Building customer confidence with Thawte SSL Web Server Certificates and SuperCerts

thawte
it's a trust thing

Security is of the utmost importance when doing business on the Web. Your customers want to know that their information is protected when crossing data lines. A Thawte SSL Web Server Certificate or SuperCert will boost your business in the following ways:

- Customers will submit information via the Web only if they are confident that their personal information, such as credit card numbers, financial data, or medical history, is secure.

- Your business will gain a competitive edge when compared to e-businesses that do not offer security.

- Your end users will know that they are working with a trustworthy partner and that any confidential information they submit (including credit card information) is safe in transit.

What is an SSL Certificate?

SSL (Secure Socket Layer) is a protocol developed by Netscape that enables a web browser and a web server to communicate securely. Security is provided in two different ways:

- Authenticating the web server to the client using a digital certificate;
- Encrypting all information sent

The SSL protocol requires that the web server should have a digital certificate installed in order to make an SSL connection. This is where Thawte comes into the picture.

Through an SSL-enabled web server and a Thawte SSL certificate, a customer connecting to a secure web site is assured of three things:

- **Authentication:** The Company that installed the certificate is the true owner of the website.
- **Message privacy:** Using a unique session key, SSL encrypts all information exchanged between your web server and your customers, such as credit card numbers and other personal data. This ensures that personal information cannot be viewed if intercepted by unauthorized persons.
- **Message integrity:** The data cannot be tampered with over the Internet.

SSL is the *de facto* standard for securing Internet transactions and is implemented by all major software vendors. Your users do not need any installation of additional software on their server or browser. When implemented correctly the process is seamless to the user.

Why do you need a Thawte SSL certificate?

Customers will only do business with you on the Web if they feel secure and know that their personal information will not be tampered with. Offering security by means of a Thawte SSL Certificate, you enter the world of e-commerce that holds the following benefits:

- **Worldwide presence** - through the Internet you have a potential global customer base.
- **Market share** - companies that can win the confidence of customers, gain loyalty and expand their business.
- **Cost-effective delivery channel** - information and software can be delivered via the Web. This saves time and transport costs, but your customers will only use this service if it is secure.
- **Applications and enrollment** - people can use the Internet to enroll or apply for services. They will however only submit information if they know that you offer a secure site.
- **One-to-one marketing** - establishing an online store enables you to customize your products and services to suit individual needs. This means that you personalize marketing communication with customers. Customers will, however not do business with you if your site is not secured.

Your customers benefit because they know that by checking the details in the SSL certificate, they can assure themselves that the web site they are dealing with is in fact the web site they want to be dealing with. They also know that a third party on the Internet cannot decrypt their credit card or personal details.

All major web merchants use SSL security backed by strong warranties to encourage customers to buy online.

If you want to assure your customers that they are not at risk when sending data over the Internet, you need an SSL certificate.

■ *Who needs an SSL certificate?*

You need a Thawte SSL Certificate if:

- You are a web site owner whose web site has online ordering facilities.
- You want to assure customers that they are not exposed to any risks associated with sending data over an open network.

If you have more than one domain name to secure, you should have more than one SSL certificate. Digital certificates are domain name and host name specific, so you will need as many certificates as you have domain names.

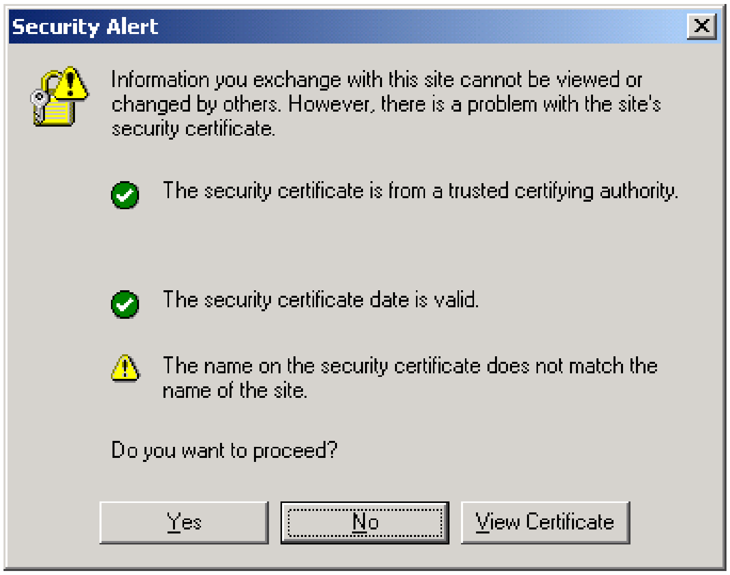
■ *How to tell if a website is secure*

If a web site does not have an SSL certificate, web users will see the "unlocked" icon in their browser windows.

If a secure SSL connection is established between the web browser and the web server, the “http” in the web address will change to “https”, for example: “**http**://www.thawte.com” becomes **https**://www.thawte.com. When an SSL session is taking place, the browser will display a lock in the frame of the browser. When you access a secure web site, you can check its digital certificate by double-clicking on the lock.

