What are the Types of SSL?

What are the different types of SSL Certificates?

Over the last few years the number of organizations using SSL Certificates has increased dramatically. The applications for which SSL is being used have also expanded. For example:

- Some organizations need SSL simply for confidentiality, e.g. encryption

- Some organizations wish to use SSL to enhance trust in their security and identity, e.g. they want to show customers they have been vetted and are a legitimate organization

As the applications for SSL have started to become wider, three types of SSL Certificates have emerged:

Extended Validation (EV) SSL Certificates: where the Certificate Authority (CA) checks the right of the applicant to use a specific domain name PLUS it conducts a THOROUGH vetting of the organization. The issuance process of EV SSL Certificates is strictly defined in the EV Guidelines, as formally ratified by the CA/Browser forum in 2007, that specify all the steps required for a CA before issuing a certificate, and includes:

- Verifying the legal, physical and operational existence of the entity

- Verifying that the identity of the entity matches official records

- Verifying that the entity has exclusive right to use the domain specified in the EV SSL Certificate

- Verifying that the entity has properly authorized the issuance of the

EV SSL Certificate

EV SSL Certificates are available for all types of businesses, including government entities and both incorporated and unincorporated businesses. A second set of guidelines, the EV Audit Guidelines, specify the criteria under which a CA needs to be successfully audited before issuing EV SSL Certificates. The audits are repeated yearly to ensure the integrity of the issuance process.

[Organization Validation (OV)](#) SSL Certificates: where the CA checks the right of the applicant to use a specific domain name PLUS it conducts some vetting of the organization. Additional vetted company information is displayed to customers when clicking on the [Secure Site Seal](#), giving enhanced visibility in who is behind the site and associated enhanced trust.

[Domain Validation (DV) SSL Certificates](#): where the CA checks the right of the applicant to use a specific domain name. No company identity information is vetted and no information is displayed other than encryption information within the Secure Site Seal.

GlobalSign – a simplified range of flexible SSL Certificates

GlobalSign is the first SSL Provider to offer a simplified range of SSL Certificates – fitting neatly into the three newly defined SSL classes of Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). By taking its 15 years of experience in delivering trusted SSL solutions, GlobalSign has pioneered a simple approach to the three classes of SSL the market has seen emerge over recent years.

Other SSL Providers favor using complex product naming and classifications, with basic features being used to differentiate otherwise identical products. GlobalSign bucks this trend by adopting simple product

naming and assigning feature sets as options within each product class. This approach is designed to eliminate the time consuming and frustrating "which Certificate do I need" issues faced by customers evaluating SSL vendor solutions.

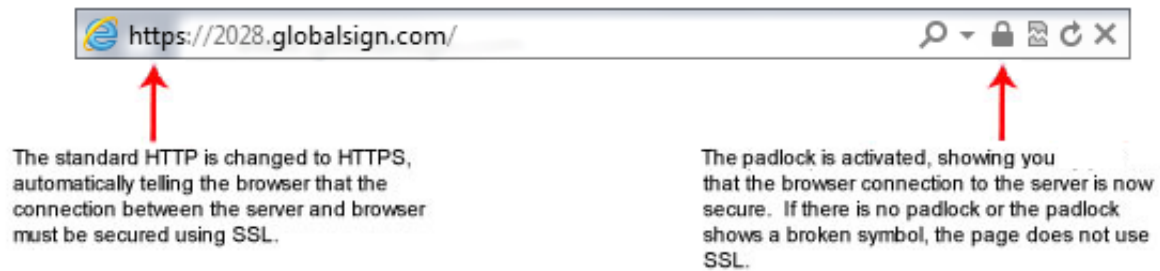The simplified classification of GlobalSign SSL consists of:

