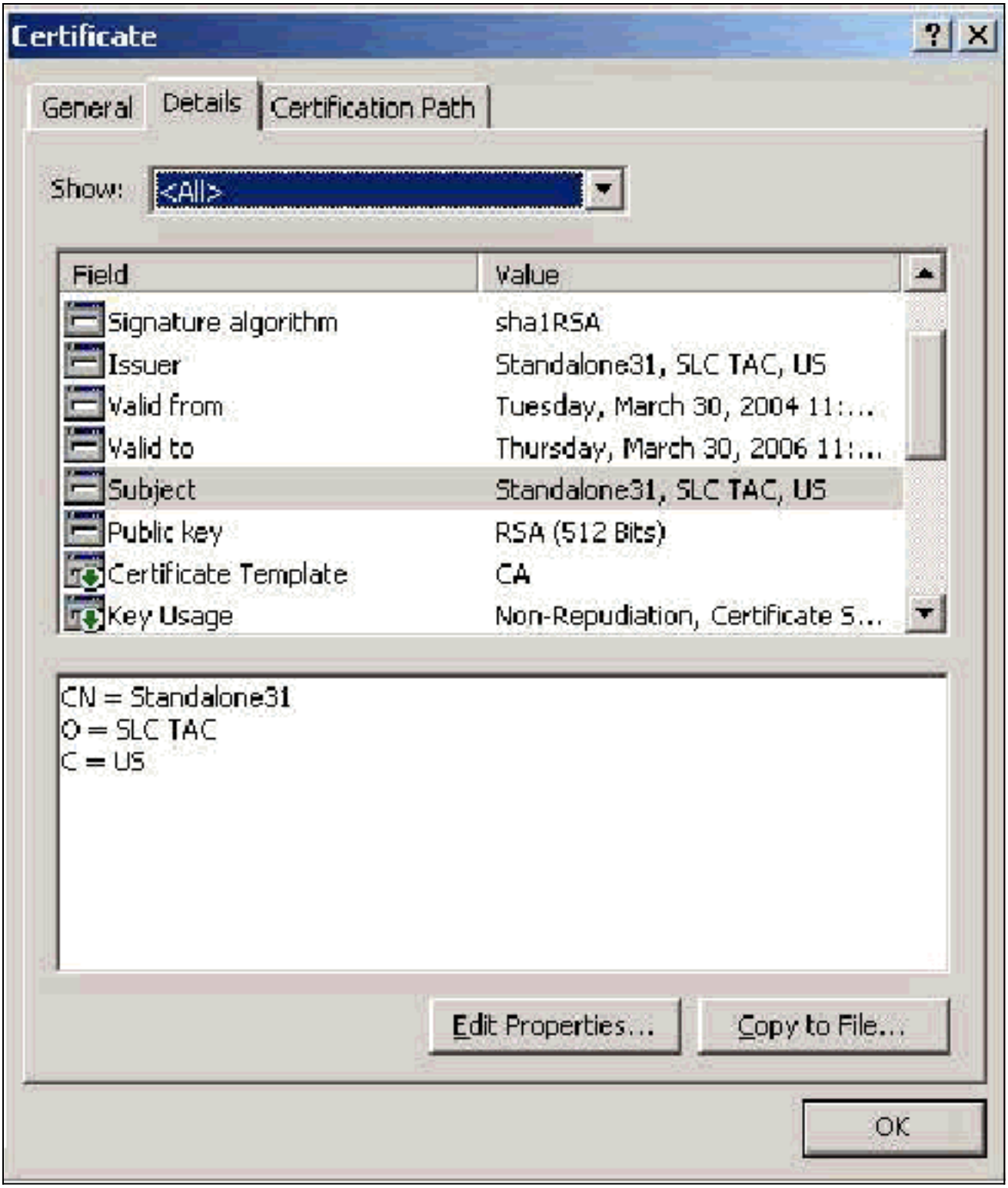
Le seul objectif du certificat d'autorité de certification racine est d'identifier le certificat de serveur (et le certificat d'autorité de certification intermédiaire, le cas échéant) comme certificat de confiance à ACS et au demandeur Windows EAP-MSCHAPv2. Il doit être situé dans le magasin Autorités de certification racines de confiance dans Windows sur le serveur ACS et, dans le cas d'EAP-MSCHAPv2, sur l'ordinateur client. La plupart des certificats d'autorité de certification racine tiers sont installés avec Windows et cela ne nécessite que peu d'efforts. Si Microsoft Certificate Services est utilisé et que le serveur de certificats se trouve sur la même machine qu'ACS, le certificat d'autorité de certification racine est installé automatiquement. Si le certificat d'autorité de certification racine est introuvable dans le magasin Autorités de certification racine de confiance de Windows, il doit être acquis de votre autorité de certification et installé. Une fois installé correctement dans le magasin de certificats Windows, le certificat d'autorité de certification racine doit apparaître dans le dossier **Certificats (Ordinateur local) > Autorités de certification**

racine de confiance > Certificats comme indiqué dans cet exemple de fenêtre.



