# Securing WCF Services with Certificates

**Jason Hodges**, 30 Jul 2008 CPOL

★★★★★ 4.93 (70 votes)

An article that describes how to secure WCF services using X.509 certificates issued from a certificate authority.

**Download source - 8.41 KB**

## Introduction

This article provides a step-by-step guide to securing WCF services with certificates. Most articles of this nature use *makecert.exe* to generate sample certificates. This is great for testing purposes, but what if you want to use certificates that are issued from a Certificate Authority (CA)? This article will show you how to generate certificates with Microsoft Certificate Services and use them to secure your WCF services.

## Prerequisites

This article assumes that you know how to create and consume a WCF service.

You should have two separate machines to follow the steps in this article:

1. Client machine — this can be your development system. You should have the .NET Framework 3.0 or higher installed.
2. Server machine — this will function as our WCF server as well as a Certificate Authority. (Note that you may want to have a separate server function as the CA.) You should have Windows Server 2003 with the .NET Framework 3.0 or higher installed. If you do not have a separate machine, it is recommended that you create a virtual machine with these specifications. This can be achieved by using Virtual PC 2007.

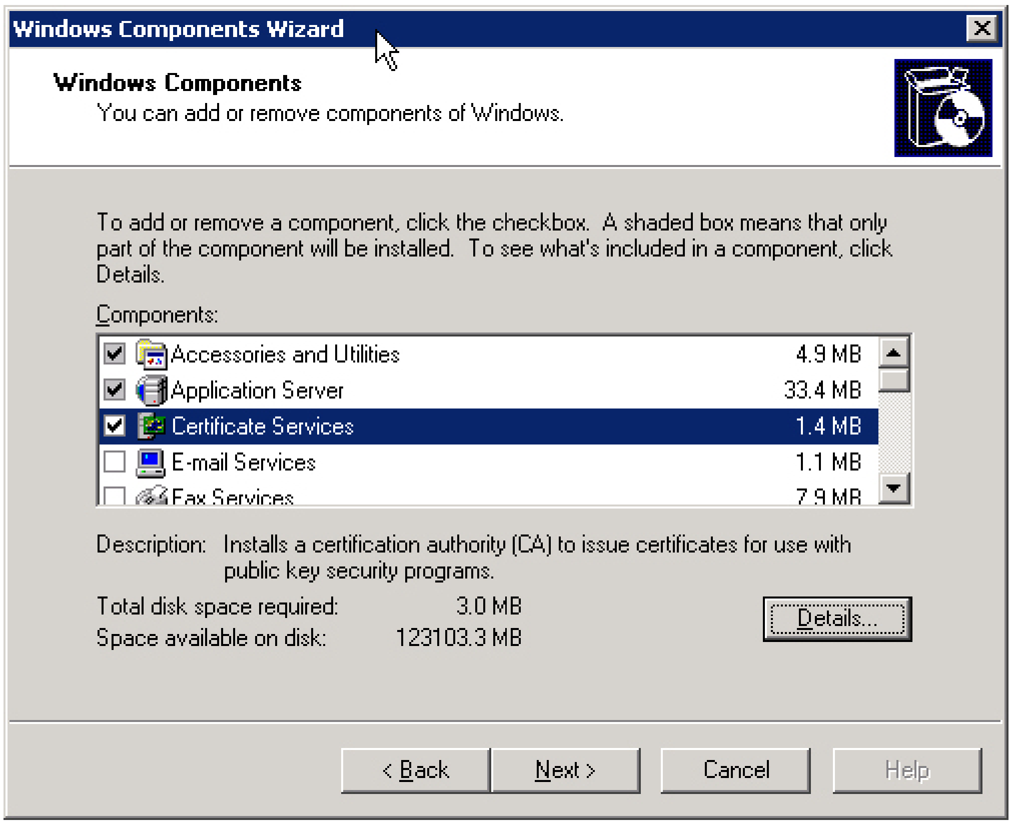
## Section 1: Install Microsoft Certificate Services on the Server

You have two options for obtaining X.509 certificates for which to secure your services:

1. Purchase a certificate from a trusted certificate authority such as VeriSign, Thawte, RapidSSL, etc.
2. Create your own certificate authority

This article focuses on the 2nd option by creating certificates using Microsoft Certificate Services. To install Microsoft Certificate Services, follow these instructions:

1. On the server machine, go to Control Panel > Add or Remove Programs
2. Select Add / Remove Windows Components
3. Check **Certificate Services** and click **Next** to complete the installation.



Windows Components Wizard

**Windows Components**

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

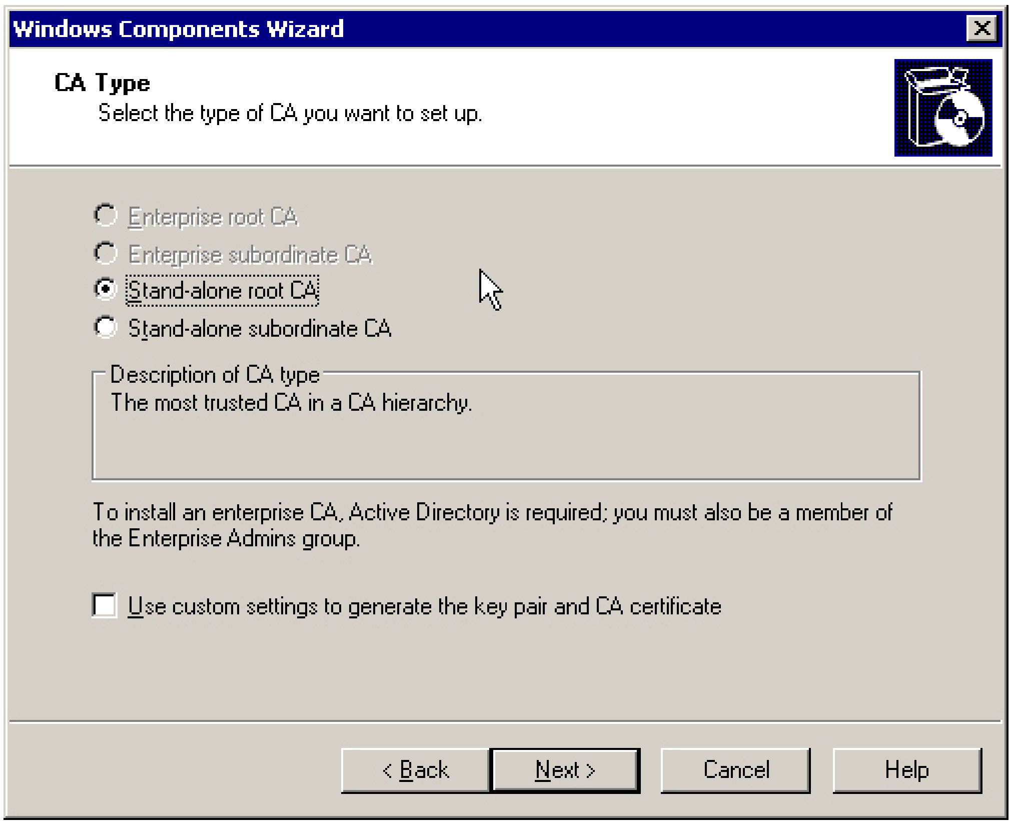
| | | |
|---|---|---|
| ✓ | Accessories and Utilities | 4.9 MB |
| ✓ | Application Server | 33.4 MB |
| ✓ | Certificate Services | 1.4 MB |
| | E-mail Services | 1.1 MB |
| | Fax Services | 7.9 MB |

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 3.0 MB

Space available on disk: 123103.3 MB

4. Select **Stand-alone root CA** and click **Next**



Windows Components Wizard

**CA Type**

Select the type of CA you want to set up.

- Enterprise root CA
- Enterprise subordinate CA
- [✓ Stand-alone root CA]
- Stand-alone subordinate CA

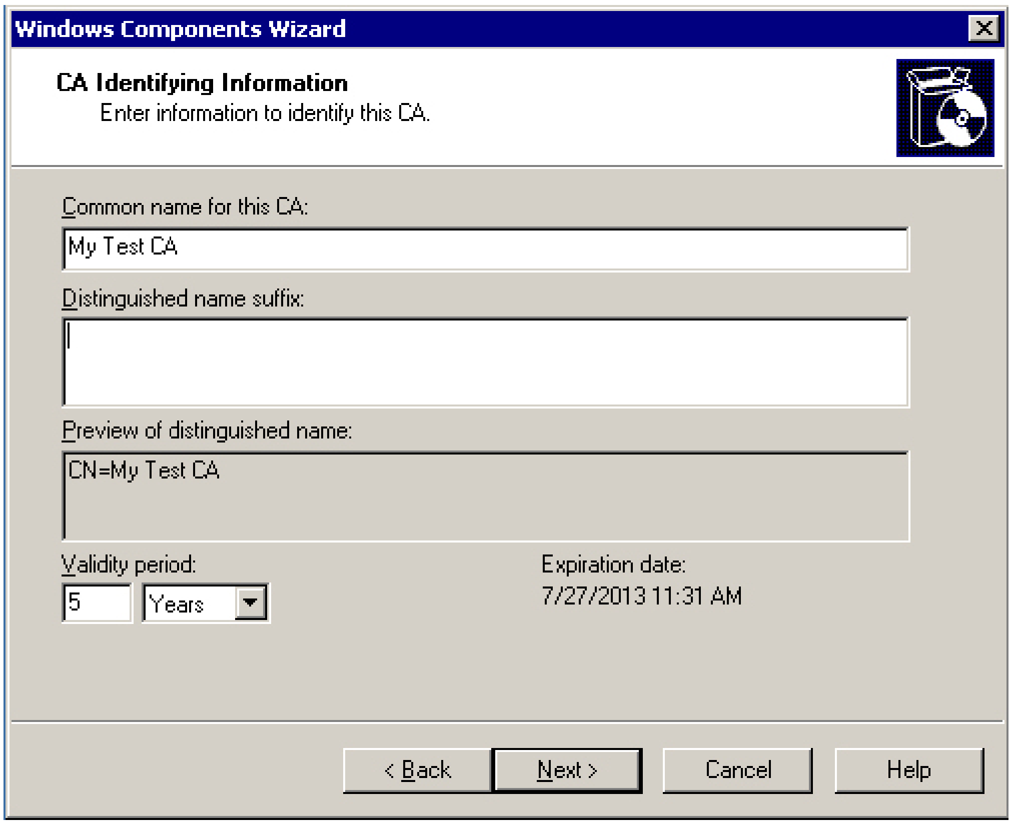
Description of CA type

The most trusted CA in a CA hierarchy.