Browser warnings

Your browser has a built-in security feature that displays a warning message when you try and submit information to a web site without a certificate. Here is the warning message given in the Netscape web browser.



Security Alert

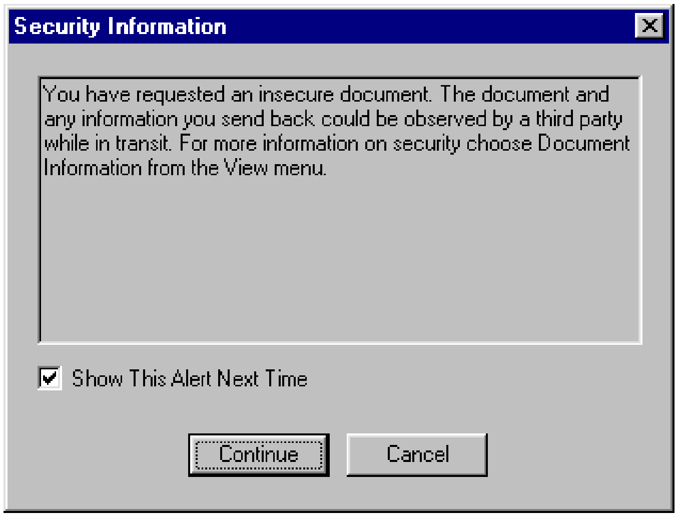
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?



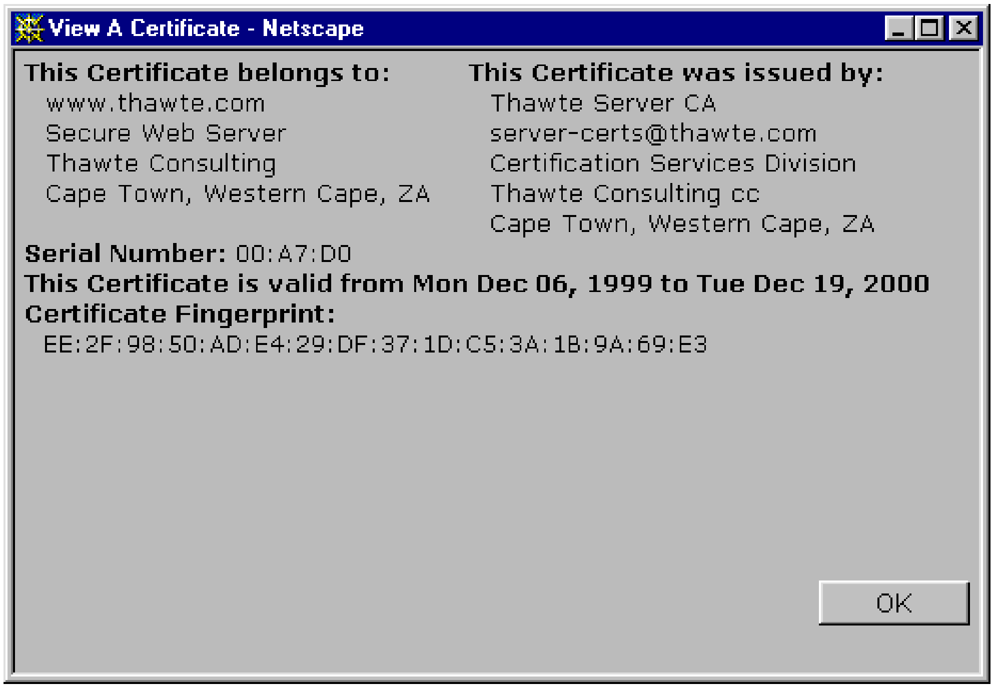
Security Information

You have requested an insecure document. The document and any information you send back could be observed by a third party while in transit. For more information on security choose Document Information from the View menu.

The user will be informed that the web site they are visiting has a digital certificate issued by a recognized Certifying Authority (CA), such as Thawte, and that any data they submit will be encrypted. By checking the certificate, the customer can verify that the web site is owned by a real company and they own the domain name being accessed.

■ *What does an SSL certificate look like?*

Below is an example of what a digital certificate looks like when viewed by a web user using a Netscape browser



