



Unlock the full potential of your
SSL Software with
Thawte SGC SuperCerts



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.

Thawte issues server certificates to organizations and individuals worldwide. We verify the true identity of the company requesting the certificate and also check that the company in question owns the relevant domain. Thawte certificates interoperate smoothly with the latest software from Microsoft and Netscape. A Thawte Server Certificate will give your customers the confidence to transact with you online.

■ ***What is SSL crypto strength?***

SSL (Secure Sockets Layer) provides encryption between web browsers and web servers. This encryption, based on the RSA algorithm, can be done at different strengths, depending on what the software supports at each end (i.e. the web browser and the web server).

The strength of the encryption is typically specified by the size of the session key (a unique value involved in the encryption that differs for every customer every time he/she visits the site). The session key can be either 40 bits, 56 bits or 128 bits in size.

Cryptographers consider 128-bit encryption impossible to crack, as it would take millions of years with the fastest computers to try all the combinations. On the other hand, 40- and 56-bit keys are not as strong and it is feasible to try all the combinations.

Historically, the USA restricted the export of strong encryption products. This meant that the browser versions developed for export from the US were not automatically enabled to encrypt communications using 128-bit encryption. All

secure communications using these international browsers used 40-bit encryption. It is important to realize that a substantial number of browsers used in the US today are international browsers. So even if you only serve US customers, you may still require a SuperCert to provide them with the strongest possible encryption.

■ ***What are SuperCerts?***

SuperCerts are SSL certificates that allow international browsers to step-up to 128-bit encryption. Internet Explorer 5.01, Netscape Communicator 4.71 and later browsers recognize Thawte's SuperCerts. In a nutshell - SuperCerts will bump up the encryption level to 128 bits, even when communicating with the latest 40-bit browsers.

■ ***Who needs a SuperCert?***

You will need a Thawte SuperCert if you are a web site owner whose customers mostly use the export versions of browsers that do not by default support the full 128-bit crypto strength. This usually applies to web sites with a significant international customer base.

A SuperCert provides the full 128-bit crypto for compatible browsers and therefore unlocks the full potential of these browsers. It is important to secure your web site with a Thawte SuperCert if your customers send highly confidential information such as financial transactions and personal information to your web site.

■ ***How to tell what crypto strength a site uses***

Internet Explorer displays a padlock symbol on the status bar (near the bottom of the screen) for a secure site:

Hold the mouse over this padlock, and a hint will appear showing the session strength:

Netscape has a security icon on the toolbar, which shows a locked padlock for a secure site:

Click on this, then click on "Open Page Info". In the resulting screen, you will see a line like this:

Security: This is a secure document that uses a high-grade encryption key for U.S. domestic use only (RC4, 128 bit).

■ ***What benefits will a Thawte SuperCert hold for my business?***

Thawte SuperCerts provide:

- A higher strength of crypto for international export browsers.
- 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-forgable proof of your web site identity.
- Ease of use. SuperCert is a stand-alone solution that requires no installation of extra software on the server or the browser.

■ ***Useful URLs***

For more detail on Thawte's SuperCerts, please visit:
<http://www.thawte.com/html/RETAIL/sgc/index.html>