EAP Version 1.01 Certificate Guide

Document ID: 64062

Contents

Introduction

This document clarifies some of the confusion that accompanies the various certificate types, formats, and requirements associated with the various forms of Extensible Authentication Protocol (EAP). The five certificate types related to EAP that this document discusses are Server, Root CA, Intermediate CA, Client, and Machine. These certificates are found in various formats and there can be differing requirements with relation to each of them based on the EAP implementation involved.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Server Certificates

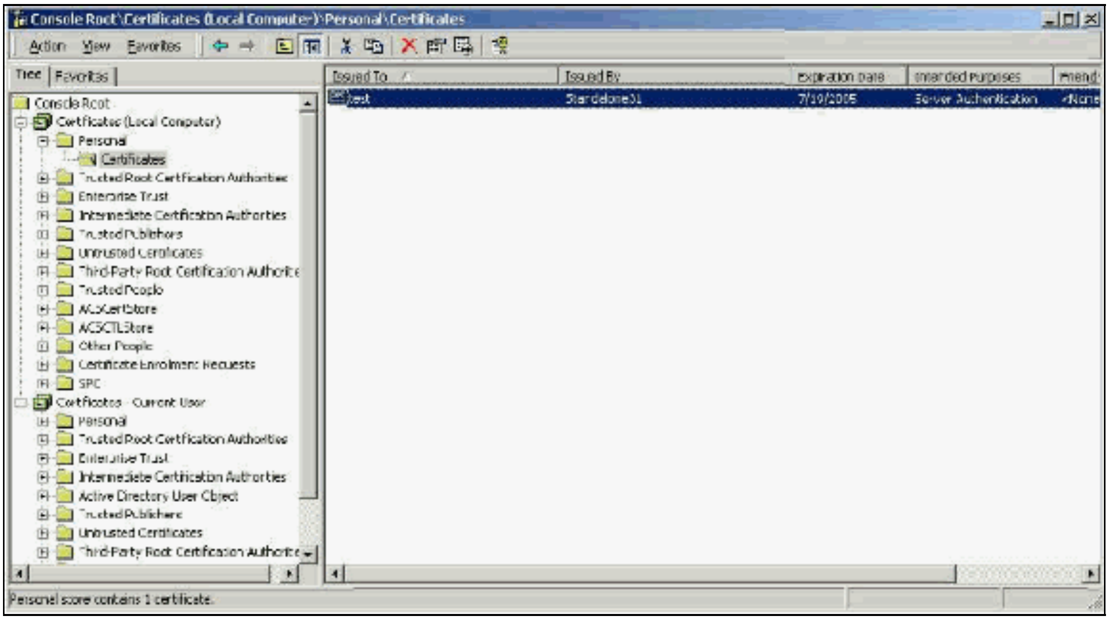
The Server Certificate is installed on the RADIUS server and its primary purpose in EAP is to create the encrypted Transport Layer Security (TLS) tunnel which protects authentication information. When you use EAP−MSCHAPv2, the Server Certificate takes on a secondary role which is to identify the RADIUS server as a trusted entity for authentication. This secondary role is accomplished through the use of the Enhanced Key Usage (EKU) field. The EKU field identifies the certificate as a valid Server Certificate and verifies that the root CA that issued the certificate is a trusted root CA. This requires the presence of the Root CA Certificate. Cisco Secure ACS requires that the certificate be either Base64−encoded or DER−encoded binary X.509 v3 format.

You can create this certificate with either the use of a certificate signing request (CSR) in ACS, which is submitted to a CA. Or, you can also cut the certificate with the use of an in−house CA (like Microsoft Certificate Services) certificate creation form. It is important to note that, while you can create the server certificate with key sizes larger than 1024, any key larger than 1024 does not work with PEAP. The client hangs even if authentication passes.

If you create the certificate with the use of a CSR, it is created with a .cer, .pem, or .txt format. On rare occasions, it is created with no extension. Ensure that your certificate is a plain text file with an extension that you can change as needed (the ACS appliance uses the .cer or .pem extension). Additionally, if you use a CSR, the private key of the certificate is created in the path you specify as a separate file which may or may not have an extension and which has a password associated with it (the password is required for installation on ACS). Regardless of the extension, ensure that it is a plain text file with an extension that you can change as needed (the ACS appliance uses the .pvk or .pem extension). If no path is specified for the private key, ACS saves the key in the C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs directory and looks in this directory if no path is specified for the private key file when you install the certificate.

If the certificate is created with the use of the Microsoft Certificate Services certificate submittal form, ensure that you mark the keys as exportable so that you can install the certificate in ACS. The creation of a certificate in this manner simplifies the installation process significantly. You can directly install it into the proper Windows store from the Certificate Services web interface and then install on ACS from storage with the use of the CN as reference. A certificate installed in the local computer store can also be exported from the Windows storage and installed on another computer with ease. When this type of certificate is exported, the keys need to be marked as exportable and given a password. The certificate then appears in .pfx format which includes the private key and the server certificate.

When correctly installed in the Windows certificate store, the Server Certificate needs to appear in the **Certificates (Local Computer) > Personal > Certificates** folder as seen in this example window.


Console Root\Certificates (Local Computer)\Personal\Certificates
Action
View
Favorites
Tree
Favorites
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
ACSCertStore
ACSCTLStore
Other People
Certificate Enrolment Requests
SPC
Certificates - Current User
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities

Issued To	Issued By	Expiration Date	Intended Purposes	Friend
test	Standalone31	7/19/2005	Server Authentication	<None

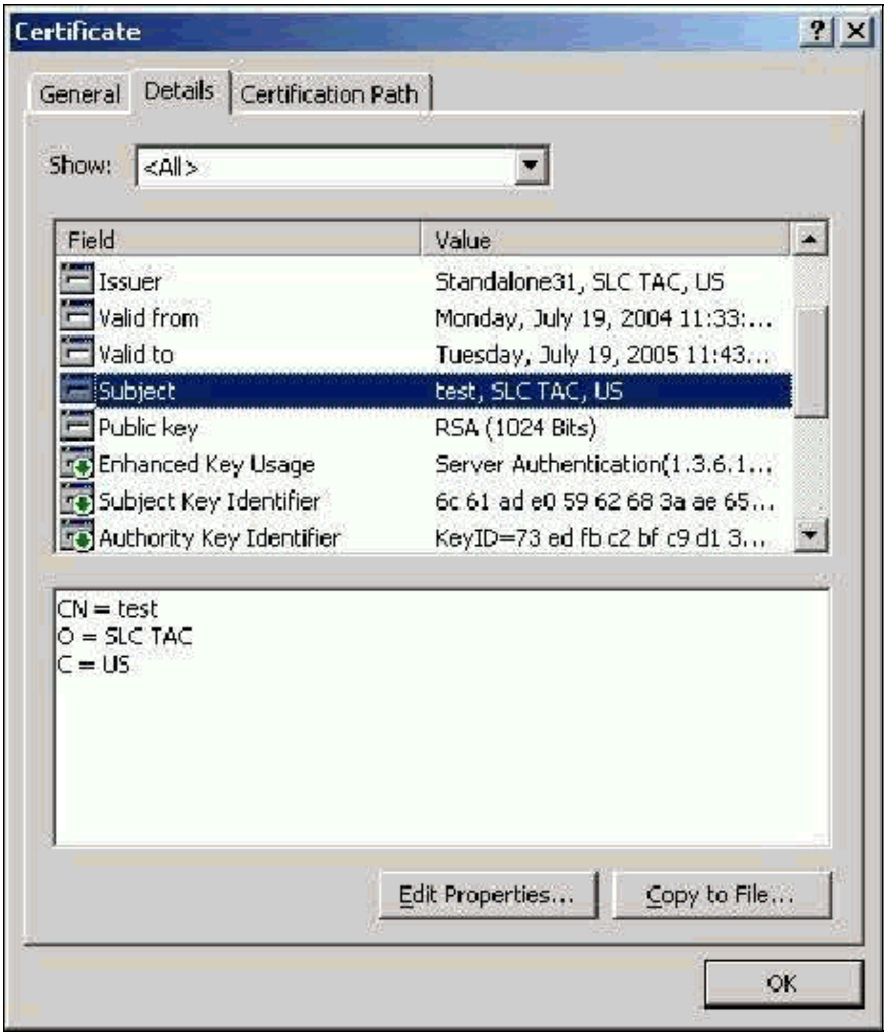
Personal store contains 1 certificate.

