

SSL GUIDE

Everything you need to know
about SSL and securing your
online business

For Microsoft IIS 5/6



Published by RapidSSL.com

RapidSSL.com US
600 17th Street, Suite 2800 South
Denver, Colorado, USA 80202
Tel: 720 359 1590
Fax: 720 528 8160

RapidSSL.com Europe
155 Regents Park Road
London, England, NW18BB
Tel: +44 870 4325190
Fax: +44 870 4325191

sales@rapidssl.com

Why is security required for the Internet?

The Internet has been a revolution to commerce and the transfer of data in general, which has developed new global business opportunities for all, including major enterprises, small to medium sized businesses and individuals alike. However e-commerce has inevitably attracted crime and developed a new breed of online criminals ranging from fraudsters and hackers to cyber terrorists. The growing concerns associated with conducting e-commerce have now resulted in the fact that security is an essential factor for online business success.

The market is now educated in the basics of online security and the majority of online users now expect security to be integrated into any online service they use and as a result they expect any details they provide via the Internet to remain confidential and secure.

This white paper explains how SSL can be utilized as the core security technology to protect customer's online transactions and informs users that the security of the online business is being taken seriously. In fact SSL provides proof of a digital identity and allows online customers to visibly see that their digital transaction will be confidential. These are essential factors in gaining customer confidence and remove the concerns and risks associated with sending sensitive data over the Internet.

SSL is essential to allow the true benefits of the Internet to be realised.

What is SSL?

SSL (Secure Sockets Layer) is a security technology that is commonly used for encrypting communications between users and e-commerce websites, thereby securing server to browser transactions. The SSL protocol utilizes encryption to prevent eavesdropping and tampering of the transmitted data, and is used to secure information passed by a browser (such as a customer's credit card number or password) to a webserver (such as an online store).

SSL protects data submitted over the Internet from being intercepted and viewed by unintended recipients and as used by hundreds of thousands of websites in the protection of their online transactions with their customers, SSL is the de-facto industry standard Internet transaction security technology.

How do website visitors know if a website is using SSL?

When a website visitor connects to a webserver using SSL they will see that the URL in the address bar begins with https:// rather than the usual http:// and also a small gold padlock will appear in their browser, e.g.



As seen by users of Internet Explorer

Whenever a browser connects to a webserver (website) over https:// - this signifies that the communication will be encrypted and secure. The actual complexities of the SSL protocol remain invisible to the end customer.

In summary, SSL is the de facto web transaction security technology. Webservers have been built to support it and web browsers have been built to use it. SSL provides the ability to secure customers transactions transparently without the customer having to do a thing!

What is required for a webserver (website) to use SSL?

In order for a website to use SSL a SSL Certificate is required (also known as Web Server Certificates and Secure Server Certificates). SSL Certificates are installed onto the webserver hosting the particular website and allow access to the security functionality of the webserver itself.

How is a SSL certificate installed onto a webserver?

When SSL is first activated on the webserver, the webserver requires information about the identity of the website including the website domain name and company details.

The webserver then creates two cryptographic keys - a Private Key and a Public Key. The Private Key is so called for a reason - this key must remain private and secure, only residing on the webserver. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file which also contains all the website credentials.

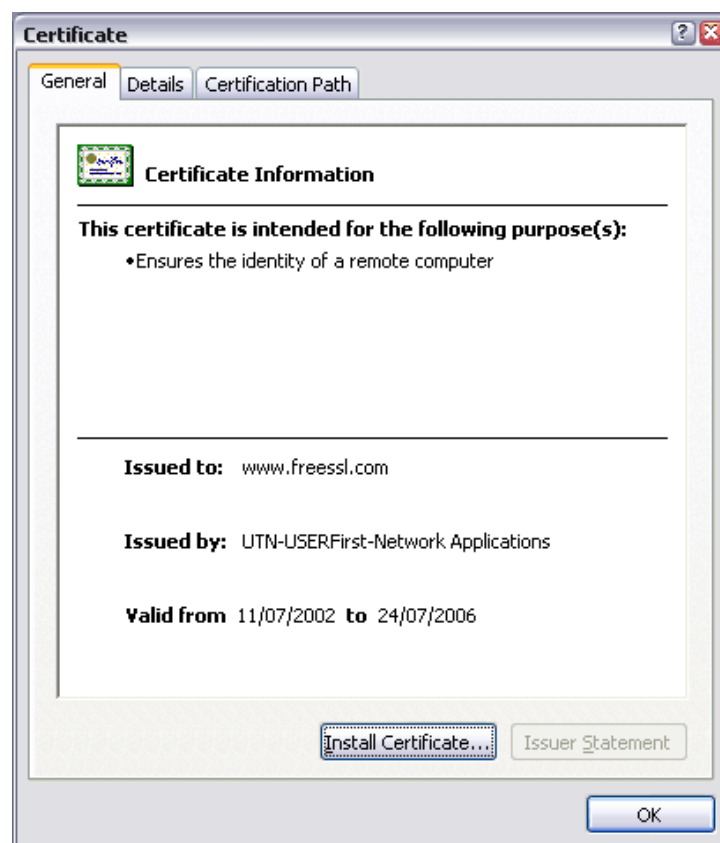
The Private and Public keys are used in the encryption process, so that the data passing between the webserver (website) and the customer's browser remains confidential and secure.

The CSR generated is submitted to Certification Authorities during the SSL Certificate application process. The Certification Authority then validates the website credentials and issues an SSL Certificate containing the digital identity of the website, binding the domain name to the company details.

The webserver will match the issued SSL Certificate to the associated Private Key and allows the webserver to establish encrypted links between the website and customer's browsers.

What does a SSL certificate look like?

SSL certificates can be seen by simply double clicking on the padlock symbol when displayed in the browser. A typical certificate will look like this;



All SSL Certificates are issued to either companies or legally accountable individuals. Typically SSL Certificates contain the domain name, the company name, the address i.e. city, state and country. It will

also contain the expiry date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, that it has been issued by a Certification Authority the browser trusts and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user.

What is a Certification Authority (CA)?

Not just anybody can issue trusted SSL Certificates. If they could then there would be no trust in SSL - and it could no longer be used commercially. Instead only Certification Authorities, or CAs as they are commonly known, can issue trusted SSL Certificates.

CAs have generally invested in establishing the technology, support, legal and commercial infrastructures associated with providing SSL certificates. Even though CAs are essentially self-regulated, the nearest to a regulatory body is the WebTrust compliancy program operated by AICPA/CICA. The majority of CAs comply to the WebTrust principles, however some CAs do not have WebTrust compliance. Those CAs who are WebTrust compliant display the WebTrust Seal, as seen below.



The WebTrust Seal of assurance for Certification Authorities symbolizes to potential relying parties [e.g. to the end customer] that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria. An unqualified opinion from the practitioner indicates that such principles are being followed in conformity with the WebTrust for Certification Authorities Criteria. These principles and criteria reflect fundamental standards for the establishment and on-going operation of a Certification Authority organization or function.

Who are the CAs and why are there so many providers of SSL?

There are actually less than 10 CAs issuing commercially available SSL certificates. The Appendix contains the full list of CAs. Until recently the SSL market has been monopolized by Verisign and Thawte. In 1999 Verisign acquired Thawte, and it became a Verisign subsidiary. In recent years, new global players providing enterprise class solutions such as GeoTrust (formerly Equifax Certificate Services) have also established themselves in the enterprise security market. In the last few months, other companies providing solutions for small to medium sized businesses have also started providing SSL certificates.

There is however confusion in the market because all CAs have reseller programs. Resellers are organizations that will resell the SSL CA's certificates, often at different prices to the SSL CA themselves. Resellers are a great way to sometimes save money through discounted pricing, but are also an easy way to be overcharged for SSL!

Be aware that some resellers will "re-brand" the CA's certificate, thereby masking who actually issues the certificate and then offer their own re-branded certificates at inflated prices above the SRP of the CA themselves.