Champs Objet et Émetteur

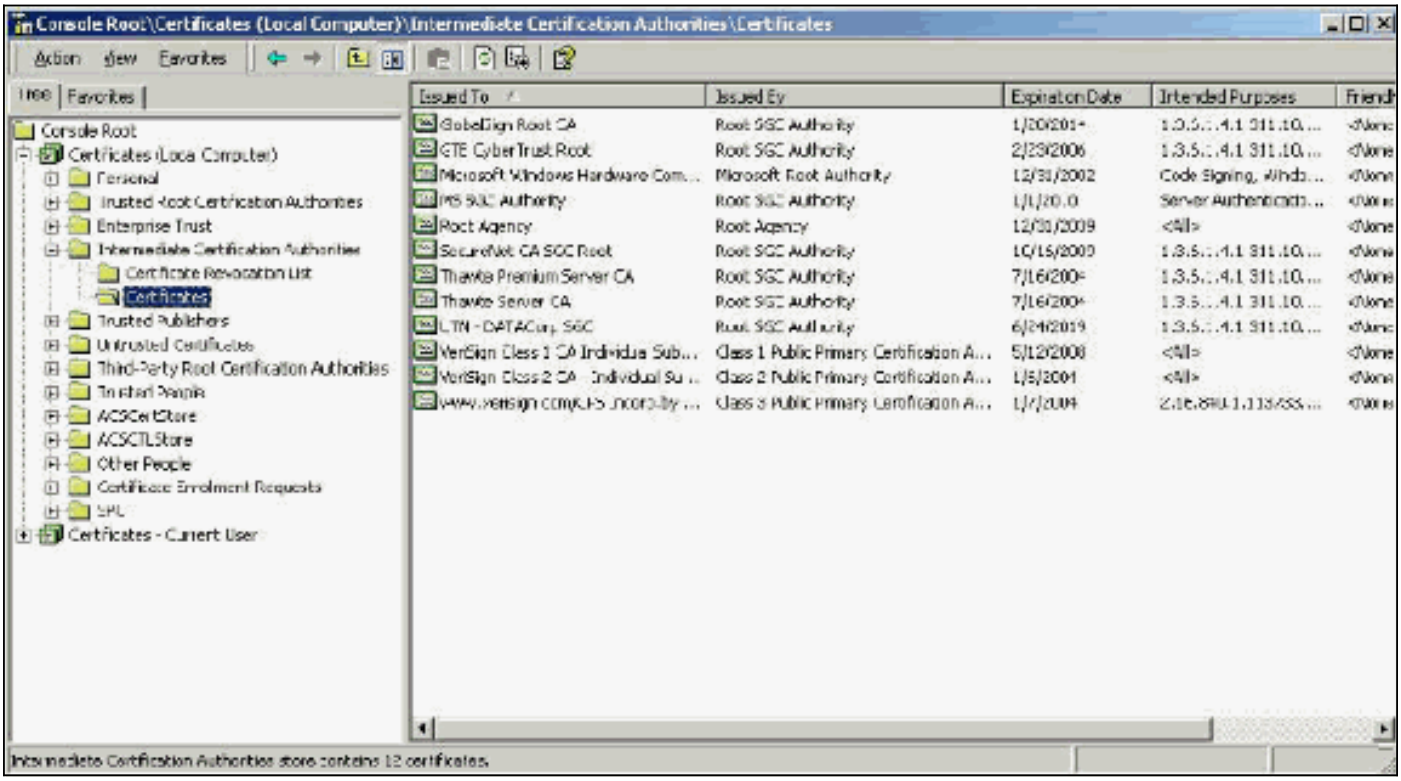
Les champs Objet et Émetteur identifient l'AC et doivent être exactement les mêmes. Utilisez ces champs pour renseigner les champs Émis et Émis par dans l'onglet Général du certificat. Ils sont renseignés avec le nom de l'autorité de certification racine.



Certificats CA intermédiaires

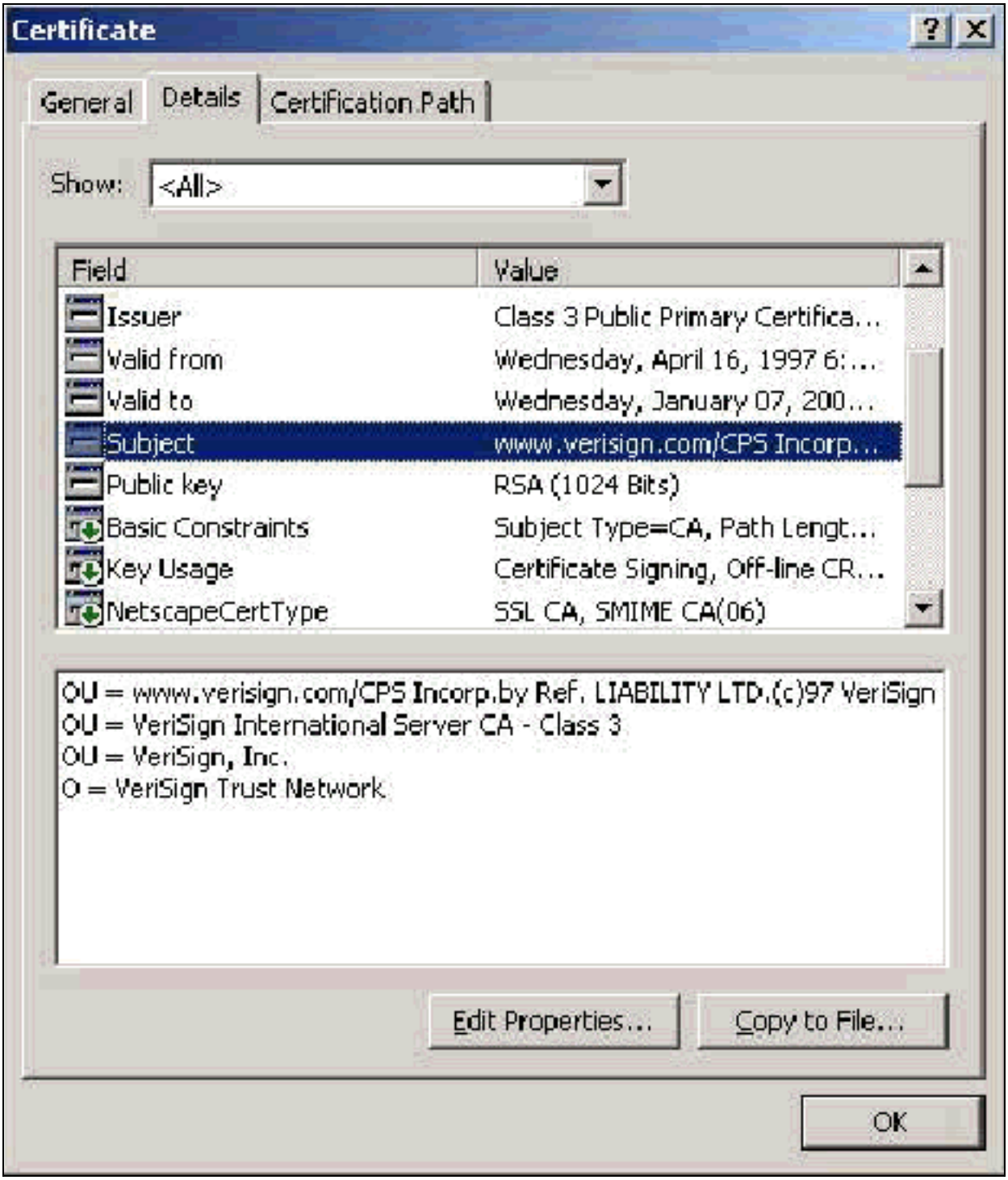
Les certificats CA intermédiaires sont des certificats que vous utilisez pour identifier une CA subordonnée à une CA racine. Certains certificats de serveur (certificats sans fil de Verisign) sont créés à l'aide d'une autorité de certification intermédiaire. Si un certificat de serveur coupé par une autorité de certification intermédiaire est utilisé, le certificat d'autorité de certification intermédiaire doit être installé dans la zone Autorités de certification intermédiaire du magasin de machines local sur le serveur ACS. En outre, si le demandeur EAP Microsoft est utilisé sur le client, le certificat d'autorité de certification racine de l'autorité de certification racine qui a créé le certificat d'autorité de certification intermédiaire doit également se trouver dans le magasin approprié sur le serveur et le client ACS afin que la chaîne de confiance puisse être établie. Le certificat d'autorité

de certification racine et le certificat d'autorité de certification intermédiaire doivent être marqués comme approuvés dans ACS et sur le client. La plupart des certificats d'autorité de certification intermédiaire ne sont pas installés avec Windows. Il est donc probable que vous ayez besoin de les acquérir auprès du fournisseur. Une fois installé correctement dans le magasin de certificats Windows, le certificat de l'autorité de certification intermédiaire apparaît dans le dossier **Certificats (Ordinateur local) > Autorités de certification intermédiaire > Certificats** comme indiqué dans cet exemple de fenêtre.



