SSL

Introduction

SSL is an abbreviation of **Secure Sockets Layer**. The **Secure Sockets Layer (SSL)** is a commonly-used protocol for managing the security of a message transmission on the Internet. **SSL** has recently been succeeded by **Transport Layer Security (TLS)**, which is based on **SSL**. **SSL** uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and **Transport Control Protocol** (TCP) layers.

How it Works with respect to SSL Certificate

Secure Sockets Layer (SSL) technology protects your Web site and makes it easy for customers to trust you.

- An **SSL Certificate** enables encryption of sensitive information during online transactions.
- Each **SSL Certificate** contains unique, authenticated information about the certificate owner.
- Every **SSL Certificate** is issued by a Certificate Authority that verifies the identity of the certificate owner.

An **SSL Certificate** consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a **Secure Sockets Layer** handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key. They can begin a secure session that guarantees message privacy and message integrity.