Self−signed certificates are certificates you create without a root or the intermediate involvement of the CA. They have the same value in both the subject and issuer fields like a Root CA Certificate. Most self−signed certificates use X.509 v1 format. Therefore, they do not work with ACS. However, as of version 3.3, ACS has the ability to create its own self−signed certificates which you can use for EAP−TLS and PEAP. Do not use a key size greater than 1024 for compatibility with PEAP and EAP−TLS. If you use a self−signed certificate, the certificate also acts in the capacity of the Root CA Certificate and must be installed in the **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** folder of the client when you use the Microsoft EAP supplicant. It automatically installs in the trusted root certificates store on the server. However, it must still be trusted in the Certificate Trust List in ACS Certificate Setup. See the Root CA Certificates section for more information.

Because self−signed certificates are used as the Root CA Certificate for Server Certificate validation when you use the Microsoft EAP supplicant, and because the validity period cannot be increased from the default of one year, Cisco recommends that you only use them for EAP as a temporary measure until you can use a traditional CA.

Subject Field

The Subject field identifies the certificate. The CN value is used to determine the Issued to field in the General tab of the certificate and is populated with the information that you enter into the Certificate subject field in ACS"CSR dialogue or with the information from the Name field in Microsoft Certificate Services. The CN value is used to tell ACS what certificate it needs to use from the local machine certificate store if the option to install the certificate from storage is used.



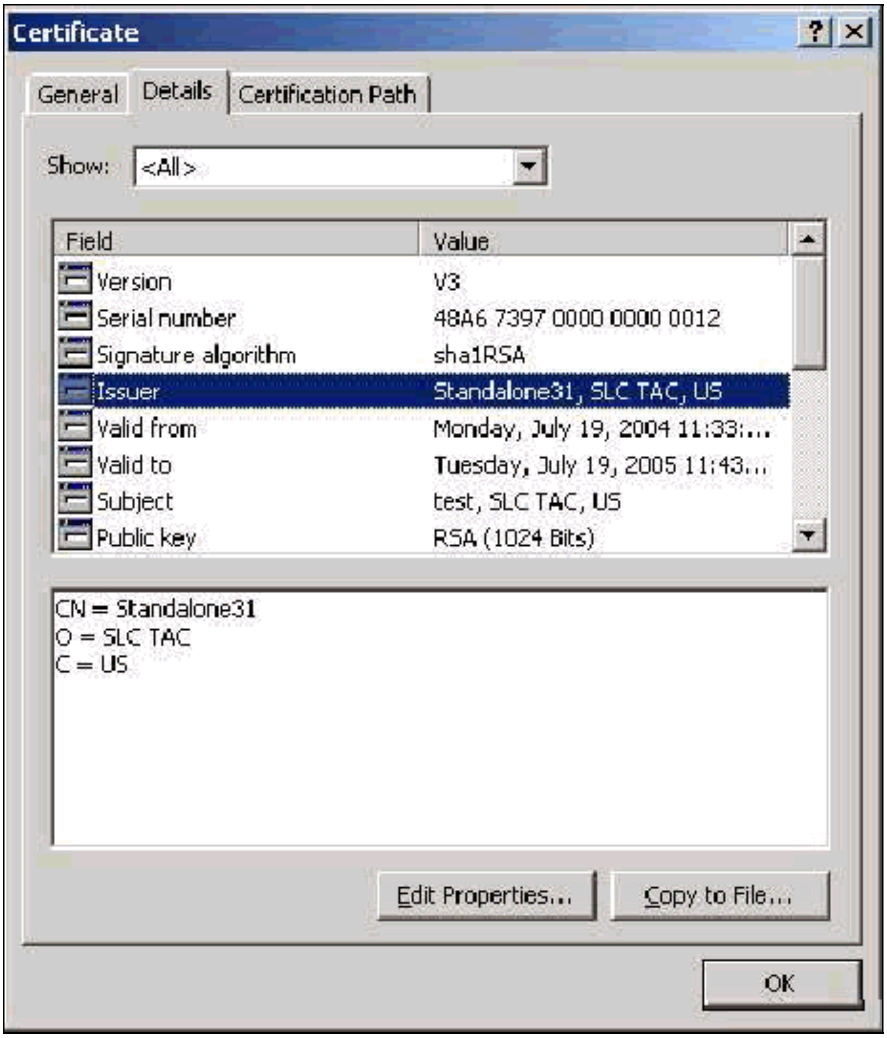
Show: <All>

Field	Value
Issuer	Standalone31, SLC TAC, US
Valid from	Monday, July 19, 2004 11:33:...
Valid to	Tuesday, July 19, 2005 11:43:...
Subject	test, SLC TAC, US
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication(1.3.6.1...
Subject Key Identifier	6c 61 ad e0 59 62 68 3a ae 65...
Authority Key Identifier	KeyID=73 ed fb c2 bf c9 d1 3...

```
CN = test
O = SLC TAC
C = US
```

Issuer Field

The Issuer field identifies the CA that cut the certificate. Use this value in order to determine the value of the Issued by field in the General tab of the certificate. It is populated with the name of the CA.



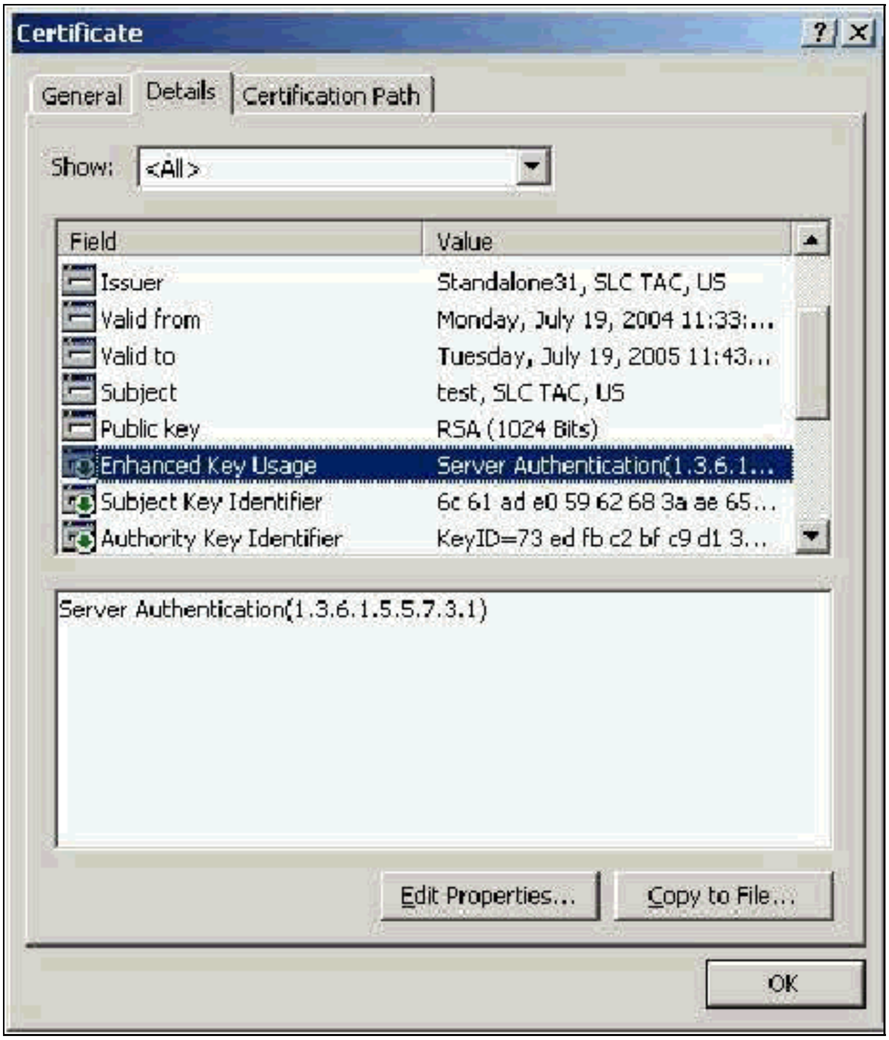
Show: <All>

Field	Value
Version	V3
Serial number	48A6 7397 0000 0000 0012
Signature algorithm	sha1RSA
Issuer	Standalone31, SLC TAC, US
Valid from	Monday, July 19, 2004 11:33:...
Valid to	Tuesday, July 19, 2005 11:43...
Subject	test, SLC TAC, US
Public key	RSA (1024 Bits)

CN = Standalone31
O = SLC TAC
C = US

Enhanced Key Usage Field

The Enhanced Key Usage field identifies the intended purpose of the certificate and needs to be listed as "Server Authentication". This field is mandatory when you use the Microsoft supplicant for PEAP and EAP−TLS. When you use Microsoft Certificate Services, this is configured in the Standalone CA with the selection of **Server Authentication Certificate** from the Intended Purpose drop−down and in the Enterprise CA with the selection of **Web Server** from the Certificate Template drop−down. If you request a certificate with the use of a CSR with Microsoft Certificate Services, you do not have the option to specify the Intended Purpose with the Standalone CA. Therefore, the EKU field is absent. With the Enterprise CA, you have the Intended Purpose drop−down. Some CAs do not create certificates with an EKU field so they are useless when you use the Microsoft EAP supplicant.