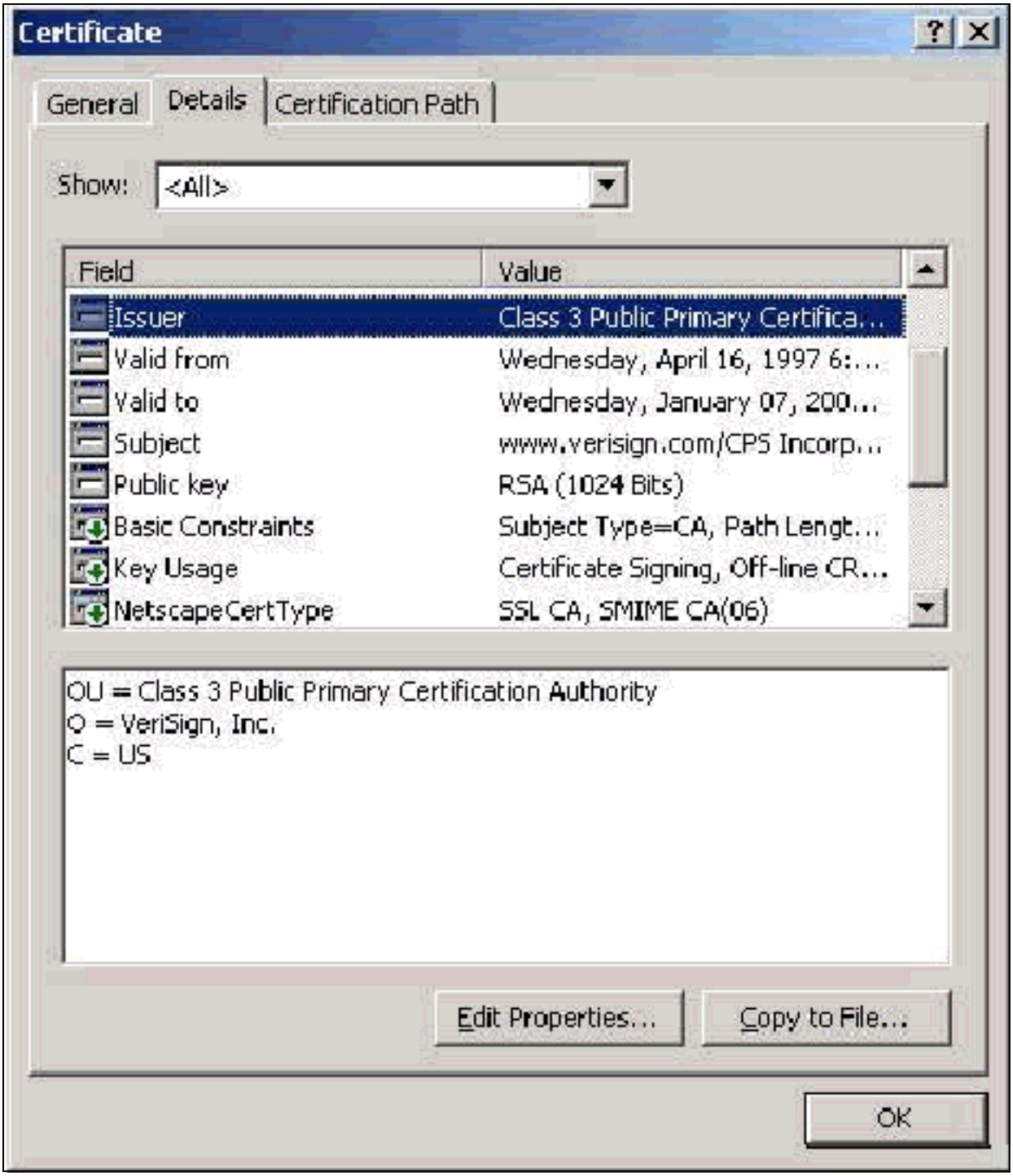
Champ Objet

Le champ Objet identifie l'autorité de certification intermédiaire. Cette valeur est utilisée pour déterminer le champ Émis à dans l'onglet Général du certificat.



Champ Émetteur

Le champ Émetteur identifie l'autorité de certification qui a supprimé le certificat. Utilisez cette valeur afin de déterminer la valeur du champ Émis par dans l'onglet Général du certificat. Il est renseigné avec le nom de l'autorité de certification.



Certificats client

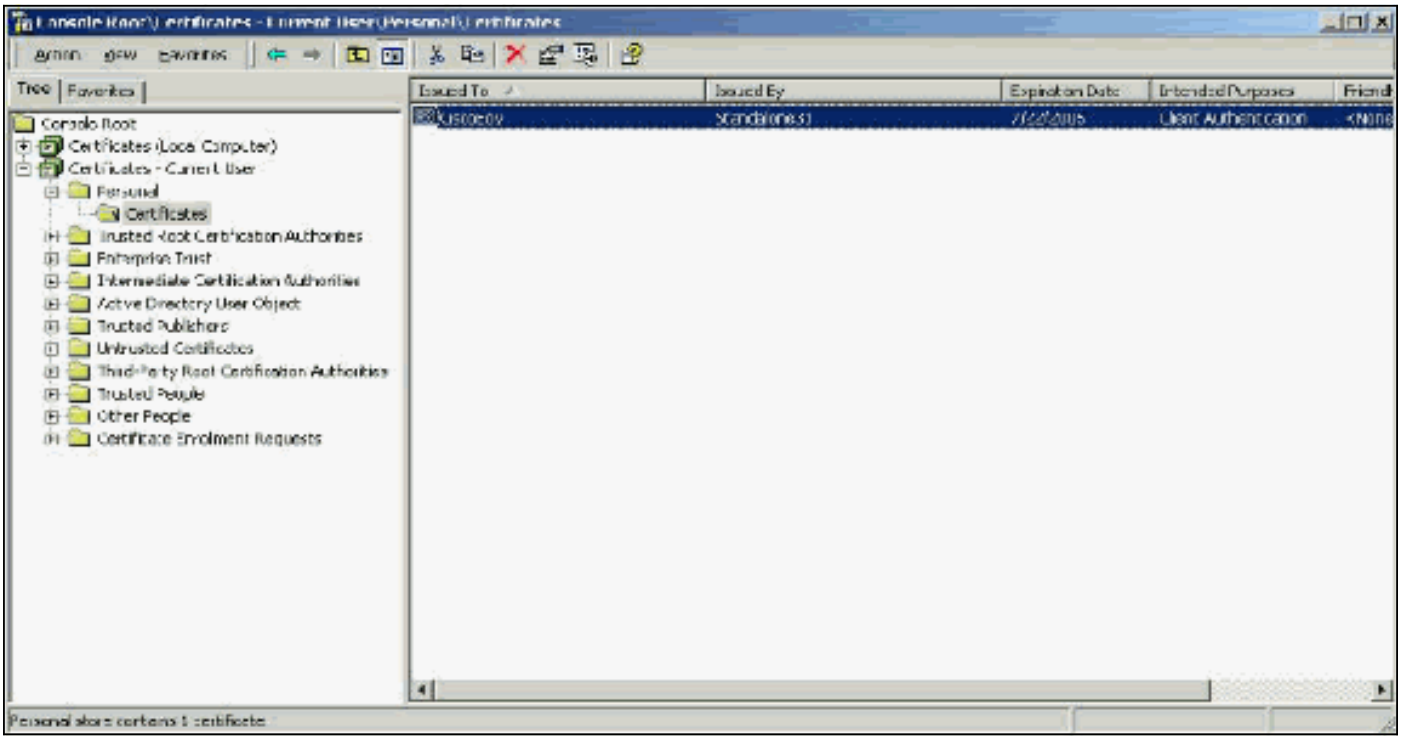
Les certificats client sont utilisés pour identifier positivement l'utilisateur dans EAP-TLS. Ils n'ont aucun rôle dans la construction du tunnel TLS et ne sont pas utilisés pour le chiffrement. L'identification positive se fait par l'un des trois moyens suivants :

