

Sales: 01622 766766

Log In

Search:

[Products](#)[SSL](#)[Enterprise](#)[Partners](#)[About Us](#)[Contact Us](#)[Resources](#)[Support](#)

What is SSL?

A brief explanation

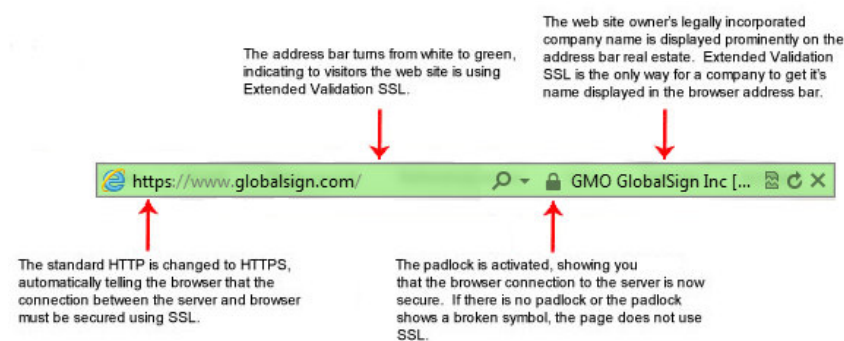
[Home](#) [SSL Information Centre](#) [What is SSL?](#)

What is SSL?

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet.

Technically, SSL is a transparent protocol which requires little interaction from the end user when establishing a secure session. In the case of a browser for instance, users are alerted to the presence of SSL when the browser displays a padlock, or, in the case of Extended Validation SSL, when the address bar displays both a padlock and a green bar. This is the key to the success of SSL – it is an incredibly simple experience for end users.

Extended Validation (EV) SSL Certificates (such as [GlobalSign ExtendedSSL](#)) display visible trust indicators:



Standard SSL Certificates (such as [GlobalSign DomainSSL](#) and [OrganizationSSL](#)) display:



As opposed to unsecured HTTP URLs which begin with "http://" and use port 80 by default, secure HTTPS URLs begin with "https://" and use port 443 by default.

HTTP is insecure and is subject to eavesdropping attacks which, if critical information like credit card details and account logins is transmitted and picked up, can let attackers gain access to online accounts and sensitive information. Ensuring data is either sent or posted through the browser using HTTPS is ensuring that such information is encrypted and secure.

In practice, how is SSL used in today's modern e-commerce enabled / online workflow and service society?

- To secure online credit card transactions.
- To secure system logins and any sensitive information exchanged online.
- To secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server.
- To secure workflow and virtualisation applications like Citrix Delivery Platforms or cloud-based computing platforms.
- To secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- To secure the transfer of files over https and FTP(s) services such as website owners updating new pages to their websites or transferring large files.
- To secure hosting control panel logins and activity like Parallels, cPanel and others.
- To secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.
- To secure network logins and other network traffic with SSL VPNs such as VPN Access Servers or applications like the Citrix Access Gateway.

SSL Information Centre

[What is SSL?](#)
[What is an SSL Certificate?](#)
[Certificate Authority Root](#)
[What are the types of SSL?](#)
[Using a Secure Site Seal](#)
[What is SGC?](#)
[CA Network Security Practices](#)
[What is EV SSL?](#)
[Telling DV & OV Apart](#)
[Choosing Safe Key Sizes](#)
[Security and website performance](#)

Contact a Solutions Specialist to discuss your needs
[Contact Us](#)



Follow us:

All these applications have a number of shared themes:

The data being transmitted over the Internet or network needs confidentiality. In other words, people do not want their credit card number, account login, passwords or personal information to be exposed over the Internet.

The data needs to remain integral, which means that once credit card details and the amount to be charged to the credit card have been sent, a hacker sitting in the middle cannot change the amount to be charged and where the funds should go.

Your organisation needs identity assurance to authenticate itself to customers / extranet users and ensure them they are dealing with the right organisation.

Your organisation needs to comply with regional, national or international regulations on data privacy, security and integrity.



GMO GlobalSign is one of the longest established Certificate Authorities (CA) and leaders in Cloud PKI identity credentialing and automated SSL Certificate management. GlobalSign x.509 Digital Certificates are trusted by all browsers and mobile devices and include: Multi-Domain & Extended Validation SSL, Code Signing, Adobe PDF Signing, Microsoft Office Digital Signatures, S/MIME Secure Email, Strong Authentication for networks and mobile access, and root signing for enterprise Certificate Authorities.



[Get a GlobalSign Site Seal](#)

[Contact GlobalSign](#) | [News](#) | [GlobalSign Blogs](#) | [Resources](#) | [Legal Repository](#) | [Site Map](#) | © 2013 GlobalSign

We use cookies to improve the quality of this site. [Read our cookie policy here](#), or simply click "Accept Cookies & Continue".

[Accept Cookies & Continue](#)