

Securing your *Microsoft Internet Information Services (MS IIS) Web Server* with a *thawte Digital Certificate*

A STEP-BY-STEP GUIDE to test, install and use a
thawte Digital Certificate on your MS IIS Web Server...

1. Overview
2. System Requirements
3. Generate your Private Key & Certificate Signing Request (CSR) Pair
4. Backing up your Private Key File
5. Requesting a *thawte* Test Certificate
6. Installing a *thawte* Test Certificate
7. Requesting a Trusted *thawte* Certificate
8. Installing a Trusted *thawte* Certificate
9. Configuring the Certificate for use in MS IIS
10. Export the Trusted *thawte* Certificate with the Private Key Attached after Installation
11. Useful URLs
12. What Role Does *thawte* Play?
13. The Value of Authentication
14. Contact *thawte*
15. Glossary of Terms

1. Overview

In this guide you will find out how to test, purchase, install and use a thawte Digital Certificate on your Microsoft Internet Information Services (MS IIS) web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

We will also touch on the role of thawte as a trusted third party and how using a thawte digital certificate can benefit your business by addressing unique online security issues to build customer confidence.

The information in this guide applies to:

Microsoft Internet Information Services version 4.0
Microsoft Internet Information Services version 5.0
Microsoft Internet Information Services version 5.1
Microsoft Internet Information Services version 6.0

2. System Requirements

You must have the latest Service Pack installed for the particular version of MS IIS being used.

Service Pack guideline:

- If you are running MS IIS 4.0, you should have Service Pack 6a installed.
- If you are running MS IIS 5.0 or MS IIS 5.1, you should have Service Pack 3 installed.

For the latest MS IIS Service Packs, please refer to the Microsoft's support web site at the following url:

[http://support.microsoft.com/default.aspx?scid=FH;\[LN\];sp&](http://support.microsoft.com/default.aspx?scid=FH;[LN];sp&)

USEFUL WEBSITES:

<http://support.microsoft.com/default.aspx?scid=fh;en-us;iis>

<http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis50>

<http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis60>

3. Generating your Private Key and Certificate Signing Request (CSR) Pair

Before you can begin the process of obtaining a Certificate, you must generate a [Private Key](#) and [CSR](#) pair off the web server. This is done through the IIS Management Console (IIS must be installed before you can generate a Private Key and CSR pair off the web server).

A CSR is basically a [Public Key](#) that you generate on your server that validates the computer-specific information about your web server and Organization when you request a Trusted Certificate from *thawte*.

Digital ID's make use of a technology called Public Key Cryptography. Before you can enroll for a Certificate, a Private Key and Certificate Request (CSR) must be generated from the server. The Public Key, also known as a Certificate Signing Request (CSR), is the key that must be sent to *thawte*.

The Private Key must remain on the server and should never be released into the public domain. *thawte* does not have access to your Private Key. It is generated locally on your server and is never transmitted to *thawte*. The integrity of your Digital ID depends on your private key being controlled and known exclusively by you.

A CSR cannot be generated without generating a Private Key file nor can the Private Key file be generated without generating a CSR file. Both are generated simultaneously through the Wizard on the web server.

Typically, you will be prompted to enter the following information about your Organization in order to generate the Private Key and CSR pair off the web server:

- Organization Name
- Organizational Units
- Country Code
- State or Province
- Locality
- Common Name*

*Important Note:

The term "common name" is X.509 terminology for the name that distinguishes the Certificate best, and ties it to your Organization. In the case of SSL Web Server Certificates and 128-bit SuperCerts, enter your exact host and domain name that you wish to secure. This may also be the root server or intranet name for your Organization.

Example: If you wish to secure www.mydomain.com, then you will need to enter the exact host (www) and domain name in this field.

If you enter mydomain.com then the Certificate issued to you will only work error free on that exact domain name. It will cause an error when you or your users access the domain name as www.mydomain.com

- To generate a Private Key and CSR pair in MS IIS 4.0, please follow the steps outlined in the following url:

<http://www.thawte.com/html/SUPPORT/keygen/iis4.html>

- To generate a Private Key and CSR pair in MS IIS 5.0 or MS IIS 5.1, please follow the steps outlined in the following url:

<http://www.thawte.com/html/SUPPORT/keygen/msiis5/msiis5.html>

- To generate a Private Key and CSR pair in MS IIS 6.0, please follow the steps outlined in the following url:

<http://www.thawte.com/html/SUPPORT/keygen/iis6/index.html>

The CSR file created in the above step is saved in text format and when viewed will look similar to the following example:

-----BEGIN CERTIFICATE REQUEST-----

```
MIIB2TCCAUICAQAwwZgx CzAJBgNVBAYTAiVTMRAwDgYDVQQIEwdHZW9yZ2IhMREwDwYD
VQQHEwhDb2x1bWJ1czEhMBkGB1UEChMSQUZMQUgSW5jb3Jwb3JhdGVkMQswCQYDVQ
QLEwJJVDEYMBYGA1UEAxMPd3d3LmFmbGFjbkuY29tMSAwHgYJKoZIhvcNAQkBFhFKR2F
ybW9uQGFmbGFjLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGgYkCgYEAAsRqHZCLlrlxqqh
8qs6hCC0KR9qEPX2buwmaA6GxeglCKpOi/IYY5+Fx3KZWXmta794nTPShh2lmRdn3iwxwQRKy
qYKmp7wHCwtNm2taCRVoboCQOuyZjS+DG9mj+bOrMK9rLME+9wz1f8i0FuArWhedDBnl2sm
OKQID45mWwB0hkCAwEAAaAAMA0GCSqGSIb3DQEBAUAA4GBAJNixhOiv9P8cDjMsqyM0
WXxXWgagdRaGoa8tv8R/UOuBOS8/Hqu73umaB9vj6VHY7d9RKqDEIFc/xlXeDwoXNiF8quTm4
3pmY0WcqnL1JZDGHMQkzzGtg502CLTHMEIUGTdKpAK6rJCkucP0DKKEJKcmTySSnvgUu7m
-----END CERTIFICATE REQUEST-----
```

4. Backing up your Private Key File

Important Note:

By far the most **common problem** users have when going through this process is related to **Private Keys** due to the Private Key export instructions not being a part of the actual Wizard when generating the CSR. The main problem is that many users do not know that the Private Key is generated at the same time as the public key (it is just that the private key is not visible to the user).

If you lose or cannot access the Private Key or lose the password used to protect the export of the Private Key file, you will not be able to use the Certificate we issue to you. To ensure this never happens, we advise that a backup of the Private Key file is made to a removable disk and that a note is made of the password used to protect the export of the Private Key.

- **To backup your Private Key file in MS IIS 4.0**, please follow the steps outlined in the following Knowledge Base solution:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs5500>

- **To backup your Private Key file in MS IIS 5.0 or MS IIS 5.1**, please follow the steps outlined in the following Knowledge Base solution:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs2065>

- **To backup your Private Key file in MS IIS 6.0**, please follow the steps outlined in the following Knowledge Base solution:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22515>

5. Requesting a *thawte* Test Certificate

To familiarize yourself with the workings of a *thawte* Certificate on a Microsoft Internet Information Services web server, you can set up a test certificate on your server using a *thawte* Test Certificate.

Our free test certificates are valid for 21 days and this service comes with ABSOLUTELY NO WARRANTY!

You can request a *thawte* test certificate online from:
<http://www.thawte.com/ucgi/gothawte.cgi?a=w39420133617014000>

You will be asked to copy and paste your CSR (Certificate Signing Request) into the text area provided on the Test Certificate System page.

Note: you will need to copy and paste the CSR, including the dashes and the full BEGIN and END line statements.

The test certificate will be generated immediately based on the CSR provided and you will be able to see it on the next page.

Copy and paste the Certificate, including the dashes and the full BEGIN and END line statements, into Notepad, as per the example below.

Save the test certificate to a file called: **testcert_mydomain.crt**

The Certificate file created in the above step will look similar to the following example:

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAm6gAwIBAgIDcxV2MA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQT
EiMCAGA1UECBMZRk9SIFRFU1RJTkcglUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGHh d3RIIENlcnRpZmljYXRpb24xZjZAVBgNVBAStDIRFU1QgVEVTVCBURVNUMRwwGgYDVQQDE
xNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTAyMTEwNTemJhDUzMloXDTAyMTEyNjE0MDU
zMlowgd8xFDASBgNVBAMTC3d3dy5jcmRiLmJIMRswGQYDVQQQLHhIAQwBPAEwAVABAAarfJ
sdQBTAfQxczBxBgNVBAoeagBDAGEAcAAgAEcAZQBtAGkAbgBpACAAVABIAGwAZQBjAG8A
bQAgaE0BZqBkAGkAYQAgaCYAIABOAGUAdAB3AG8AcgBrAHMAIABCAGUAbABnAGkAdQB
BkRpZWdlbTeCXMBUGA1UECBMOVmxhYW1zIEJyYWJhbnQxZCZAJBgNVBAYTAkFmIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDaNm3HPzG6Rbk5Am0HI6JFHodQku2/YmVMGb
Zk5AHeR13QxIP7UVa08/k8qR3B7B0mfbxaNlxdwV9c7c1z4mZYQRfAeryoW4sU2jh1OHc4Cin+i
9UarkHm8WnUnlcVZEnJrySdfLZNuxtbnkXBNkca8rk6tnlbXodD3gEQJBMJtQIDAQABoyUwIzAT
-----END CERTIFICATE-----
```

6. Installing a *thawte* Test Certificate

- **To install the Certificate in MS IIS 4.0**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs8385>
- **To install the Certificate in MS IIS 5.0 or MS IIS 5.1**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7547>
- **To install the Certificate in MS IIS 6.0**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22518>

Once installed, please proceed to Step 9 Configuring Certificate for use in MS IIS.

Notes for *thawte* Test Certificates:

The test certificate will provide encryption, but whenever an SSL session is established to your server with a test certificate installed, a warning message will be displayed. This message informs the user connecting that the certificate is not Trusted, and as such the integrity of the site cannot be guaranteed.

You can get your browser to Trust that test certificate by clicking <http://www.thawte.com/html/SUPPORT/keygen/servertest.crt> and following the instructions provided in the Wizard for installing the thawte Test CA Root Certificate.

7. Requesting a Trusted *thawte* Certificate

You will need to follow the steps outlined in Steps 3 and 4 in order to be able to request a Trusted Certificate from *thawte*.

You should **NOT** get a Test Certificate and then request a Trusted Certificate from *thawte* using the **SAME CSR and PRIVATE KEY PAIR**. The process to replace a Test Certificate with a Trusted Certificate that used the same Private Key/CSR is not an easy process and is therefore not recommended.

thawte's certification practices are of the highest standard. We believe that excellent authentication and verification procedures are absolutely essential in order to ensure trust on the Internet.

thawte SSL Web Server Certificates and 128-Bit SuperCerts may be requested online from <https://www.thawte.com/buy>

During the certificate request process, you will be asked to copy and paste your CSR (Certificate Signing Request) into a text area on the online enrollment form.

Note: you will need to copy and paste the CSR, including the dashes and the full *BEGIN* and *END* line statements.

You will need to provide all the requested information during the enrollment process, and send us documentation proving you, or your Company's identity (a Company Registration certificate for instance). Further detailed instructions for obtaining *thawte* SSL Web Server Certificates or 128-bit SuperCerts are available at: <http://www.thawte.com/html/whatyouneed.html>

Once you have completed the online request process, *thawte* will initiate a number of steps to verify your identity and the details you provided in the CSR. *thawte* performs a considerable amount of background checking before it issues a Certificate. As a result, it may take a few days to verify your Company identity and details, and issue the Certificate.

During this period, you can track the progress of your request

<https://www.thawte.com/cgi/server/status.exe>

Should you have any queries during this period, you may contact the Customer Service Representative assigned to your request. The details of the Representative can be found on your Status Page, at the above URL, under "*thawte* Contact Person".

Once your identity and CSR details have been verified, the Certificate will be issued. The Technical Contact listed for the request will receive an email with a link to where the Certificate can be downloaded from, once the Certificate has been issued.

Copy and paste the Certificate, including the dashes and the full BEGIN and END line statements, into Notepad, as per the example below.

Save the issued Certificate to a file called: **realcert_mydomain.crt**

Note: You should preferably assign the Certificate a name that will distinguish it from the Test Certificate requested earlier.

The Certificate file created in the above step will look similar to the following:

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAm6gAwIBAgIDcxV2MA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJaQT
EiMCAGA1UECBMZk9SIFRFU1RJTkcglUFVSUE9TRVMgT05MWTEdMBsGA1UEChMUUVGhh
d3RIIENlcnRpb24xZmZAVBgNVBAsTDIRFU1QgVEVTVCBURVNUMRwwGgYDVQQDE
xNUaGF3dGUgVGZzdCBDQSBSb290MB4XDTAyMTEwNTemJhDUzMloXDTAyMTEyNjE0MDU
zMlowgd8xFDASBgNVBAMTC3d3dy5jcmRlLmJIMRswGQYDVQQLHhIAQwBPAEwAVABAAarfJ
sdQBTAfQxczBxBgNVBAoeagBDAGEAcAAgAECZQBtAGkAbgBpACAAVABIAGwAZQBjAG8A
bQAgaE0BZqBkAGkAYQAgACYAIABOAGUAdAB3AG8AcgBrAHMAIABCAGUAbABnAGkAdQB
BkRpZWdlbTeCxMBUGA1UECBMOVmxhYW1zIEJyYWJhbnQxXzAjBjBjNVBAYTAkJFMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDaNm3HPzG6Rbk5Am0HI6JFHODQku2/YmVMGg
Zk5AHeR13QxIP7UVa08/k8qR3B7B0mfbxaNlxdwV9c7c1z4mZYQRfAeryoW4sU2jh1OHc4Cin+i
9UarkHm8WnUnlcVZEnJrySdfLZNuxtbnXBNkca8rk6tnlbXodD3gEQJBMJtQIDAQABoyUwlzAT
-----END CERTIFICATE-----
```