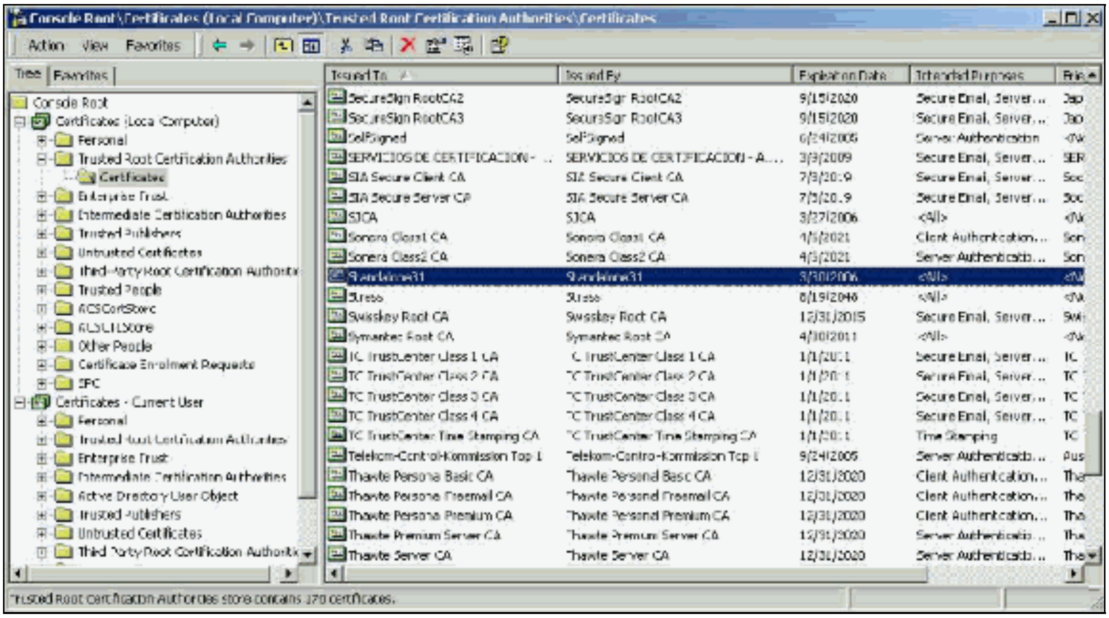


Field	Value
Issuer	Standalone31, SLC TAC, US
Valid from	Monday, July 19, 2004 11:33:...
Valid to	Tuesday, July 19, 2005 11:43...
Subject	test, SLC TAC, US
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication(1.3.6.1...
Subject Key Identifier	6c 61 ad e0 59 62 68 3a ae 65...
Authority Key Identifier	KeyID=73 ed fb c2 bf c9 d1 3...

Server Authentication(1.3.6.1.5.5.7.3.1)

Root CA Certificates

The one purpose of the Root CA Certificate is to identify the Server Certificate (and Intermediate CA Certificate if applicable) as a trusted certificate to ACS and to the Windows EAP−MSCHAPv2 supplicant. It must be located in the Trusted Root Certification Authorities store in Windows on both the ACS server and, in the case of EAP−MSCHAPv2, on the client computer. Most third party Root CA Certificates are installed with Windows and there is little effort involved with this. If Microsoft Certificate Services is used and the certificate server is on the same machine as ACS, then the Root CA Certificate is installed automatically. If the Root CA Certificate is not found in the Trusted Root Certification Authorities store in Windows, then it must be acquired from your CA and installed. When correctly installed in the Windows certificate store, the Root CA Certificate needs to appear in the **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** folder as seen in this example window.



Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates
Action View Favorites
Tree Favorites

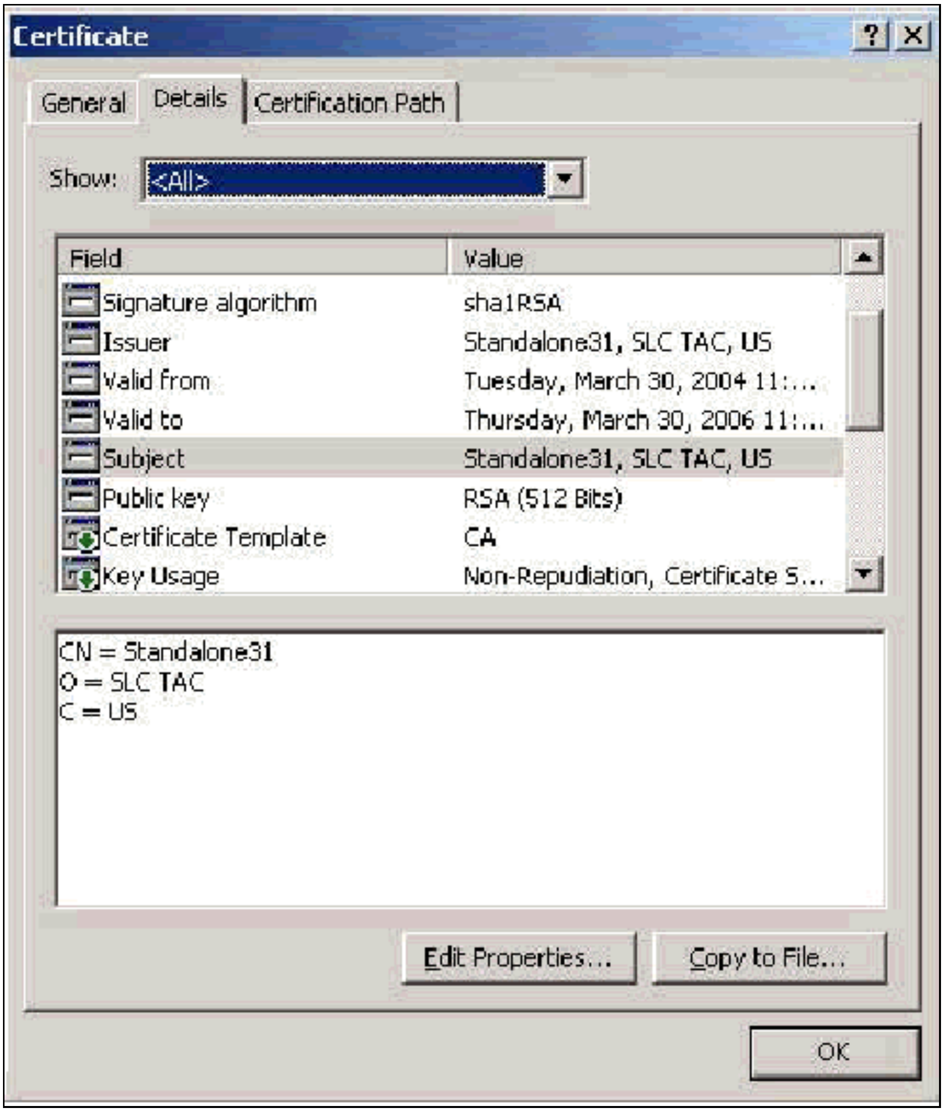
- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoriti
    - Trusted People
    - ACSCertStore
    - ACSCTLStore
    - Other People
    - Certificate Enrolment Requests
    - SPC
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third Party Root Certification Authoriti

Issued To	Issued By	Expiration Date	Intended Purposes	Frie
SecureSign RootCA2	SecureSign RootCA2	9/15/2020	Secure Email, Server...	Jap
SecureSign RootCA3	SecureSign RootCA3	9/15/2020	Secure Email, Server...	Jap
SelfSigned	SelfSigned	6/24/2005	Server Authentication	<N
SERVICIOS DE CERTIFICACION - ...	SERVICIOS DE CERTIFICACION - A...	3/9/2009	Secure Email, Server...	SER
SIA Secure Client CA	SIA Secure Client CA	7/9/2019	Secure Email, Server...	Soc
SIA Secure Server CA	SIA Secure Server CA	7/9/2019	Secure Email, Server...	Soc
SJCA	SJCA	3/27/2006	<All>	<N
Sonera Class1 CA	Sonera Class1 CA	4/6/2021	Client Authentication...	Son
Sonera Class2 CA	Sonera Class2 CA	4/6/2021	Server Authenticatio...	Son
Standalone31	Standalone31	3/30/2006	<All>	<N
Stress	Stress	8/19/2040	<All>	<N
Swisskey Root CA	Swisskey Root CA	12/31/2015	Secure Email, Server...	Swi
Symantec Root CA	Symantec Root CA	4/30/2011	<All>	<N
TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Class 3 CA	TC TrustCenter Class 3 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/2011	Secure Email, Server...	TC
TC TrustCenter Time Stamping CA	TC TrustCenter Time Stamping CA	1/1/2011	Time Stamping	TC
Telekom-Control-Kommission Top 1	Telekom-Control-Kommission Top 1	9/24/2005	Server Authenticatio...	Aus
Thawte Personal Basic CA	Thawte Personal Basic CA	12/31/2020	Client Authentication...	Tha
Thawte Personal Freemail CA	Thawte Personal Freemail CA	12/31/2020	Client Authentication...	Tha
Thawte Personal Premium CA	Thawte Personal Premium CA	12/31/2020	Client Authentication...	Tha
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticatio...	Tha
Thawte Server CA	Thawte Server CA	12/31/2020	Server Authenticatio...	Tha

Trusted Root Certification Authorities store contains 170 certificates.

