GlobalSign SSL Secure Server Certificates

Understanding the basics of SSL Certificates

GLOBALSIGN WHITE PAPER

GMO GlobalSign Inc.

www.globalsign.com

CONTENTS

INTRODUCTION

SSL (Secure Sockets Layer) is a widely used security protocol that most web servers use to ensure a secure machine to machine connection over an unsecure network such as the Internet. From a business perspective, using SSL can seem overly complicated and choosing the most suitable type of SSL Certificate for a business's requirements, whether an internal network or external website can confuse many, even experienced IT professionals. This white paper will enlighten readers of the features and benefits of using SSL and details the different types of certificates available and when each type is most appropriately used. It also aims to reassure readers that SSL is not as complicated as it has historically been made out to be and with GlobalSign, SSL management is actually rather easy!

WHAT IS SSL?

The Secure Sockets Layer (SSL) along with Transport Layer Security (TLS) is the most widely used security protocol today. Essentially, it provides a secure channel between two machines operating over the Internet or an internal network. We typically see SSL in use when a web browser needs to securely connect to a web server over the unsecure Internet.

The key success of SSL is the simplicity to the end user. Technically, SSL is a transparent protocol, which requires little interaction from the end user when establishing a secure session. In the instance of a browser, the end user is alerted about the use of SSL as they will be able to see a yellow padlock, or in the case of Extended Validation SSL, the address bar displays both a padlock and turns the address bar green, as well as the URL displaying as HTTPS. Websites as standard will use HTTP, which is unsecure in its nature and subject to eavesdropping attacks, which if critical information like credit card details and account logins are transmitted, can give attackers access to online accounts and sensitive information, consequently leading to fraud or even identity theft.

SSL growth is driven by a number of factors, such as increased online shopping, but also from a number of other web services and applications now requiring browser-based security. At present the SSL market is continuing to grow with 25% global growth year on year, but interestingly, approximately only 2% of all websites worldwide currently USE an SSL Certificate, but arguably a lot more actually NEED an SSL Certificate.

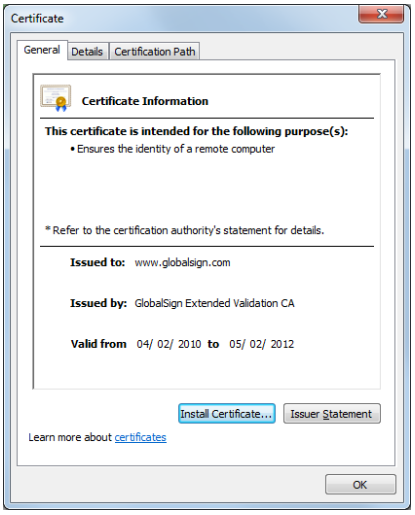
WHAT IS AN SSL CERTIFICATE?

SSL is a protocol and an SSL Certificate is required in order to be able to access and use the protocol. An SSL Certificate is a small data file issued by one of a limited number of trusted Certificate Authorities (CAs), such as GlobalSign, that digitally bind a cryptographic key to an organizations corporate details. Such details can include domain, server or host name, company name and location and in some cases organizational contact details.

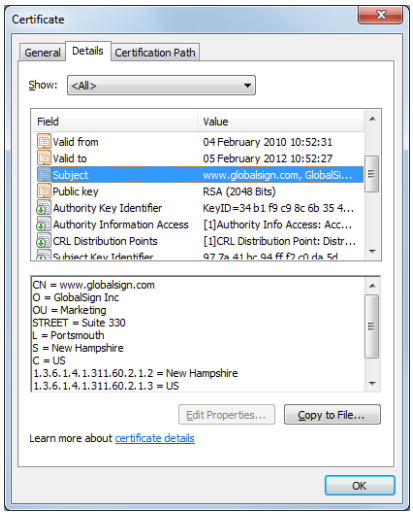
Organizations need to install the SSL Certificate onto their web servers to initiate SSL sessions with browsers. There are varying levels of vetting for each type of certificate an individual/organization can apply for.

Once a certificate is installed it is possible to connect to a website using a HTTPS connection, as this tells the server to establish a secure connection with the browser. Once the secure connection is established all web traffic between the server and browser is secure.

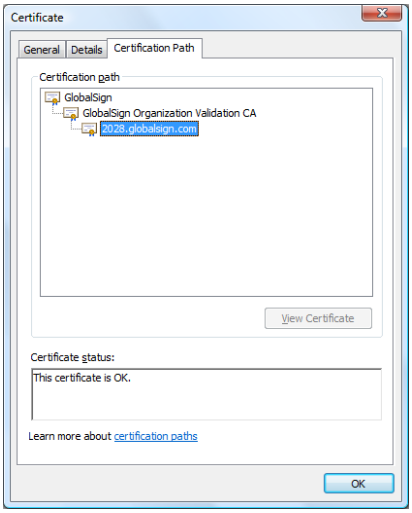
Anyone can view an SSL Certificate on a browser by clicking on a padlock and selecting View Certificate. All browsers show the certificate in different ways but the information stays the same.