- **Comparaison CN (ou Name)** : compare le CN du certificat au nom d'utilisateur de la base de données. Plus d'informations sur ce type de comparaison sont incluses dans la description du champ Objet du certificat.
- **Comparaison SAN** : compare le SAN du certificat avec le nom d'utilisateur de la base de données. Cette fonctionnalité n'est prise en charge qu'à partir de ACS 3.2. Plus d'informations sur ce type de comparaison sont incluses dans la description du champ Nom alternatif du sujet du certificat.

- **Comparaison binaire** : compare le certificat à une copie binaire du certificat stocké dans la base de données (seuls AD et LDAP peuvent le faire). Si vous utilisez la comparaison binaire de certificat, vous devez stocker le certificat utilisateur au format binaire. En outre, pour LDAP générique et Active Directory, l'attribut qui stocke le certificat doit être l'attribut LDAP standard nommé « usercertificate ».

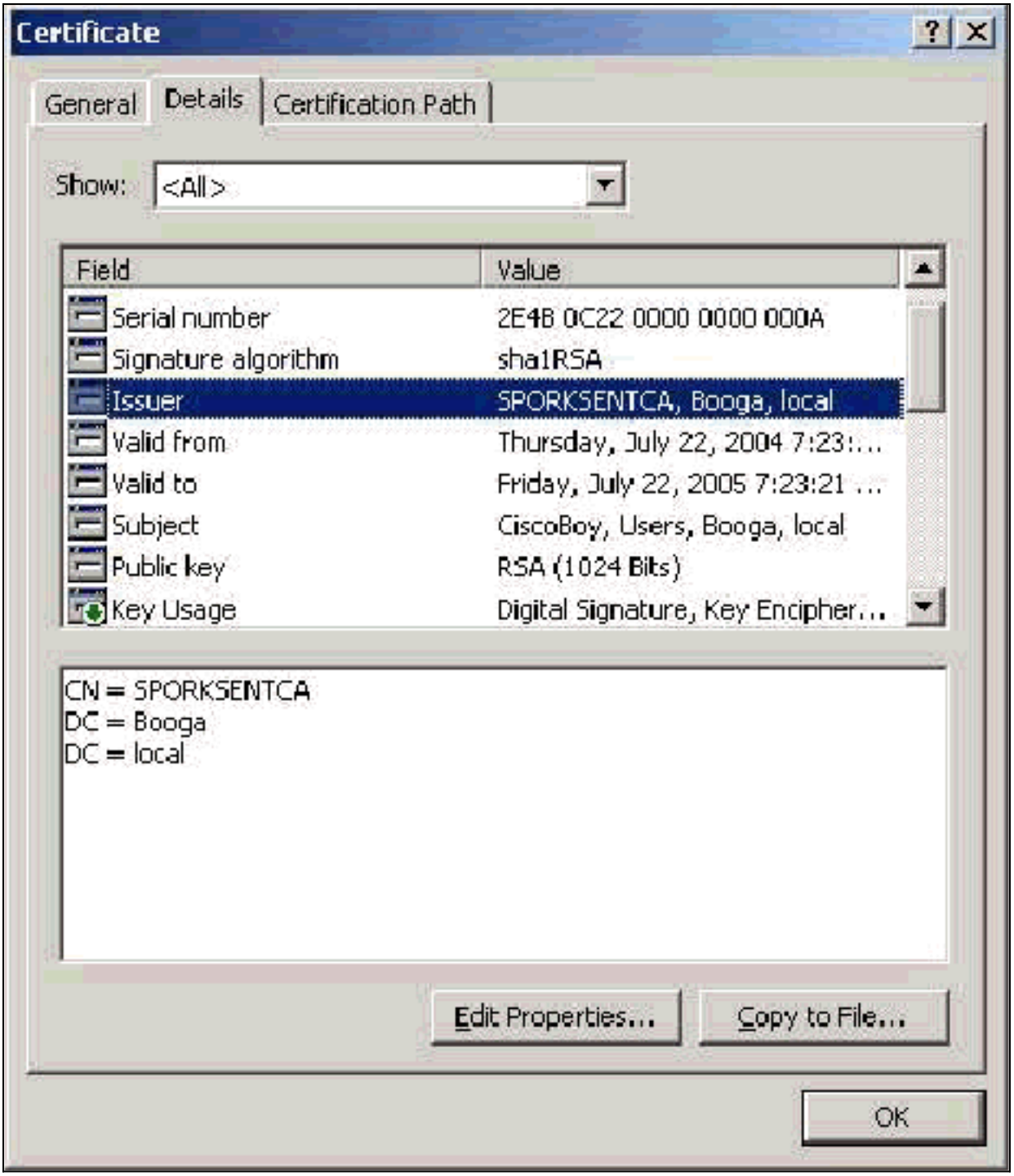
Quelle que soit la méthode de comparaison utilisée, les informations du champ approprié (CN ou SAN) doivent correspondre au nom utilisé par votre base de données pour l'authentification. AD utilise le nom NetBios pour l'authentification en mode mixte et l'UPN en mode natif.

Cette section traite de la génération de certificats client à l'aide de Microsoft Certificate Services. EAP-TLS nécessite un certificat client unique pour que chaque utilisateur puisse être authentifié. Le certificat doit être installé sur chaque ordinateur pour chaque utilisateur. Une fois installé correctement, le certificat se trouve dans le dossier **Certificats -Utilisateur actuel > Personnel > Certificats** comme indiqué dans cet exemple de fenêtre.