Subject and Issuer Fields

The Subject and Issuer fields identify the CA and need to be exactly the same. Use these fields to populate the Issued to and Issued by fields in the General tab of the certificate. They are populated with the name of the root CA.



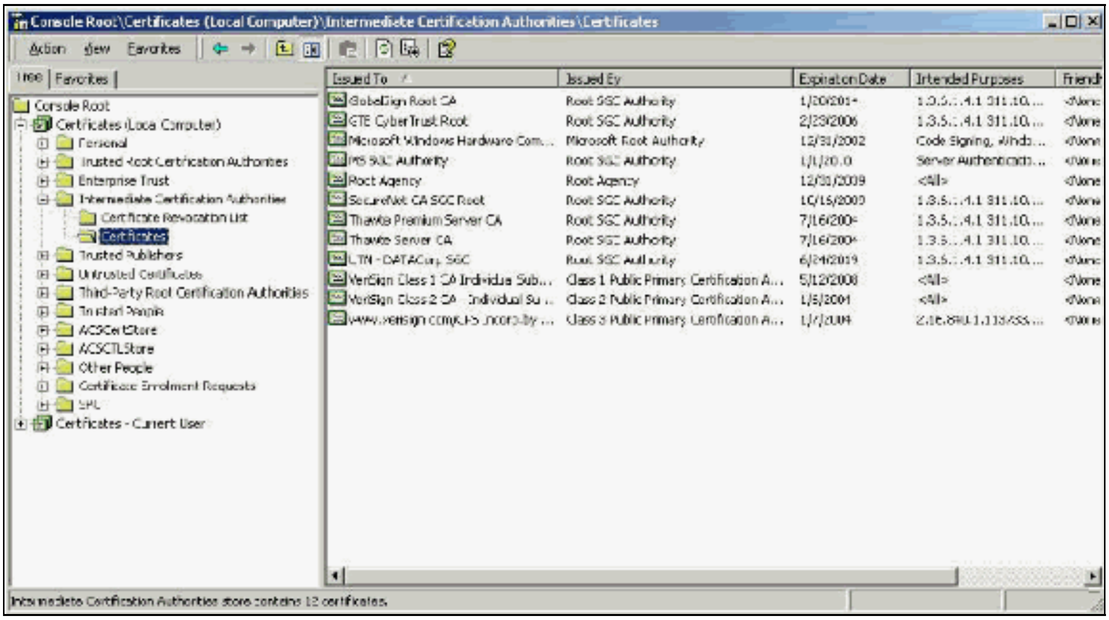
Show: <All>

Field	Value
Signature algorithm	sha1RSA
Issuer	Standalone31, SLC TAC, US
Valid from	Tuesday, March 30, 2004 11:...
Valid to	Thursday, March 30, 2006 11:...
Subject	Standalone31, SLC TAC, US
Public key	RSA (512 Bits)
Certificate Template	CA
Key Usage	Non-Repudiation, Certificate S...

```
CN = Standalone31
O = SLC TAC
C = US
```

Intermediate CA Certificates

Intermediate CA Certificates are certificates that you use to identify a CA that is subordinate to a root CA. Some Server Certificates (Verisign's wireless certificates) are created with the use of an intermediate CA. If a Server Certificate that is cut by an Intermediate CA is used, the Intermediate CA Certificate must be installed in the Intermediate Certification Authorities area of the local machine store on the ACS server. Also, if the Microsoft EAP supplicant is used on the client, the Root CA Certificate of the root CA that created the Intermediate CA Certificate must also be in the appropriate store on the ACS server and client so that the chain of trust can be established. Both the Root CA Certificate and the Intermediate CA Certificate must be marked as trusted in ACS and on the client. Most Intermediate CA Certificates are not installed with Windows so you most likely need to acquire them from the vendor. When correctly installed in the Windows certificate store, the Intermediate CA Certificate appears in the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder as seen in this example window.



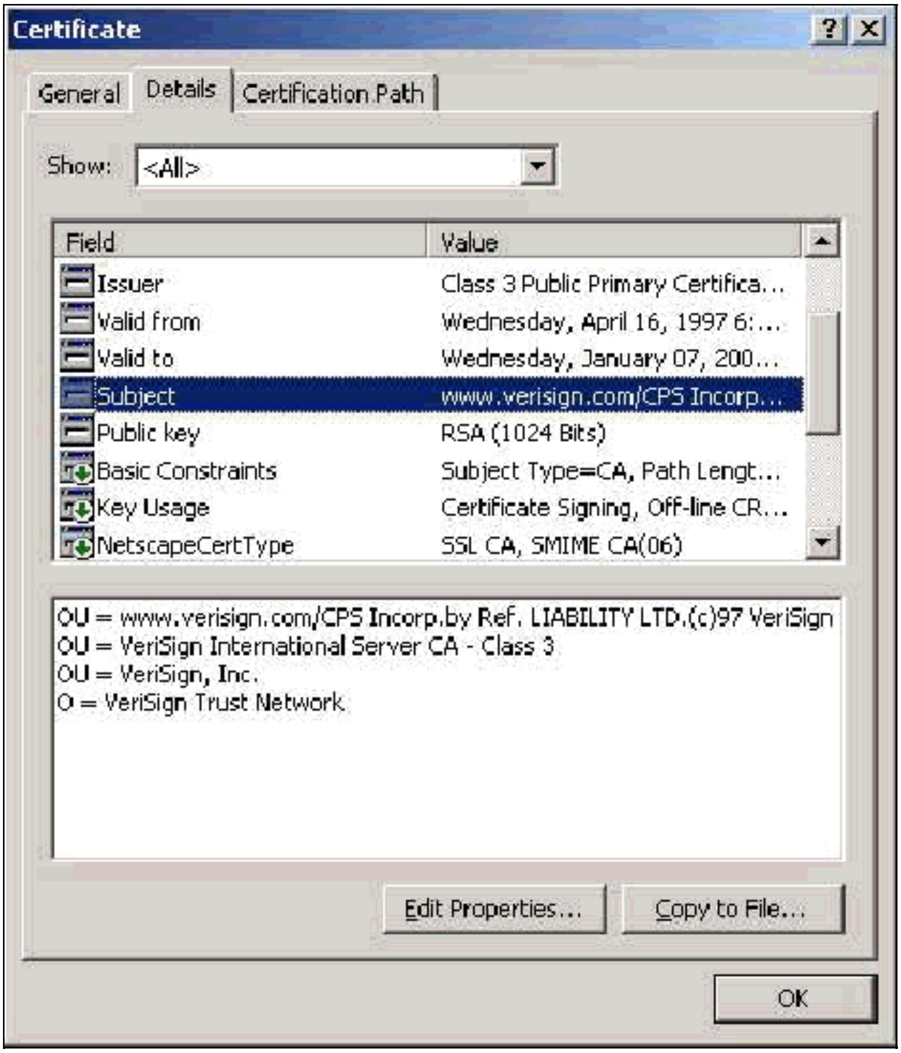
Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates
Action View Favorites
Tree Favorites
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
ACSCertStore
ACSCTLStore
Other People
Certificate Enrolment Requests
SPC
Certificates - Current User

Issued To	Issued By	Expiration Date	Intended Purposes	Friendl
GlobalSign Root CA	Root SGC Authority	1/20/2014	1.3.6.1.4.1.311.10....	<None
GTE CyberTrust Root	Root SGC Authority	2/23/2006	1.3.6.1.4.1.311.10....	<None
Microsoft Windows Hardware Com...	Microsoft Root Authority	12/31/2002	Code Signing, Windo...	<None
MS SGC Authority	Root SGC Authority	1/1/2010	Server Authenticatio...	<None
Root Agency	Root Agency	12/31/2039	<All>	<None
SecureNet CA SGC Root	Root SGC Authority	10/16/2009	1.3.6.1.4.1.311.10....	<None
Thawte Premium Server CA	Root SGC Authority	7/16/2004	1.3.6.1.4.1.311.10....	<None
Thawte Server CA	Root SGC Authority	7/16/2004	1.3.6.1.4.1.311.10....	<None
UTN - DATACorp SGC	Root SGC Authority	6/24/2019	1.3.6.1.4.1.311.10....	<None
VeriSign Class 1 CA Individual Sub...	Class 1 Public Primary Certification A...	5/12/2008	<All>	<None
VeriSign Class 2 CA - Individual Su...	Class 2 Public Primary Certification A...	1/6/2004	<All>	<None
www.verisign.com/CPS Incorp.by ...	Class 3 Public Primary Certification A...	1/7/2004	2.16.840.1.113733....	<None

Intermediate Certification Authorities store contains 12 certificates.

