Building Customer Confidence through SSL Certificates and SuperCerts

Contents

1. Overview

In this guide you'll read about the need for security on the Internet, what an SSL certificate is, and how such a digital certificate is used to meet the demand for safe interaction over the Net. Finally, we'll tell you about the role of Thawte as a trusted third party.

2. Why SSL?

When you walk into a store, you know who you are dealing with. You see the products, the branding and the store assistant. You can be sure that if something should be wrong with your purchase, you'll have recourse to the store manager or owner.

But on the Internet, website visitors generally have no reliable way of knowing who owns the website (the virtual store). When customers visit a website with the intent of making an online purchase, they want to know whom they'll be paying. They want proof of the identity of the website owner, and they want to know that the personal information they send to the website cannot be intercepted by other Internet users. This is where SSL digital certificates come to the fore.

SSL (Secure Socket Layer) is a protocol developed by Netscape that enables a web browser and a web server to communicate securely; it allows the web browser to authenticate the web server. The SSL protocol requires the web server to have a digital certificate installed on it in order for an SSL connection to be made.

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

- **Authentication:** The website really is owned by the company that installed the certificate.
- **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 it is intercepted by unauthorized parties.
- **Message integrity:** The data cannot be tampered with over the Internet.

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

If it is important for you to assure your customers that they are not at risk when sending data over the Internet, you should get an SSL certificate. If you have more than one domain name to secure, then 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.

Reassurance pays. Your e-commerce business will benefit from the SSL-enabled web server and digital certificate, and you'll see an increase in online purchases from customers who feel more secure buying from you online.

3. Who needs an SSL certificate?

Any website owner whose website has online ordering facilities and who wants to assure customers that they are not exposed to any of the risks associated with sending data over an open network (such as the Internet).

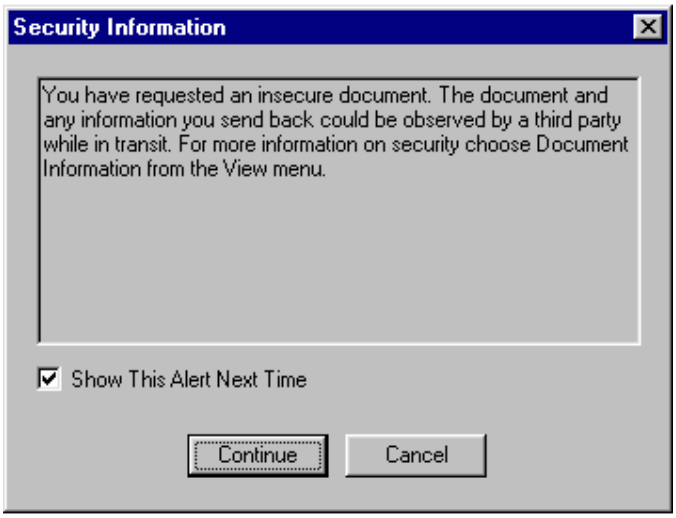
4. How to tell if a website is secure

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

Valid certificate: If a secure SSL connection is established between the web browser and the web server, the “http” in the web address will normally change to “https”, for example: “http://**www.thawte.com**” becomes **https://www.thawte.com**. The SSL connected browser will also display the "locked" icon. To test whether a site has a valid certificate, try to initiate a secure connection with that website by accessing the URL using the **https://** prefix instead of **http://**.

5. Browser warnings

When you submit information to a website that does not have an SSL certificate, your browser will present you with a warning message. Below is an example of such a warning given in a Netscape browser:



If, however, a website is using a valid digital certificate, then the web user will be informed that the website they are visiting has a digital certificate issued by a recognized Certifying Authority (such as Thawte), and that any data they submit to that site will be encrypted. By checking the certificate, the customer can verify that the website is valid, and who it belongs to.

6. What is an SSL Certificate?

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

An SSL certificate contains the following information:

- The domain for which the certificate was issued.
- The owner of the certificate (who is the also the person/entity who has the right to use the domain).
- The physical location of the owner.
- The validity dates of the certificate.

When you connect to a secure web server such as https://www.thawte.com, that server authenticates itself to the web browser by presenting a digital certificate.

This authentication is quite a complex process that involves the exchange of a "public key" and the use of a "session key " for encryption. The process is seamless to the user. The certificate serves as proof that an independent trusted third party, such as Thawte, has verified that the server belongs to the company it claims to belong to. A valid certificate gives customers confidence that they are sending personal information securely, and to the right place.

Public/private key pairs

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; nobody else has access to it.

Your matching "public key," is also 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 use the public key in your Server ID to encrypt information before sending it to you. (Again, this is a seamless process.) Only the private key can decrypt this information. Customers will feel secure in the knowledge that nothing they submit to your server will be seen by a third party.

7. What is a SuperCert?

Historically, the USA restricted the export of strong encryption products from the USA. This meant that the browser versions developed for export from the US were not automatically enabled to encrypt communications using 128-bit strong encryption. All secure communications using these "international" browsers used 40-bit encryption. It is important to realize that a substantial number of browsers in use today in the US are "international" browsers, so even if your customers are situated within the US, you may still require a SuperCert to provide them with the strongest possible encryption.

SuperCerts are SSL certificates that allow "international" browsers to "step-up" to 128-bit encryption. Internet Explorer 5.01, Netscape Communicator 4.7 and later browsers recognize Thawte's SuperCerts. 128-bit encryption is regarded as being impossible to "crack". Stated another way, SuperCerts will bump up the encryption level to 128 bits, even when communicating with the latest 40-bit browsers.

For more information on SuperCerts please see
http://www.thawte.com/certs/server/128bit/contents.html

8. The benefits of SSL certificates to your business

Thawte SSL Certificates and SuperCerts provide:

- Confidence in the integrity and security of your online business and network infrastructure. Customers are becoming increasingly aware of the advantages of SSL security and will often not purchase online from non-secure stores. All major web merchants use SSL security backed by strong warranties to encourage customers to buy online.
- Interoperability and support for standard applications and browsers, such as Microsoft Internet Explorer and Netscape Communicator.
- Non-forgeable proof of your website identity.
- Ease of use.

A stand-alone solution: no installation of any extra software on the server or the browser is required.

9. The role of Thawte

Thawte Certification issues server certificates to organizations and individuals worldwide. Thawte verifies that the company requesting the certificate is who it says it is, and 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, so you can rest assured that your purchase of a Thawte Server Certificate will give your customers the confidence to transact with you online.

Thawte offers efficient personal service and a straightforward certification process. You can be sure of our excellent after sales support.

To find out more about putting Thawte Certification to work for your business, visit us at: www.thawte.com, or contact us at: info@thawte.com .