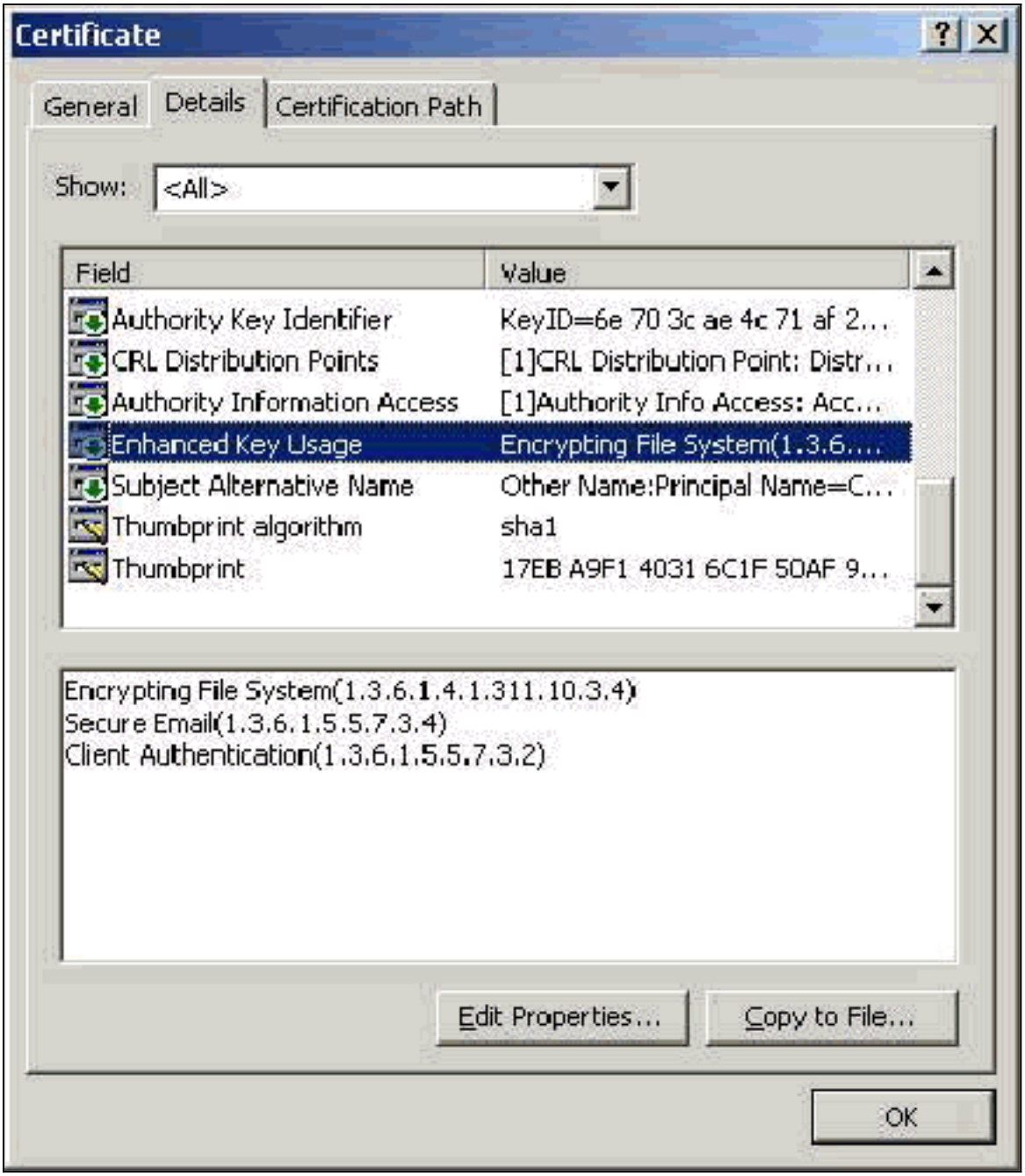
Champ Émetteur

Le champ Émetteur identifie l'autorité de certification qui coupe le certificat. Utilisez cette valeur afin de déterminer la valeur du champ Émis par dans l'onglet Général du certificat. Le nom de l'autorité de certification est renseigné.