Subject Field

The Subject field identifies the Intermediate CA. This value is used to determine the Issued to field in the General tab of the certificate.

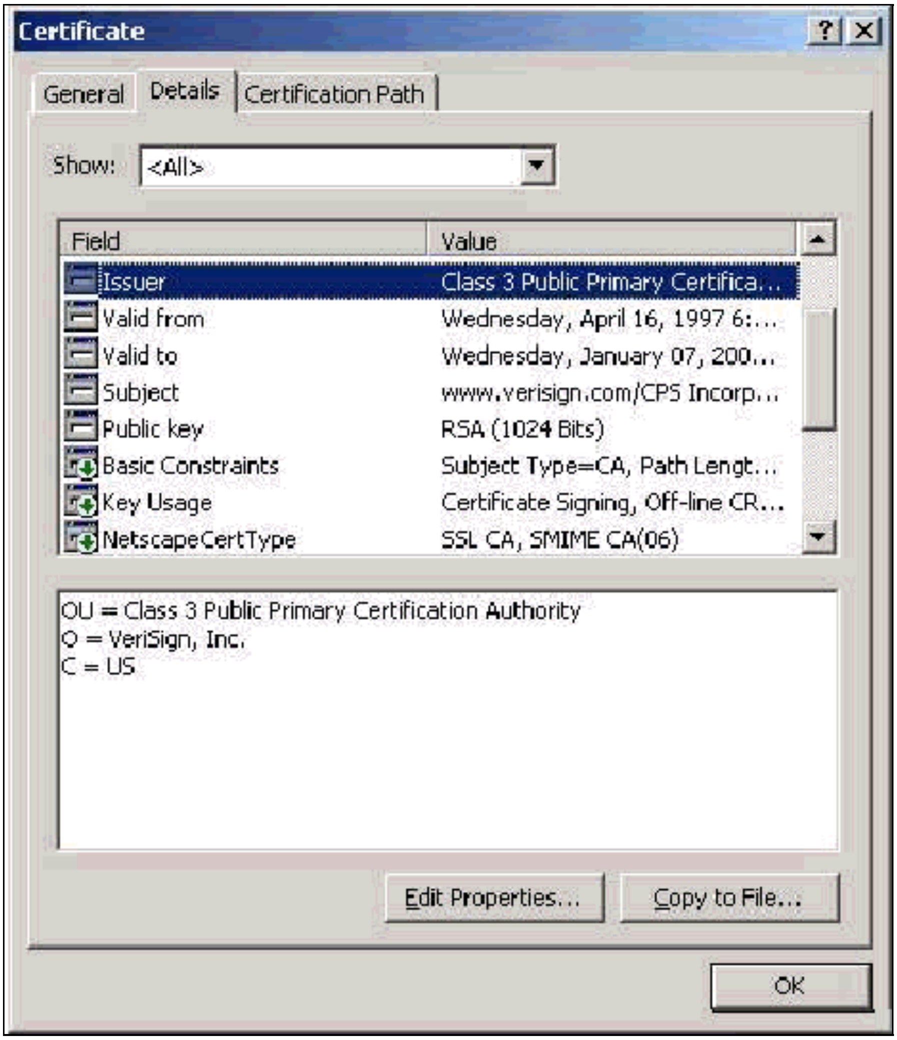


Field	Value
Issuer	Class 3 Public Primary Certifica...
Valid from	Wednesday, April 16, 1997 6:...
Valid to	Wednesday, January 07, 200...
Subject	www.verisign.com/CPS Incorp...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...
NetscapeCertType	SSL CA, SMIME CA(06)

OU = www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
OU = VeriSign International Server CA - Class 3
OU = VeriSign, Inc.
O = VeriSign Trust Network

Issuer Field

The Issuer field identifies the CA that cut the certificate. Use this value in order to determine the value of the Issued by field in the General tab of the certificate. It is populated with the name of the CA.



Show: <All>

Field	Value
Issuer	Class 3 Public Primary Certifica...
Valid from	Wednesday, April 16, 1997 6:...
Valid to	Wednesday, January 07, 200...
Subject	www.verisign.com/CPS Incorp...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...
NetscapeCertType	SSL CA, SMIME CA(06)

OU = Class 3 Public Primary Certification Authority
O = VeriSign, Inc.
C = US

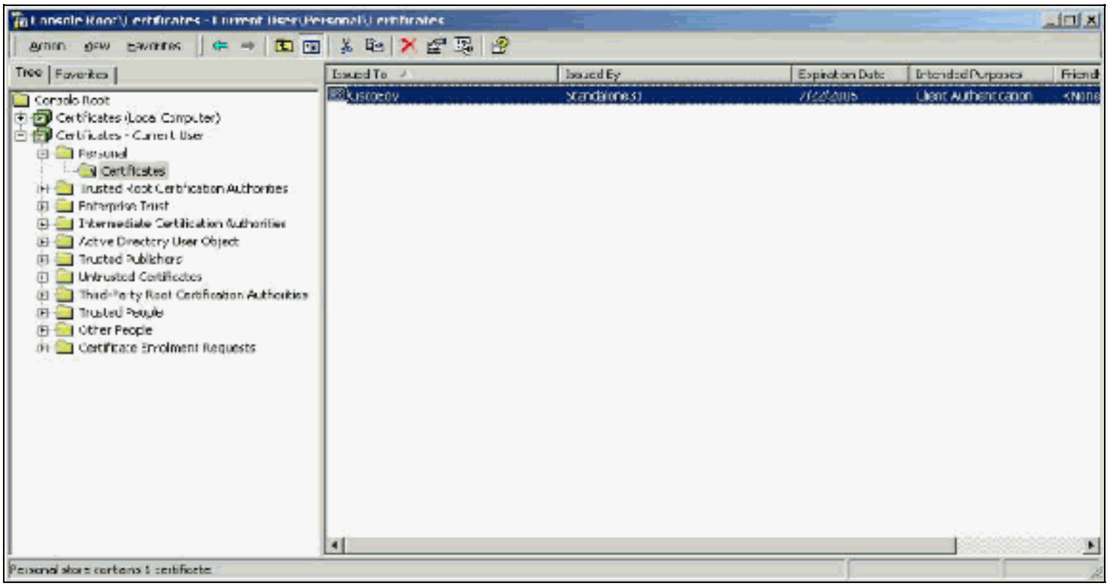
Client Certificates

Client Certificates are used to positively identify the user in EAP−TLS. They have no role in building the TLS tunnel and are not used for encryption. Positive identification is accomplished by one of three means:

- **CN (or Name)Comparison** Compares the CN in the certificate with the username in the database. More information on this comparison type is included in the description of the Subject field of the certificate.
- **SAN Comparison** Compares the SAN in the certificate with the username in the database. This is only supported as of ACS 3.2. More information on this comparison type is included in the description of the Subject Alternative Name field of the certificate.
- **Binary Comparison** Compares the certificate with a binary copy of the certificate stored in the database (only AD and LDAP can do this). If you use certificate binary comparison, you must store the user certificate in a binary format. Also, for generic LDAP and Active Directory, the attribute that stores the certificate must be the standard LDAP attribute named "usercertificate".

Whatever comparison method is used, the information in the appropriate field (CN or SAN) must match the name that your database uses for authentication. AD uses the NetBios name for authentication in mixed mode and the UPN in native mode.

This section discusses Client Certificate generation with the use of Microsoft Certificate Services. EAP−TLS requires a unique Client Certificate in order for each user to be authenticated. The certificate must be installed on each computer for each user. When properly installed, the certificate is located in the **Certificates −Current User > Personal > Certificates** folder as seen in this example window.