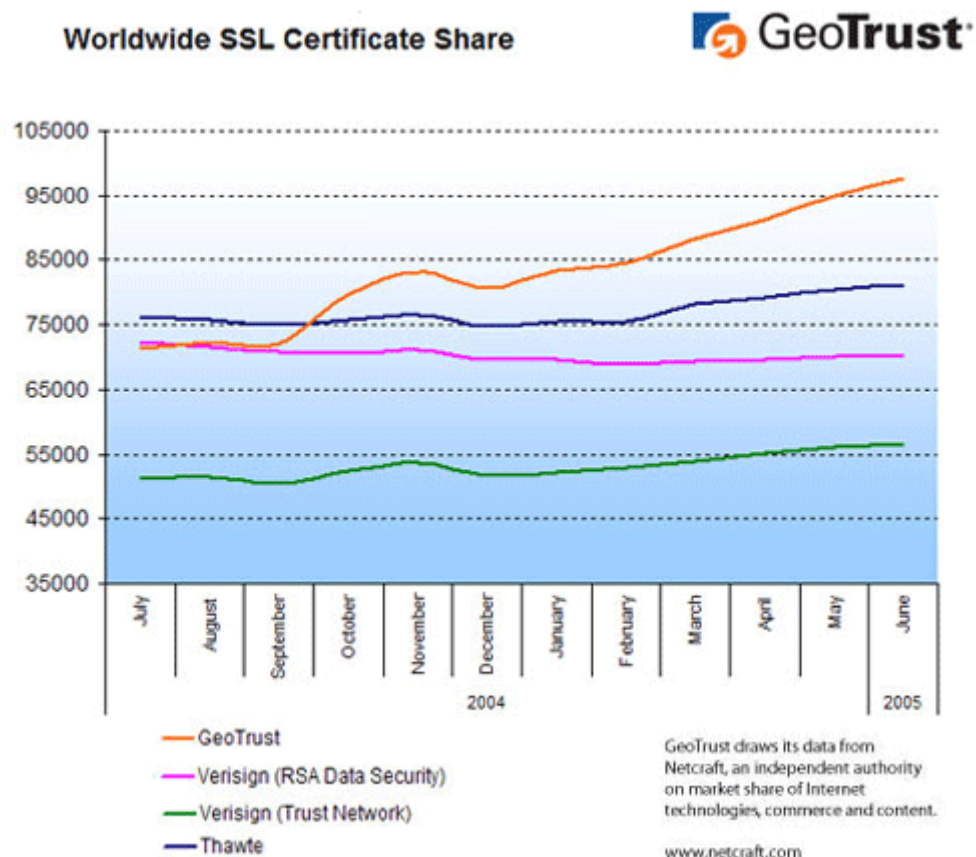
Don't be fooled by unknown brands - if an SSL Certificate is being sold under a brand that is not contained in the attached Appendix, the buyer should examine one of the reseller's example certificates before purchase. It is very likely that the certificate has been issued by a CA featured in this white paper and will probably be available directly from the CA at a different cost, maybe even lower than the reseller offers it.

Resellers provide exactly the same certificate and features provided by the CA themselves, so it is essential for buyers to know which CA that will issue the SSL certificate before purchasing through a reseller!

Who are the top 2 CAs?

Each month Netcraft (www.netcraft.com) publishes the market share of each CA.

The following chart summarizes the market share of the top 2 enterprise players in the .net market, namely Verisign and GeoTrust. The chart also shows the market share of Thawte (Thawte is a Verisign company).



What do I need to consider when purchasing a SSL certificate?

The following 10 considerations must be taken into account before deciding which CA and which type of SSL certificate to purchase? Each point will be discussed in more detail later.

1. What type of web site application. Low volume, professional or development?
2. How credible and stable is the CA issuing the SSL certificate?
3. What browser recognition is required?
4. Do I require a single root or intermediate SSL certificate?
5. What certificate strength is required?
6. Is technical support available from the CA for installation or CSR issues?
7. Do I need warranty?
8. What type of validation is required?
9. How fast do I want my certificate?

10. What budget do I have for my certificate?

Lets look at each point in turn.

1. What type of web site application. Low volume, professional or development?

Perhaps the most important differentiation between all the SSL certificates available on the market today, is the strength of the brand behind the SSL technology. SSL technology besides ensuring secure transmission of data, is an essential element in providing online customers with the confidence to buy or use a product or service.

For example, the greater the number of users visiting a website, the greater the probability that some customers may not complete a transaction, simply because they do not recognise or trust the brand behind the SSL technology.

Inevitably the well known brands from the credible long standing CAs are the most expensive SSL certificates on the market. If you have a low volume or development website and you decide that your customer's confidence is not affected at all by the brand behind the SSL certificate or the volume of customers that would have an issue are insignificant in number then the choice of CA and certificate is increased. Low volume websites can therefore enjoy significant savings on the SSL purchases by purchasing the lesser known brands of SSL certificates.

We suggest as a guide that if a website is performing more than 50 transactions per week then, it is advisable to use a known SSL brand.

Another important consideration is the typical or average transaction value that a website will process. If customers are expected to pay high amounts online the greater the probability that some customers may not complete a transaction because they do not trust the brand behind the SSL technology.

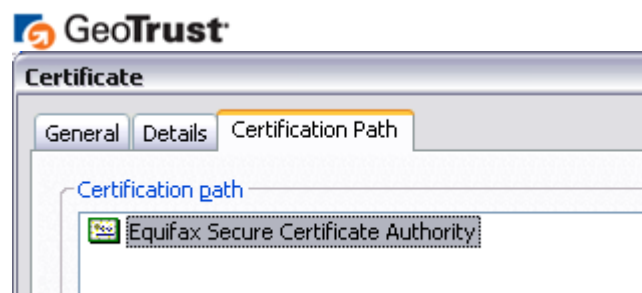
We suggest as a guide that if a website has an average transaction of greater than 50 USD, it is advisable to use a known SSL brand from a reputable CA.

2. How credible and stable is the CA issuing the SSL certificate?

Clearly for any SSL certificate to be taken seriously, it is important to ensure that the CA issuing the SSL certificate is well established and credible. The best way of determining the credibility of a CA is by simply establishing whether the CA in question owns its own trusted root i.e. does the CA own a root that is already present in all popular browsers?

You can examine trusted root ownership by double clicking the padlock seen in the browser during an SSL connection with a webserver. When the SSL Certificate appears, simply click the "Certification Path" tab to see which trusted root CA certificate issued the SSL certificate.

It is also possible to see the trusted roots referenced in a browser e.g. for IE6, go to "Tools", "Internet Options" and select "Content", "Certificates" and then the tab "Trusted Root Certification Authorities".



GeoTrust owns the Equifax root (Equifax Digital Certificate services became GeoTrust in 2001).

RapidSSL.com's RapidSSL and RapidSSL Wildcard product owns its own root. RapidSSL.com uses a different Equifax root (Equifax Secure eBusiness CA-1).

Business stability is also an essential component when selecting any supplier. Whilst we do not examine financial stability of each CA in detail in this white paper, enterprise class accounts are advised to conduct their own due diligence into each CA, as well as examine the root CA certificate ownership.

When selecting a CA, always therefore consider the long term stability of the CA, especially if a longer term enterprise solution is required.

If the CA relies on an intermediate certificate - consider the long-term stability of the CA supplying the intermediate, and obviously the stability of the supplier relationship between the two CAs.

Clearly it is very advisable to ensure the integrity of the CA and to establish which CA is issuing the SSL certificate to be used.

3. What browser recognition is required?

Browser recognition or ubiquity is the term used in the industry to describe the estimated percentage of Internet users that will inherently trust an SSL certificate.

Certification Authorities who own their own roots, have what are known as Root CA Certificates. These root CA certificates are added into releases of all the major browsers such as Internet Explorer, Netscape, Opera, etc by the browser vendor (such as Microsoft). When a browser is used, it automatically relies on a "list" of root CA certificates that the browser vendor has deemed trustworthy. If a SSL certificate is issued by one of the trusted root CAs, then the browser will inherently trust the SSL certificate and the gold padlock will appear transparently during secure sessions.