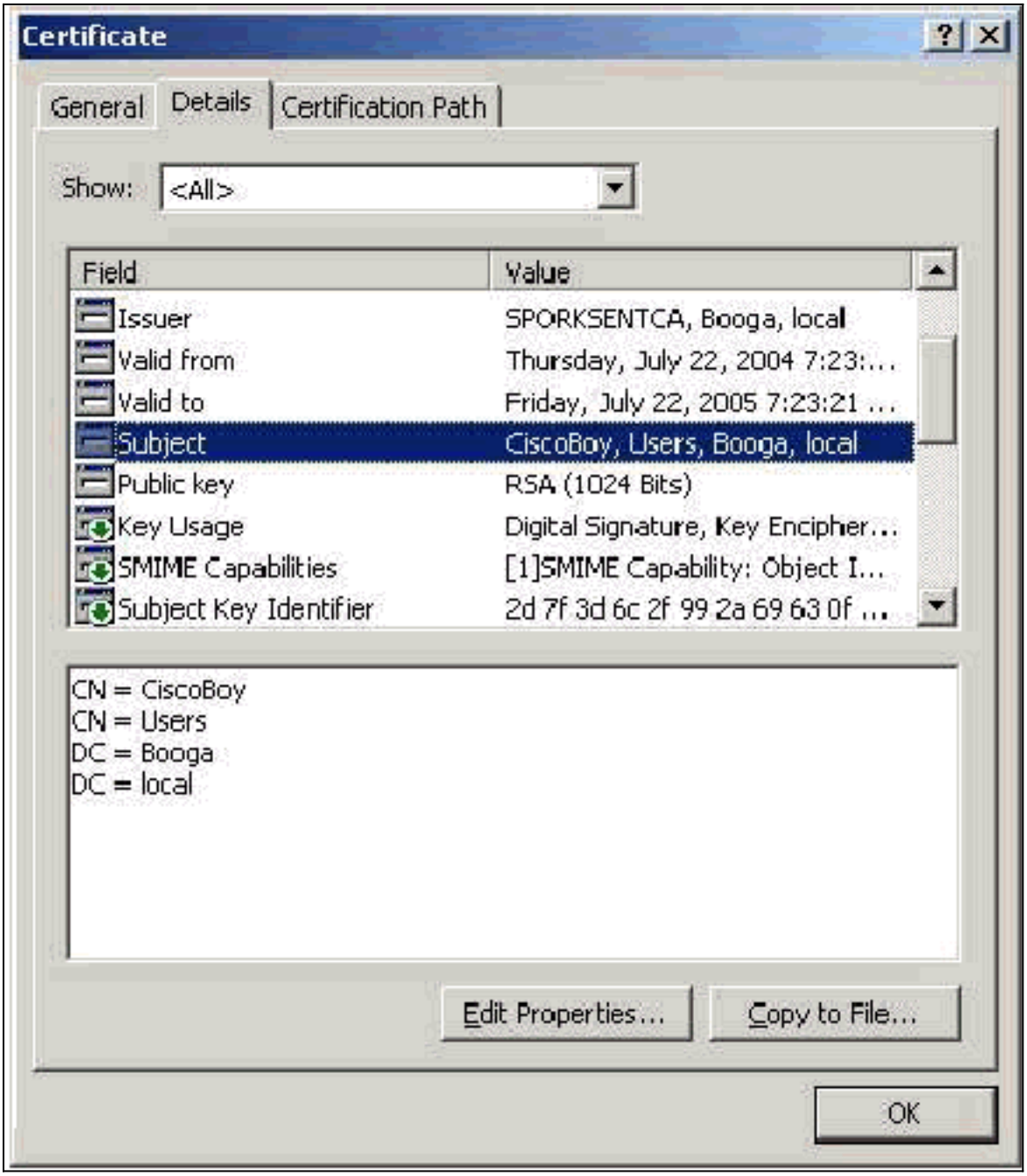
Champ Utilisation de clé améliorée

Le champ Utilisation améliorée de la clé identifie l'objectif prévu du certificat et doit contenir l'authentification du client. Ce champ est obligatoire lorsque vous utilisez le demandeur Microsoft pour PEAP et EAP-TLS. Lorsque vous utilisez Microsoft Certificate Services, ceci est configuré dans l'autorité de certification autonome lorsque vous sélectionnez **Client Authentication Certificate** dans la liste déroulante Fonction prévue et dans l'autorité de certification d'entreprise lorsque vous sélectionnez **User** dans la liste déroulante Modèle de certificat. Si vous demandez un certificat avec l'utilisation d'un CSR avec Microsoft Certificate Services, vous n'avez pas la possibilité de spécifier l'objectif prévu avec l'autorité de certification autonome. Par conséquent, le champ EKU est absent. Avec l'Autorité de certification d'entreprise, vous disposez de la liste déroulante Fonction prévue. Certaines autorités de certification ne créent pas de certificats avec un champ EKU. Ils sont inutiles lorsque vous utilisez le demandeur Microsoft EAP.



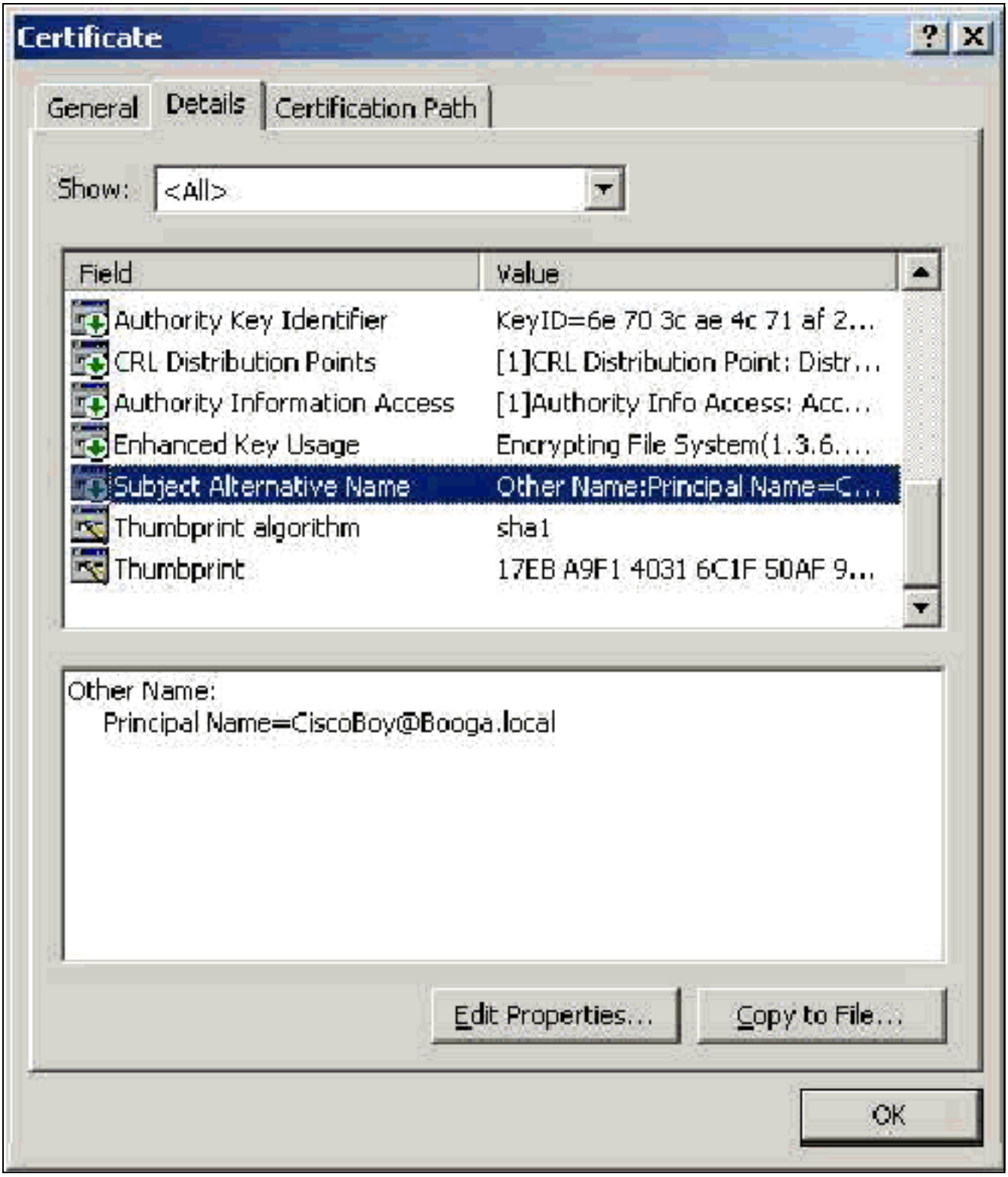
Champ Objet

Ce champ est utilisé dans la comparaison CN. Le premier CN répertorié est comparé à la base de données pour trouver une correspondance. Si une correspondance est trouvée, l'authentification réussit. Si vous utilisez une autorité de certification autonome, le CN est renseigné avec tout ce que vous mettez dans le champ Nom du formulaire de soumission de certificat. Si vous utilisez l'autorité de certification d'entreprise, le CN est automatiquement renseigné avec le nom du compte tel qu'il est indiqué dans la console Utilisateurs et ordinateurs Active Directory (cela ne correspond pas nécessairement au nom UPN ou NetBios).



