





-  Introduction
-  Using security in Mosaic
-  Security menu options

 **Introduction**

[Introduction](#)

[Where to learn more](#)

 **Using security in Mosaic**

 **Security menu options**

SPRY Mosaic implements the [SSL](#) standard of privacy and [encryption](#) to allow secure transactions over the Internet. SPRY Mosaic uses security technology from RSA Data Security, Inc.

Using SSL, SPRY Mosaic allows you to send and receive encrypted messages with SSL servers. It also allows you to verify, or authenticate, the identity of the secure server.

Secure transactions in Mosaic will occur when you are connected to an SSL server. An SSL server can be identified by a URL that begins with **https://**. These servers cannot be accessed directly, but must be reached indirectly through links from other documents.

There are many SSL servers in existence. Most Web-based commerce relies on SSL for the safe transmission of credit card information or customer data. **SPRY SafetyWEB** is an SSL Web server for UNIX and Windows NT that provides security for online businesses and organizations. For more information on SPRY SafetyWEB, see <http://server.spry.com/>.

 [Where to learn more](#)

For information on:

See this Web page:

**Cryptography
Concepts**

<ftp://www.rsa.com/rsalabs/faq/>


A frequently asked questions (FAQ) document on cryptography that provides a fairly thorough background on secure transaction technology.

SSL

<http://home.netscape.com/newsref/std/SSL.html>


Information on Netscape's SSL specification.

 **Introduction**

 **Using Security in Mosaic**

Overview

Sending encrypted information

 **Security menu options**



SPRY Mosaic supports the [SSL](#) protocol, which provides [encryption](#), and [server authentication](#). Below is an example of a secure transaction in Mosaic.




Cyber Books, a small company with a Web page, wants to allow customers to provide their credit card numbers so that they can order books over the World Wide Web. They want to assure their customers that the credit card information cannot be read by anyone else. Cyber Books uses [public key encryption](#), generating a key pair; the public key is shared, but the private key is stored only on the Cyber Books system, in an encrypted format.

After a customer fills out an order form and clicks a Submit button on the Cyber Books web page, an encrypted connection is established between the customer and Cyber Books. The server sends a [certificate](#), along with a copy of its public key, which enables SPRY Mosaic to verify the identity of the server. The client then constructs and returns a [session key](#), which is used to encrypt messages transferred between SPRY Mosaic and Cyber Books. The message, containing a credit card number and shipping information, is now private and secure. Even if intercepted by someone else, it cannot be decrypted.

Show Me

Secure transactions happen automatically in SPRY Mosaic when you request a **secure document**. To interact with a secure document:

1. Connect to a secure page. Many servers have a button or link to use their pages with a security. Also, pages with financial transactions will sometimes have a Submit button to send information securely. A URL can also be entered using Mosaic's Open command. A URL to a secure page begins with **https://**.
2. When Mosaic begins the connection to the secure server, a box will appear notifying you that you are about to retrieve a secure document. If you do not want to see this notification every time you request a secure document, deselect the checkbox to the left.
3.  The icon in the status bar will change to a solid key, to notify you that the page is secure.
4. After a private and secure encrypted transfer, the document will appear in the Mosaic window. Any forms, imagemaps, buttons or links will function normally, and you can print and save the document the same way as a non-secure item.
5. If links are used to move to any other secure page, the secure connection will not be interrupted.
6. When you open a page not secured with SSL, a box will appear notifying you that you are about to leave a secure document. If you do not want to see this notification every time you leave a secure document, deselect the checkbox to the left.
7.  After the non-secure page opens, the icon returns to its prior form.

-  Introduction
-  Using Security in Mosaic
-  Security menu options
- Options

Glossary items

SSL

The Secure Sockets Layer protocol. SSL is used to protect data integrity and prevent eavesdropping in Web transactions. When SPRY Mosaic or other SSL-enabled browsers connect to an SSL server, all information transmitted is encrypted, ensuring privacy and security.

Certificate Authority

An organization that verifies the identity of users on the World Wide Web. Before a server can be used for secure transactions, its owner must have a key certified by a Certificate Authority.

Some Certificate Authorities require you to identify yourself before issuing a certificate; they may require you to appear in person and show identification such as a birth certificate or passport, or sending identification via US Mail. These organizations usually require a fee. There are also low assurance Certificate Authorities that issue certificates without a high level of verification.

certificate

Since anyone can generate a public/private key pair, there must be some way to authenticate a person's identity. Certificates are documents that include a user's public key and have been signed by [Certificate Authorities](#), organizations that attest to the identity of the person with that public key.

A certificate is like a form that has been signed by a notary public; in this case, the Certificate Authority is the "notary public" for the certificate and attests to a person's identity. Certificates become part of digital signatures, so that identities can be verified by checking the certificate information associated with a signature.

public key encryption

A method used for encrypting and decrypting messages which uses public and private key pairs in order to ensure security.

A pair of numbers is generated using a sophisticated generation scheme involving prime numbers. One of these numbers, the **private key**, is kept secret, and is never transmitted over the Internet. The other number, the **public key**, is available to others.

Although the private key cannot be derived from the public key (and vice versa), there is a scheme by which the two numbers can be matched. This means that a message encrypted using the **public key** can only be decrypted by the holder of the private key. This ensures that a message can be encrypted so that only one user can read it.

shared key

Shared keys are a method used for low-level encryption and authentication. A server will require a person to provide a **shared secret** in order to access server information. A shared secret is

much like a password; it is a piece of information known by both sides of a transaction.

You will not be able to access the protected information unless you know the shared secret for that information. This will be provided to you by the site you are trying to access, if they want you to access their information.

trusted root

You can specify that Mosaic display only secure pages signed by one or more particular [Certificate Authorities](#). These Certificate Authorities are known as trusted roots. Web pages must be signed with the certificate from a trusted root before you will accept their signatures as valid.

Three trusted roots from RSA, Inc., are pre-defined in Mosaic: the Secure Server Certification Authority, the Commercial Certification Authority and the Low Assurance Certification Authority. You can display and add trusted roots by choosing **Trusted Roots** from the **Security** menu.

You can add additional trusted roots if you have a certificate file from the Certificate Authority.

NOTE If you are getting "Cannot Create Certificate Chain" messages when trying to access a home page, it may be because you do not have the Certificate Authority that was used to sign that home page defined as a trusted root.

encryption

A method or system of altering data or information in such a way that it is hidden from unwelcome recipients. Encryption typically relies on a mathematically based code to prevent tampering from simple methods such as guessing or 'brute force' attacks by powerful computers.

server authentication

A process where the server's identity is verified. SPRY Mosaic analyzes the server's certificate with its public key to determine if they are both valid. If they do not match, Mosaic will warn that communication with the server may not be secure.

session key

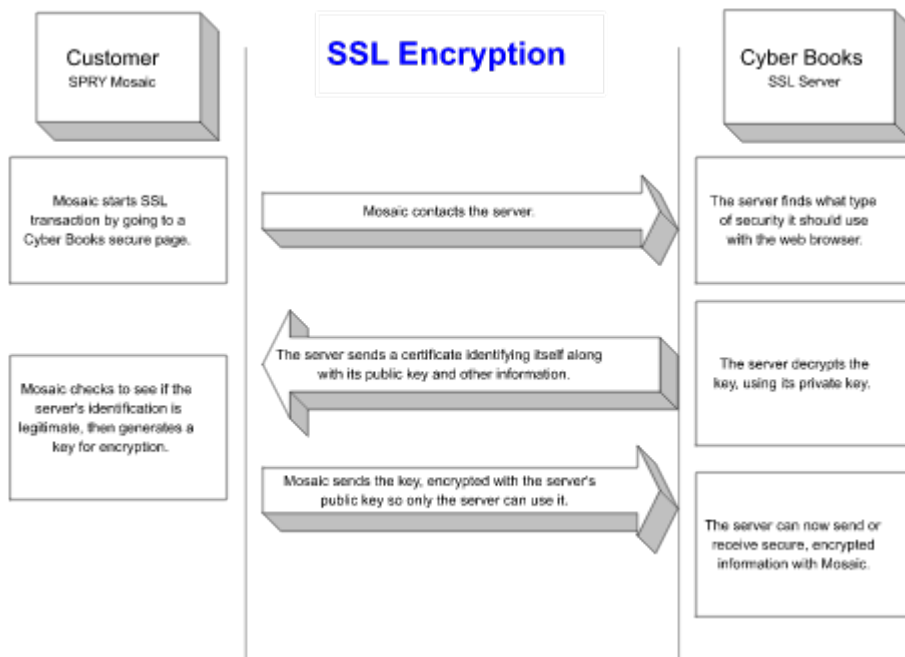
A [shared key](#) used for the encryption of exchanged information in an SSL transaction. Session keys are created by SPRY Mosaic using information exchanged during connection establishment. Session keys expire after a short period of time and are re-generated, to insure both the server and Mosaic's security.

secure document

A web page which is on a secure web server using SSL or another

method of security. When requested by a secure browser, the document will be transported in an encrypted format. Instead of the typical **http://** URL prefix, secure pages begin with **https://**. No other format changes are necessary for a secure document, but the server must support a form of security such as SSL. When a secure document is viewed in SPRY Mosaic, an icon of a key appears in the status bar.

Diagrams



Configures options pertaining to SSL security.

Notify when entering secured document Shows notification each time you enter a [secure document](#).

Notify when leaving secured document Shows notification each time you leave a [secure document](#).

