# What is SSL?

## .Introduction

Secure Sockets Layer (SSL) is a system to encrypt transmissions of information on the Internet so that data transfer may be accomplished securely. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

SSL was developed by Netscape Communications Corporation, and supports server and client authentication. The SSL protocol is application independent, allowing protocols such as HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), and Telnet to be layered on top of it transparently. SSL is, however, optimized for HTTP.

SSL is an enhancement to Layer 4 of the OSI Model.

Without SSL

| | |
|---|---|
| Layer 7 | Application |
| Layer 6 | Presentation |
| Layer 5 | Session |
| Layer 4 | TCP, UDP |
| Layer 3 | Network Layer (IP) |
| Layer 2 | Data Link Layer (Ethernet, Token Ring, ATM, etc.) |
| Layer 1 | Physical Layer (twisted pair, coax, fiber, wireless) |

With SSL

| | |
|---|---|
| Layer 7 | Application |
| Layer 6 | Presentation |
| Layer 5 | Session |
| Layer 4+ | SSL |
| Layer 4 | TCP, UDP |
| Layer 3 | Network Layer (IP) |
| Layer 2 | Data Link Layer (Ethernet, Token Ring, ATM, etc.) |
| Layer 1 | Physical Layer (twisted pair, coax, fiber, wireless) |

## .Definitions

### ..Client-Server

When a User is communicating with a site on the Internet, the User is called the Client. The site with which the User is communicating is called the Server. SSL works in the context of this Client-Server communication scheme.

### *..Certificates*

This paper refers to sending certificates. Certificates are used to allow a Server or a Client to prove its identity. This is done through a trusted third party and involves the Public Key Infrastructure (PKI). A discussion of Certificates is beyond the scope of this paper.

## .SSL Operation

In support of the need for secure communications, SSL encrypts data before sending it. Encryption requires a key or keys. In a majority of the applications for which SSL is intended, there are no keys established or agreed-upon prior to the initiation of a Client-Server communication. Therefore, Public Key-Private-Key (Asymmetric) encryption is the only option, at least to begin the communication, because Asymmetric encryption allows one party (the Client or the Server) to send a Public Key to the other without being concerned that the key is being intercepted.

The SSL Client-Server process begins with the Client and Server exchanging Public Keys. Specifically:
- The Server sends its Public Key to the Client to allow the Client to encrypt data that it sends to the Server.
- The Client sends its Public Key to the Server to allow the Server to encrypt data that it sends to the Client.

The server sends its certificate and cipher preferences in response to a client's request. Once this is done, a Master Key is generated by the Client. It is encrypted using the Server's Public Key, and is sent to the Server. This Master Key is used, in part, as the Symmetric Key for another type of encryption - Symmetric Encryption. For the actual exchange of application data, for which the whole Client-Server communication was established, Symmetric Encryption will hereinafter be used.

The seemingly round-about process is done to accommodate:
- Symmetric Encryption is faster (fewer CPU cycles to encrypt or decrypt) and far more robust than Asymmetric Encryption
- Asymmetric encryption is required first to allow secure exchange of the Symmetric Keys

In the optional second phase, the server sends a challenge to the client. The client authenticates itself to the server by returning the client's digital signature on the challenge, as well as its public-key certificate.

## .Browser Information

The reader will commonly read specifications for the encryption strength of Browsers such as Microsoft Internet Explorer and Netscape Navigator. The most commonly heard Key lengths associated with this encryption are 40 bit and 128 bit. These key lengths refer-to the above-described Symmetric Key length.

A 128 bit Symmetric key length is probably quite adequate for the next 20 years. It is however, important to understand the Asymmetric Key lengths used in SSL**, because the Asymmetric Keys, i.e. the Public Keys that are exchanged by the Client and Server, are used to encrypt the Symmetric Key**. Recall that the Symmetric Key is part of the Master Key. If insufficient key length is used in the Public Keys that are exchanged, then the Master Key can be found and the entire communication is compromised.

The Public Key lengths are generally not known by the Client. You think that you have 128 bit Symmetric Key length and are therefore "safe". **You may not be**. The Public Keys may be 512 bits and above. From a previous paper, I have discussed that 512 bit Asymmetric Key is probably not at all secure and that various experts in the encryption business think that 1024 may not be secure.

The only way to know the Asymmetric Key length that you are using is to contact the Webmaster of the **particular site** with which you are communicating and ask the length of the Asymmetric Key (or Public Key).