Champ Nom alternatif de l'objet

Le champ Subject Alternative Name est utilisé dans la comparaison SAN. Le SAN répertorié est comparé à la base de données pour trouver une correspondance. Si une correspondance est trouvée, l'authentification réussit. Si vous utilisez l'autorité de certification d'entreprise, le SAN est automatiquement renseigné avec le nom d'ouverture de session Active Directory @domain (UPN). L'autorité de certification autonome n'inclut pas de champ SAN. Vous ne pouvez donc pas utiliser la comparaison SAN.



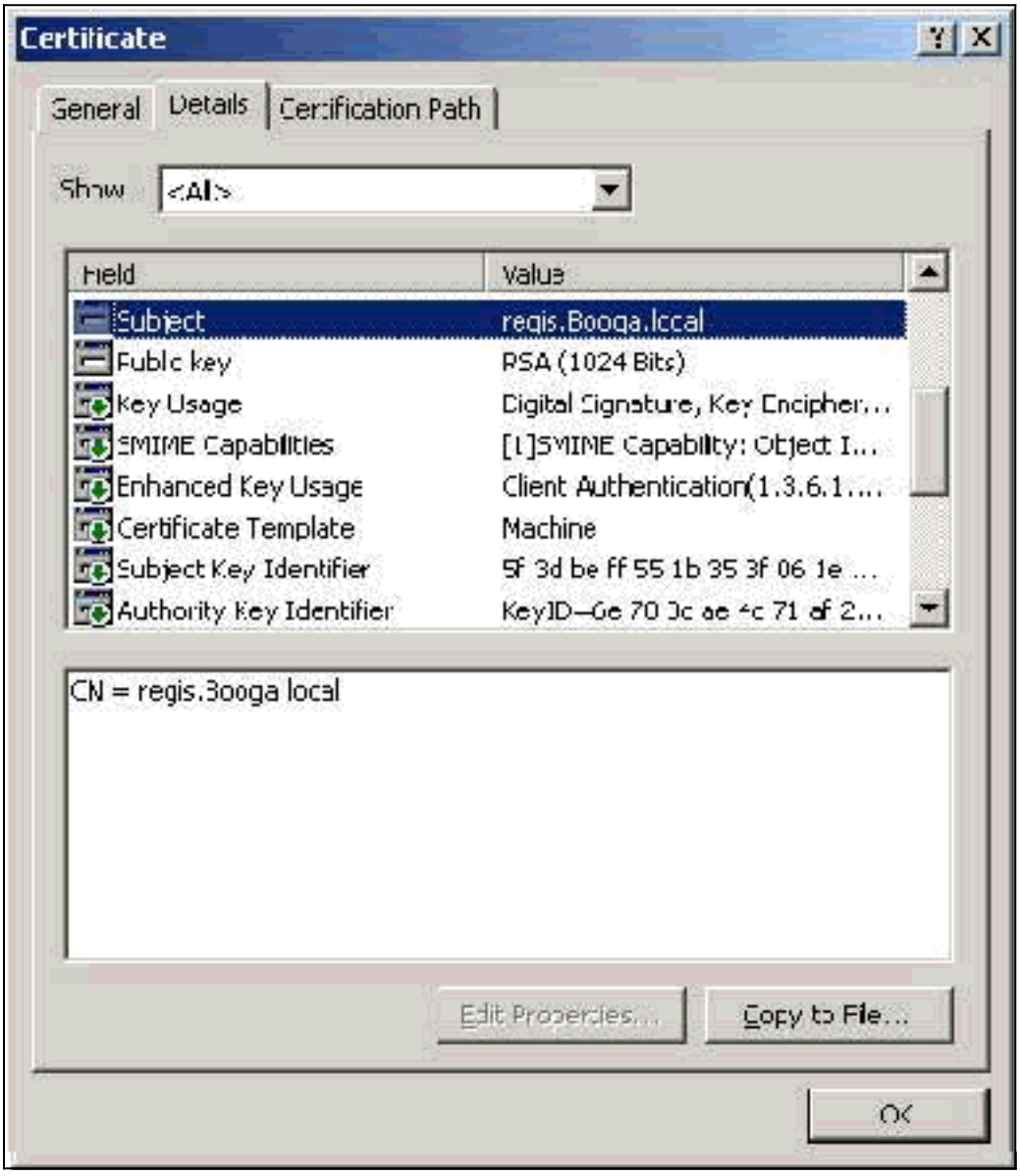
Certificats de machine

Les certificats de machine sont utilisés dans EAP-TLS pour identifier positivement l'ordinateur lorsque vous utilisez l'authentification de machine. Vous ne pouvez accéder à ces certificats que lorsque vous configurez votre autorité de certification Microsoft Enterprise pour l'inscription automatique des certificats et que vous joignez l'ordinateur au domaine. Le certificat est automatiquement créé lorsque vous utilisez les informations d'identification Active Directory de l'ordinateur et que vous les installez dans le magasin d'ordinateurs local. Les ordinateurs qui sont déjà membres du domaine avant de configurer l'inscription automatique reçoivent un certificat lors du prochain redémarrage de Windows. Le certificat d'ordinateur est installé dans le dossier **Certificates (Local Computer) > Personal > Certificates** du composant logiciel enfichable MMC

Certificates (Local Computer), tout comme les certificats de serveur. Vous ne pouvez pas installer ces certificats sur un autre ordinateur, car vous ne pouvez pas exporter la clé privée.