8. Installing a Trusted *thawte* Certificate

Once the Trusted certificate has been issued, you will be able to download it from your Status Page by clicking on the "Fetch Certificate" button (which only appears once the Certificate has been issued).

For detailed instructions on how to download your Trusted Certificate, please refer to the instructions listed in the following *thawte* Knowledge Base solution:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7791>

Important Note:

This Certificate is tied to the Private Key that you created earlier in Step 3, and can only be 'attached' to this Private Key.

If you lose the Private Key to which a certificate is tied or the password used to protect the export of the Private Key file, then your issued certificate is unusable.

- **To install the Certificate in MS IIS 4.0**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs8385>
- **To install the Certificate in MS IIS 5.0 or MS IIS 5.1**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7547>
- **To install the Certificate in MS IIS 6.0**, please follow the steps outlined in the following Knowledge Base solution:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22518>

9. Configuring the Certificate for use in MS IIS

Now that the certificate has been installed, you will need to enable the server as well as any firewall or routers that are in place for secure communications.

To do so, enable the SSL port, which is by default port 443, and assign a unique IP Address for your Certificate on your website.

The Certificate is only issued and tied to the Fully Qualified Domain Name (common name), for which the Certificate was requested. Even though it is not tied to the IP address assigned to the website, a unique IP address is required for each SSL enabled website, as SSL works with IP based virtual hosts.

The IP address assigned to the website can be changed and it will not affect the Certificate at all, provided it remains unique.

Important Note:

SSL does not function when using Host Headers, because they are included in the encrypted request. This is not a limitation of IIS and this behavior is by design.

For further information with regards to this matter, please refer to Microsoft's Knowledge Base article:

[http://support.microsoft.com/default.aspx?scid=kb;\[LN\];Q187504](http://support.microsoft.com/default.aspx?scid=kb;[LN];Q187504)

To enable SSL on MS IIS 4.0, follow the instructions listed below:

1. From the "**Internet Server**" program group, open "**Key Manager**".
2. In the "**Key Manager**" window, select the Key on which your certificate is installed.
3. Right-click on the Key and select "**Properties**".
4. At the "**Server Bindings**" window, click on "**Add**".
5. The "**IP Address**" field must contain the IP address (typed out) of the web site in question.

If you only have one website, then the default "**All Un-assigned**" for your IP address will suffice.

6. Under "**Port Number**", click on the radio button next to "**Port Number**" and add 443. Click on "**OK**" when done.
7. From the "**Computers**" menu, select "**Commit Changes Now**" and when prompted to "**Commit all changes now?**" select "**Yes**".

To enable SSL on MS IIS 5.0, MS IIS 5.1 and MS IIS 6.0, follow the instructions listed below:

1. In the "**Web Site**" tab, the IP address field must contain the IP address (typed out) of the web site in question.

If you only have one website, then the default "**All Un-assigned**" for your IP address will suffice.

2. Click on the "**Advanced**" button next to the IP address field - make sure the SSL port number is listed under "**Multiple SSL identities for this Web site**" section.

You will now be able to access your machine securely via: <https://www.mydomain.com> and view your certificate details.

A golden padlock will appear in the lower toolbar of your browser when the SSL session has been established.

10. Export the Trusted *thawte* Certificate with the Private Key Attached after Installation

Important Note:

It is recommended that you make a backup of the installed Certificate with the Private Key file attached to a removable disk, noting the password used to protect the export of the file.

This is done as a preventative measure to ensure that if your server does crash due to unforeseen circumstances, you will have a backup of both your Certificate and Private Key file.