To view the actual contents of the certificate you can click the Details tab:



The Certification path shows which Trusted Root Certificate belonging to which Certificate Authority has been used to issue the SSL Certificate:



WHEN SHOULD SSL BE USED?

SSL should be used whenever information is submitted online, over the Internet or internal network, for example when filling in forms or logging into online accounts. It is commonly misunderstood that SSL should be used purely for securing payment pages and credit card transactions, but any exchange or personal information from an end user submitted to a website should be encrypted. SSL should be the minimum security standard used when collecting and submitting data and should be used in all of the following situations:

- To secure online credit card transactions
- To secure online logins, sensitive information transmitted via web forms, or protected areas of websites
- To secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server
- To secure workflow and virtualisation application 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 panels 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

GlobalSign provides products and technology to secure any of the applications mentioned which are discussed below in more detail.

TYPES OF SSL CERTIFICATE

Domain Validated (DV) SSL

This level of certificate is where the CA checks the right of the applicant to use a specific domain name via email challenge. No company identity information is vetted and therefore company information is not displayed within the certificate. This means that issuance time is fast and can be issued within minutes.

When should DV SSL be used?

A Domain Validated SSL Certificate should be used when basic encryption is all that is required, such as internal and lower profile public sites, or in such instances where the applicant is not a legally incorporated entity, or those that wish to have the certificate issued quickly. In addition it can be used when company documents are not readily available and when shared VPS or Managed Hosting is required.

GlobalSign offers two types of Domain Validated SSL Certificates. DomainSSL which is feature-packed and includes all of our advanced options, as well as AlphaSSL, which is a GlobalSign sub-brand containing basic level features.

Organization Validated (OV) SSL

Before issuing the Certificate Authority checks the right of the applicant to use a specific domain name and a check into the existence of the organization is conducted. This vetted company information is displayed to customers when viewing the certificate details, giving more visibility into the entity behind the site and provides enhanced trust to the website visitor. Due to the requirement to vet the organization, from application to issuance it takes longer to obtain an OV certificate than a DV certificate.

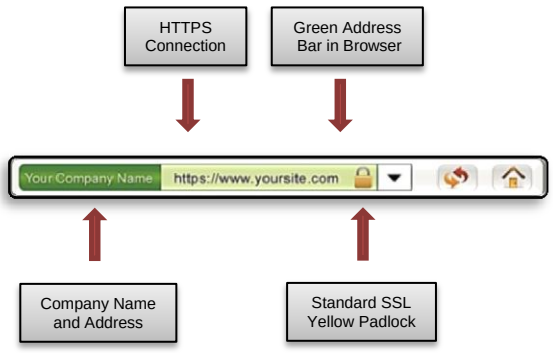
When should OV SSL be used?

An Organization Validated SSL Certificate, branded as OrganizationSSL by GlobalSign, is ideal when identity assurance and higher trust is as important as encryption, customers are able to wait 2 business days to receive the certificate, sub domains need to be secured with a single SSL Certificate and if a Public IP address needs to be secured. It can also be used for the same reasons as a Domain Validated SSL Certificate.

Extended Validation (EV) SSL

Extended Validation SSL is the most visually noticeable SSL Certificate for end users, as it activates the green address bar in browsers, as well as displaying the standard gold padlock. The green bar also alternates between the organization name and issuing Certification Authority, enhancing levels of customer trust.

EV SSL Features:



With the most advanced type of SSL Certificate available, the CA checks the right of the applicant to use a specific domain name, plus conducts a thorough vetting of the organization. The issuance process of EV SSL Certificates is strictly defined within the EV guidelines, as formally approved by the CA/Browser forum in 2007, which specify all the steps required for a CA before issuing a certificate. This includes verification of the following:

- The legal, physical and operational existence of the entity
- That the identity of the entity matches official records
- That the entity has exclusive right to use the domain specified in the EV SSL Certificate
- That the entity has properly authorized the issuance of the EV SSL Certificate
- Issuance time is 3-5 business days

When should EV SSL be used?

EV SSL, branded as ExtendedSSL by GlobalSign, should be used when the highest level of identity assurance, visible trust and encryption level is required, such as incorporated companies and organizations. It is also recommended that it should be used by high profile brands that are more susceptible to phishing attacks and those that want to protect themselves against the threat of copycat websites. This includes public facing websites where the organization wishes to increase customers trust, provide maximum assurance, increase sales conversions, as well as elevate their site image to compete with large companies who have already adopted EV SSL.