To install an enterprise CA, Active Directory is required; you must also be a member of the Enterprise Admins group.

☐ Use custom settings to generate the key pair and CA certificate

5. Fill out the CA Identifying Information


Windows Components Wizard

CA Identifying Information
Enter information to identify this CA.

Common name for this CA: My Test CA

Distinguished name suffix:

Preview of distinguished name: CN=My Test CA

Validity period: 5 Years

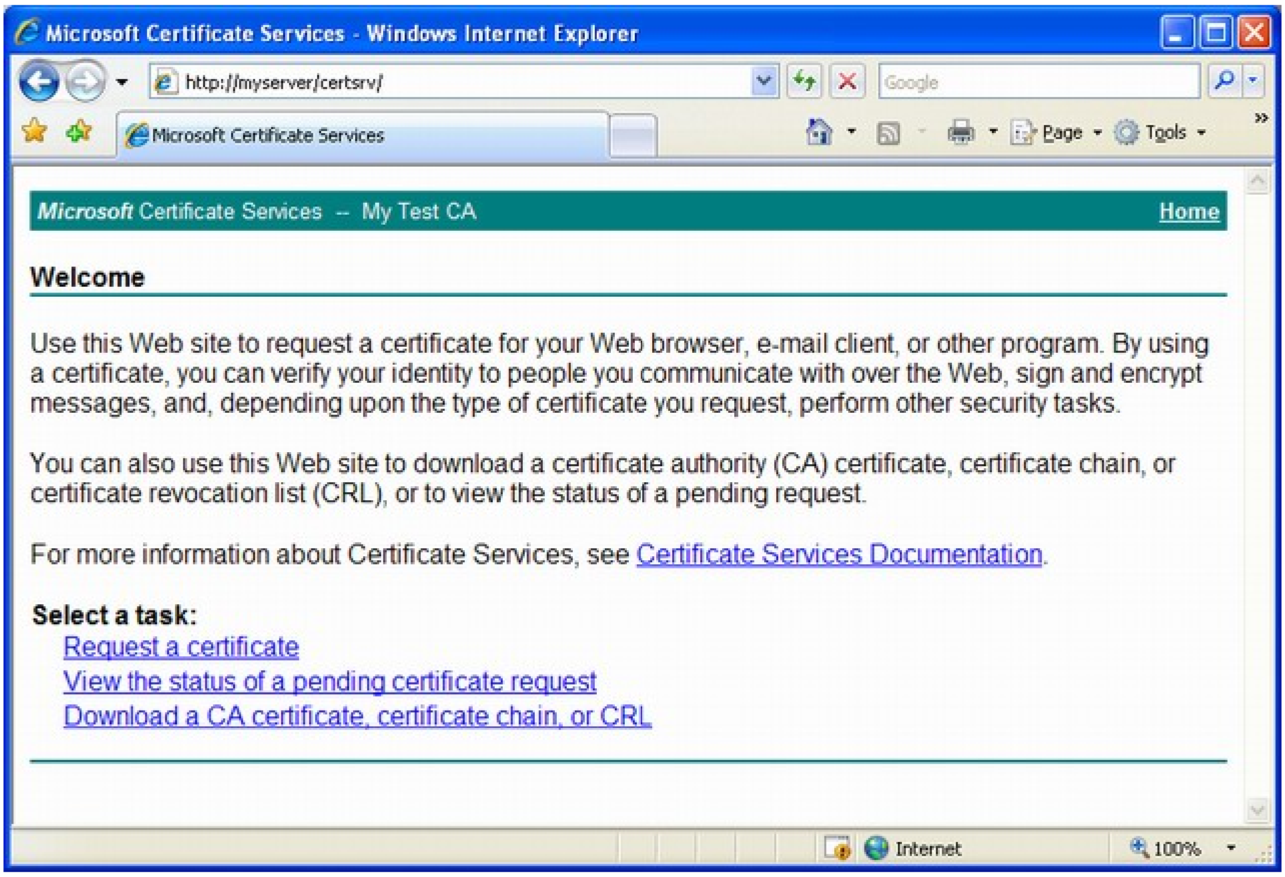
Expiration date: 7/27/2013 11:31 AM

6. Complete the installation by accepting the remaining defaults

## Section 2: Configure the client to trust the new certificate authority

Windows is preconfigured with a set of trusted certificate authorities. Of course, our new certificate authority isn't in this list. Follow these steps to allow your client machine to trust the new certificate authority.

1. On the client machine, open a web browser and go to *http://<server name>/certsrv*. This will bring up a page similar to the following:


Microsoft Certificate Services - Windows Internet Explorer

http://myserver/certsrv/

Microsoft Certificate Services -- My Test CA

Welcome

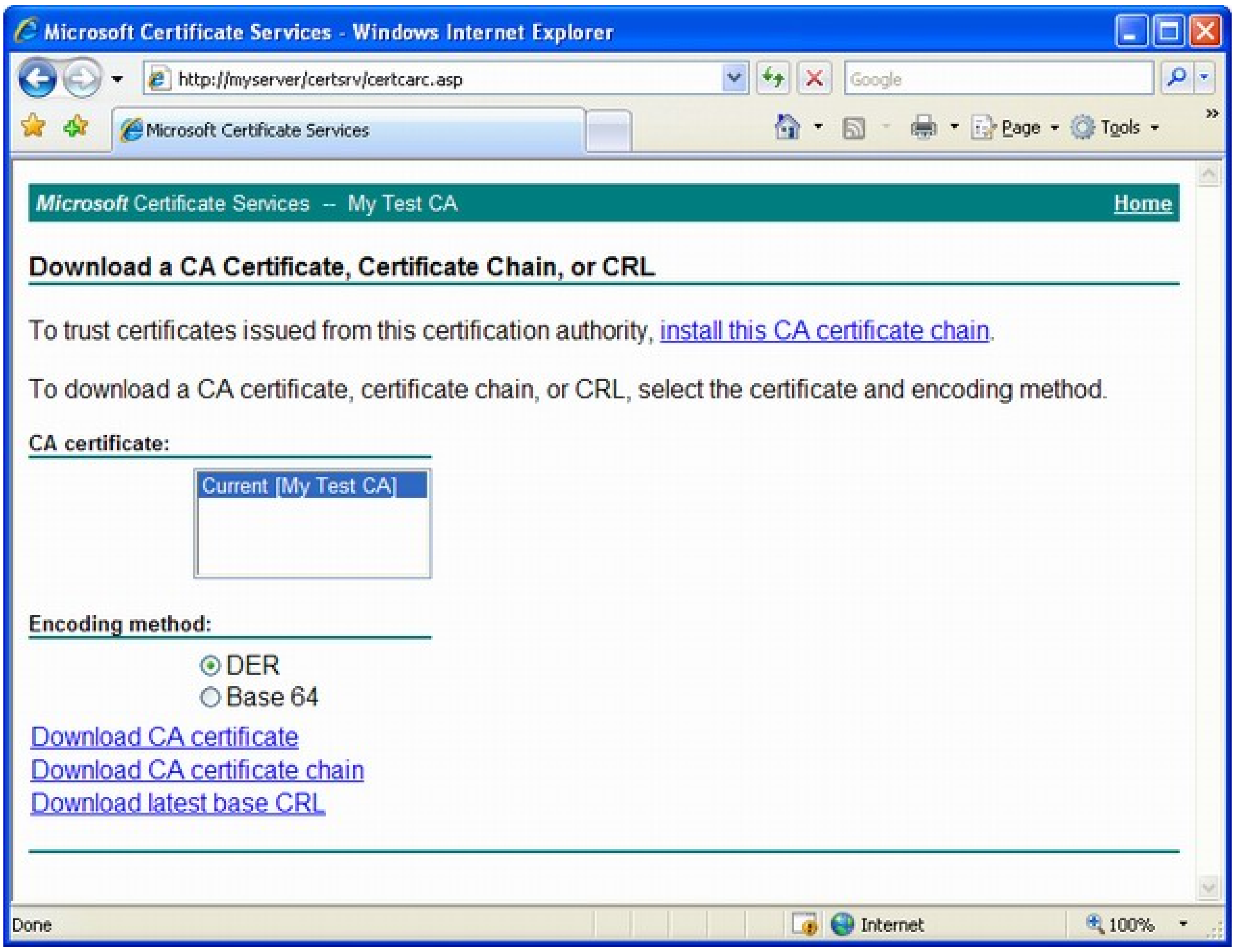
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. Click **Download a CA certificate, certificate chain, or CRL**


Microsoft Certificate Services - Windows Internet Explorer
http://myserver/certsrv/certcarc.asp
Google
Microsoft Certificate Services
Page
Tools
Done
Internet
100%

Microsoft Certificate Services -- My Test CA Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [My Test CA]

Encoding method:

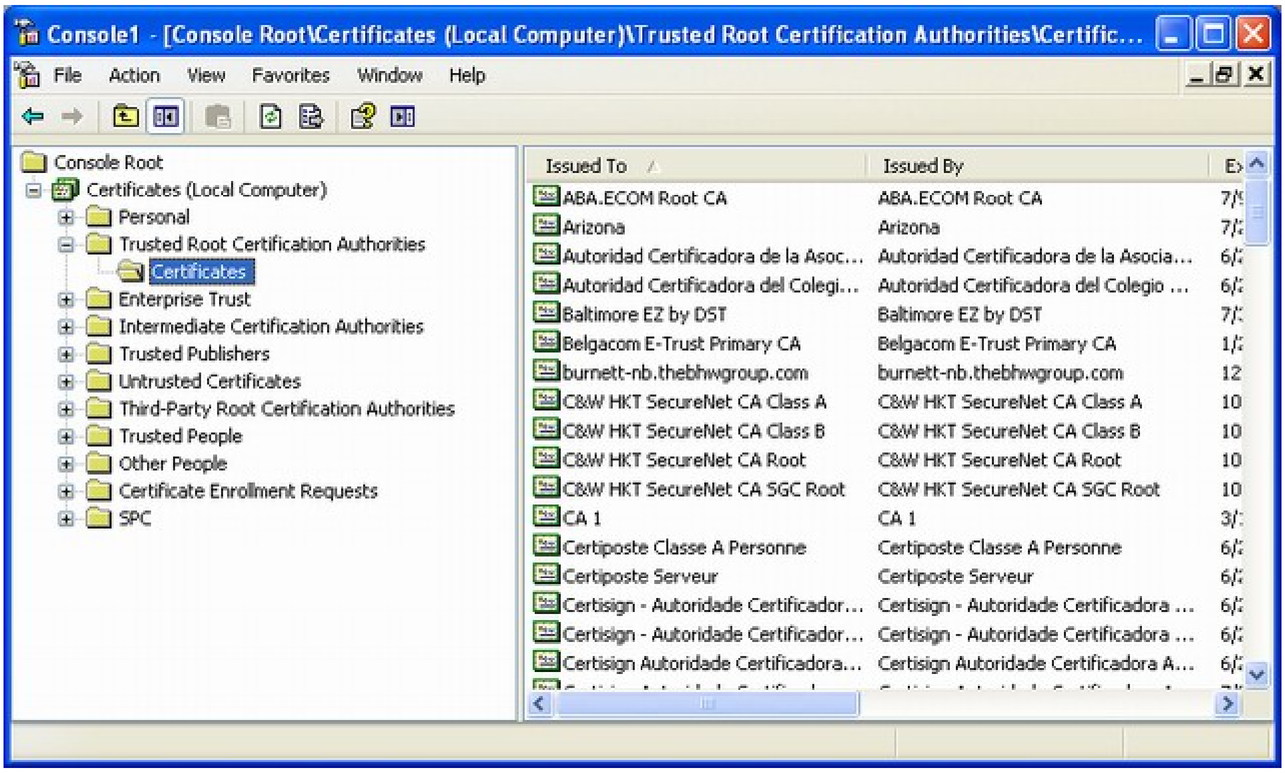
[✓ DER] Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

3. Click **Download CA certificate chain**. Save the *certnew.p7b* file to your file system.
4. Load the Certificates MMC Snap-In. Note that several steps in this article will require loading this snap-in. The following instructions show how to do this, and they will not be repeated in subsequent sections.