1. Extended Validation: GlobalSign ExtendedSSL

The latest, and possibly most significant, advancement in SSL technology since its initial inception follows the standardized Extended Validation guidelines. New high security browsers such as Microsoft Internet Explorer 7+, Opera 9.5+, Firefox 3+, Google Chrome, Apple Safari 3.2+ and iPhone Safari 3.0+ identify ExtendedSSL Certificates as EV Certificates and activate the browser interface security enhancements, such as the Green Bar. For customers who wish to assert the highest levels of authenticity, ExtendedSSL is the ideal solution.
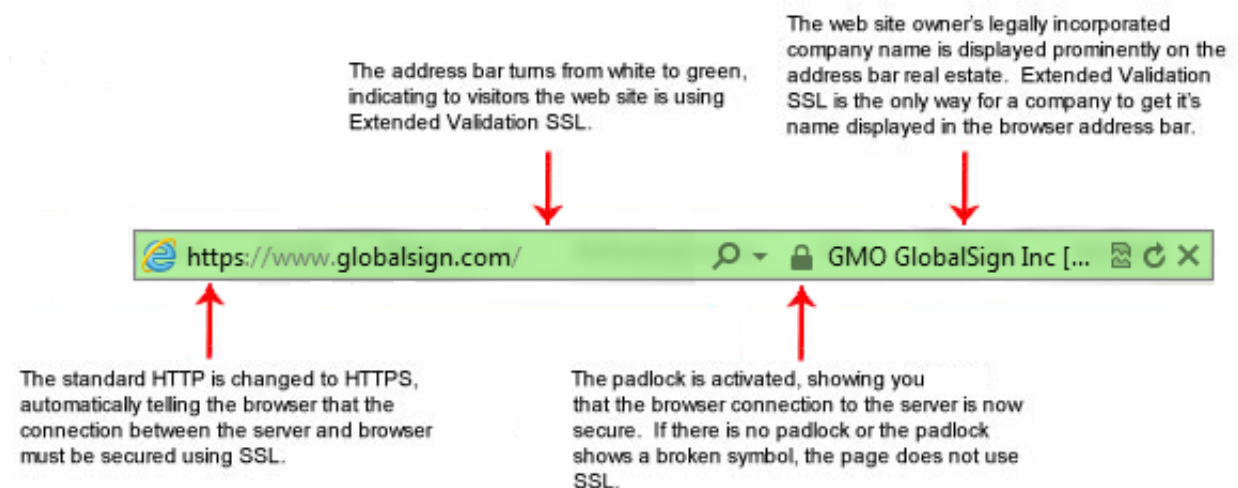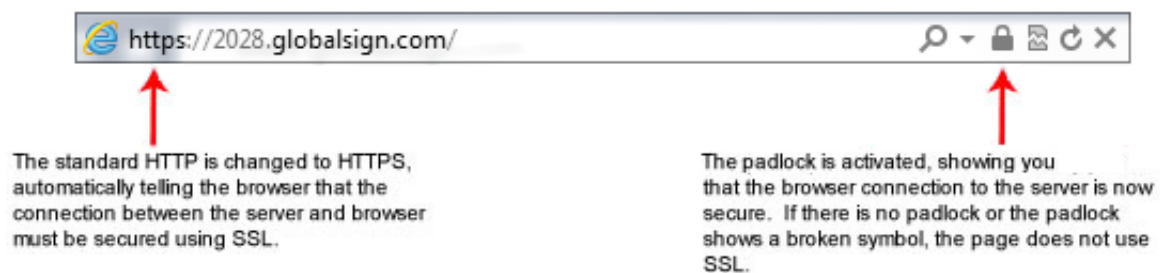

2. Organization Validation: GlobalSign OrganizationSSL

GlobalSign has been issuing organization validation Certificates for 15 years. Companies applying for OrganizationSSL have their company details vetted before issuance.

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

3. Domain Validation: GlobalSign DomainSSL

DomainSSL Certificates are fully supported and share the same browser recognition with OrganizationSSL, but come with the advantage of being issued almost immediately and without the need to submit company paperwork. This makes DomainSSL ideal for businesses needing a low cost SSL quickly and without the effort of submitting company documents.

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

Multi-Domain & Wildcard SSL

Secure multiple domains and
sub domains on the same server with a single SSL Certificate &
single IP address with Wildcard and Subject Alternative Names (SANs).

Learn More

Not sure which type of certificate is right for you? Compare SSL Certificates and Pricing

SSL Certificate Reviews

Quick renewals

I appreciate how quick the renewal process is.

Stan Swiercz

,

01/17/2017

It's just easy

It's just easy and simple to work with / order from Globalsign.

David Chung

,

01/17/2017

More Reviews Add a Review