The browser stores the CA roots that can be trusted, therefore if a browser encounters a website using a SSL certificate issued by a CA root it does not trust, the browser will display warning messages to the website visitor. The lower the browser ubiquity, the less people will trust a certificate - clearly, a commercial site will require as many people as possible to trust a SSL certificate.


The general rule is that any SSL certificate with over 95% browser ubiquity is acceptable for a commercial site.

As with any form of statistics, browser ubiquity is open to interpretation, hence in the Appendix, the table does not place a great deal of validity in presenting browser recognition "percentages", instead it simply concludes whether a SSL Certificate is acceptable for commercial sites.

Why is browser recognition important?

If a website visitor is using a browser that does not contain the root CA certificate used to issue the SSL certificate, they will be prompted with a security warning:



The  signifies that the SSL Certificate has been issued by a CA that the browser does not trust. As more people upgrade their old browsers, this message becomes less frequent. It is also worth noting that people who do not upgrade their browsers are less technically and security savvy and hence are less likely to purchase from websites.

Another consideration often overlooked concerning the overall ubiquity of a SSL certificate is the issue over Webserver Compatibility. The SSL Certificate is required to be installed onto a webserver. Generally, all webserver accept all SSL certificates currently available but it is recommended to check with the CA to be sure. Webserver such as Apache (including the website control panel variants), IIS, Webstar, Website Pro, Java based, iPlanet, Zeus, Netscape server, Cobalt support the certificates of all SSL certificates featured in this whitepaper.

There are few webserver still in use that do not support the use of intermediate certificates. Such webserver are not SSL v3 compliant. If your webserver does not support SSL v3, then you will need to select a CA that issues certificates directly off its root such as GeoTrust and RapidSSL.com.

4. Do I require a single root or intermediate SSL certificate?

Most SSL certificates are issued by CAs who own and use their own Trusted Root CA certificates, such as those issued by GeoTrust and RapidSSL.com. As GeoTrust and RapidSSL.com is known to browser vendors as a trusted issuing authority, its Trusted Root CA certificate has already been added to all popular browsers, and hence is already trusted. These SSL certificates are known as "single root" SSL certificates. RapidSSL.com, a subsidiary of GeoTrust, owns the Equifax Secure eBusiness CA-1 root used to issue its certificates.

Some Certification Authorities, do not have a Trusted Root CA certificate present in browsers, or do not use the root they do own, and use a "chained root" in order for their SSL certificates to be trusted. Essentially a CA with a Trusted Root CA certificate issues a "chained" certificate which "inherits" the browser recognition of the Trusted Root CA. These SSL certificates are known as "chained root" SSL certificates.

For a Certification Authority to have and use its own Trusted Root CA certificate already present in browsers is a clear sign that they are long-time, stable and credible organizations who have long term relationships with the browser vendors (such as Microsoft and Netscape) for the inclusion of their Trusted Root CA certificates. For this reason, such CAs are seen as being considerably more credible and stable than chained root certificate providers who do not have a direct relationship with the browser vendors, or do not use their own root certificates to issue SSL certificates.

Installation of chained root certificates are more complex and some web servers are not compatible with chained root certificates.

RapidSSL.com does not bother inconveniencing you by issuing anything other than single root SSL certificates.

5. What certificate strength is required?

Generally there are two strengths of certificate in existence - 40 bit & 128 bit. 256 bit is now also available but requires a combination of the use of specific browsers (currently Firefox) and a specific web server (currently Apache). All RapidSSL.com and GeoTrust certificates support 256 bit encryption.

The bit size indicates the length of the key size used for the encryption during a secure SSL session. Hovering the mouse over the gold padlock will detail the current strength of encryption being used:



Why is encryption strength important?

The bigger the number, the longer it takes for computer(s) to crack or break the code.

- 40 bit: It is computationally feasible to crack a 40 bit key. For this reason 40 bit encryption is rarely used.
- 128 /256 bit: It is computationally unfeasible to crack a 128 / 256 bit key. All banking infrastructures use 128 / 256 bit encryption. We strongly recommend the use of 128 / 256 bit SSL encryption for any application or website.

6. Is technical support available from the CA should I need it?

Installing a SSL certificate can sometimes be tricky - you will need to first generate a CSR and then install your issued certificate. For this reason it is essential that the CA provides sufficient and timely support.

All CAs provide some level of support, even if it is only email and web based. Most issues can easily be solved using the expansive online resources and knowledge bases provided by the CA. However, should an issue arise, it is highly recommended that there is access to technical support staff, therefore make sure the CA clearly publishes a technical support telephone number. Also, be aware that some CAs charge extra for telephone support.

7. Do I need warranty?

The warranty level is the financial protection awarded to end customers against the CA misissuing an SSL Certificate. If a customer relies on the information within a misissued SSL Certificate and suffers financial loss as a direct result of relying on the certificate, the CA will hold insurance to cover claims made by the customer against the CA. Effectively, the warranty is the insurance taken out by the CA to protect itself in the event it makes a mistake.

Verisign offers a more advanced insurance policy in that it will also provide insurance against a compromise of a private key or loss of certificate - but such insurance comes at a price.

How likely is a mississuance?

It is highly unlikely that a WebTrust compliant CA will misissuance a certificate. All WebTrust compliant CAs have passed certification to ensure that procedures and policies are in place that make misissuance improbable. For this reason, many WebTrust compliant CAs do not offer a warranty at all.

Some CAs will offer the warranty as a means of adding perceived value to their SSL certificates.

8. What type of validation is required?

A trust hierarchy demands that entities "vouch" for each other. Companies that issue SSL certificates are in the business of establishing that entities on the web are, in fact, who they claim to be. The potential for criminal activity on the web (in relevance to SSL anyway), is in online 'hijacking' of sites or connections to siphon encrypted data. Persons so inclined can easily "copy" web site interfaces and pose as well known vendors, simply to collect these data.

SSL certificates work to prevent this through ensuring that www.abc.com is, in fact, ABC Co. In the "real world" we use identification procedures like photo ids, telephone calls and papers of incorporation to know with whom we are dealing. If products or services are defective, buyers can seek recourse. In the "online world", companies wishing to use SSL certificates must prove to the certificate authority that they have the right to present themselves online as ABC Co.

This is done through a variety of means in different SSL products. For the sake of simplicity, consider the method started and championed by Verisign, as the 'traditional' model. The process involves certificate petitioners faxing in their articles of incorporation, and then waiting several days to be granted a certificate to do business online under that name. There is a fair amount of overhead related to this task, as these credentials are examined and reviewed, and full-service products in this arena can cost hundreds of dollars.

There are newer, lower-cost alternatives in which certificates are issued more quickly. These certificates verify that the certificate holder is the owner of that domain, ensuring customers that domain name "owners" are who they claim to be.

There are also other validation options, like two-way, real-time telephony. Certificate applicants are required to provide telephone numbers, and certificate authorities call to verify basic information, yet another way to seek recourse in the event of problems.

So there are essentially two types of validation available, manual and automated.

Manual Validation.

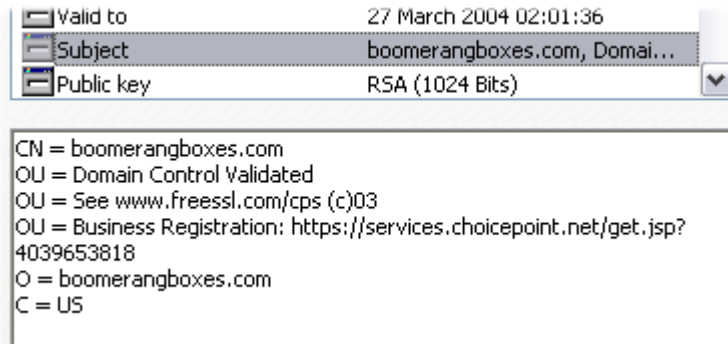
Involves the validation of domain name ownership and business legitimacy using humans. This process is traditionally slow and takes up to two working days, often longer. A manually validated certificate usually contains the following information within the certificate:



Auto-Validation.