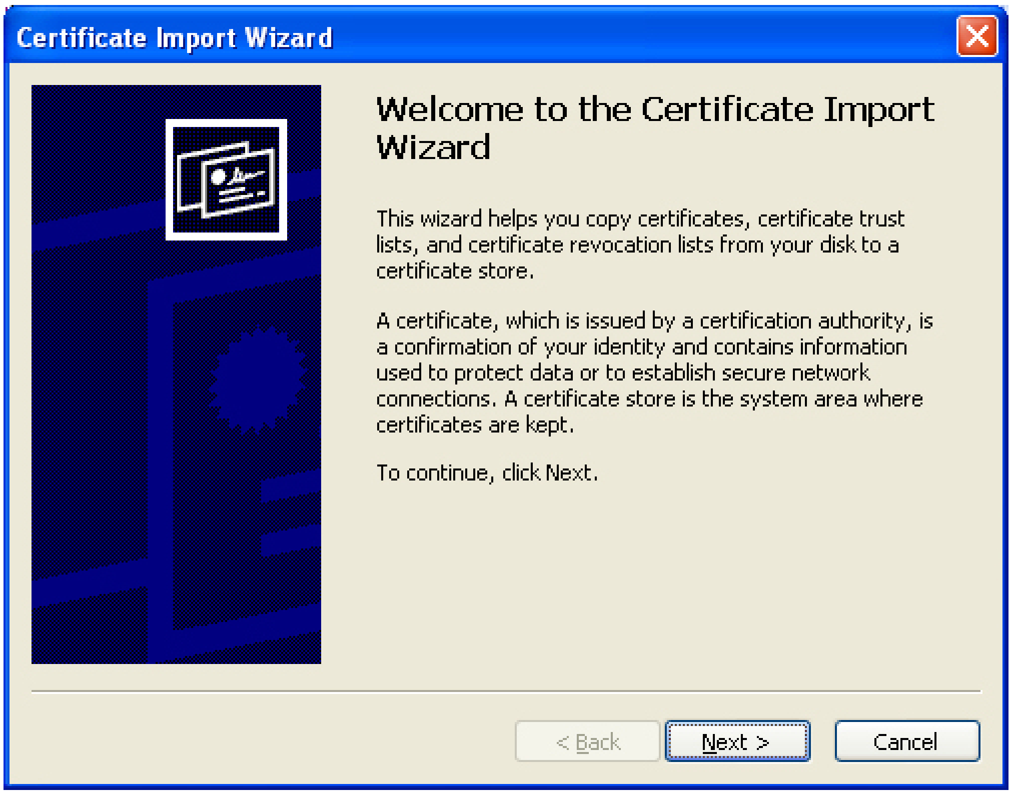
   1. Select **Start** > **Run** and type "mmc" to open the Microsoft Management Console
   2. Select **File** > **Add / Remove Snap-in**
   3. Click the **Add** button
   4. Select **Certificates** and click the **Add** button
   5. Select **Computer Account** and click the **Next** button
   6. Click the **Finish** button
   7. Click the **Close** and **OK** buttons

5. Expand **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates**


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certific...
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
SPC

| Issued To | Issued By | E> |
|---|---|---|
| ABA.ECOM Root CA | ABA.ECOM Root CA | 7/ |
| Arizona | Arizona | 7/ |
| Autoridad Certificadora de la Asoc... | Autoridad Certificadora de la Asocia... | 6/ |
| Autoridad Certificadora del Colegi... | Autoridad Certificadora del Colegio ... | 6/ |
| Baltimore EZ by DST | Baltimore EZ by DST | 7/ |
| Belgacom E-Trust Primary CA | Belgacom E-Trust Primary CA | 1/ |
| burnett-nb.thebhwgroup.com | burnett-nb.thebhwgroup.com | 12 |
| C&W HKT SecureNet CA Class A | C&W HKT SecureNet CA Class A | 10 |
| C&W HKT SecureNet CA Class B | C&W HKT SecureNet CA Class B | 10 |
| C&W HKT SecureNet CA Root | C&W HKT SecureNet CA Root | 10 |
| C&W HKT SecureNet CA SGC Root | C&W HKT SecureNet CA SGC Root | 10 |
| CA 1 | CA 1 | 3/ |
| Certiposte Classe A Personne | Certiposte Classe A Personne | 6/ |
| Certiposte Serveur | Certiposte Serveur | 6/ |
| Certisign - Autoridade Certificador... | Certisign - Autoridade Certificadora ... | 6/ |
| Certisign - Autoridade Certificador... | Certisign - Autoridade Certificadora ... | 6/ |
| Certisign Autoridade Certificadora... | Certisign Autoridade Certificadora A... | 6/ |

6. Right-click the **Certificates** folder and select **All Tasks** > **Import**



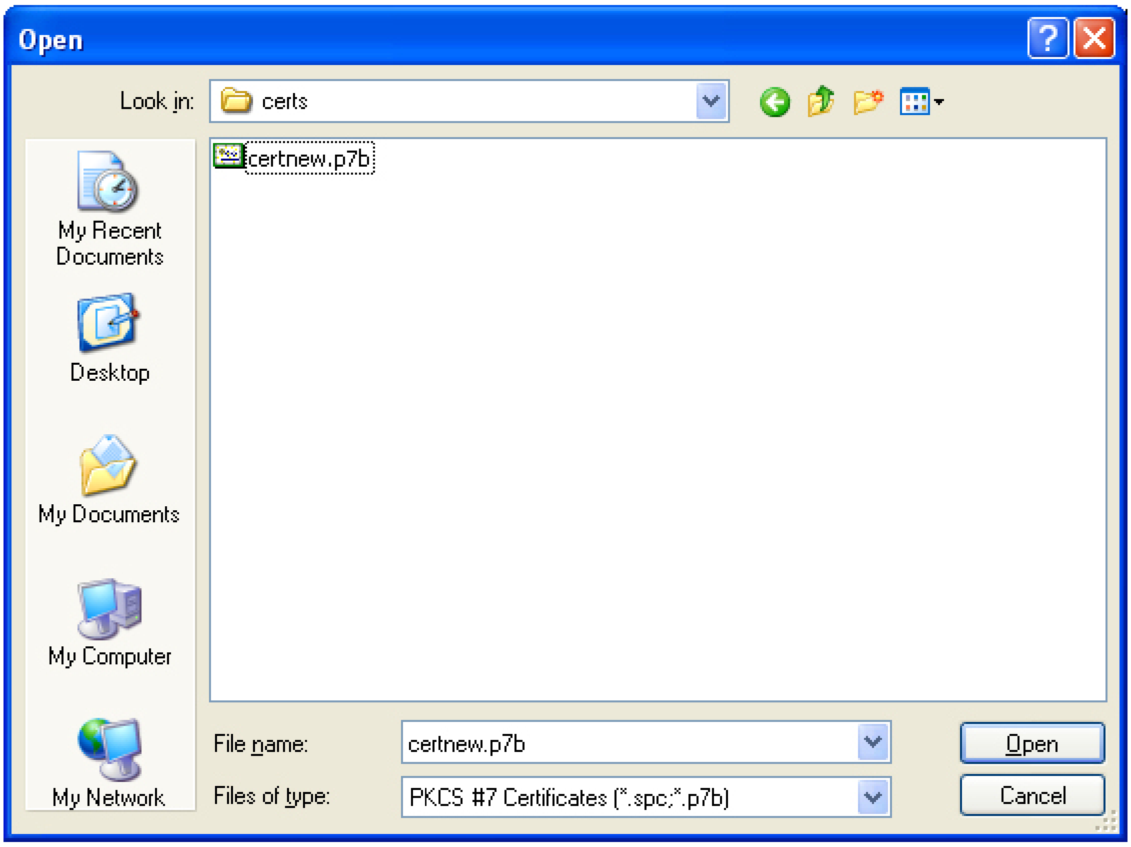
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

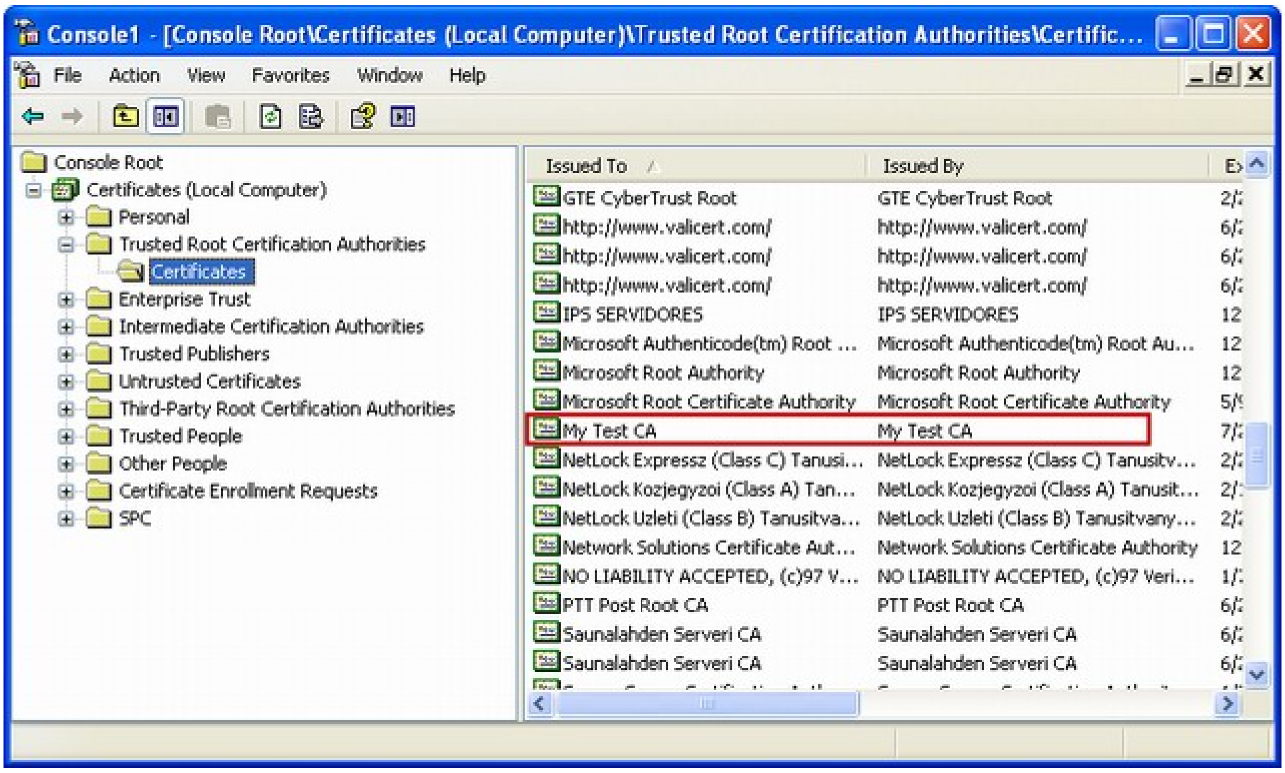
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Click **Next**, then click **Browse**
8. Select **PKCS #7 Certificates** from the **Files of type** drop down list
9. Browse to the *certnew.p7b* file that you saved in step 3. Click the **Open** button



10. Click **Next**, **Next**, and **Finish**. You should now see your CA listed as a Trusted Root Certificate Authority.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certific...
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
Certificate Enrollment Requests
SPC

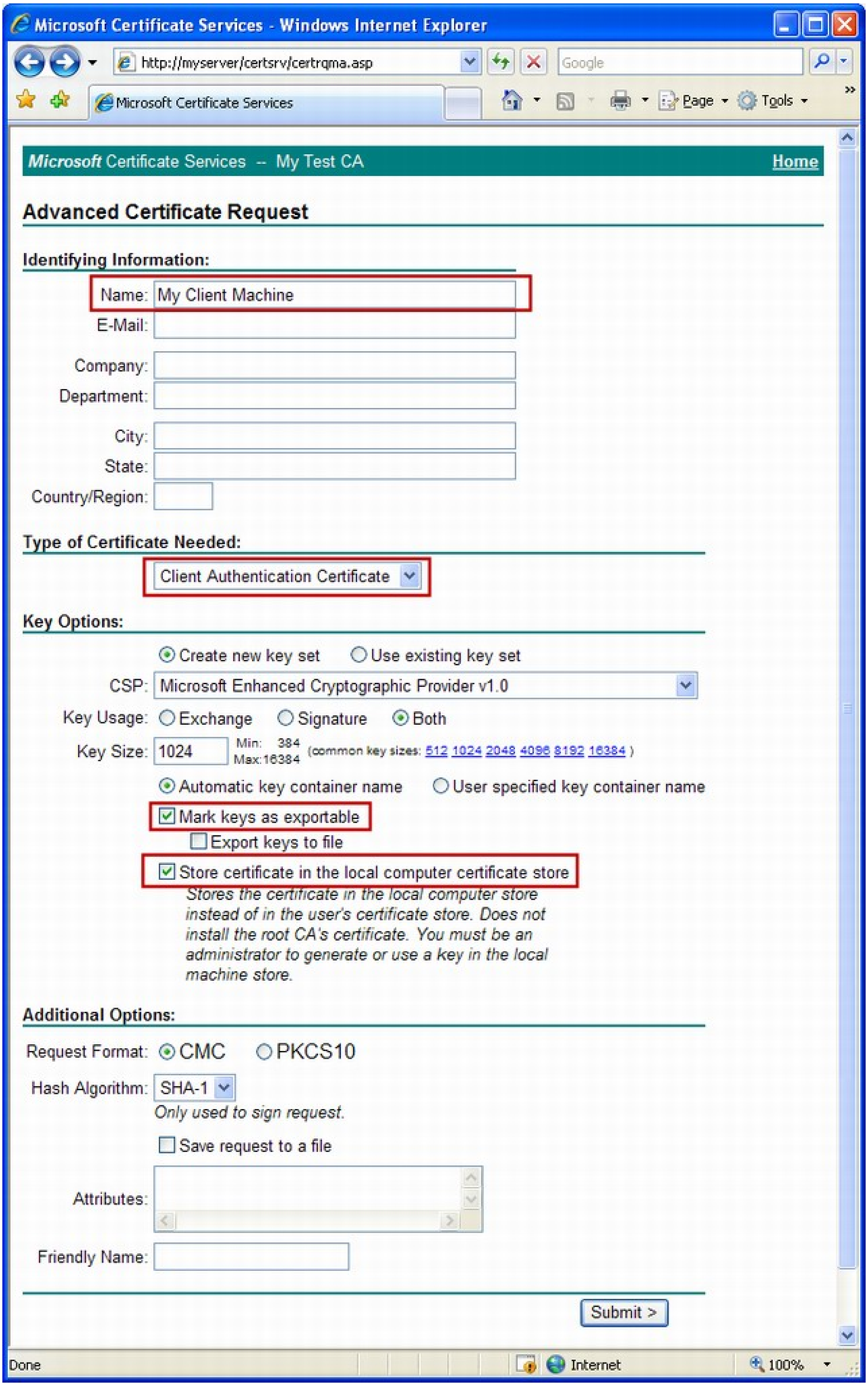
| Issued To | Issued By | Ex |
|---|---|---|
| GTE CyberTrust Root | GTE CyberTrust Root | 2/ |
| http://www.valicert.com/ | http://www.valicert.com/ | 6/ |
| http://www.valicert.com/ | http://www.valicert.com/ | 6/ |
| http://www.valicert.com/ | http://www.valicert.com/ | 6/ |
| IPS SERVIDORES | IPS SERVIDORES | 12 |
| Microsoft Authenticode(tm) Root ... | Microsoft Authenticode(tm) Root Au... | 12 |
| Microsoft Root Authority | Microsoft Root Authority | 12 |
| Microsoft Root Certificate Authority | Microsoft Root Certificate Authority | 5/ |
| My Test CA | My Test CA | 7/ |
| NetLock Expressz (Class C) Tanusi... | NetLock Expressz (Class C) Tanusitv... | 2/ |
| NetLock Kozjegyzoi (Class A) Tan... | NetLock Kozjegyzoi (Class A) Tanusit... | 2/ |
| NetLock Uzleti (Class B) Tanusitva... | NetLock Uzleti (Class B) Tanusitvany... | 2/ |
| Network Solutions Certificate Aut... | Network Solutions Certificate Authority | 12 |
| NO LIABILITY ACCEPTED, (c)97 V... | NO LIABILITY ACCEPTED, (c)97 Veri... | 1/ |
| PTT Post Root CA | PTT Post Root CA | 6/ |
| Saunalahden Serveri CA | Saunalahden Serveri CA | 6/ |
| Saunalahden Serveri CA | Saunalahden Serveri CA | 6/ |

Note: If your WCF server is different than your CA server, you will need to repeat Section 2 for the WCF server machine.

## Section 3: Create a Client Certificate

This section explains how to create a certificate for our WCF client.

1. On the client machine, open a web browser and go to *http://<server name>/certsrv*
2. Click **Request a certificate**
3. Click **advanced certificate request**
4. Click **Create and submit a request to this CA**
5. Fill out the form as shown in the image below:


Microsoft Certificate Services - Windows Internet Explorer

http://myserver/certsrv/certrqma.asp

*Microsoft* Certificate Services -- My Test CA | Home

**Advanced Certificate Request**

**Identifying Information:**

| | |
|---|---|
| Name: | My Client Machine |
| E-Mail: | |
| Company: | |
| Department: | |
| City: | |
| State: | |
| Country/Region: | |

**Type of Certificate Needed:**

Client Authentication Certificate

**Key Options:**

[✓ Create new key set] Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange Signature [✓ Both]

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384 )

[✓ Automatic key container name] User specified key container name

[✓] Mark keys as exportable

[ ] Export keys to file

[✓] Store certificate in the local computer certificate store

*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

**Additional Options:**

Request Format: [✓ CMC] PKCS10

Hash Algorithm: SHA-1

*Only used to sign request.*

[ ] Save request to a file

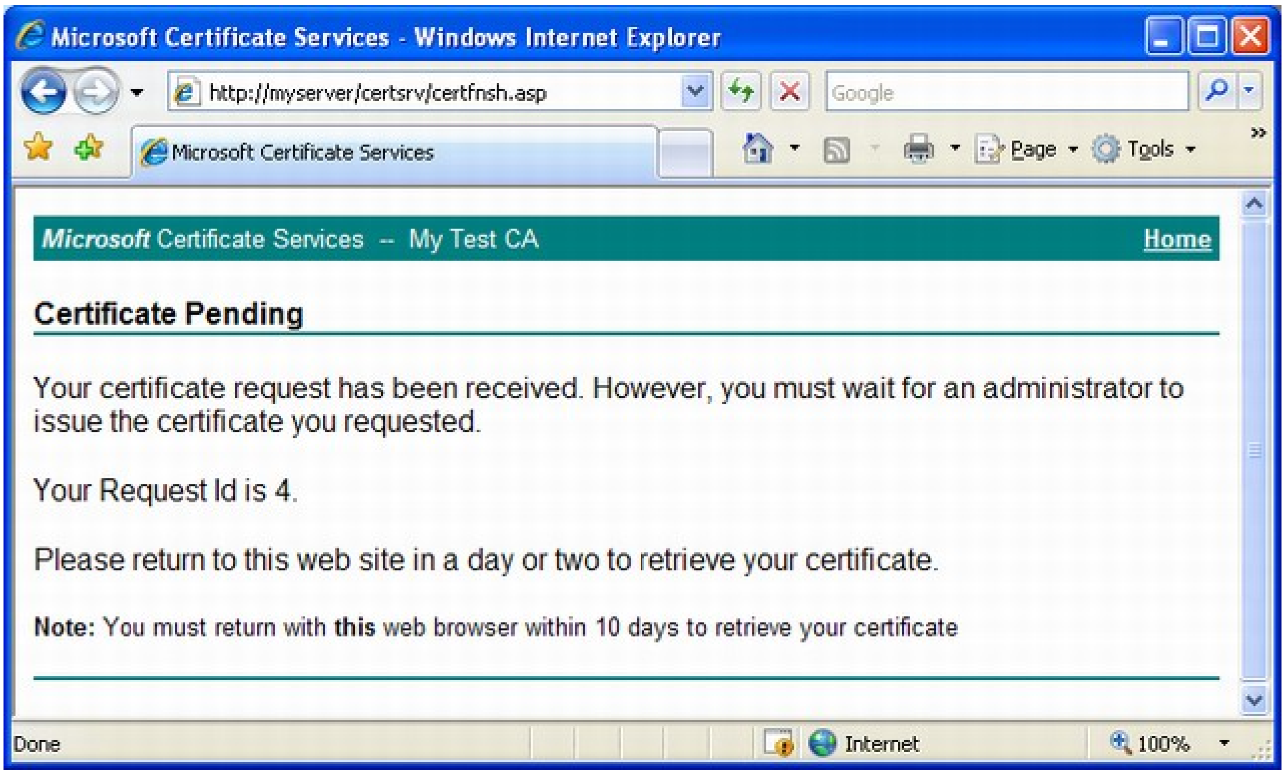
Attributes:

Friendly Name:

Submit >

Done | Internet | 100%

6. Click **Submit** and accept the warning message. You will see a confirmation that your request has been received and is pending.


Microsoft Certificate Services - Windows Internet Explorer
http://myserver/certsrv/certfnsh.asp
Microsoft Certificate Services -- My Test CA
Home
Done
Internet
100%

Certificate Pending

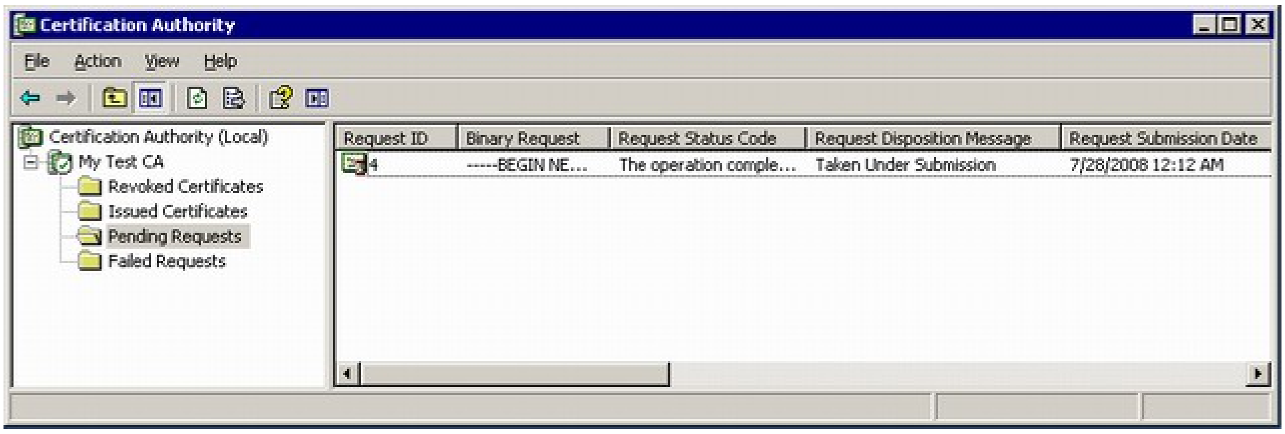
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 4.

Please return to this web site in a day or two to retrieve your certificate.

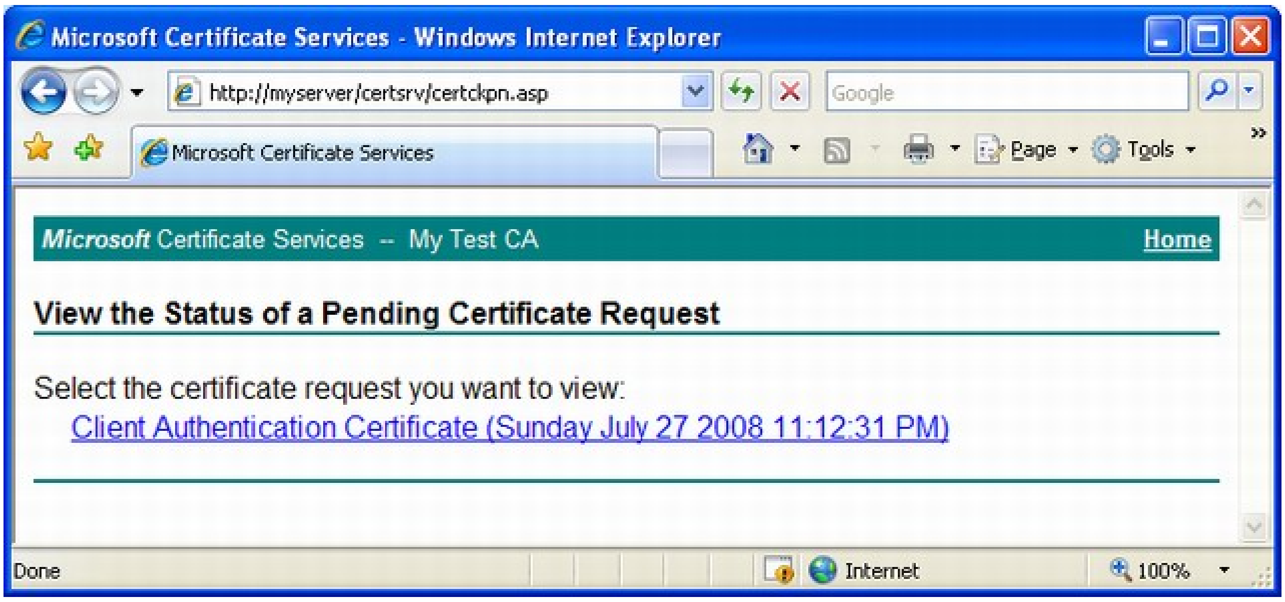
**Note:** You must return with **this** web browser within 10 days to retrieve your certificate

7. On the server, select **Start** > **Programs** > **Administrative Tools** > **Certification Authority**
8. Expand the CA and click **Pending Requests**. You should see your client certificate request in the list.



| Request ID | Binary Request | Request Status Code | Request Disposition Message | Request Submission Date |
|---|---|---|---|---|
| 4 | -----BEGIN NE... | The operation comple... | Taken Under Submission | 7/28/2008 12:12 AM |

9. Right-click the request, select **All Tasks** > **Issue** to approve the certificate
10. On the client machine, go back to *http://<server name>/certsrv*
11. Click **View the status of a pending certificate request**

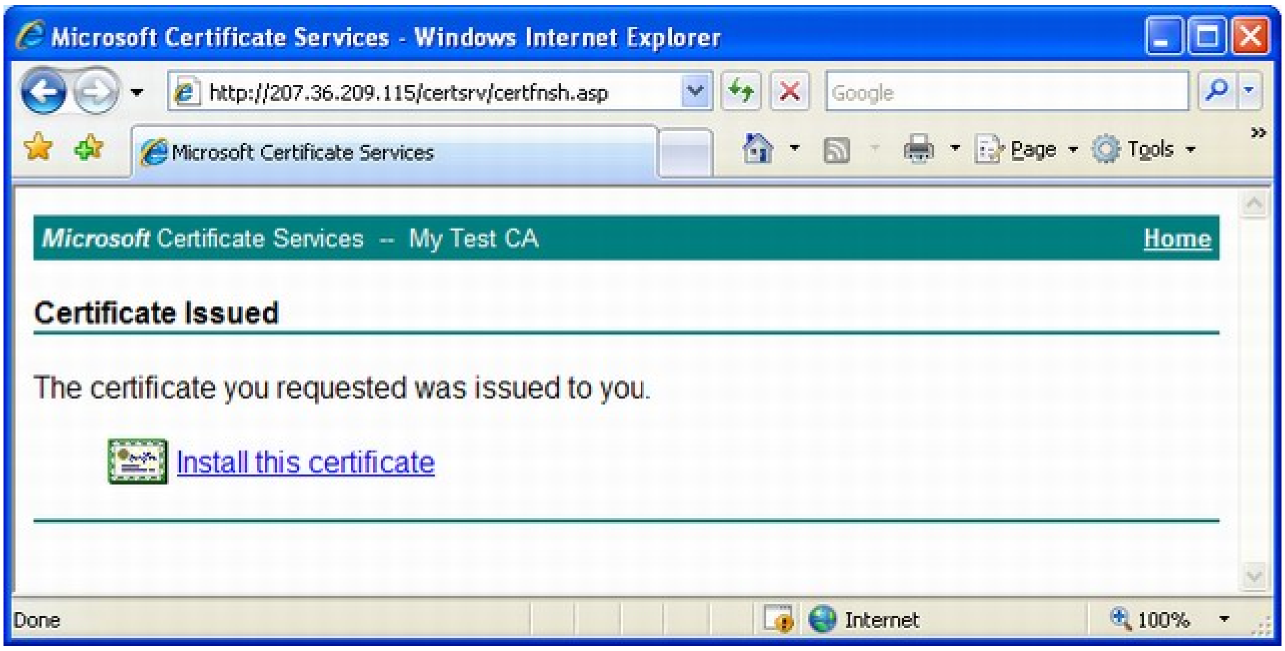

Microsoft Certificate Services - Windows Internet Explorer
http://myserver/certsrv/certckpn.asp
Microsoft Certificate Services
Microsoft Certificate Services -- My Test CA
Home
Done
Internet
100%

View the Status of a Pending Certificate Request

Select the certificate request you want to view:

Client Authentication Certificate (Sunday July 27 2008 11:12:31 PM)

12. Click the **Client Authentication Certificate** link and accept the warning message.


Microsoft Certificate Services - Windows Internet Explorer
http://207.36.209.115/certsrv/certfnsh.asp
Microsoft Certificate Services
Microsoft Certificate Services -- My Test CA
Home
Done
Internet
100%

Certificate Issued

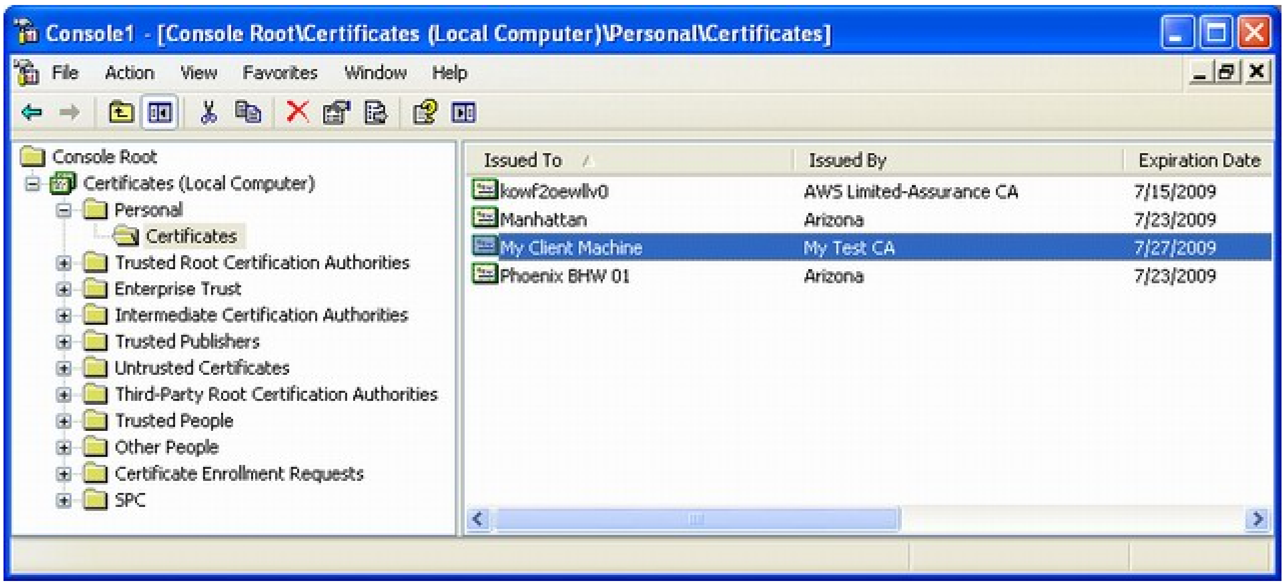
The certificate you requested was issued to you.

Install this certificate

13. Click **Install this certificate** and accept the warning message.

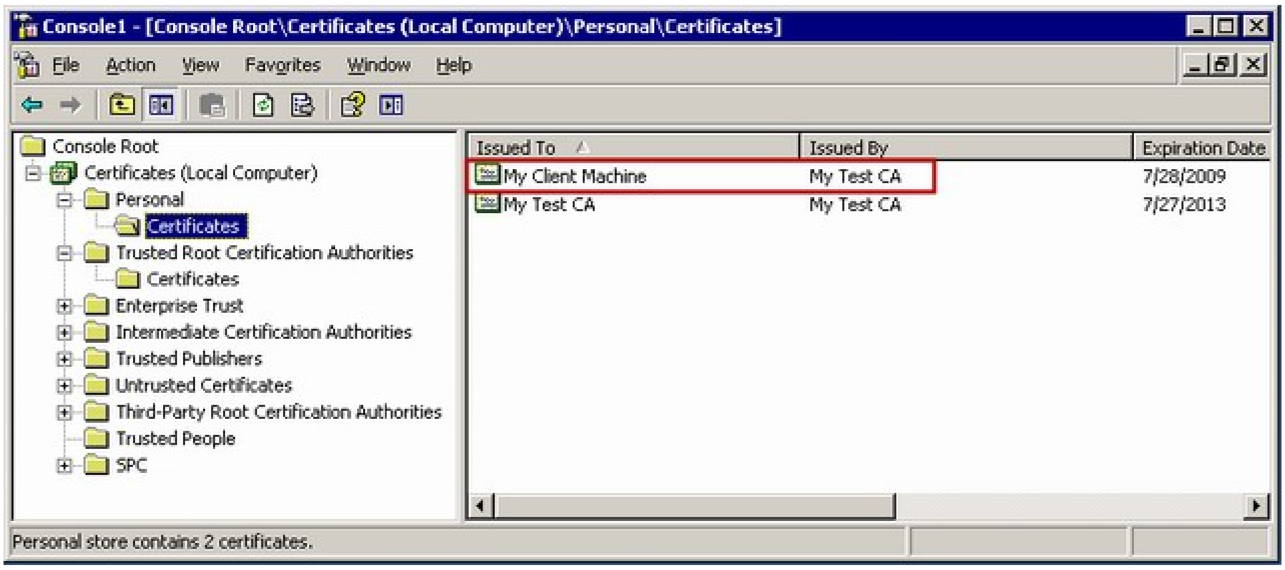
    At this point, the certificate's public and private key are now installed on the client machine. The next step is to install the certificate's public key on the server.

14. Load the Certificates MMC Snap-In on the client machine. Follow these instructions to load the snap-in.
15. Expand **Certificates (Local Computer)** > **Personal** and click **Certificates**


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
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
Other People
Certificate Enrollment Requests
SPC

| Issued To | Issued By | Expiration Date |
|---|---|---|
| kowf2oewllv0 | AWS Limited-Assurance CA | 7/15/2009 |
| Manhattan | Arizona | 7/23/2009 |
| My Client Machine | My Test CA | 7/27/2009 |
| Phoenix BHW 01 | Arizona | 7/23/2009 |

16. Right-click the client certificate and select **All Tasks** > **Export**
17. In the Certificate Export Wizard, click **Next**, **Next**, **Next**, select a file name, **Next**, and **Finish**
18. Copy the exported certificate file to the server
19. Load the Certificates MMC Snap-In on the server machine. Follow these instructions to load the snap-in.
20. Expand **Certificates (Local Computer)** > **Personal**.
21. Right-click **Certificates**, select **All Tasks** > **Import**
22. In the Certificate Import Wizard, click **Next**, select the file that you exported in step 17, click **Next**, **Next**, and **Finish**. The client's public key should now be installed on the server.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
SPC

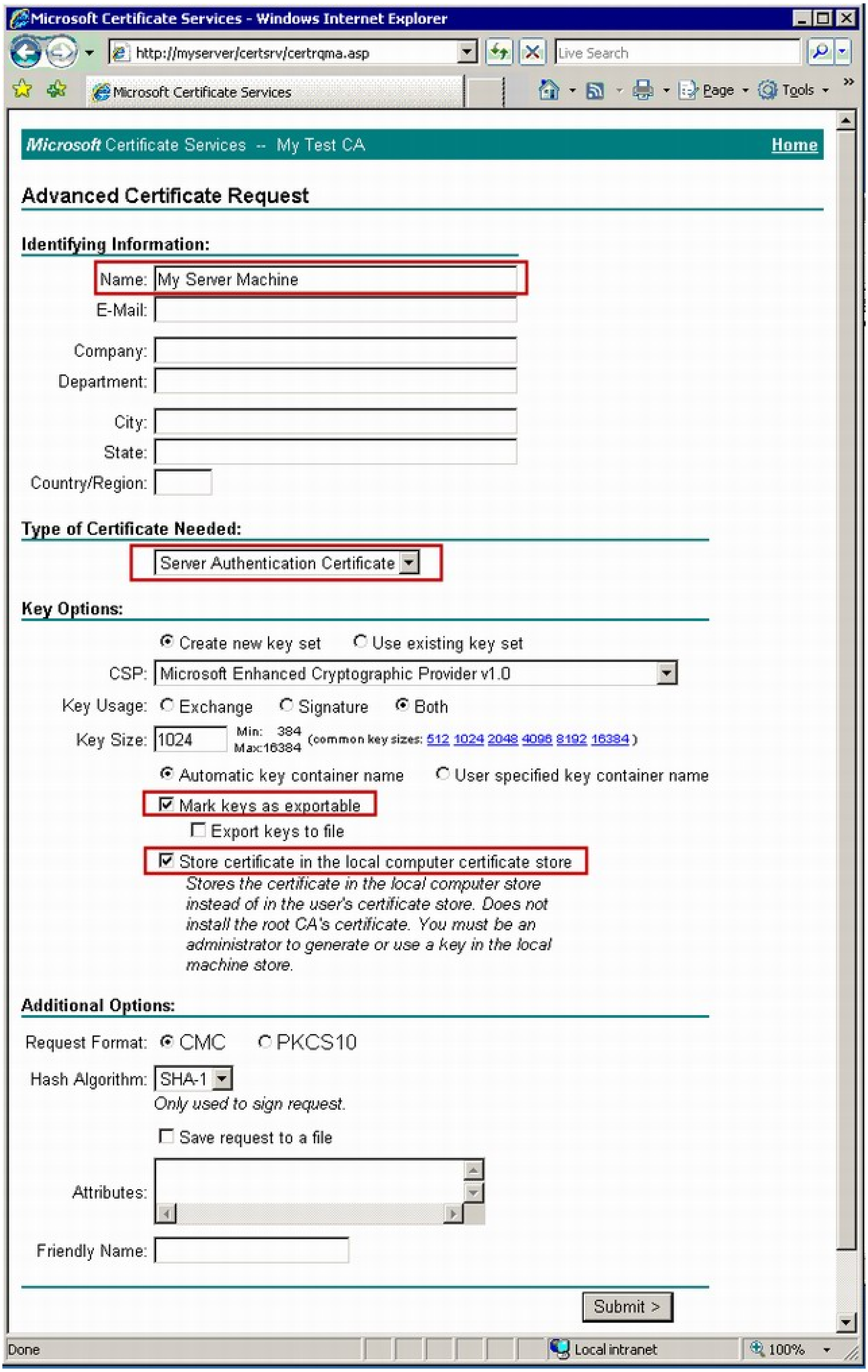
| Issued To | Issued By | Expiration Date |
|---|---|---|
| My Client Machine | My Test CA | 7/28/2009 |
| My Test CA | My Test CA | 7/27/2013 |

Personal store contains 2 certificates.

## Section 4: Create a server certificate

Creating a server certificate is very similar to creating a client certificate, so this section doesn't contain as many screenshots as Section 3.

1. On the server machine, open a web browser and go to *http://<server name>/certsrv*
2. Click **Request a certificate**
3. Click **advanced certificate request**
4. Click **Create and submit a request to this CA**
5. Fill out the form as shown in the image below:


Microsoft Certificate Services - Windows Internet Explorer
http://myserver/certsrv/certrqma.asp
Live Search
Microsoft Certificate Services
Page
Tools
Microsoft Certificate Services -- My Test CA
Home

Advanced Certificate Request

Identifying Information:

Name: My Server Machine
E-Mail:
Company:
Department:
City:
State:
Country/Region:

Type of Certificate Needed:

Server Authentication Certificate

Key Options:

[✓ Create new key set] Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange Signature [✓ Both]

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384 )

[✓ Automatic key container name] User specified key container name

☑ Mark keys as exportable

☐ Export keys to file

☑ Store certificate in the local computer certificate store

*Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.*

Additional Options:

Request Format: [✓ CMC] PKCS10

Hash Algorithm: SHA-1

*Only used to sign request.*

☐ Save request to a file

Attributes:

Friendly Name:

6. Click **Submit** and accept the warning message. You will see a confirmation that your request has been received and is pending.
7. On the server, select **Start** > **Programs** > **Administrative Tools** > **Certification Authority**
8. Expand the CA and click **Pending Requests**. You should see your client certificate request in the list.
9. Right-click the request, select **All Tasks** > **Issue** to approve the certificate
10. Go back to *http://<server name>/certsrv*
11. Click **View the status of a pending certificate request**
12. Click the **Server Authentication Certificate** link and accept the warning message.
13. Click **Install this certificate** and accept the warning message.
14. Now, if you try to load your service in a browser, you would likely get an error similar to the following:

    *System.Security.Cryptography.CryptographicException: Keyset does not exist*
    *ArgumentException: The certificate 'CN=My Server Machine' must have a private key that is capable of key exchange. The process must have access rights for the private key.*

    To fix this problem, we need to give the ASPNET or NETWORK SERVICE account permission to read the certificate. This can be achieved with the following tool:

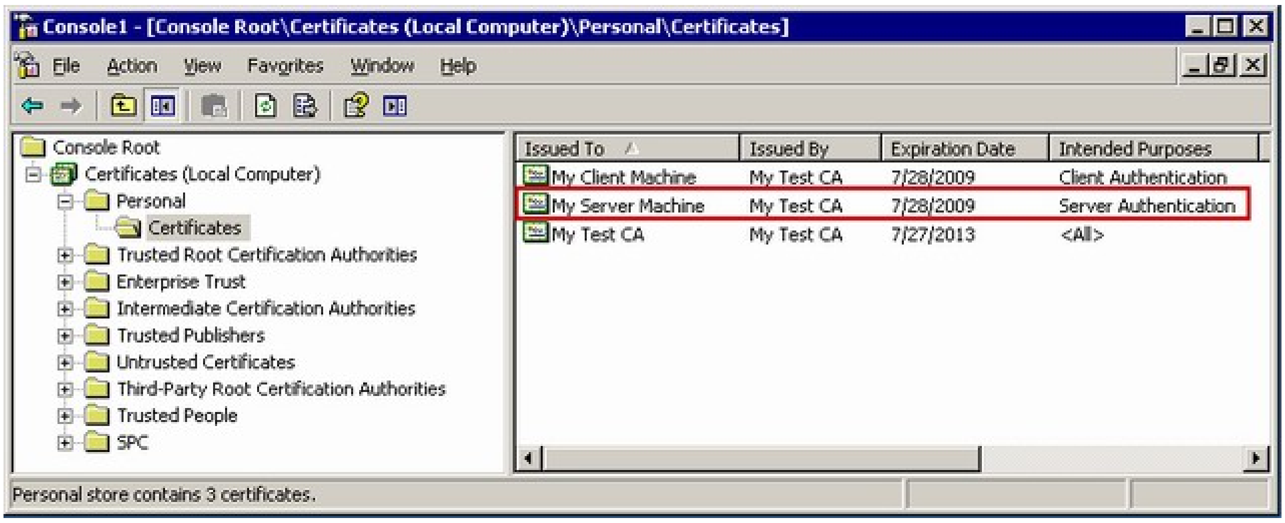
    Windows HTTP Services Certificate Configuration Tool

    Once this tool is downloaded, execute one of the following commands (depending on your server configuration).

```
C:\Program Files\Windows Resource Kits\Tools>winhttpcertcfg -g -c
     LOCAL_MACHINE\My -s "My Server Machine" -a ASPNET
C:\Program Files\Windows Resource Kits\Tools>winhttpcertcfg -g -c
     LOCAL_MACHINE\My -s "My Server Machine" -a "NETWORK SERVICE"
```

    At this point, the certificate's public and private key are now installed on the server machine. The next step is to install the certificate's public key on the client.

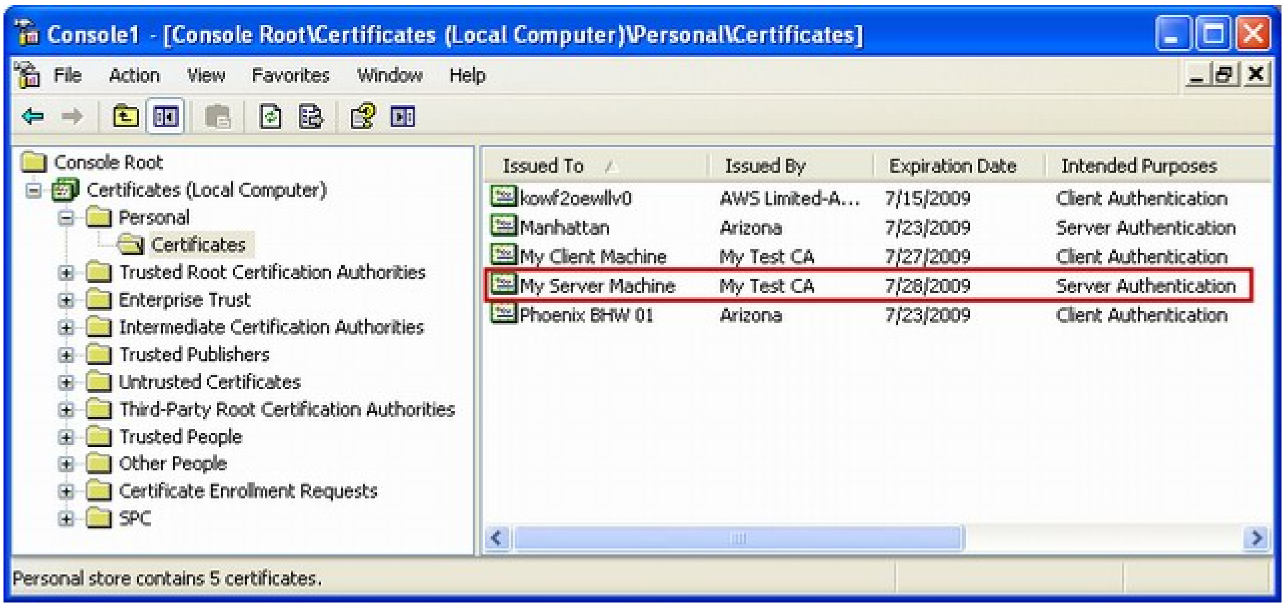
15. Load the Certificates MMC Snap-In on the server machine. Follow these instructions to load the snap-in.
16. Expand **Certificates (Local Computer)** > **Personal** and click **Certificates**


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
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
SPC

| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| My Client Machine | My Test CA | 7/28/2009 | Client Authentication |
| My Server Machine | My Test CA | 7/28/2009 | Server Authentication |
| My Test CA | My Test CA | 7/27/2013 | <All> |

Personal store contains 3 certificates.

17. Right-click the server certificate and select **All Tasks** > **Export**
18. In the Certificate Export Wizard, click **Next**, **Next**, **Next**, select a file name, **Next**, and **Finish**
19. Copy the exported certificate file to the client
20. Load the Certificates MMC Snap-In on the client machine. Follow these instructions to load the snap-in.
21. Expand **Certificates (Local Computer)** > **Personal**.
22. Right-click **Certificates**, select **All Tasks** > **Import**
23. In the Certificate Import Wizard, click **Next**, select the file that you exported in step 17, click **Next**, **Next**, and **Finish**. The server's public key should now be installed on the client.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
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
Other People
Certificate Enrollment Requests
SPC

| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| kowf2oewllv0 | AWS Limited-A... | 7/15/2009 | Client Authentication |
| Manhattan | Arizona | 7/23/2009 | Server Authentication |
| My Client Machine | My Test CA | 7/27/2009 | Client Authentication |
| My Server Machine | My Test CA | 7/28/2009 | Server Authentication |
| Phoenix BHW 01 | Arizona | 7/23/2009 | Client Authentication |

Personal store contains 5 certificates.

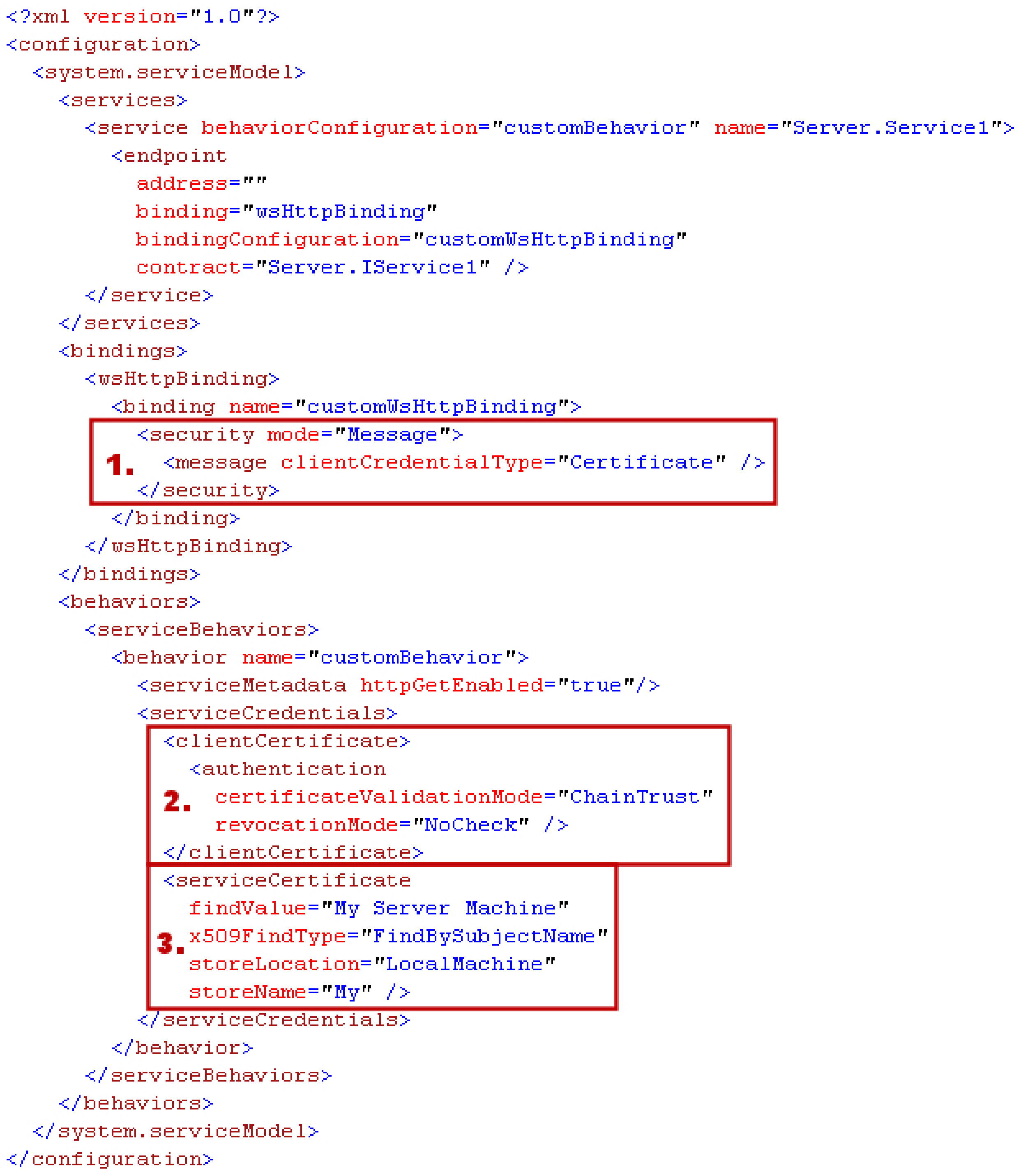
## Section 5: Certificate Review

We have now accomplished the following:

- Created a Certificate Authority on the server machine
- Trusted the Certificate Authority on the clinet machine
- Created a client certificate on the client machine
- Installed the client certificate's public key on the server machine
- Created a server certificate on the server machine
- Installed the server certificate's public key on the client machine

## Section 6: WCF Service Configuration Changes

The following is the WCF service's *web.config* file:



```
<?xml version="1.0"?>
<configuration>
  <system.serviceModel>
    <services>
      <service behaviorConfiguration="customBehavior" name="Server.Service1">
        <endpoint
          address=""
          binding="wsHttpBinding"
          bindingConfiguration="customWsHttpBinding"
          contract="Server.IService1" />
      </service>
    </services>
    <bindings>
      <wsHttpBinding>
        <binding name="customWsHttpBinding">
          <security mode="Message">
            <message clientCredentialType="Certificate" />
          </security>
        </binding>
      </wsHttpBinding>
    </bindings>
    <behaviors>
      <serviceBehaviors>
        <behavior name="customBehavior">
          <serviceMetadata httpGetEnabled="true"/>
          <serviceCredentials>
            <clientCertificate>
              <authentication
                certificateValidationMode="ChainTrust"
                revocationMode="NoCheck" />
            </clientCertificate>
            <serviceCertificate
              findValue="My Server Machine"
              x509FindType="FindBySubjectName"
              storeLocation="LocalMachine"
              storeName="My" />
          </serviceCredentials>
        </behavior>
      </serviceBehaviors>
    </behaviors>
  </system.serviceModel>
</configuration>
```

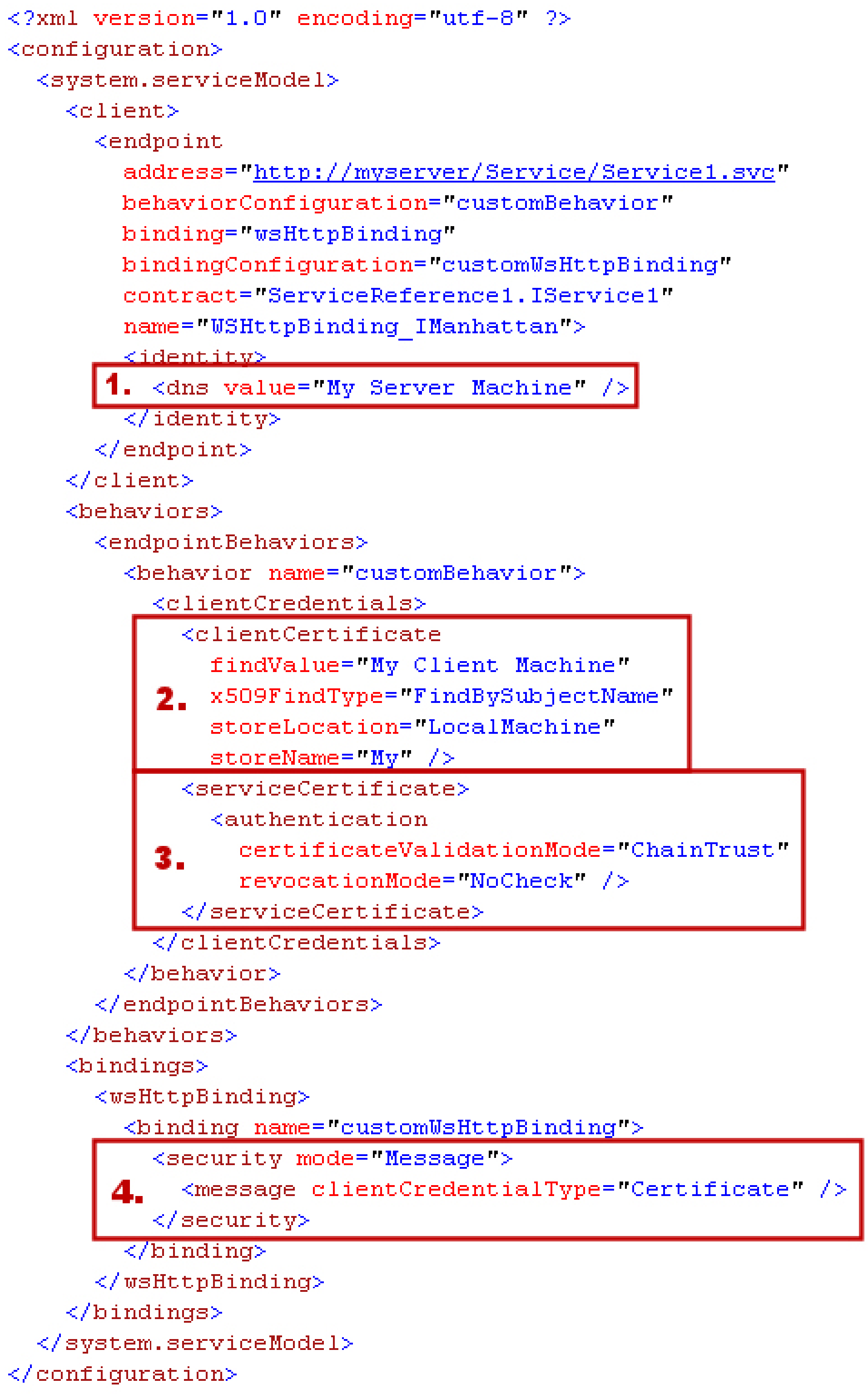
1. Message security via certificates has been enabled on the custom binding.
2. The client certificate requirements have been defined on the custom behavior. The **ChainTrust** value specifies that the certificate chain must be validated. The `revocationMode` is set to **NoCheck**. It is recommended that this value be set to **Online** in a production environment so that revoked certificates are not allowed. This requires that you have a properly configured revocation server. This is outside of the scope of this article, but the following page will point you in the right direction:

   Specify certificate revocation list distribution points in issued certificates

3. The Location of the server certificate has been specified on the custom behavior. Note that you may want to use a more specific search method than `FindBySubjectName` since you may have multiple certificates with the same subject. `FindByThumbprint` should be sufficient for locating a unique certificate.

## Section 7: WCF Client Configuration Changes

The following is the WCF client's *app.config* file:



```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.serviceModel>
    <client>
      <endpoint
        address="http://myserver/Service/Service1.svc"
        behaviorConfiguration="customBehavior"
        binding="wsHttpBinding"
        bindingConfiguration="customWsHttpBinding"
        contract="ServiceReference1.IService1"
        name="WSHttpBinding_IManhattan">
        <identity>
          <dns value="My Server Machine" />
        </identity>
      </endpoint>
    </client>
    <behaviors>
      <endpointBehaviors>
        <behavior name="customBehavior">
          <clientCredentials>
            <clientCertificate
              findValue="My Client Machine"
              x509FindType="FindBySubjectName"
              storeLocation="LocalMachine"
              storeName="My" />
            <serviceCertificate>
              <authentication
                certificateValidationMode="ChainTrust"
                revocationMode="NoCheck" />
            </serviceCertificate>
          </clientCredentials>
        </behavior>
      </endpointBehaviors>
    </behaviors>
    <bindings>
      <wsHttpBinding>
        <binding name="customWsHttpBinding">
          <security mode="Message">
            <message clientCredentialType="Certificate" />
          </security>
        </binding>
      </wsHttpBinding>
    </bindings>
  </system.serviceModel>
</configuration>
```

1. The client is communicating with a server called **myserver**, but the server is identifying itself as **My Server Machine** (as defined in the certificate). As a workaround, we have set the **dns** value to **My Server Machine**. This is not necessary if the certificate matches the host name.
2. The Location of the client certificate has been specified on the custom behavior.
3. The server certificate authentication options have been defined on the custom behavior.
4. Message security via certificates has been enabled on the custom binding.

Your client should now be able to securely communicate with the service.

## Conclusion

As you can see, using WCF with certificates can be a tedious process, but there are certain scenarios that warrant this level of security. I hope this article helps you avoid some of the common pitfalls associated with this security solution.

## License

This article, along with any associated source code and files, is licensed under The Code Project Open License (CPOL)

## Share

## About the Author

**Jason Hodges**
Software Developer Auctane LLC
United States

Jason Hodges develops applications for eBay sellers that help improve their productivity. Jason has been developing Microsoft solutions since 1996 and has consulted with such organizations as Hewlett-Packard, Dell, eBay, and the State of Texas. He is a Microsoft Certified Solution Developer.

## You may also be interested in...

**The Hybrid Cloud**

**IoT Reference Implementation: How to Build an Environment Monitor Solution**

**Creating a WCF Service with MSMQ Communication and Certificate Security**

**Equipment Activity Monitor in Python**

**An easy way to use certificates for WCF security**

**10 Ways to Boost COBOL Application Development**

## Comments and Discussions

**36 messages** have been posted for this article Visit **https://www.codeproject.com/Articles/28248/Securing-WCF-Services-with-Certificates** to post and view comments on this article, or click **here** to get a print view with messages.

Permalink | Advertise | Privacy | Terms of Use | Mobile
Web02 | 2.8.170422.1 | Last Updated 30 Jul 2008

Select Language ▼

Article Copyright 2008 by Jason Hodges
Everything else Copyright © CodeProject, 1999-2017