- **To backup the Certificate with the Private Key attached in MS IIS 4.0**, please see the following url:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs5500>
- **To backup the Certificate with the Private Key attached in MS IIS 5.0 or MS IIS 5.1**, please see the following url:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs1689>
- **To backup the Certificate with the Private Key attached in MS IIS 6.0**, please see the following url:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22520>

11. Useful URLs

Common problems experienced with MS IIS are dealt with in our FAQ's:

- <http://www.thawte.com/html/SUPPORT/server/msiis4.html>
- <http://www.thawte.com/html/SUPPORT/server/msiis5.html>

Troubleshooting Guide for MS IIS 4:

- <http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs6349>

Troubleshooting Guide for MS IIS 5:

- <http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs12399>

Common problems experienced with MS IIS using a *thawte* SSL Web Server Certificates are dealt with in the following FAQ's:

- <http://www.thawte.com/html/SUPPORT/server/general.html>
- <http://www.thawte.com/html/SUPPORT/server/enrollment.html>
- <http://www.thawte.com/html/SUPPORT/server/using.html>
- <http://www.thawte.com/html/SUPPORT/server/renewal.html>

Common problems experienced with MS IIS using *thawte* 128-bit SuperCerts are dealt with in the following FAQ's:

- <http://www.thawte.com/html/SUPPORT/sgc/general.html>
- <http://www.thawte.com/html/SUPPORT/sgc/enrollment.html>
- <http://www.thawte.com/html/SUPPORT/sgc/using.html>
- <http://www.thawte.com/html/SUPPORT/sgc/renewal.html>

12. What Role Does *thawte* Play?

thawte Technologies is a **Certification Authority (CA)** which issues SSL Web Server Certificates and 128-bit SuperCerts to organizations and individuals worldwide. *thawte* verifies that the Organization ordering the certificate is a registered organization and that the person in the organization who ordered the certificate is authorized to do so.

thawte also checks that the organization in question owns the relevant domain. *thawte* digital certificates interoperate smoothly with the latest software from Microsoft and Netscape, so you can rest assured that your purchase of a *thawte* Web Server Certificate will give your customers confidence in your system's integrity - they will feel secure about transacting online.

13. The Value of Authentication

Information is a critical asset to your business. To ensure the integrity and safety of your information, it is important to identify with whom you are dealing, and that the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in all types of transactions by addressing a unique set of security issues including:

Spoofing: The low cost of website design and the ease with which existing pages can be copied makes it all too easy to create illegitimate websites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional looking storefronts that mimic legitimate businesses.

Unauthorized Action: A competitor or disgruntled customer can alter your website so that it malfunctions or refuses to service potential clients.

Unauthorized Disclosure: When transaction information is transmitted "in the clear", hackers can intercept the transmissions to obtain sensitive information from your customers.

Data Alteration: The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers and currency amounts sent "in the clear" are all vulnerable to alteration.

14. Contact *thawte*

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:

E-Mail: sales@thawte.com

Telephone: +27 21 917 8902

Fax: +27 21 917 8967

15. Glossary of Terms

Asymmetrical Cryptography

A cryptographic method using a combined public and private key pair to encrypt and decrypt messages. To send an encrypted message, a user encrypts a message with the recipient's public key. Upon receipt, the message is decrypted with the recipient's private key. Using different keys to perform the encryption and decryption functions is known as a trap-door one way function, that is, the public key is used to encrypt a message but it cannot be used to decrypt the same message. Without knowing the private key, it is practically impossible to reverse this function when modern strong encryption is used.

Certification Authority

A certificate authority (CA) is an organization (such as *thawte*) that issues and manages security credentials and public keys for message encryption.

Certificate Signing Request (CSR)

A CSR is a Public Key that you generate on your server that validates the computer-specific information about your web server and Organization when you request a Certificate from *thawte*.

Private Key

A private key is numeric code used to decrypt messages encrypted with a unique corresponding public key. Integrity of encryption depends on the private key being kept secret.

Public Key

A public key is a numeric code which enables encryption of messages sent to the holder of the corresponding unique private key. The public may be freely circulated without compromising encryption increasing the efficiency and convenience of enabling encrypted communication.

Public Key Infrastructure (PKI)

A method for exchanging information securely within organizations, industries, nations or even worldwide. A PKI uses the asymmetric encryption method for encrypting IDs and documents or messages. (this is also known as the "public/private key" method).

A PKI starts with a certificate authority (CA) such as *thawte*, which issues and revokes digital certificates (digital IDs) authenticating the identity of people and organizations over a public system such as the Internet.

Symmetric Cryptography

A cryptographic method where the same key is used for both encryption and decryption. This approach is handicapped by the security risks involved in secure distribution of the key since it must be communicated to and known by both sender and receiver without being disclosed to third parties.