Secure Sites:

Sites requiring secure access must have a dedicated IP address. In order to provide security, a secure certificate must be purchased. Secure certificates are available from various vendors, and must be installed on your website using prescribed methods.

To obtain a secure certificate, certain documentation is sometimes required depending on the level of secure certificate one purchases. See **Required Documentation for SSL Certificates** below for more.

Credit Cards:

Sites requiring credit card processing must obtain these processing services, a.k.a. merchant account, from a reputable credit card servicing company. We can offer some suggestions for this service, but the responsibility for investigation and approval of these services lies with the client. We do not take responsibility for these services or any problems that may result from their use, we only implement these services on a client's website at the client's request.

There are several ways to handle credit cards, listed in order of expense (lowest to highest):

a) Use Paypal, which maintains its own secure site and can process credit cards for you. They also provide a shopping cart for the purpose. You would not require a secure certificate in this case since security is provided by Paypal.

b) Collect user credit card numbers with user orders, then process them at your location manually using credit card processing services you've purchased.

c) Real time credit card processing directly on your website—for cost-effectiveness we recommend not using this option until your website is well-established and you're getting enough business coming in via that route that you find it is a problem keeping up with the manual processing. Some merchant accounts offer this service as part of their package.

Required Documentation for SSL Certificates

Before we can order a secure certificate for you, you must send us appropriate documentation—this is required by the issuing certificate company, and varies somewhat depending on the company used. Thawte's requirements for Secure certificates are listed below since they are fairly stringent. We will advise you based on the company you choose to use.

Thawte's Required Documents:

The links below take you to detailed descriptions of the documents we need.   We must have the correct company name documentation in our possession underline before we create your certificate request. Your certificate request will contain your company name, province and country, which must match exactly the documentation you send us. It's easier to get it right if we have the documentation in hand first!

1. Proof of Organizational Name - Your certificate request must contain a company name exactly as stated in this document. (see below for more about this item)

2. Proof of Right to Use Domain Name - The common name in your certificate request must be for this domain - please read the requirements below to see if you need to send this to us.

General Guidelines

1. **Repeat Requests**
    If you have had a previous certificate for the same organization within the last 90 days, you may not have to send ALL the documentation again. You will need to ask your assigned representative if the

documentation from the previous request will apply to the new one. The city, state, and business name must be exactly the same for the rule to apply.

2. **Faxes and Originals**
   You can usually fax your documentation to your chosen representative for faster processing. Please ask your representative whether they will accept a faxed copy of the documentation. Your representative will notify you if you must send the original documentation by mail.

3. **Notarization and Translation**
   Notarization of the documentation is not usually required. Occasionally a notarization of the telephone verification letter (where applicable) will be required. Your representative will inform you if this is necessary. If we do not have a representative who speaks your language, please make certified English translations of the documentation and send them to us along with copies of the originals.

I. Proof of Organizational Name

Thawte will not issue any certificate unless you can prove that you have the right to use a given company name. This is to prevent impostors from receiving certificates and then pretending to be firms they are not. To receive a Thawte certificate you must be a recognized organization or non-profit entity and have the appropriate documentation to prove it.

Thawte will accept different kinds of documentation from each type of organization as proof of its right to use that organizational name. Your "proof of org name document" needs to be official, and needs to be independently verifiable. For example, if you are claiming to be "XYZ, Inc." then you should produce a certificate of incorporation from your Secretary of State that proves that you have been registered in your state under that name.

Most organizations fall into one of the following categories:

- **Companies, Corporations, Incorporations Inc, (Pty) Ltd., Plc., B.V., S.A. GmbH, LLC, State issued Trademarks, etc.**
  We will need a copy of an official city, state, or country document, articles of incorporation, or a DUNS number in your state and country. These documents can be faxed.

- **Partnerships**
  You should be registered with national, state or local authorities. Please provide us with a copy of some form of verifiable proof of the partnership name.

- **Proprietorships, DBA's and Fictitious/Assumed Names**
  If you are a sole proprietor, you may send documents from the department of revenue. DBA ("Doing Business As") or Assumed/Fictitious names will need to send a copy of your DBA registration papers. Any other official city, state, or country documents will generally be sufficient, as long as we can cross check with the relevant authority.

- **Government Departments**
  We require an original signed letter from the head of that department on the appropriate letterhead, along with contact information for his or her office and immediate superiors.

- **NGO's (Non-Government Organizations)**
  We require an original signed letter from the Chief Executive, Chairman or Managing Director of the NGO, on the appropriate letterhead.

- **Universities and University Departments**
  We will require an original signed letter from the Dean or Vice-Chancellor responsible for that department. Note that this must be on the appropriate letterhead, accompanied by contact information for the University concerned.

- **Special Interest Groups**
  We will issue such groups with certificates but request that you contact us first to discuss verification and authentication details.

- **Private Individuals**
  If you want a certificate but are not registered, incorporated or licensed to do business in your area, we can issue a certificate to you in your personal capacity using your name as the organization name. Please note that we only do this on rare occasions under special circumstances. In order for us to issue a certificate to you, we will need the following:

    1. A photocopy of your passport/identity document or driver's license, notarized or certified by a relevant authority in the country where you live. The person certifying this documentation needs to provide their name and telephone number for further confirmation if necessary. Please post the original copy to the Thawte representative you chose during the application process.

    2. A copy of a valid, current bank statement in your name (you may black out your financial details) OR a valid, voided check from your bank account.

Please make sure to send us the correct documentation the first time around. This will ensure that your request is verified in good time and your certificate issued in a timely fashion. If you have any questions, <u>please contact us</u>.

What if I am Different?

If you believe you have a right to use an organizational name but you do not fit into the categories described above, please contact your nearest Thawte representative to discuss your situation.

II. Proof of the Right to a Domain Name

Most of the time we can handle this without anything additional from you. If your domain name is registered to the exact same company name that appears in your company's registration documents and can be seen in a "Who Is" from a domain registrar, you will not need to be concerned about submitting this additional information to us.

The "common name" of a web server certificate is by convention set to the domain name of the server upon which the certificate will be used. Please put this "common name" into Microsoft Authenticode and Netscape Object Signing certificates. The domain name can be a wildcard, such as "*.microsoft.com", or it can be the name of a standard host, like "www.microsoft.com".

Your organization will have gone through a process of registration in order to register your domain name. Because we will be issuing a certificate tied to a domain name we need to be sure that you have the right to use that domain.

Please check the following cases to see if you need to send us proof of your right to use the domain name. If in doubt, please check the WHOIS output for your domain. Your system administrator or ISP will know what that is.

- WE DO NOT NEED PROOF if your **domain is registered to your company exactly** as it is in your Certificate Signing Request (CSR), **unless** we specifically ask for it.

- If your **domain is registered to a person or company other than the one requesting the certificate** we will require a letter from the person to which the domain is registered authorizing your organization to use the domain for business purposes.

- If you are a **subdivision of the company** who owns the domain, we will require a letter proving this.

- If your domain is registered to a company and you have subsequently **changed the organization name** in any way, we will need documentation to prove that.

If you are required by the above instructions to send us proof, we will need to know the following about your domain name registration:

1. Through which authority you registered.

2. The name and contact information you gave as a corporate contact.

3. The name and contact information you gave as a technical contact.

A faxed copy of the WHOIS output for your domain will be sufficient.

We will use this information to verify your right to use the domain name we are certifying.