

Securing your
Online Data Transfer
with *SSL*

*A GUIDE TO UNDERSTANDING SSL CERTIFICATES,
how they operate and their application...*

1. Overview
2. What is SSL?
3. How to tell if a Website is Secure
4. What does a SSL Certificate Look Like?
5. Browser Security Alerts
6. How does an SSL Session get Set Up?
7. Public and Private Keys
8. Applications of SSL
9. When is the Deployment of SSL Certificates Appropriate?
10. *thawte* SSL Certificate Solutions
11. Testing SSL Certificates on Your Web Server
12. *thawte* Trusted Site Seal
13. Useful URLs
14. What Role does *thawte* Play?
15. The Value of Authentication
16. Contact *thawte*
17. Glossary of Terms

1. Overview

thawte is a leading provider of SSL certificates globally. By making use of a *thawte* SSL Certificate on your company's Web server(s), you can securely collect sensitive information online, and increase business by giving your customers confidence that their transactions are safe.

This guide aims to provide an introduction to SSL security covering the basics of how it operates. A discussion of the various applications of SSL certificates and their appropriate deployment is also included, along with details of how you may test SSL certificates on your web server.

2. What is SSL?

Secure Socket Layer (SSL) is a protocol developed by Netscape in 1996 which quickly became the method of choice for securing data transmissions across the Internet. SSL is an integral part of most web browsers and web servers and makes use of the public-and-private key encryption system developed by RSA.

In order to make an SSL connection, the SSL protocol requires that a server should have a digital certificate installed. A digital certificate is an electronic file that uniquely identifies individuals and servers. Digital certificates serve as a kind of digital passport or credential which authenticate the server prior to the SSL session being established. Typically, digital certificates are signed by an independent and trusted third party to ensure their validity. The "signer" of a certificate is known as a Certification Authority (CA), such as *thawte*.

SSL provides secure communication by combining the following two elements:

1] Authentication –

A digital certificate is tied to a specific domain and a CA performs a number of checks to confirm the identity of the organization requesting the certificate prior to issuing it. In this way, the certificate may only be installed on the domain against which it has been authenticated, providing users with the assurance they need. Various levels of authentication are performed across various products.

2] Encryption –

Encryption is the process of transforming information to make it unintelligible to all but the intended recipient. This forms the basis of data integrity and privacy necessary for e-commerce.

Important Note

The most common application of SSL certificates is to secure data transfer between web browsers and web servers. Although SSL may be used to secure server to server communications, this guide will make use of browser-server examples to explain the workings of SSL.

To find out more about securing server to server communications with SSL, speak to a *thawte* sales representative.


3. How to Tell if a Website is Secure

The first clue to establishing whether or not a website is secured with a SSL certificate lies in the browser status bar – look for the padlock icon. In IE browsers, when pages are not secured the padlock icon will not be visible. However, when a SSL session is established the padlock icon will appear. In Netscape, there are both “locked” and “unlocked” padlock icons indicating secure and unsecured websites respectively.

Microsoft IE

Secure: 

NetScape Navigator

Secure: 

Unsecure: 

The next clue to look for is in the address bar. If a secure session is established between the browser and the web server, the “http:” portion of the web address will change to “https”, for example: “<http://www.thawte.com>” becomes “<https://www.thawte.com>”.

It is also possible to tell the strength of encryption of a particular SSL session. In IE, simply mouse over the padlock to view the encryption strength.

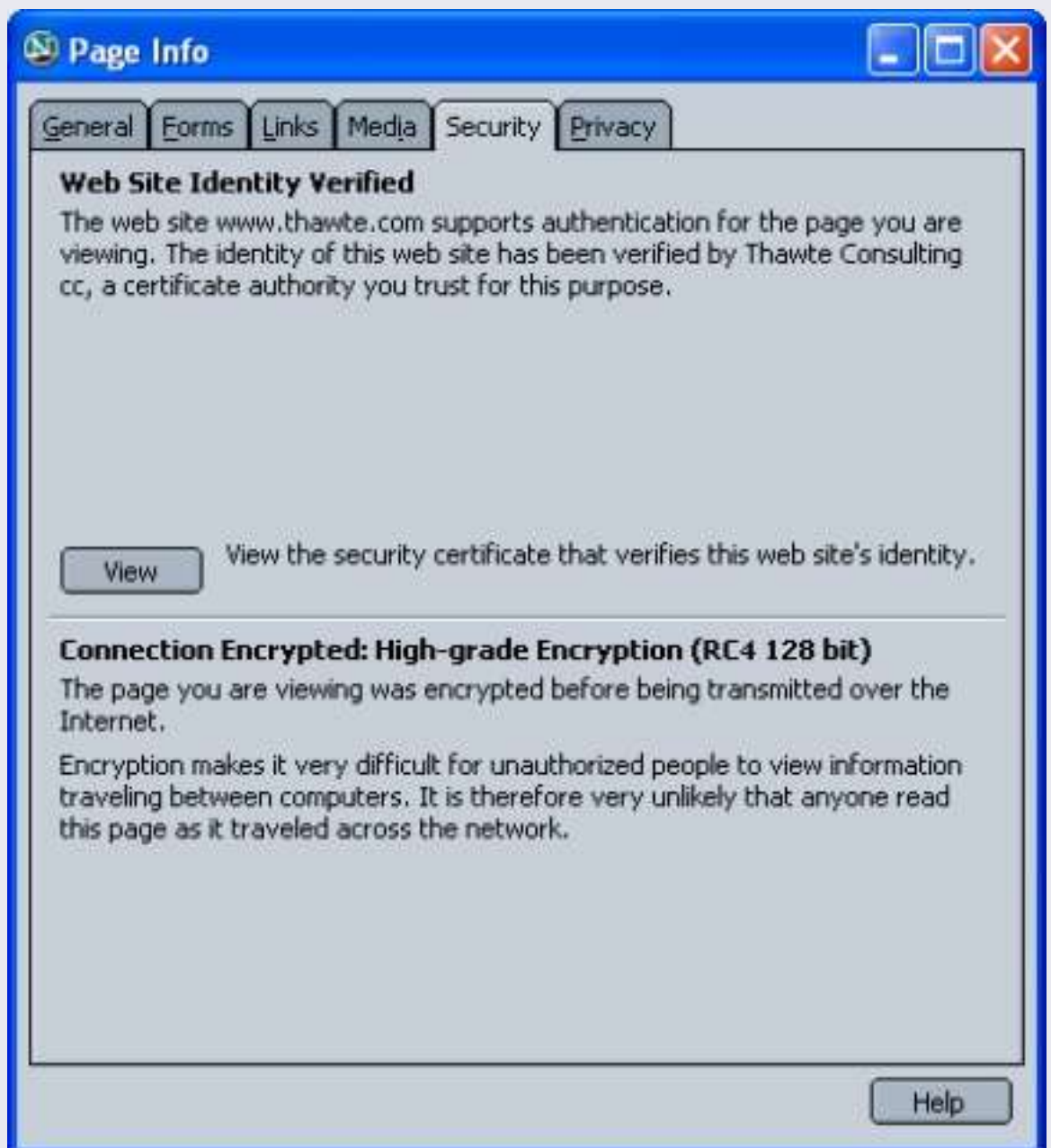


In Netscape, double click on the padlock to view the certificate. The encryption strength is detailed on the first tab of the certificate.

4. What does a SSL Certificate Look Like?

To view a website's certificate, double click on the locked padlock icon which appears in the bottom status bar.

Digital certificate when view with a Netscape 7.0 browser:



Digital certificate when used with an IE 6.0 browser:



An SSL Web Server Certificate or SGC SuperCert from *thawte* enables your customers to view the following information:

- The domain for which the certificate was issued. This allows them to check that the SSL Web Server Certificate was issued for your exact host and domain (www.mydomain.com).
- The owner of the certificate. This acts as further reassurance, since customers are able to see whom they are doing business with.
- The physical location of the owner. Once again this reassures customers that they are dealing with an actual entity.
- The validity dates of the certificate. This is extremely important, since it shows users that your Digital Certificate is current.

5. Browser Security Alerts

Your browser has a built-in security feature that displays a warning message when you try and submit information to a website where there is a problem with the certificate.

This is an example warning message given in Microsoft IE:



In the previous example, the security alert is triggered as the domain name does not match that of the website being accessed indicating that the site on which the certificate is installed has no right of use for the certificate. Other security warnings are triggered should the period of validity for a certificate have expired. Similarly, the warning will be displayed in the event that the certificate is signed with an unrecognized root (a root that is not installed by default in the browser).

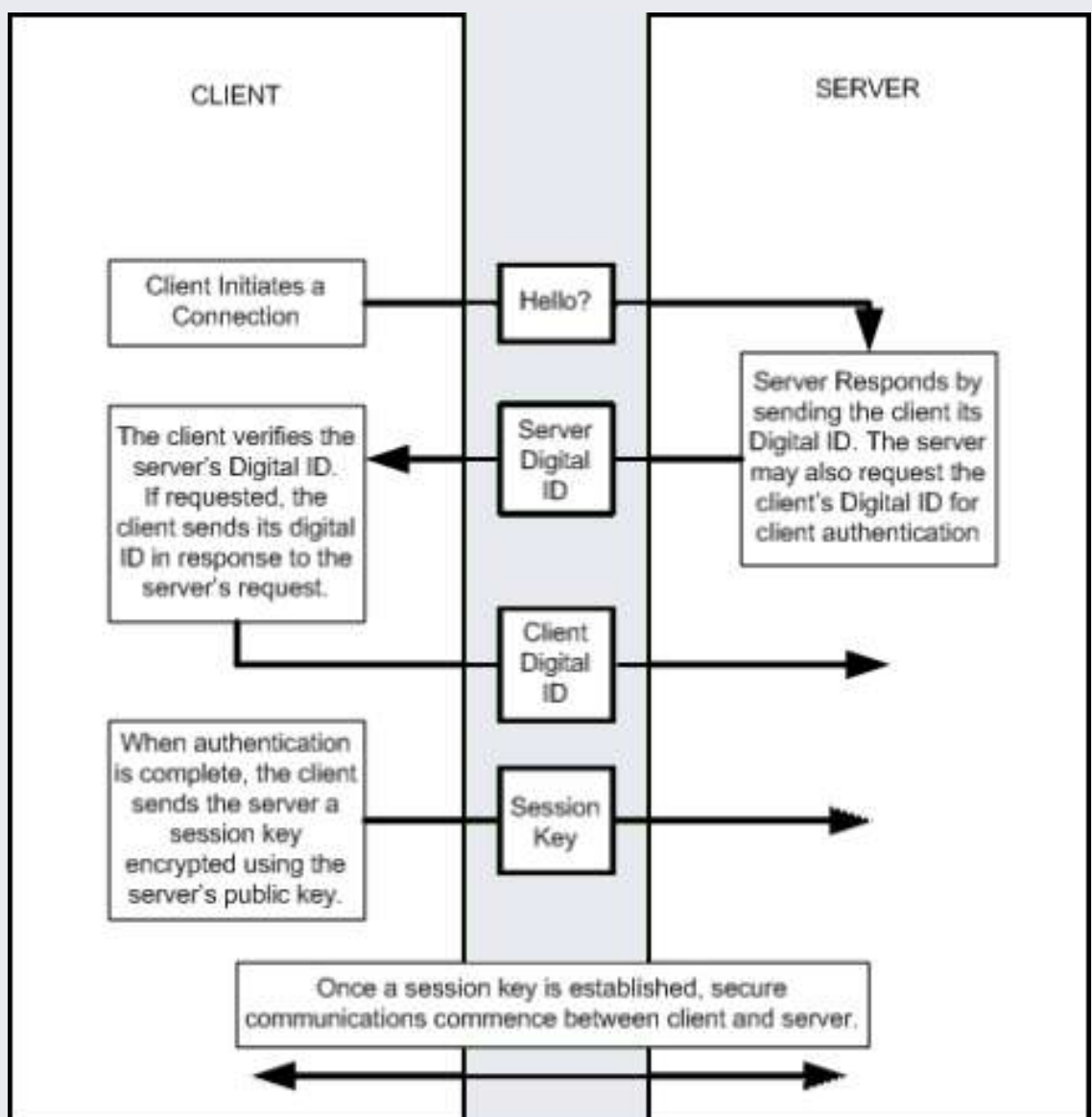
On the other hand, a user accessing a website with a valid certificate will be informed that the website they are visiting has a digital certificate issued by a recognized Certification Authority (CA), such as *thawte*, and that any data they submit will be encrypted. By checking the certificate, the customer can verify that the website is owned by a real legal company and they own the domain name being accessed.



6. How is a SSL Session Set Up?

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 following diagram illustrates the steps which take place when a SSL session is set up:



During this process, the web browser checks that:

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

The process is seamless thus, the user does not see the above steps 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.

7. Public and Private Keys

When you request a certificate, you generate a key pair on your server – a public and a private key. When a key pair is generated for your business, your private key is installed on your server and it is critical that 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. Should you lose your private key, you will no longer be able to use your certificate. For this reason it is essential that you make a back-up of the private key as a best practice for ongoing key management.

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.

8. Applications of SSL

There are two broad areas of application for SSL certificates:

1] Securing Browser to Web Server Communication -

Securing of browser to web server communication is currently the major application and is most frequently applied to ecommerce websites to secure transfer of payment information. The type of data that is considered sensitive is currently expanding from financial data to include all personally identifiable information including identity and social security numbers, and increasingly e-mail addresses.

2] Securing Server to Server Communication -

More and more companies are turning to SSL certificates to secure server to server communications. This is an area of application which provides companies with various options for improving data security and network privacy. At present, securing communication between e-mail servers is the most common application although it is also possible to secure ftp sites, database and application servers amongst others.

9. When is the Deployment of SSL Certificates Appropriate?

The decision to deploy SSL certificates revolves around the importance attached to security of online data transfer. For instance, if you are handling financial transactions on your web site, there is no question that SSL certificates are required. If you are managing sensitive customer data such as social security numbers or identity numbers, the use of SSL certificates is worth serious consideration – especially if customer/member security and privacy is high on your list of priorities.

From a business stand point, the deployment of SSL certificates provides customers/users with the assurance that they will not be exposed to any risks associated with transmitting data over an open network. This in itself has many benefits to your business, most of which flow from increased trust when dealing with your organization online. So, if your business relies on establishing relationships of trust with customers in order to facilitate online transactions, then the deployment of SSL certificates is essential.

10. *thawte* SSL Certificate Solutions

SSL123 Certificates

SSL123 is a secure domain validated certificate capable of 128-bit encryption depending on the level of encryption supported by the client's browser. This product can be issued within minutes and is ideal for businesses wanting to set up basic security between their website and their online users as well as general applications such as securing intranets. [Read more...](#)

SSL Web Server Certificates

The *thawte* SSL Web Server Certificate is capable of 128-bit encryption depending on the level of encryption supported by the client's browser. These certificates are an ideal product for organizations that are serious about doing business online and recognize the value and benefits of having their verified organizational details included in the certificate. [Read more...](#)

SGC SuperCerts

A SGC SuperCert from *thawte* will allow you to extend 128-bit encryption to your clients, even if they use one of the following older browsers: IE 5.01 and Netscape 4.7x and later – which are limited to 40-bit or 56-bit encryption capabilities. These are the certificates of choice if you are securing highly sensitive information and 128-bit encryption is a preference. [Read more...](#)

Starter PKI Program (SPKI)

thawte's SPKI Program is ideal for any company or organization requiring three or more digital certificates per year for its own use on an ongoing basis. Our SPKI Program allows you to take full control of your certification needs while also reaping the benefits of considerable savings.

[Read more...](#)

11. Testing SSL Certificates on Your Web Server

In order to provide you with practical understanding of SSL certificates, you may wish to download a *thawte* SSL test certificate for evaluation purposes. These certificates are valid for 21 days and will allow you to familiarize yourself with the installation process as well as ensure compatibility with your web server configuration. The free Test Certificate is available from: <http://www.thawte.com/ucgi/gothawte.cgi?a=w46840165367049000>

You may also wish to download one of *thawte's* specialist step-by-step guides which deal with requesting, configuration and installation of SSL certificates for the two most popular web server platforms:

[Apache Guide / Microsoft IIS Guide](#)

Installation guidelines for other web server platforms are available on our Support Site – [click here](#).

12. The *thawte* Trusted Site Seal

All *thawte* SSL Web Server Certificate or SGC SuperCert clients may display the *thawte* Trusted Site Seal on their websites. The *thawte* Trusted Site Seal is a secure image which provides visible proof of your trusted status, that you are fully authenticated and that users may transact safely and securely with you.



The *thawte* Trusted Site Seal is available in various languages and sizes allowing for easy integration into your existing website design. More information is available at: <http://www.thawte.com/ssl123/index.html>

13. Useful URLs

For more detail on *thawte's* SSL Web Server Certificates, please visit:

<http://www.thawte.com/ssl/index.html>

Common problems experienced with SSL Web Server Certificates are dealt with in the *thawte* Knowledge Base:

<http://kb.thawte.com>

You can also find useful information in our FAQs:

<http://www.thawte.com/support/ssl/index.html>

Buy SSL Web Server Certificates:

<http://www.thawte.com/buy/>

14. What Role Does *thawte* Play?

thawte is a Certification Authority (CA) that issues SSLvarious digital certificates to organizations and individuals worldwide. *thawte* performs various levels of authentication depending on the product.

thawte digital certificates interoperate smoothly with the most common web servers and browsers, so you can rest assured that you purchase of a *thawte* Digital Certificate will give your customers confidence in your system and integrity – they will feel secure about transacting online.

15. The Value of Authentication

Information is a critical asset to your business. To ensure the integrity and safety of your information, it is important to identify with whom you are dealing, and the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in all types of transactions by addressing a unique set of security issues including:

Spoofting:

The low cost of website design and the ease with which existing pages can be copied makes it all too easy to create illegitimate websites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional looking storefronts that mimic legitimate businesses.

Unauthorized Action:

A competitor or disgruntled customer can alter your website so that it malfunctions or refuses to service potential clients.

Unauthorized Disclosure:

When transaction information is transmitted “in the clear”, hackers can intercept the transmissions to obtain sensitive information from your customers.

Data Alteration:

The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers and currency amounts sent “in the clear” are all vulnerable to alteration.

16. Contact *thawte*

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:

E-Mail: sales@thawte.com

Telephone: +27 21 937 8902

Fax: +27 21 937 8967

17. Glossary of Terms

Asymmetrical Cryptography

A cryptographic method using a combined public and private key pair to encrypt and decrypt messages. To send an encrypted message, a user encrypts a message with the recipient's public key. Upon receipt, the message is decrypted with the recipient's private key.

Using different keys to perform the encryption and decryption functions is known as a trap-door one way function, that is, the public key is used to encrypt a message but it cannot be used to decrypt the same message. Without knowing the private key, it is practically impossible to reverse this function when modern strong encryption is used.

Certification Authority

A certification authority (CA) is an organization (such as *thawte*) that issues and manages security credentials and public keys for message encryption.

Certificate Signing Request (CSR)

A CSR is a Public Key that you generate on your server that validates the computer-specific information about your web server and Organization when you request a Certificate from *thawte*.

Private Key

A private key is numeric code used to decrypt messages encrypted with a unique corresponding public key. Integrity of encryption depends on the private key being kept secret.

Public Key

A public key is a numeric code which enables encryption of messages sent to the holder of the corresponding unique private key. The public key may be freely circulated without compromising encryption while increasing the efficiency and convenience of enabling encrypted communication.

Public Key Infrastructure

A method for exchanging information securely within organizations, industries, nations or even worldwide. A PKI uses the asymmetric encryption method for encrypting IDs and documents or messages. (this is also known as the "public/private key" method). A PKI starts with a certificate authority (CA) such as *thawte*, which issues and revokes digital certificates (digital IDs) authenticating the identity of people and organizations over a public system such as the Internet.

Symmetric Cryptography

A cryptographic method where the same key is used for both encryption and decryption. This approach is handicapped by the security risks involved in secure distribution of the key since it must be communicated to and known by both sender and receiver without being disclosed to third parties.