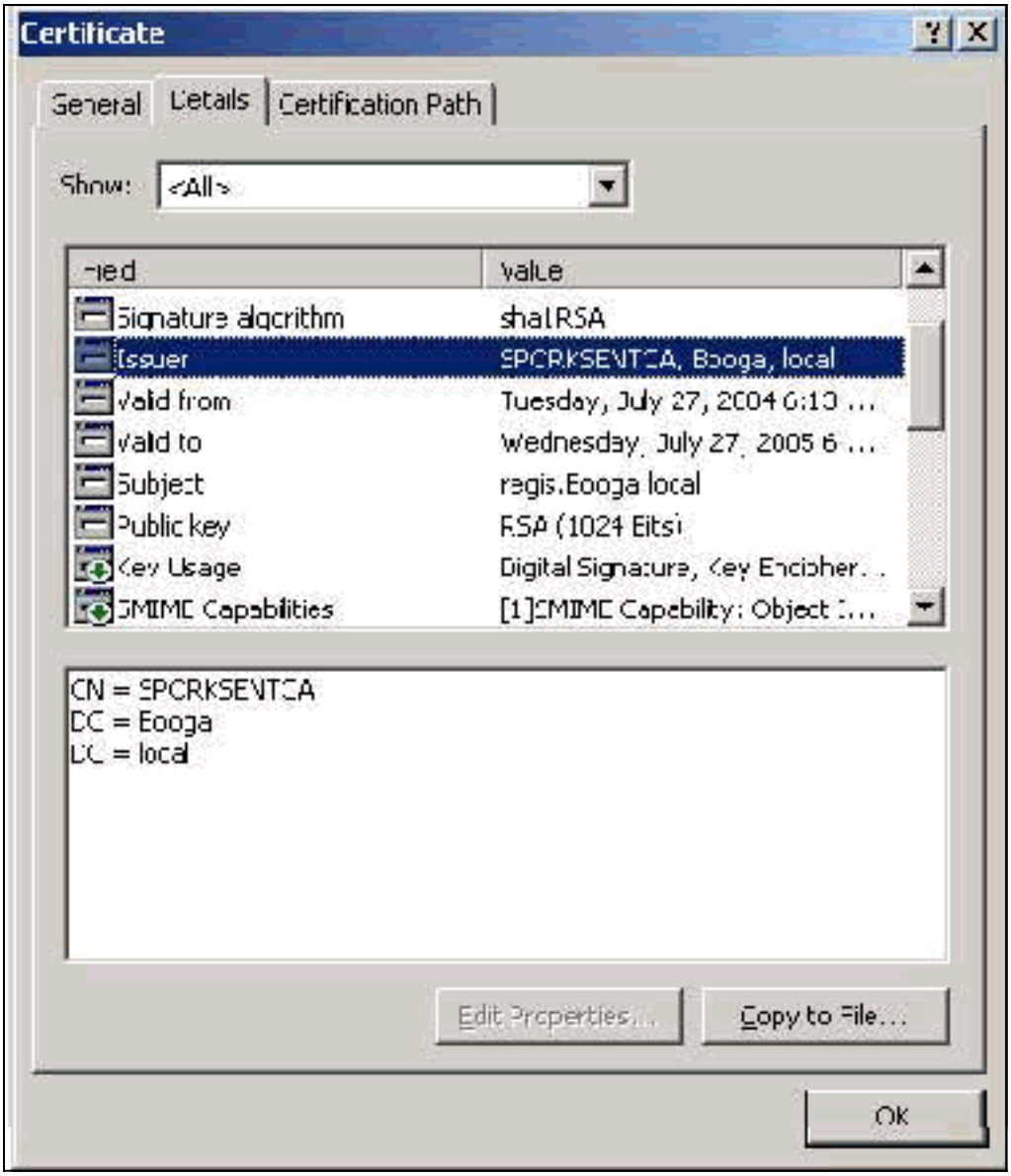
Objet et champs SAN

Les champs Subject et SAN identifient l'ordinateur. La valeur est renseignée par le nom complet de l'ordinateur et est utilisée afin de déterminer le champ Émis à dans l'onglet Général du certificat et est identique pour les champs Objet et SAN.



Champ Émetteur

Le champ Émetteur identifie l'autorité de certification qui a supprimé le certificat. Utilisez cette valeur afin de déterminer la valeur du champ Émis par dans l'onglet Général du certificat. Il est renseigné avec le nom de l'autorité de certification.



Annexe A - Extensions de certificat communes

.csr : il ne s'agit pas d'un certificat mais d'une demande de signature de certificat. Il s'agit d'un fichier texte brut au format suivant :

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

.pvk : cette extension indique une clé privée, mais elle ne garantit pas que le contenu est en fait une clé privée. Le contenu doit être en texte brut avec ce format :

```
-----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 : il s'agit d'une extension générique qui désigne un certificat. Les certificats de serveur, d'autorité de certification racine et d'autorité de certification intermédiaire peuvent être dans ce format. Il s'agit généralement d'un fichier texte brut avec une extension que vous pouvez modifier selon vos besoins et qui peut être au format DER ou Base 64. Vous pouvez importer ce format dans le magasin de certificats Windows.

.pem : cette extension signifie Privacy Enhanced Mail. Cette extension est couramment utilisée avec UNIX, Linux, BSD, etc. Il est généralement utilisé pour les certificats de serveur et les clés privées, et il s'agit généralement d'un fichier texte brut avec une extension que vous pouvez modifier selon vos besoins de .pem à .cer afin de pouvoir l'importer dans le magasin de certificats Windows.

Le contenu interne des fichiers .cer et .pem ressemble généralement à la sortie suivante :

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

.pfx : cette extension correspond à Personal Information Exchange. Ce format est une méthode que vous pouvez utiliser pour regrouper des certificats dans un seul fichier. Par exemple, vous pouvez regrouper un certificat de serveur et sa clé privée associée et le certificat d'autorité de certification racine dans un seul fichier et importer facilement le fichier dans le magasin de certificats Windows approprié. Il est généralement utilisé pour les certificats serveur et client. Malheureusement, si un certificat d'autorité de certification racine est inclus, le certificat d'autorité de certification racine est toujours installé dans le magasin d'utilisateurs actuels au lieu du magasin d'ordinateurs locaux, même si le magasin d'ordinateurs locaux est spécifié pour l'installation.

.p12 : ce format n'est généralement visible qu'avec un certificat client. Vous pouvez importer ce format dans le magasin de certificats Windows.

.p7b : format supplémentaire qui stocke plusieurs certificats dans un fichier. Vous pouvez importer ce format dans le magasin de certificats Windows.

Annexe B - Conversion du format du certificat

Dans la plupart des cas, la conversion de certificat se produit lorsque vous modifiez l'extension

(par exemple, de .pem à .cer), car les certificats sont généralement au format texte brut. Parfois, un certificat n'est pas en texte clair et vous devez le convertir à l'aide d'un outil tel que OpenSSL . Par exemple, ACS Solution Engine ne peut pas installer de certificats au format .pfx. Par conséquent, vous devez convertir le certificat et la clé privée dans un format utilisable. Voici la syntaxe de commande de base pour OpenSSL :

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

Vous êtes invité à saisir le mot de passe d'importation et la phrase de passe PEM. Ces mots de passe doivent être identiques et correspondre au mot de passe de clé privée spécifié lors de l'exportation de .pfx. La sortie est un fichier .pem unique qui inclut tous les certificats et les clés privées dans le fichier .pfx. Ce fichier peut être appelé dans ACS à la fois certificat et clé privée et il s'installe sans problème.

Annexe C - Période de validité du certificat

Un certificat n'est utilisable que pendant sa période de validité. La période de validité d'un certificat d'autorité de certification racine est déterminée lorsque l'autorité de certification racine est établie et peut varier. La période de validité d'un certificat d'autorité de certification intermédiaire est déterminée lorsque l'autorité de certification est établie et ne peut pas dépasser la période de validité de l'autorité de certification racine à laquelle elle est subordonnée. La période de validité des certificats serveur, client et machine est automatiquement définie sur un an avec les services de certificats Microsoft. Ceci ne peut être modifié que lorsque vous piratez le Registre Windows conformément à l'article 254632 de la Base de connaissances Microsoft et que vous ne pouvez pas dépasser la période de validité de l'autorité de certification racine. La période de validité des certificats auto-signés générés par ACS est toujours d'un an et ne peut pas être modifiée dans les versions actuelles.

Informations connexes

- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems