GEOCERTS SSL™
SSL Made Simple

How SSL Works

The Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) is a protocol that provides secure communication between client and server. Here the client is your browser and server is the web site you're communicating with. Secure communication has three main goals: privacy, message integrity, and authentication.

A Typical Scenario

Alice wants to buy a book from Bob's online bookstore. In order to complete the process she'll need to transmit sensitive personal information, such as her credit card number. Alice wants to make sure that the information she sends to Bob is kept confidential (privacy), and cannot be altered along the way (message integrity). She also wants to make sure that she's really sending the information to Bob and not an imposter (authentication).

Privacy

The sensitive information Alice sends to Bob is kept private by cryptography. A plaintext message is encrypted into ciphertext. To anyone who might eavesdrop and intercept the message, the ciphertext is meaningless. It's estimated that trying to crack the ciphertext by brute force alone (trying every possible combination) would take millions of years even if all the computers in the world were linked together to solve the puzzle.

Note: The Alice and Bob scenario is an adopted convention used in cryptographic circles. Other characters include Eve the eavesdropper and Victor the verifier.

Public Key Cryptography

The information used to turn a plaintext message into an

encrypted ciphertext message is a key. Public key cryptography makes use of a pair of keys, one is public, and the other is private. Alice wants to send Bob private information, so Bob says, "Here Alice, use this public key to encrypt your message before sending it to me. When I receive your encrypted message I will use my private key to decrypt your message." It's okay for anyone to have a copy of the public key, but only Bob should have a copy of his private key. A plaintext message encrypted with the public key can only be decrypted with the private key.

Message Integrity

When Alice sends a message to Bob, someone could intercept that message, alter it, and send it on its way. She could end up buying the wrong book or more copies than she really wanted. Message integrity is achieved by sending a message digest along with the encrypted message. A message digest is a fixed-length representation of a message. Think of it as a fingerprint of the original message. Alice says to Bob, "I'm going to send you an encrypted message. So that you know my message to you hasn't been intercepted and altered along the way, I'm also sending a fingerprint of my original message. Please check the fingerprint to see if it matches when you receive my message."

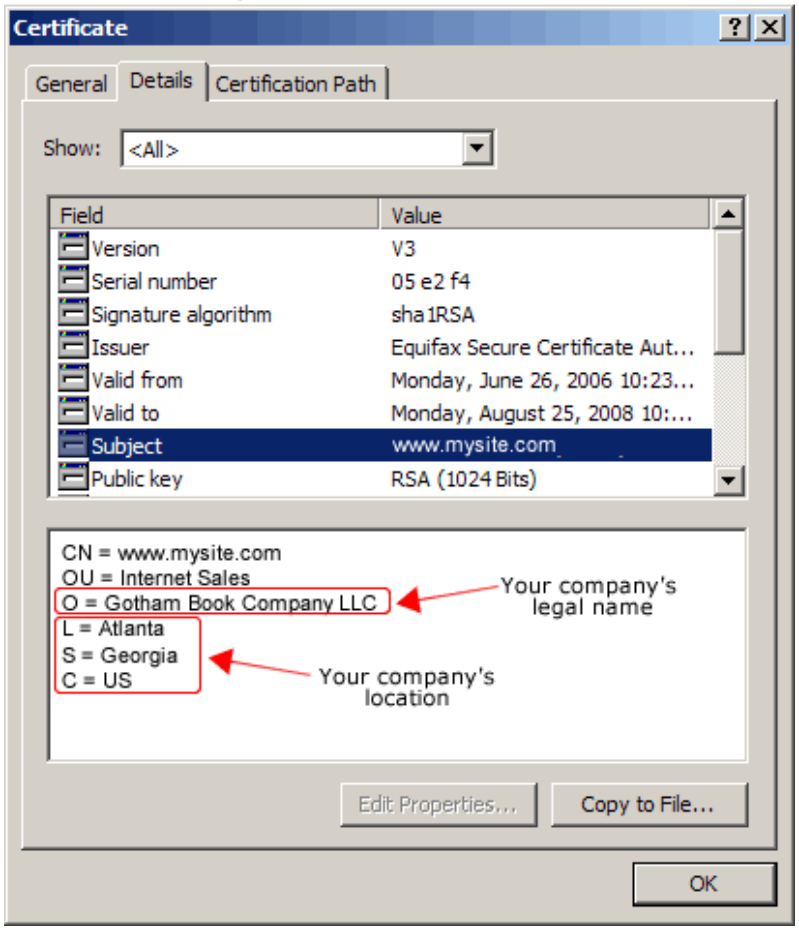
Authentication

Alice's message to Bob is encrypted for privacy, and fingerprinted for message integrity, but how does Alice know that she is really sending the message to Bob? Alice needs to authenticate Bob, to make sure he's really Bob and not someone else. Authentication is achieved by digital certificates.

Digital SSL Certificates

When Alice and Bob first negotiate their SSL session, Bob sends Alice a copy of his digital certificate. A digital certificate is an electronic document. Inside that certificate is a copy of Bob's public key and information about its owner (domain name, organization name, location).

A Fully-Authenticated SSL Certificate



Why Should Alice Trust the Information

Because the SSL certificate is verified or "signed" by a trusted third party Certificate Authority, such as GeoTrust. The trusted Certificate Authority's job is to verify Bob's application for a digital SSL certificate. The authentication process can range from verifying that Bob has authoritative control of his domain (for GeoTrust QuickSSL), to requiring Bob to submit legal documents that verify Bob's business or organization (for GeoTrust True BusinessID). Once Bob's identity has been verified he will be issued a digital SSL certificate.

All of these concepts- privacy by encryption, integrity by message digests (fingerprinting), and authentication by digital SSL certificates- are integrated into the SSL protocol to allow Alice and Bob to communicate securely.

Browse GeoTrust SSL Certificates


Symantec.
Website Security
Platinum Partner


VERIFY
Norton
SECURED
powered by Symantec