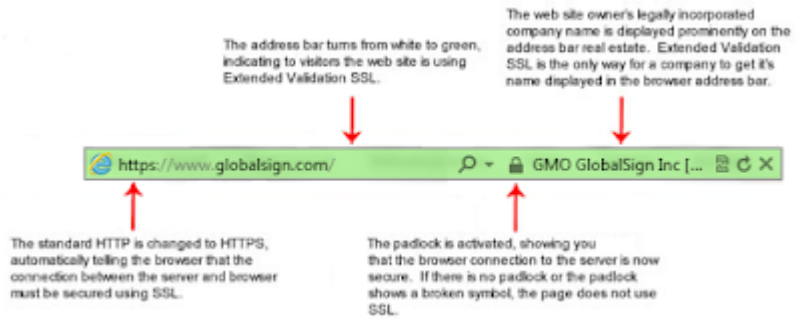
Stands for “Secure Sockets Layer.” SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to “log in” on a website, the resulting page is secured by SSL.

SSL encrypts the data being transmitted so that a third party cannot “eavesdrop” on the transmission and view the data being transmitted. Only the user’s computer and the secure server are able to recognize the data. SSL keeps your name, address, and credit card information between you and merchant to which you are providing it. Without this kind of encryption, online shopping would be far too insecure to be practical.

When you visit a Web address starting with “https,” the “s” after the “http” indicates the website is secure. These websites often use SSL certificates to verify their authenticity.

While SSL is most commonly seen on the Web (HTTP), it is also used to secure other Internet protocols, such as SMTP for sending e-mail and NNTP for newsgroups. Early implementations of SSL were limited to 40-bit encryption, but now most SSL secured protocols use 128-bit encryption or higher.



SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the

web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys – a Private Key and a Public Key.

The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) – a data file also containing your details. You should then submit the CSR. During the SSL Certificate application process, the Certification Authority will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser.

How SSL Works

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols were approved by the Internet Engineering Task Force (IETF) as a standard.

Related Posts:

1. Types of Attack
2. Security threats

3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intoduction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
11. Intrusion terminology
12. Cryptography attacks
13. Cryptography
14. SSH
15. MD5
16. Message digest functions
17. Digital signature
18. Authentication Functions
19. One way hash function
20. Hash function in network web security
21. Digital signature standard