Computers, databases and automated routines validate domain name ownership and business legitimacy. The process takes minutes rather than days. The GeoTrust QuickSSL product and RapidSSL.com FreeSSL products use automated validation to issue SSL certificates within 10 minutes. Their automated validation processes are WebTrust compliant and use Domain Control validation and Unique Business Registration to validate the applicant before issuing the certificate.

An automatically validated certificate, such as the GeoTrust or RapidSSL.com certificates, contain the following information within the certificate:



9. How fast do I want my certificate?

The principal delay associated with the issuance process of SSL is the validation process adopted.

For fast issuance of certificates, it is advisable to use automated methods of validation.

Be very careful when confirming the issuance time with a CA. Some may suggest immediate delivery once they have obtained all your company documentation in the format required and have initiated the validation. This process may still take up to 2 days from start to finish.

10. What budget do I have for my certificate?

Certificates range dramatically in price from one CA to another. The highest prices are 40 times the lowest prices!

This white paper has examined numerous points of consideration in determining which SSL certificate to purchase.

The correct choice of SSL certificate is principally dependent on the application type and on whether there is a need for a well known brand of SSL that has been issued from a highly trusted and credible CA.

There are however significant savings available for websites conducting low volume / low value transactions. Some SSL certificate types are perfect for development environments, whilst other certificate types suit professional requirements. Buyers are therefore urged to carefully consider their choice of CA before purchasing.

Give me 10 reasons why I should buy from RapidSSL.com?

- 1. A Complete Range of SSL Certificates.**
RapidSSL.com offers a range of certificates suitable for low volume/ low transaction value, Professional level and Development applications.
- 2. Credibility.**
RapidSSL.com is a subsidiary of GeoTrust, a highly trusted, credible and long standing CA with an Internationally recognized brand. GeoTrust own the Equifax roots that are already present in all popular browsers and used to issue the Professional Level certificates. RapidSSL.com also owns the root used to issue RapidSSL, FreeSSL and RapidSSL Wildcard certificates. GeoTrust is a WebTrust compliant CA and holds the WebTrust Seal.
- 3. Browser recognition.**
RapidSSL.com certificate range offers browser recognition rates from 99 percent suitable for both test/development, lite ecommerce and high volume / high transaction value ecommerce.
- 4. Single root not Chained root.**
RapidSSL.com offers SSL certificates utilizing single roots (owned by RapidSSL.com and GeoTrust) making installation far quicker and simpler than chained root certificate installations.
Issued in minutes, installed in seconds!
- 5. Certificate strength.**
All certificates offered through RapidSSL.com use 128 / 256 bit industry standard SSL encryption.
- 6. Industry Leading Expert Support.**
Both telephone, web and email support is available for all certificates sold through RapidSSL.com, covering 1am to 9pm EST, 6am -2am Europe. Unlike some of our competitors, RapidSSL.com does not charge extra for technical support.
- 7. Warranty.**
All certificates are issued from a WebTrust compliant CA. Our automated validation processes have been audited as part of WebTrust compliance, making mis-issuance extremely unlikely. Do not be fooled by other SSL Providers offering "mis-issuance warranty". There has never been a recorded case of a mis-issuance warranty being used ever, so beware of paying inflated prices for additional warranty.
- 8. Automated Online Validation.**
Our validation system is conducted online and is completely automated. There is no faxing or documentation required and we complete the online validation in only minutes.

As part of the provisioning process with both RapidSSL and FreeSSL, businesses are assigned a Unique Business Identifier - equivalent to a DUNS number. The Unique Business Identifier provides a corporate profile to the Internet users through information imbedded in to the certificate. With the Unique Business Identifier, industry-recognized domain control authentication, and two-factor telephony authentication, RapidSSL.com offers the strongest real-time authentication process on the market today.
- 9. Issuance speed.**
RapidSSL.com's 2nd generation validation and issuance infrastructure allows certificates to be issued immediately 24 hours per day, 7 days per week, 365 days each year.
- 10. Lowest cost.**
RapidSSL.com is the lowest cost provider of SSL certificates in the market today and offers the lowest priced certificates suitable for all application categories namely, low volume /low transaction value, Professional Level and test/development.

In summary...

In summary...

There is absolutely no reason why buyers of SSL should have to;

- Pay more for their certificates irrespective whether the application is for low volume, professional or development
- Wait more than 10 minutes for their SSL certificate to be issued
- Buy a certificate that cannot be installed in seconds (such as a chained root / intermediate certificate)
- Buy from SSL Providers who DO NOT own their own root
- Not enjoy FREE excellent customer service levels

RapidSSL.com has a very simple mission in life and that is;

- To be focused on providing small to medium sized businesses (SMB) and entry level web sites with strong 128 /256 bit encryption, industry standard SSL certificates
- To be dedicated to being the lowest cost provider of SSL to the SMB market place
- To deliver the ultimate customer service through fast issuance and leading customer care
- A commitment to quality in all aspects of the business through meeting the industries most stringent Certification Authority quality standards

Secure your webserver with a **SSL Certificate** at RapidSSL.com. The **lowest cost** provider of highly trusted stable & single root **128 / 256 bit SSL Certificates** (we own all our own root certificates!) suitable for lite and professional level ecommerce - fully supported and delivered immediately!

Microsoft Internet Information Server 5 / 6

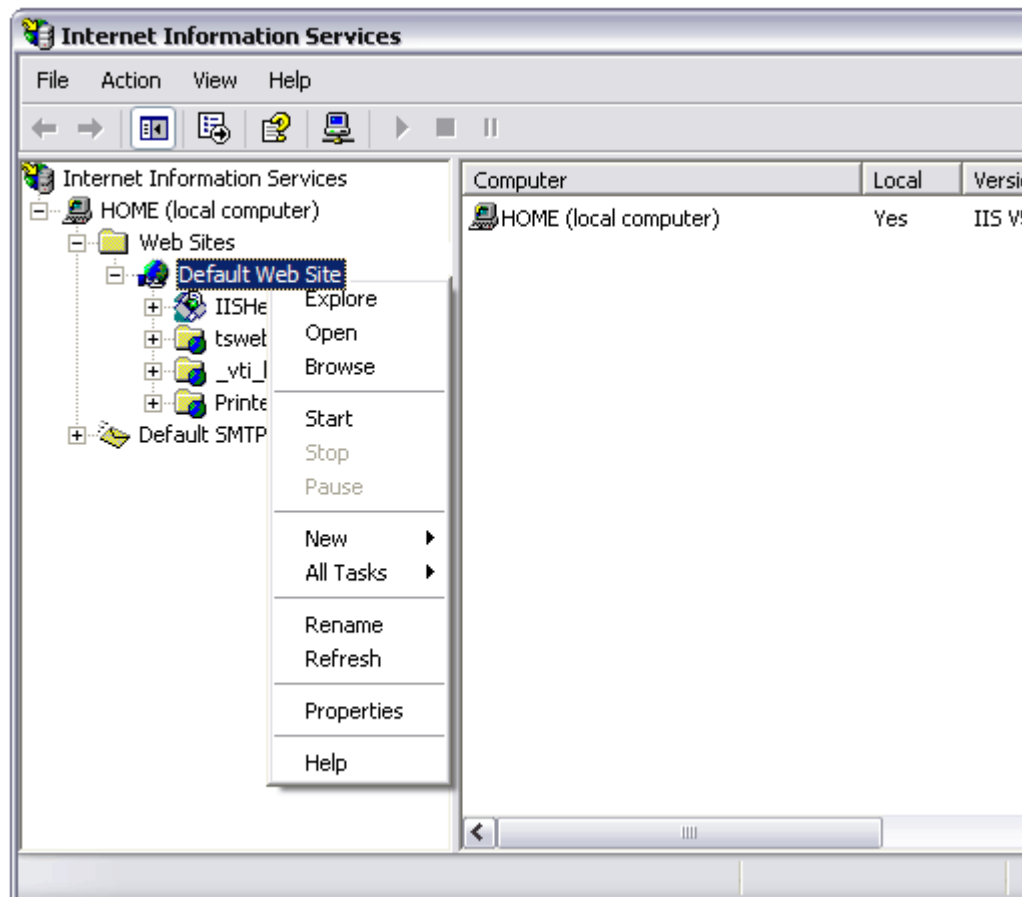
Generate a Certificate Signing Request (CSR)

Follow these instructions to generate a CSR for your Web site. When you have completed this process, you will have a CSR ready to submit to your provider in order to be generated into a SSL Security Certificate.