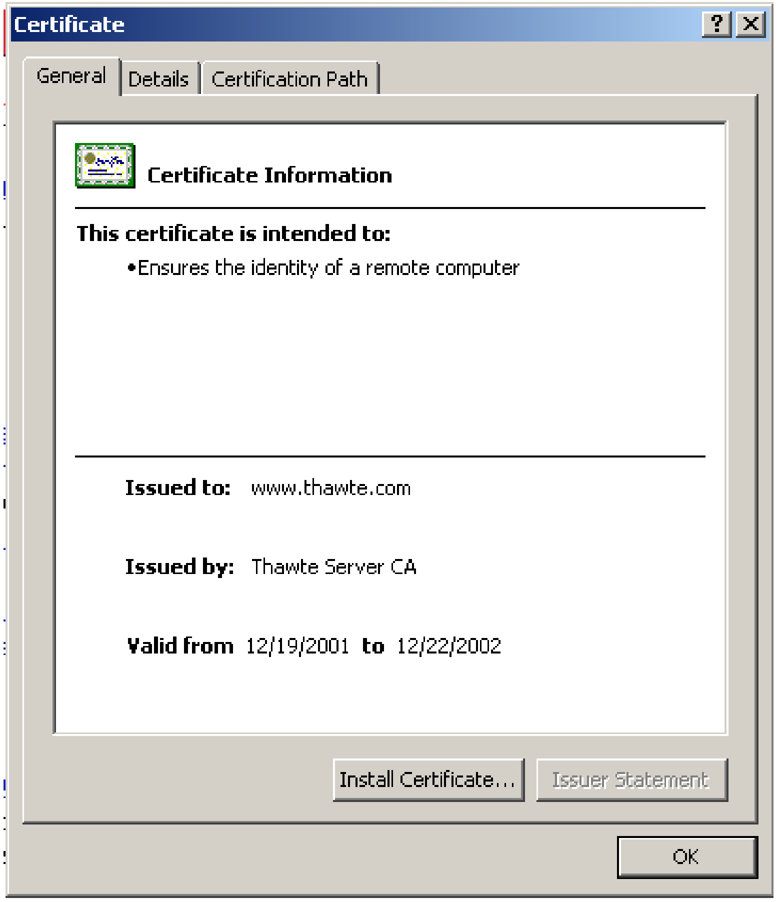
View A Certificate - Netscape

This Certificate belongs to:
www.thawte.com
Secure Web Server
Thawte Consulting
Cape Town, Western Cape, ZA

This Certificate was issued by:
Thawte Server CA
server-certs@thawte.com
Certification Services Division
Thawte Consulting cc
Cape Town, Western Cape, ZA

Serial Number: 00:A7:D0
This Certificate is valid from Mon Dec 06, 1999 to Tue Dec 19, 2000
Certificate Fingerprint:
EE:2F:98:50:AD:E4:29:DF:37:1D:C5:3A:1B:9A:69:E3

Below is an example of what a digital certificate looks like when viewed by a web user using a IE browser



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: www.thawte.com

Issued by: Thawte Server CA

Valid from 12/19/2001 to 12/22/2002

An SSL certificate contains the following information:

- The domain name for which the certificate was issued.
- The company who owns the certificate and domain name.
- The registered location of the company.
- The name of the CA who verified the information displayed in the certificate.
- The period of time for which the CA has verified the information in the certificate.

When you connect to a secure web server such as https://www.thawte.com, that server must first authenticate itself to the web browser with a digital certificate before a secure connection is established.

The web browser checks that:

- the domain name in the certificate matches the domain it was sent from;
- the certificate has not expired; and
- the CA who signed the certificate is trusted by the web browser.

The process is seamless thus the user does not see all of the above taking place. The certificate serves as proof that an independent trusted third party, such as Thawte, has verified that the domain belongs to a real company and can therefore be trusted. A valid certificate gives customers confidence that they are sending personal information securely to the authenticated party.

■ *Protecting your private key*

When you request a certificate, you generate a key pair on your server. When a key pair is generated for your business, your private key is installed on your server and nobody else has access to it.

Your private key creates digital signatures that effectively serve as your online company stamp. It is essential that this key is kept as secure as possible. You will no longer be able to use your certificate should you lose your private key.

Your matching public key is installed on your web server as part of the digital certificate. The public and private keys are mathematically related, but are not identical. Customers who want to communicate with you privately (using SSL) use the public key in your certificate to encrypt information before sending it to you. This process is instant and seamless to the user. Only the web server's private key can decrypt this information. Customers will feel secure that nothing they submit to your server will be seen by a third party.

■ *What is a SuperCert?*

Historically browsers exported from the US or "International" browsers were enabled to 40-bit encryption, while US versions were capable of encrypting communications using 128-bit encryption. A substantial number of browsers in use today are 40-bit or "International" browsers. In order to guarantee that all your customers can use the strongest encryption available, you need a SuperCert to provide them with the strongest possible encryption.

SuperCerts are SSL certificates that force compatible "International" 40-bit browsers to step-up to 128-bit encryption. Roughly speaking, 128-bit encryption is 309,485,009,821,345,068,724,781,056 times stronger than 40-bit encryption.

Internet Explorer 5.01, Netscape Communicator 4.71 and later browsers recognize Thawte's SuperCerts.

For more information on SuperCerts, please see
http://www.thawte.com/html/RETAIL/sgc/index.html

■ *Who is Thawte?*

Thawte issues server certificates to organizations and individuals worldwide. Thawte verifies the true identity of the company requesting the certificate by using real world identity checks and it also determines that it has authorized the certificate. Thawte also checks that the company in question owns the relevant domain. Thawte certificates interoperate smoothly with the latest software from Microsoft and Netscape, Oracle, Sun and the like. You can rest assured that your purchase of a Thawte Server Certificate will give your customers the confidence to transact with you online.