GLOBALSIGN CERTIFICATE FEATURES

With so many CAs providing SSL Certificates, it's not easy for website owners to decide which one to choose. GlobalSign's SSL Certificates are trusted by all known devices, as well as including numerous advanced features, many of which competing SSL Providers offer as paid-for premium options:

- 2048 bit future proof issuing authority
- SGC Security for minimum 128 bit minimum to 256 bit SSL encryption levels
- Unlimited Server Licensing - means that you can use a single SSL Certificate across a number of servers
- Wildcard SSL & Unified Communications – simple cost effective support for complex multi-domain server configuration
- Secure Site Seal
- Multi-year discounts
- AutoCSR – CSRs are optional not mandatory
- Unlimited reissues and multi-year savings
- Malware distribution monitoring and detection service
- GlobalSign Certificate Centre Account
- Installation Healthcheck

- Universal Compatibility with all browsers, mobile phones and devices
- Secures both www.domain.com and domain.com (without the www)
- Warranty – underwritten Liability Program
- For more feature details visit: www.globalsign.com/ssl

WHY CHOOSE GLOBALSIGN OVER OTHER SSL PROVIDERS?

As a leader in public trust service, GlobalSign has been issuing trusted digital certificates since 1996. As Europe's first CA, and one of the first worldwide, our root certificate is trusted by all major web browsers and devices. GlobalSign SSL Certificates currently secure global websites including Virgin Atlantic, Land Rover Jaguar, Walmart & Ford. By choosing our SSL Certificates, customers benefit from:

- A simple but sophisticated product range
- An easy ordering system and customer account accessible 24/7
- Trust from a truly global company with localized language support as well as superior customer service levels
- A well-established brand that consumers recognize and trust

WHERE ARE GLOBALSIGN SSL CERTIFICATES AVAILABLE?

Directly from our Websites

There are various ways you can purchase GlobalSign SSL Certificates, the most direct method being from GlobalSign range of websites. The full product range is available to buy in 3 currencies via several languages, plus DomainSSL and OrganizationSSL Certificates are available to trial for free.

For more information visit: http://www.globalsing.com/ssl

Enterprise Solutions

When an organization has the requirements for multiple certificates, GlobalSign's Managed SSL is the perfect solution. Managed SSL allows enterprises of all sizes to conveniently and quickly purchase SSL Certificates through a web based management interface or web service API. Once the organization is pre-vetted, certificates can be applied for and issued instantly across even the most distributed of departments and organizations. The net result? A significantly reduction in the costs and time associated with SSL management.

For more information about GlobalSign's SSL Managed service why not read our white paper: http://www.globalsign.com/resources/white-paper-simplifying-ssl-management.pdf

Or visit: http://www.globalsign.com/ssl/managed-ssl

Reseller Partner Solutions

Our reseller option allows organizations, such as hosting companies, domain registrars, web designers, integrators and VARs to add SSL Certificates to their existing product portfolio as a standalone product or value add. Hosting companies in particular can benefit from reselling SSL Certificates, as they can easily become an added feature/option within their hosting plans. Features of the reseller program include discounted pricing and high margins, sales and technical training, a free Certificate for site and an official Partner site seal. For more information about reselling GlobalSign SSL Certificates visit: http://www.globalsign.com/partners/

INQUIRE ABOUT GLOBALSIGN'S SSL SOLUTION

To inquire about SSL for your organization, please contact us at www.globalsign.com. We would be happy to discuss your specific requirements.

For further information, data sheets, guides, pricing and FAQs on GlobalSign SSL Certificates please go to: http://www.globalsign.com/ssl/

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication and Enterprise Digital ID Solutions, internal PKI & Microsoft Certificate Service root signing. Our trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, and member of the Online Trust Alliance, CAB Forum and Anti-Phishing Working Group, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign US & Canada
Tel: 1-877-775-4562
www.globalsign.com
sales-us@globalsign.com

GlobalSign EU
Tel: +32 16 891900
www.globalsign.eu
sales@globalsign.com

GlobalSign UK
Tel: +44 1622 766766
www.globalsign.co.uk
sales@globalsign.com

GlobalSign FR
Tel: +33 1 82 88 01 24
www.globalsign.fr
ventes@globalsign.com

GlobalSign DE
Tel: +49 30 8878 9310
www.globalsign.de
verkauf@globalsign.com

GlobalSign NL
Tel: +31 20 8908021
www.globalsign.nl
verkoop@globalsign.com