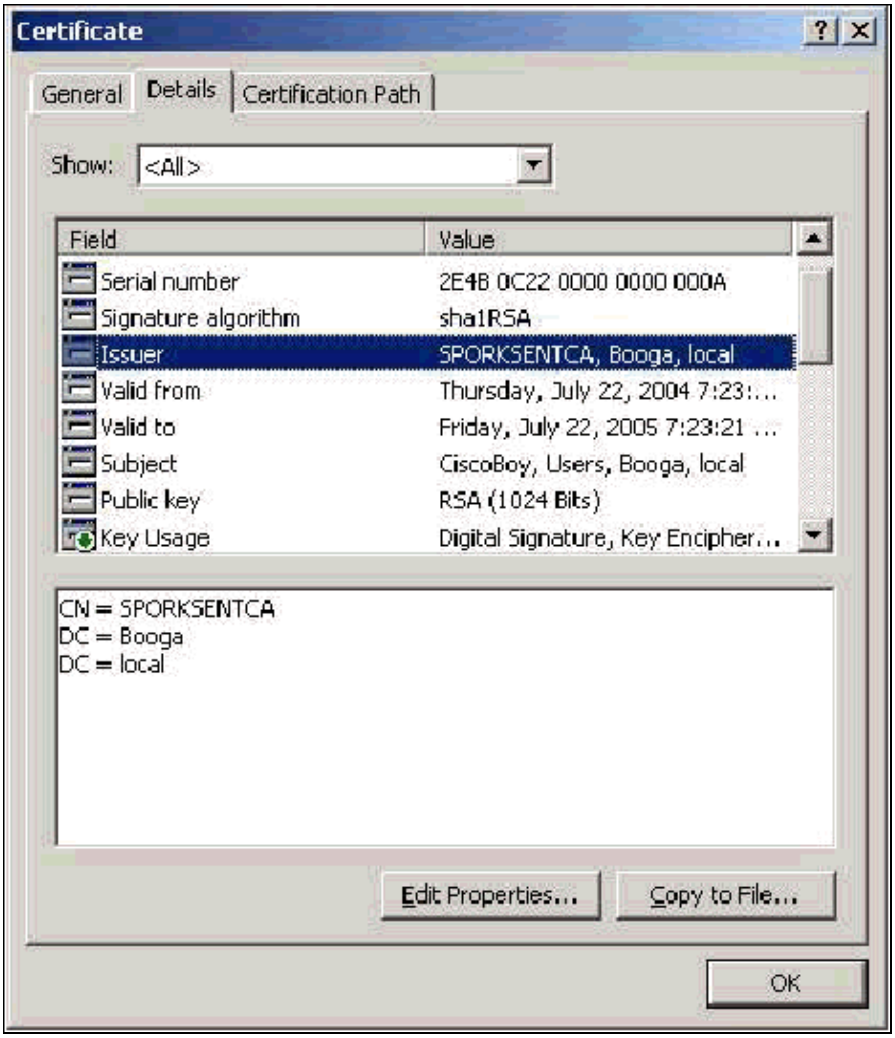

Console Root\Certificates - Current User\Personal\Certificates
Action
View
Favorites
Tree
Favorites
Console Root
Certificates (Local Computer)
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date	Intended Purposes	Friendl
[illegible]	[illegible]	[illegible]	Client Authentication	<None

Personal store contains 1 certificate.

Issuer Field

The Issuer field identifies the CA that cuts the certificate. Use this value in order to determine the value of the Issued by field in the General tab of the certificate. This is populated with the name of the CA.



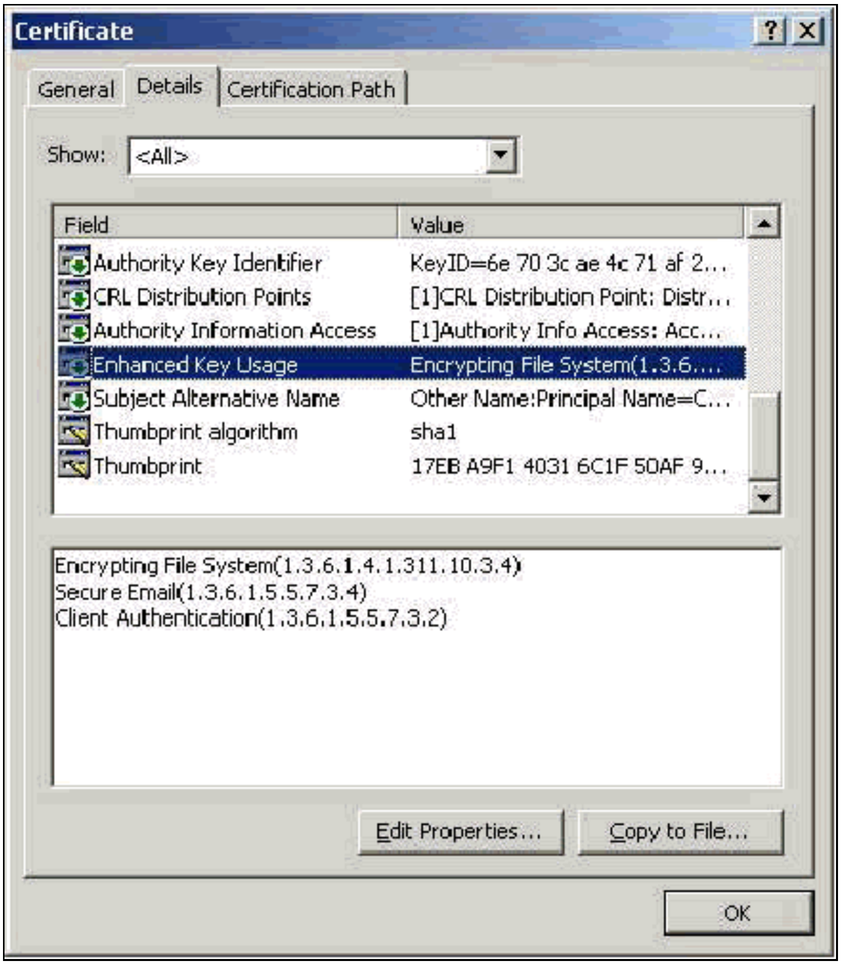
Show: <All>

Field	Value
Serial number	2E4B 0C22 0000 0000 000A
Signature algorithm	sha1RSA
Issuer	SPORKSENTCA, Booga, local
Valid from	Thursday, July 22, 2004 7:23:...
Valid to	Friday, July 22, 2005 7:23:21 ...
Subject	CiscoBoy, Users, Booga, local
Public key	RSA (1024 Bits)
Key Usage	Digital Signature, Key Encipher...

CN = SPORKSENTCA
DC = Booga
DC = local

Enhanced Key Usage Field

The Enhanced Key Usage field identifies the intended purpose of the certificate and needs to contain Client Authentication. This field is mandatory when you use the Microsoft supplicant for PEAP and EAP−TLS. When you use Microsoft Certificate Services, this is configured in the Standalone CA when you select **Client Authentication Certificate** from the Intended Purpose drop−down and in the Enterprise CA when you select **User** from the Certificate Template drop−down. If you request a certificate with the use of a CSR with Microsoft Certificate Services, you do not have the option to specify the Intended Purpose with the Standalone CA. Therefore, the EKU field is absent. With the Enterprise CA, you have the Intended Purpose drop−down. Some CAs do not create certificates with an EKU field. They are useless when you use the Microsoft EAP supplicant.