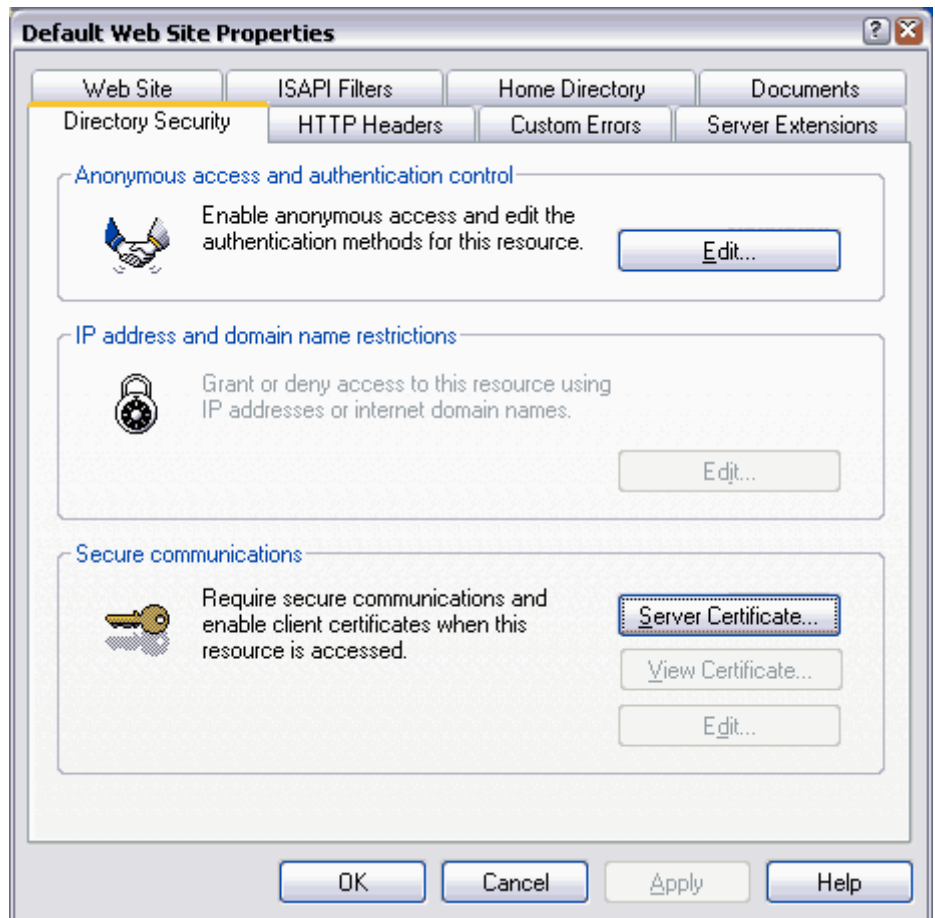
Note: If you are **renewing** your certificate or your site is currently running a web server certificate please refer to renewal section at the bottom of this document.

You must have at least Service Pack 1 installed

1. Select the **Internet Information Services** console within the Administrative Tools menu.
2. Select the computer and web site (host) that you wish to secure.
Right mouse-click to select **Properties**.



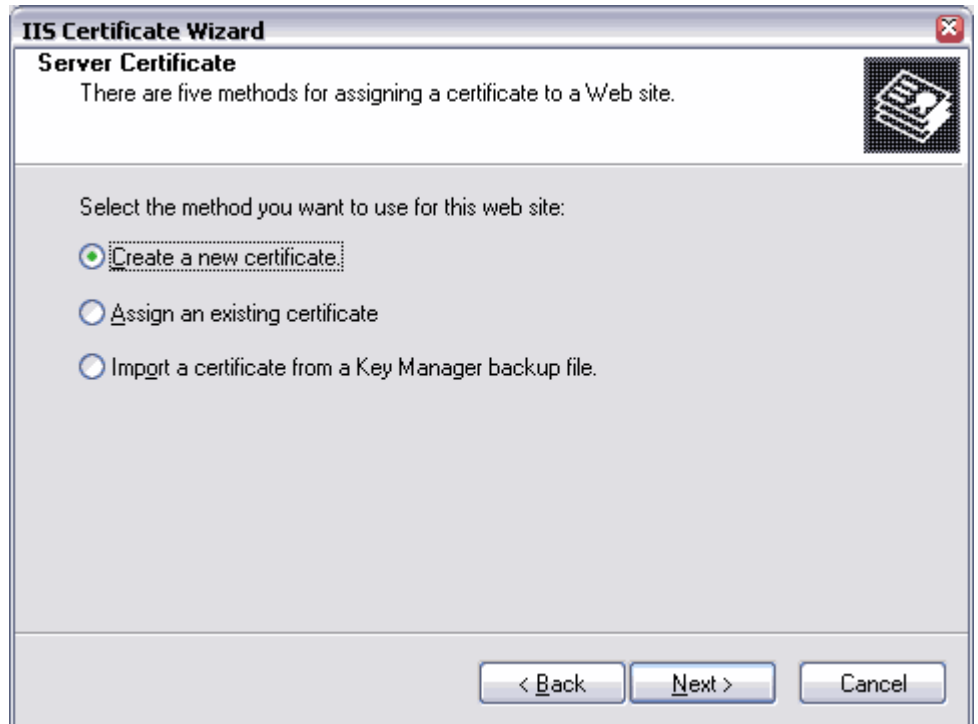
3. Select the **Directory Security** tab.



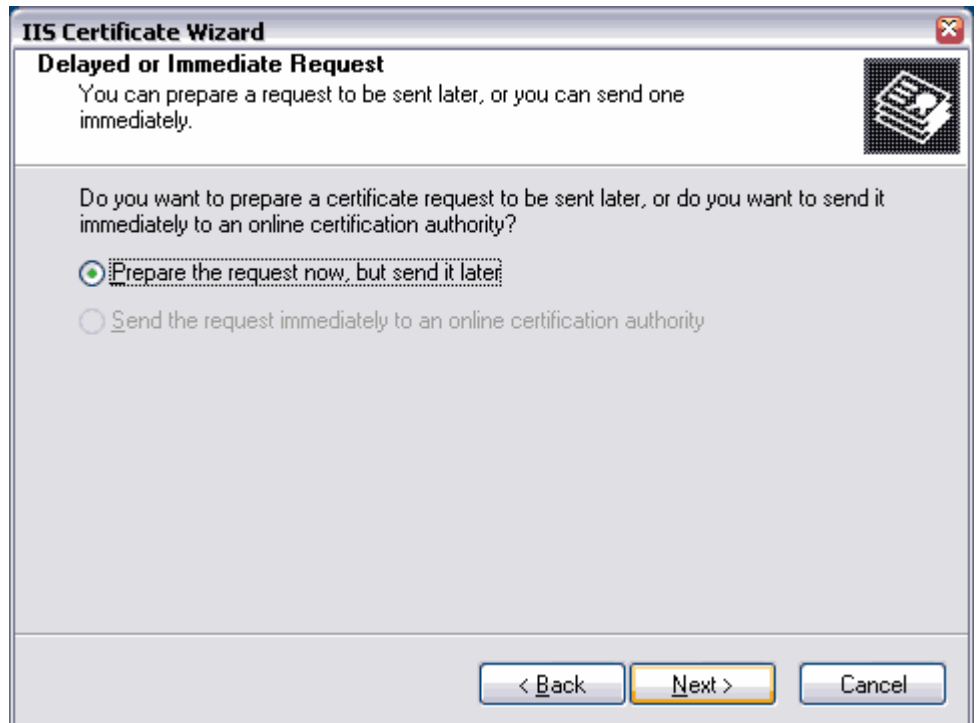
4. Select **Server Certificate** under Secure Communications
5. Click **Next** in the Welcome to the Web Server Certificate Wizard window.



6. Select **Create a new certificate**, Click **Next**.



7. Select **Prepare the request now, but send it later**.



8. At the **Name and Security Settings** screen, give your new certificate a name - this will help you identify this request if you work with multiple domain names on the same webserver. Select bit length. We recommend using 1024-bit length (note: To generate 128 bit encryption you will need to select a 1024 bit length). Click **Next**.

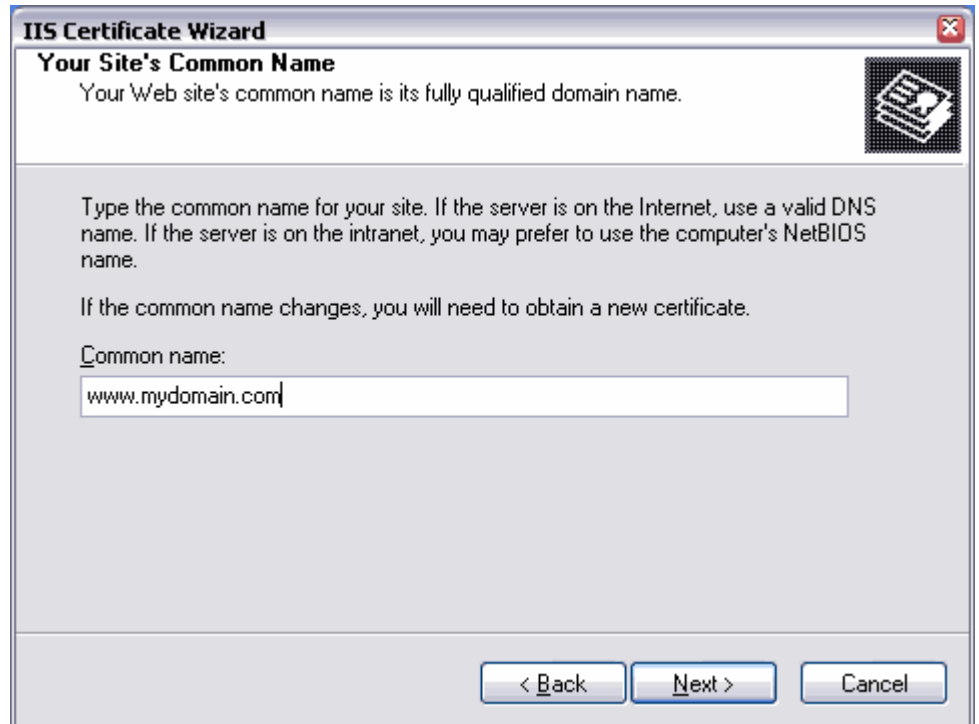
The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Name and Security Settings' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the section is titled 'Name and Security Settings' with a subtitle: 'Your new certificate must have a name and a specific bit length.' There is a small icon of a certificate in the top right corner. The main text says: 'Type a name for the new certificate. The name should be easy for you to refer to and remember.' Below this, there is a label 'Name:' followed by a text input field containing 'My Web Site'. Another instruction follows: 'The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' Below this is a label 'Bit length:' followed by a dropdown menu set to '1024'. There are two checkboxes: the first is 'Server Gated Cryptography (SGC) certificate (for export versions only)' and the second is 'Select cryptographic service provider (CSP) for this certificate'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. You will now be asked for details about your company and your website. When creating a CSR you must follow these conventions.
The following characters can not be accepted: < > ~ ! @ # \$ % ^ * / \ () ? & .
This includes **commas**.
10. At the **Organization Information**, state your **Company Name** and **Department**.

The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the section is titled 'Organization Information' with a subtitle: 'Your certificate must include information about your organization that distinguishes it from other organizations.' There is a small icon of a certificate in the top right corner. The main text says: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' Below this, there is a label 'Organization:' followed by a dropdown menu containing 'My Company Name'. Another label 'Organizational unit:' is followed by a dropdown menu containing 'My Department'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

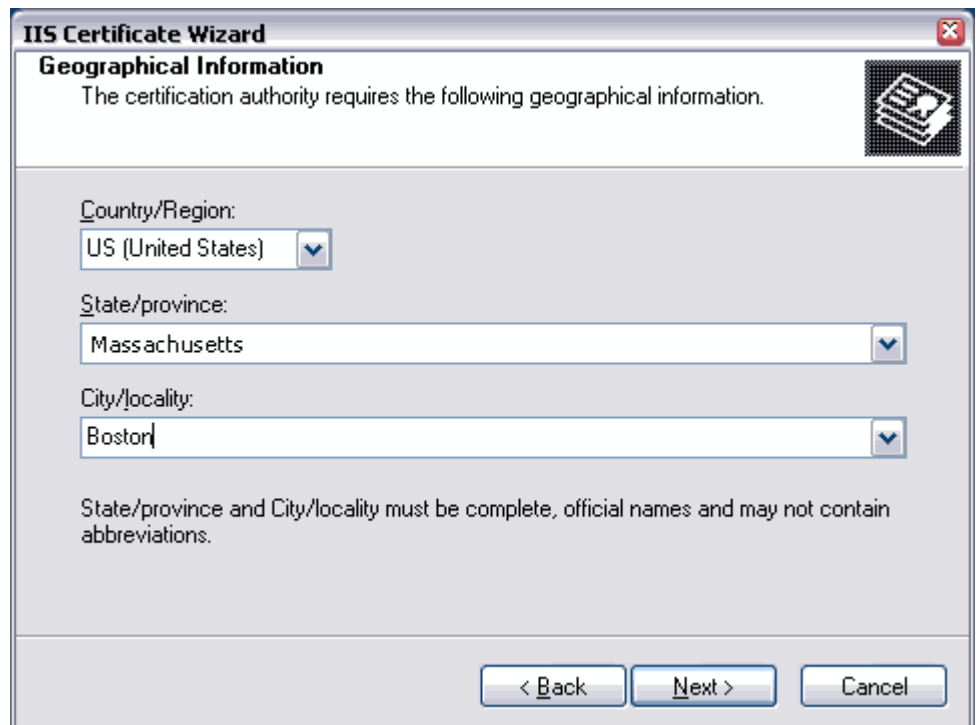
11. At the **Your Site's Common Name** screen, enter the domain name (e.g. yourdomain.com) or fully qualified domain name (e.g. www.yourdomain.com).
Whatever you enter here will be **exactly** what the certificate will be able to be used

on.



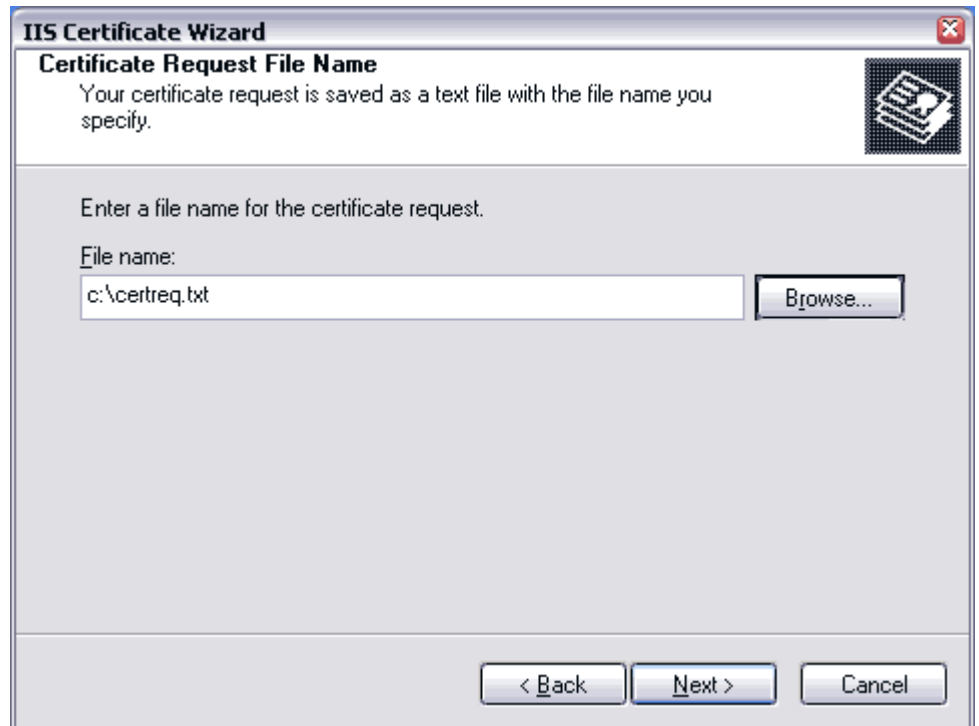
The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the main heading is 'Your Site's Common Name' and the subtitle is 'Your Web site's common name is its fully qualified domain name.' To the right of the subtitle is a small icon of a certificate. The main text area contains the following instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.' Below this text is a label 'Common name:' followed by a text input field containing 'www.mydomain.com'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

12. At the **Geographical Information** screen, enter your **country, state** and **city**.

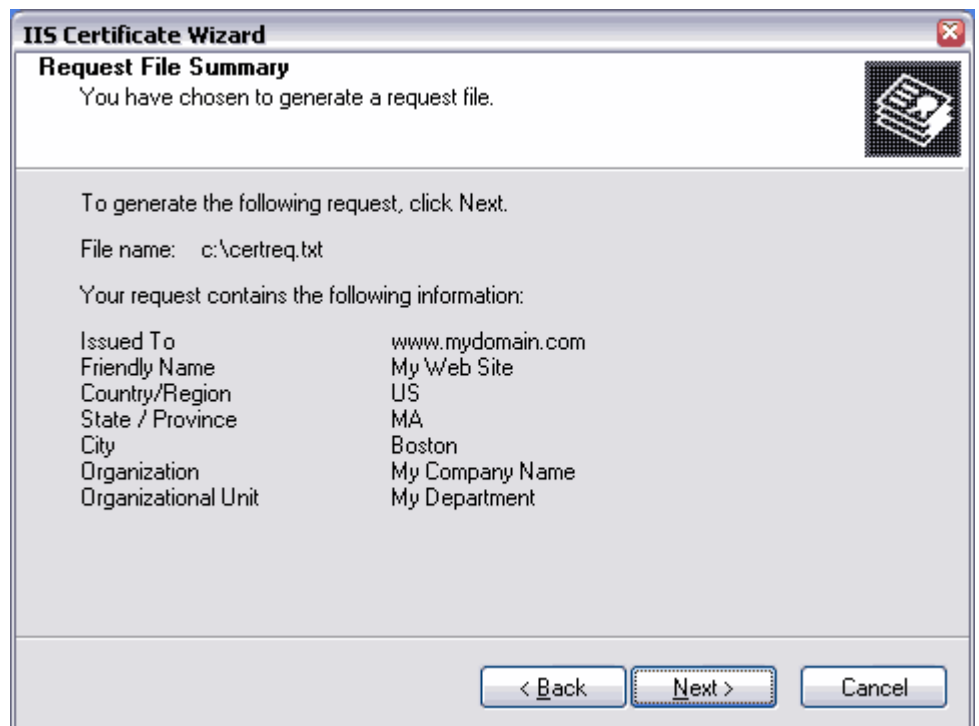


The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the main heading is 'Geographical Information' and the subtitle is 'The certification authority requires the following geographical information.' To the right of the subtitle is a small icon of a certificate. The main text area contains the following labels and input fields: 'Country/Region:' with a dropdown menu showing 'US (United States)'; 'State/province:' with a dropdown menu showing 'Massachusetts'; and 'City/locality:' with a dropdown menu showing 'Boston'. Below these fields is a note: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

13. You have now finished entering information. Your CSR will now be saved to a text file. Give your CSR a filename and select a location where you can easily find your CSR.



14. **Important:** Now review what you have entered. If you notice a mistake, use the **Back** button to return to the relevant screen to make changes. Pay particular attention to the **Issued To** field.



15. You have now generated your CSR! Click **Finish** to close the wizard.



IMPORTANT DO NOT REMOVE the pending request from your IIS or your issued certificate will not install. Attempting to create another CSR will automatically remove the pending request and this should be attempted until you have installed your issued certificate.

12. Now go to your SSL Provider, select your certificate product and click the relevant Order Now button. Make sure that you have your CSR file handy - you will need this during the enrollment process.

Renewals or Sites currently running ssl

The renewal request option within IIS 5.0 does not create a request in a PKCS10 format. This may be corrected with a future Service Pack. IIS 5.0 does not allow your site that is currently running SSL to generate a certificate signing request (CSR) without removing the existing certificate. For most sites this is not an option since your site will not be able to run a SSL session while your certificate is being processed. To obtain a certificate for your existing web site you will have to do the following. Please read and print these instructions before submitting your new certificate request.

1. Leave your existing site that currently has the certificate installed alone.
2. Create another virtual site within IIS (this does not have to be a functional site).
3. Enter **Properties** for the newly created virtual site, then go to the **Certificate Wizard to create a new certificate request**. The information you enter on this certificate request should match exactly the information on your production certificate, since that is the existing certificate this new CSR will replace.
4. Submit the new request through the GeoTrust website
5. Wait for the new certificate file to be emailed to you from our mailservers.
6. Install this certificate into your new virtual site; follow the **process the pending request** by selecting the certificate file we sent you. Complete the installation of your new certificate into your virtual web site.
7. Now delete the new virtual site!
8. Go to your Production web site, enter Properties, and select **Replace the current certificate** - choose the new certificate from the list.

9. Make sure you bind the web site to a unique IP address at https Port 443, then Stop and then Start your web site. Your new certificate should be installed.
10. When convenient, go into your MMC console (with Certificate snap-in added) and delete the old certificate.