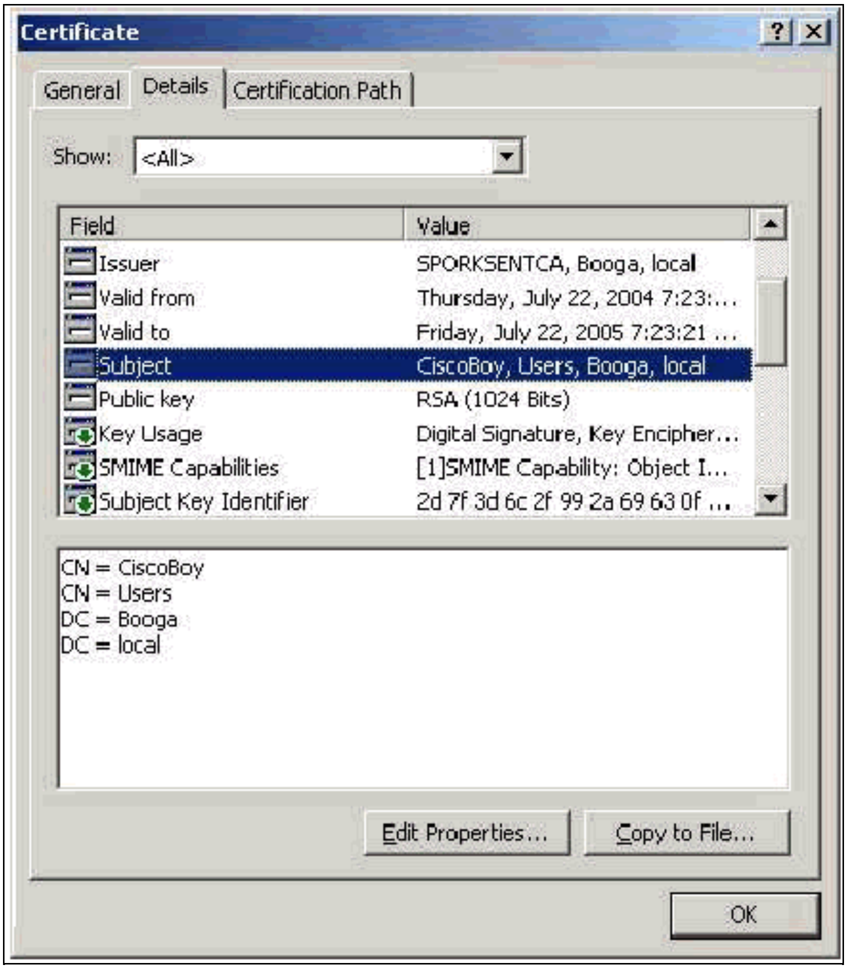
Show: <All>

Field	Value
Authority Key Identifier	KeyID=6e 70 3c ae 4c 71 af 2...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Encrypting File System(1.3.6....
Subject Alternative Name	Other Name:Principal Name=C...
Thumbprint algorithm	sha1
Thumbprint	17EB A9F1 4031 6C1F 50AF 9...

```
Encrypting File System(1.3.6.1.4.1.311.10.3.4)
Secure Email(1.3.6.1.5.5.7.3.4)
Client Authentication(1.3.6.1.5.5.7.3.2)
```

Subject Field

This field is used in CN comparison. The first CN listed is compared against the database to find a match. If a match is found, authentication succeeds. If you use a Standalone CA, the CN is populated with whatever you put in the Name field in the certificate submittal form. If you use the Enterprise CA, the CN is automatically populated with the name of the account as listed in the Active Directory Users and Computers console (this does not necessarily match the UPN or the NetBios name).



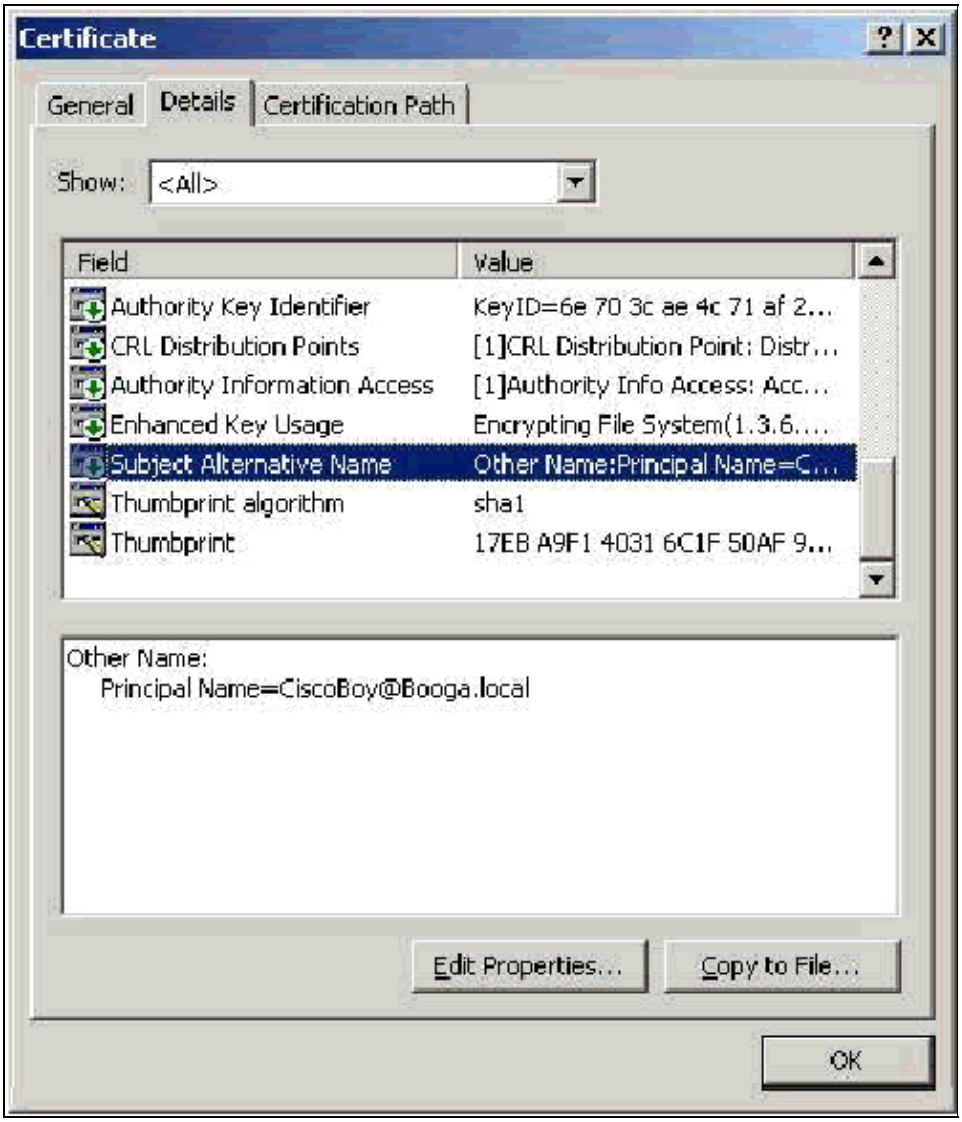
Show: <All>

Field	Value
Issuer	SPORKSENTCA, Booga, local
Valid from	Thursday, July 22, 2004 7:23:...
Valid to	Friday, July 22, 2005 7:23:21 ...
Subject	CiscoBoy, Users, Booga, local
Public key	RSA (1024 Bits)
Key Usage	Digital Signature, Key Encipher...
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	2d 7f 3d 6c 2f 99 2a 69 63 0f ...

CN = CiscoBoy
CN = Users
DC = Booga
DC = local

Subject Alternative Name Field

The Subject Alternative Name field is used in SAN comparison. The SAN listed is compared against the database to find a match. If a match is found, authentication succeeds. If you use the Enterprise CA, the SAN is automatically populated with the Active Directory logon name @domain (UPN). The standalone CA does not include a SAN field so you cannot use SAN comparison.



Show: <All>

Field	Value
Authority Key Identifier	KeyID=6e 70 3c ae 4c 71 af 2...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Encrypting File System(1.3.6....
Subject Alternative Name	Other Name:Principal Name=C...
Thumbprint algorithm	sha1
Thumbprint	17EB A9F1 4031 6C1F 50AF 9...

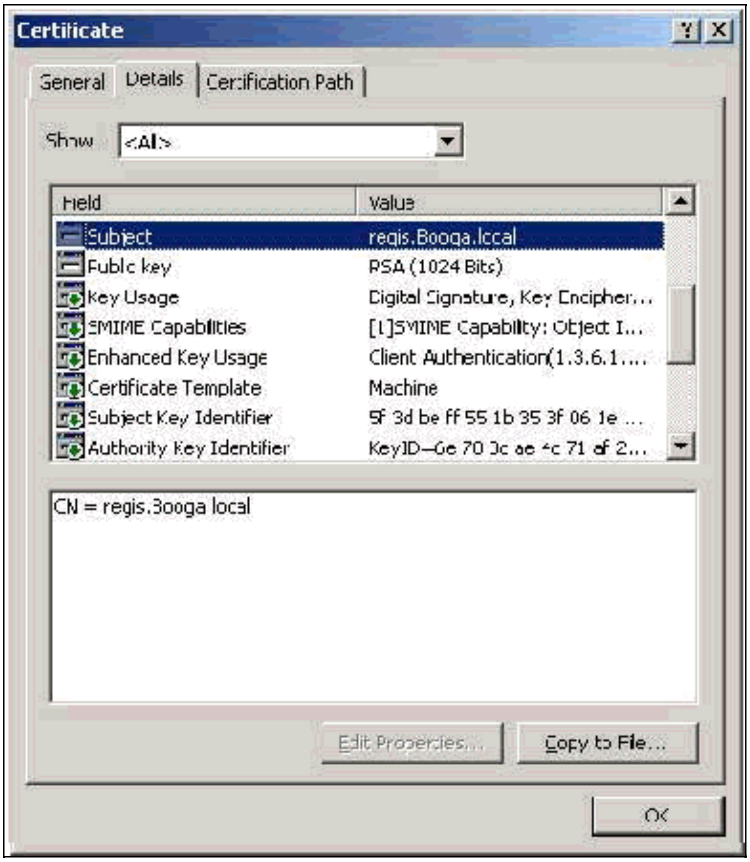
```
Other Name:
    Principal Name=CiscoBoy@Booga.local
```

Machine Certificates

Machine certificates are used in EAP−TLS to positively identify the computer when you use machine authentication. You can only access these certificates when you configure your Microsoft Enterprise CA for certificate auto−enrollment and join the computer to the domain. The certificate is automatically created when you use the Active Directory credentials of the computer and install them in the local computer store. Computers that are already members of the domain before you configure auto−enrollment receive a certificate the next time that Windows restarts. The Machine Certificate is installed in the **Certificates (Local Computer) > Personal > Certificates** folder of the Certificates (Local Computer) MMC snap−in just like Server Certificates. You cannot install these certificates on any other machine since you cannot export the private key.

Subject and SAN Fields

The Subject and SAN fields identify the computer. The value is populated by the fully qualified name of the computer and is used in order to determine the Issued to field in the General tab of the certificate and is the same for both Subject and SAN fields.



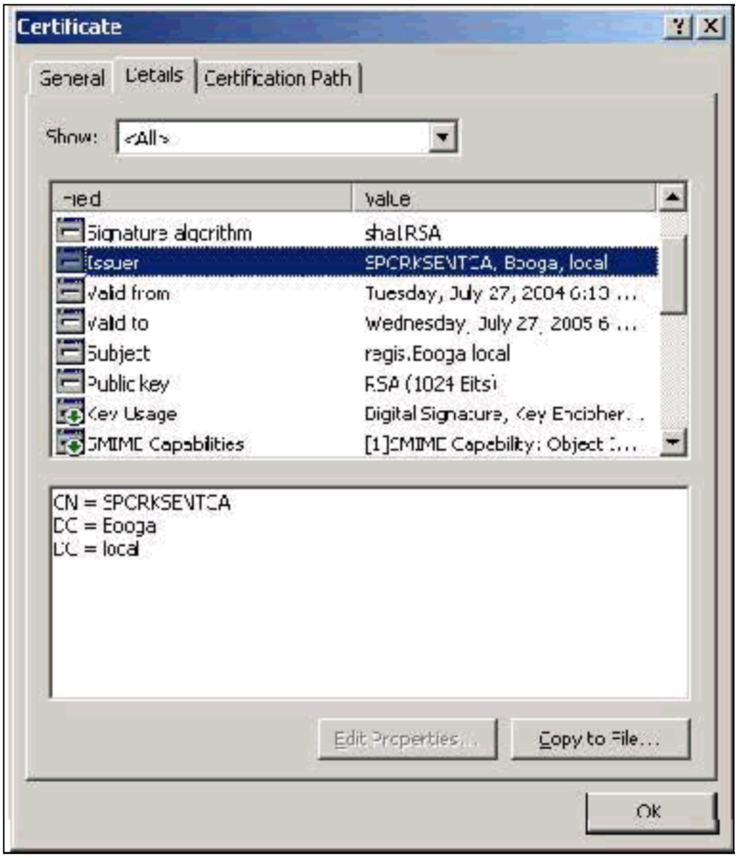
Show <All>

Field	Value
Subject	regis.Booga.local
Public key	RSA (1024 Bits)
Key Usage	Digital Signature, Key Encipher...
SMIME Capabilities	[1]SMIME Capability: Object I...
Enhanced Key Usage	Client Authentication(1.3.6.1....
Certificate Template	Machine
Subject Key Identifier	5f 3d be ff 55 1b 35 3f 06 1e ...
Authority Key Identifier	KeyID=6e 70 3c ae 4c 71 af 2...

CN = regis.Booga.local

Issuer Field

The Issuer field identifies the CA that cut the certificate. Use this value in order to determine the value of the Issued by field in the General tab of the certificate. It is populated with the name of the CA.



Show: <All>

Field	Value
Signature algorithm	sha1RSA
Issuer	SPORKSENTCA, Booga, local
Valid from	Tuesday, July 27, 2004 6:10 ...
Valid to	Wednesday, July 27, 2005 6 ...
Subject	regis.Booga local
Public key	RSA (1024 Bits)
Key Usage	Digital Signature, Key Encipher. .
SMIME Capabilities	[1]SMIME Capability: Object ...

CN = SPORKSENTCA
DC = Booga
DC = local

Appendix A − Common Certificate Extensions

.csr This is not actually a certificate but rather a Certificate Signing Request. It is a plain text file with this format:

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

.pvk This extension denotes a private key though the extension does not guarantee that the content is actually a private key. The content need to be plain text with this format:

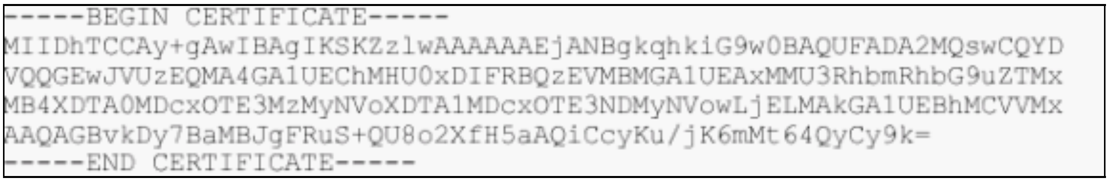
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,751DA1C8E250B96B

YyLE3zsDTY1+Kq+6gAUF+YCO452KHmQJQn7AKxMnDqHeQrAePReL/zuxHiKsBjrN
h2FGzV17bBVnBQZ/Ci/j92HYeQ2VZD8wB6lYFsWV/30kYeyPYRctweteKFfgpFHi
/ES9B0bWzrpFS1El+I2L6o1dwnUkmMBIC1j1WNV3Xo+/5NFei1mdlgRMRtzR85Ub
4hUWzWCsRSFEcHEcNcsfxkach9stzkIMWB6d7RyvWyqNfb627O2MhMhA9T01LYri
NdM/Tsdz3Kfc7AXiNMvti5R0mSV89d6epLLE69PTWZLNxasCsCybhNt/ya/z7y1S
bE4iBAwdZ9jCyuBB9viLBqps39zfiYrRTDkDXiVH3oIWKBbM3OEw3apgLFZiVRqZ
07xaX7oQyy4tQfo4UNnhPTX3kiMBA6t6UJvs6VIHsIIXYEYlHbL6bA==
-----END RSA PRIVATE KEY-----
```

.cer This is a generic extension that denotes a certificate. Server, Root CA, and Intermediate CA certificates can be in this format. It is commonly a plain text file with an extension that you can change as you need and can be either DER or Base 64 format. You can import this format into the Windows certificate store.

.pem This extension stands for Privacy Enhanced Mail. This extension is commonly used with UNIX, Linux, BSD, and so forth. It is generally used for server certificates and private keys, and is commonly a plain text file with an extension that you can change as you need from .pem to .cer so that you can import it to the Windows certificate store.

The internal content of .cer and .pem files generally look like this output:



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

.pfx This extension stands for Personal Information Exchange. This format is a method you can use to bundle certificates into a single file. For example, you can bundle a Server Certificate and its associated private key and Root CA Certificate into one file and easily import the file into the appropriate Windows certificate store. It is most commonly used for Server and Client Certificates. Unfortunately, if a Root CA Certificate is included, the Root CA Certificate is always installed in the Current User store instead of the Local Computer store even if the Local Computer store is specified for installation.

.p12 This format is generally only seen with a Client Certificate. You can import this format into the Windows certificate store.

.p7b This is another format that stores multiple certificates in one file. You can import this format into the Windows certificate store.

Appendix B − Certificate Format Conversion

In most cases, certificate conversion occurs when you change the extension (for example, from .pem to .cer) since the certificates are commonly in plain text format. Sometimes, a certificate is not in plaintext format and you must convert it with the use of a tool such as OpenSSL . For example, the ACS Solution Engine cannot install certificates in the .pfx format. Therefore, you must convert the certificate and the private key into a usable format. This is the basic command syntax for OpenSSL:

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

You are prompted for the Import Password and the PEM pass phrase. These passwords need to be the same and are the private key password that is specified when the .pfx is exported. The output is a single .pem file which includes all of the certificates and private keys in the .pfx. This file can be referred to in ACS as both the certificate and the private key file and it installs with no problems.

Appendix C − Certificate Validity Period

A certificate is only usable during its validity period. The validity period for a Root CA Certificate is determined when the root CA is established and can vary. The validity period for an Intermediate CA Certificate is determined when the CA is established and cannot exceed the validity period of the root CA to which it is subordinate. The validity period for Server, Client, and Machine Certificates is automatically set to one year with Microsoft Certificate Services. This can only be changed when you hack the Windows registry as per Microsoft Knowledge Base article 254632 and cannot exceed the validity period of the root CA. The validity period of the self−signed certificates that ACS generates is always one year and cannot be changed in current versions.

Related Information

- **RADIUS Support Page**
- **Requests for Comments (RFCs)** ↗
- **Technical Support − Cisco Systems**

Updated: Feb 02, 2006 Document ID: 64062