Installing your certificate from FreeSSL.com

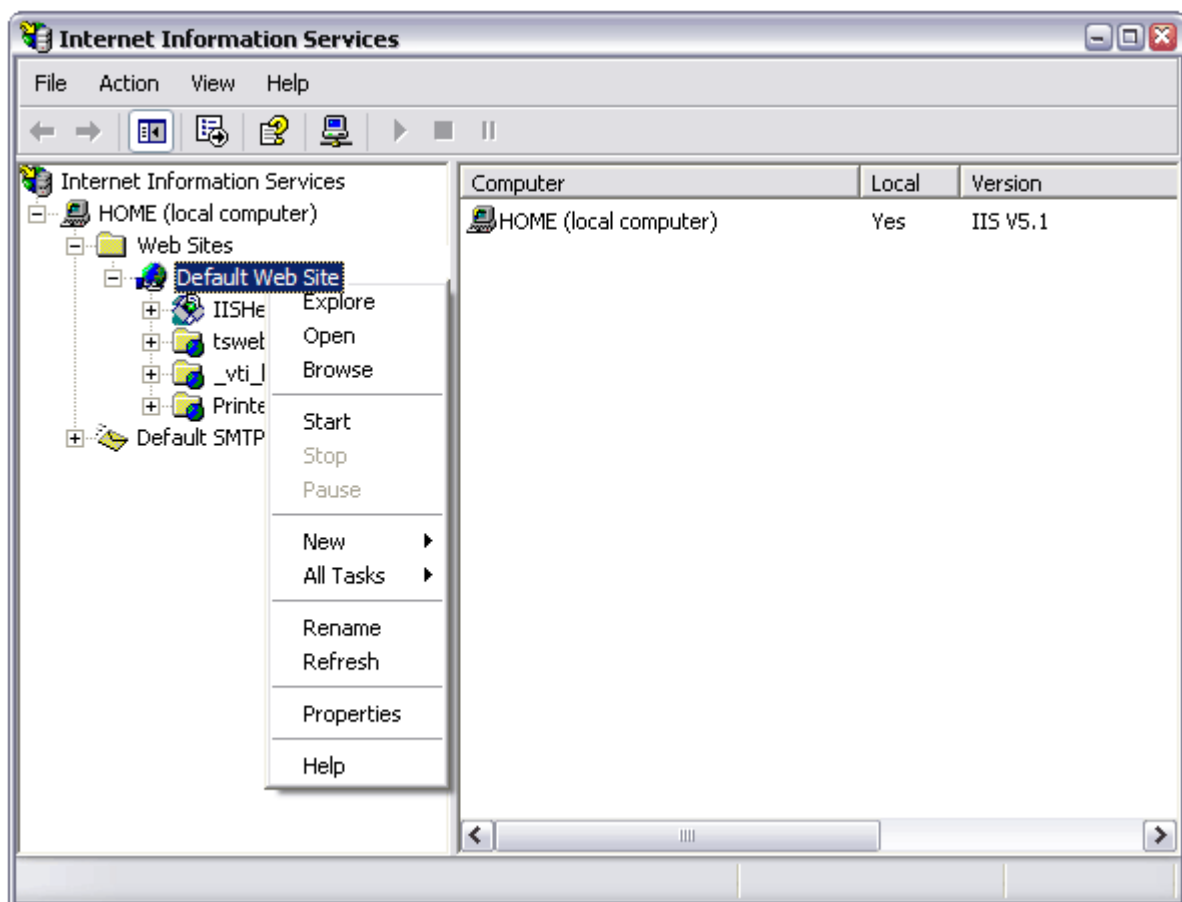
Firstly when your issuance email arrives it will contain your web server certificate. Copy your web server certificate into a text editor such as notepad including the header and footer. You should then have a text file that looks like:

```
-----BEGIN CERTIFICATE-----  
[encoded data]  
-----END CERTIFICATE-----
```

Make sure you have 5 dashes to either side of the BEGIN CERTIFICATE and END CERTIFICATE and that no white space, extra line breaks or additional characters have been inadvertently added. Copy your web server certificate into a text editor such as notepad and save as yourdomain.cer.

Installing your web server certificate

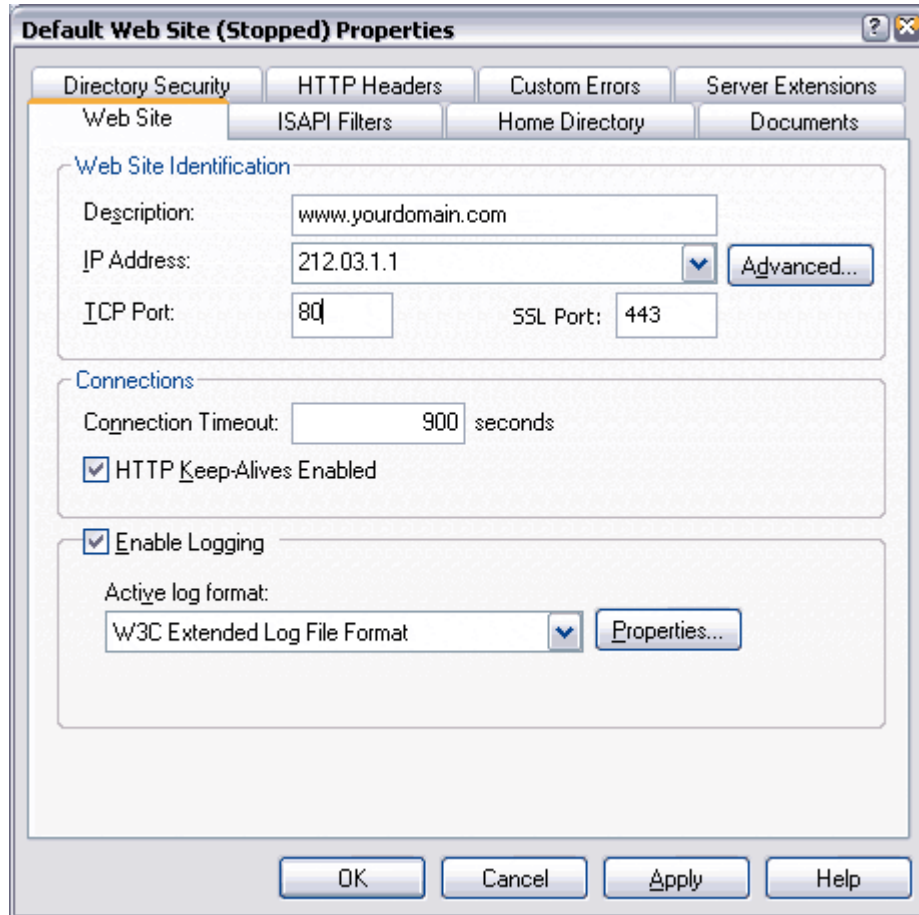
1. Start IIS and right click **Default Web Site** and select **Properties** from the menu.



2. When the **Properties** appear, click on the **Directory Security** tab.
3. Click on **Server Certificate** and follow the on screen wizard:

- Ensure that you select **Process the pending request and install the certificate**. Click **Next**.
- Locate the yourdomain.cer file when prompted to locate your webserver certificate. Click **Next**.
- Review the summary screen and ensure that you are processing the correct certificate. Click **Next**.
- Click **Next** on the confirmation screen.

4. Make sure that you have assigned **Port 443** as the SSL port for https for your site. To do this, right click Properties for your website and make sure that 443 has been entered into the SSL port box:



Test your certificate by connecting to your server. Use the https protocol directive (e.g. https://your server/) to indicate you wish to use secure HTTP. The padlock icon on your Web browser will be displayed in the locked position if you have set up your site properly.

Backing up your key pair file

Creating your Snap-in Management Console

Certificate Snap-in consoles (MMC) are not preconfigured. You will need to configure the Snap-in before you can perform any Export/Import functionality. To configure your Snap-in, follow the steps below. The system administrator will have to create the console.

1. Go to **Start**. Select **Run**, Type **mmc** and click **OK**. This will bring up an empty console with no management functionality.
2. Click on **Console** select **Add/Remove Snap-in**.
3. The Snap-ins added to box will list only the Console Root. Click **Add**.
4. Select **Certificates** and then click **Add**.
5. Select **Computer Account**.
6. Click on **Finish**.
7. Click **Close**.
8. Click on **OK**.

Managing your certificates

1. Go to the **Microsoft Management Console** (MMC) and add the Snap-in for Certificates.
2. Select the folders **Console Root\Certificates(Local Computer)\Personal\Certificates**.
3. Right click on the certificate to export.
4. Select **All Tasks** and **Export**.
5. The Welcome to the Certificate Manager Import Wizard window opens. Click **Next**.
6. Select **Yes, export the private key**. Click **Next**.
7. Make sure the Personal Information Exchange- PKCS # 12 (.pfx) box is selected.
Warning: Make sure that the "Delete the private key if the export is successful" is NOT checked.
8. Check the box **Enable strong protection requires IE5.0, NT4.0 SP4 or above**. Select **Next**.
9. Check the box to **Include all certificates in the chain**.
10. Type and confirm your export password. (Note: this password field can be left blank, but we recommend using a good password for security)

Warning: If you lose the password, you must purchase another certificate.

Save the file to a disk or other form of media. You should choose a form of media that you would be able to recover if your system has to be rebuilt. Save this file in a secure location.

***** Microsoft has an alert addressing a problem with exporting and importing certificates.*****

Service Pack 2 is intended to correct this problem. There is also a hotfix that may be obtained from Microsoft that must be run prior to exporting and importing your certificate. Please go to the following URL for more information contact us.

<http://support.microsoft.com/support/kb/articles/Q261/6/55.ASP>