General Customer Ready Content for SSL

Use for Email, Newsletters, Web & Social Media

General Customer Ready Content for SSL Resellers

What SSL Actually Does for You?

SSL is the acronym for Secure Sockets Layer and is the Internet standard security technology used to establish an encrypted (or safe) link between a web server (website) and your browser (i.e. Internet Explorer, Chrome, Firefox, etc…). This secured link ensures that the data/information that is passed from your web browser to the web server remain private; meaning safe from hackers or anyone trying to spy/steal that info. SSL is the industry standard and is used by millions of websites to protect and secure any sensitive or private data that is sent through their website. One of the most common things SSL is used for is protecting a customer during an online transaction.

To establish a secured SSL connection on a web server it requires an SSL Certificate to be properly installed. When completing the process to activate SSL on your web server you will be asked to complete a number of questions to verify the identity of your domain and your company. Once properly completed, your web server will create 2 types of cryptographic keys – one is called a *Private Key* and the other is called the *Public Key*.

The Public Key isn't a secret and it's placed into something called a *Certificate Signing Request* or most commonly referred to as the CSR. The CSR is a file that contains all the data of your details. Once this CSR is generated, you can begin the SSL application process. During this process, the Certification Authority (CA) will go through the validation process to verify your submitted details and then once verified will issue an SSL Certificate with your details and allow you to use SSL. Your web server will automatically match the CA issued SSL Certificate to your Private Key. This means you are now ready to establish an encrypted and secure link between your website and your customer's web browser.

SSL protocol is complex, but the complexities always remain invisible to your customers. Instead the browser they are using provides them with a key indicator letting them know that their session is currently protected by an SSL encryption – sometimes it is the lock icon in the lower right-hand corner, or the addition of an "s" in https rather than just http, on high-end SSL Certificates, a key indicator is the green bar in the browser. Clicking on the indicators will display all the details about it. All trusted Certification Authorities issue SSL Certificates to either legit companies or legally accountable individuals.

Generally speaking, SSL Certificates include and display (at least one or all) your domain name, your company name, your address, your city, your state and your country. It also always has an expiration date of that particular certificate and of course the details of the Certification Authority responsible for issuing the certificate. Browser connect to a secured site and then retrieves the site's SSL Certificate and first makes sure that it has not expired, then it checks to see if it was issued by a known Certification Authority that the browser trusts, and then that it is actually being used by the website that is was actually issued to. If any one of these parameters does not check out properly, the browser will display a warning to the user to let them know that this site is not secure by SSL. It says to leave or proceed with extreme caution. That is the last thing you would want to say to your potential customer. That is why SSL is of high importance to any successful company doing business on the web.

Are All SSL Certificates the Same?

The number of businesses that use SSL have increased tremendously over the past few years and the reasons for which SSL is used has also increased, for example:

- Some businesses need SSL to simply provide confidentiality (i.e. encryption)
- Some businesses like to use SSL to add more trust or confidence in security and identity (they want you to know that they are a legitimate company and can prove it)

As the reasons companies use for SSL have become wider, three different types of SSL Certificates have been established:

- **Extended Validation (EV) SSL Certificates**
- **Organization Validation (OV) SSL Certificates**
- **Domain Validation (DV) SSL Certificates**

Extended Validation (EV) SSL Certificates are issued only when a Certification Authority (CA) checks to make sure that the applicant actually has the right to the specific domain name **plus** the CA conducts a very THOROUGH vetting (investigation) of the organization. The issuance process of EV Certificates is standardized and is strictly outlined in the EV Guidelines, which was created at the CA/Browser Forum in 2007, specifies the required steps that a CA must do before issuing an EV certificate:

1. **Must verify the legal, physical & operational existence of the entity**
2. **Must verify that the identity of the entity matches official records**
3. **Must verify that the entity has the exclusive right to use the domain specified in the EV Certificate**
4. **Must verify that the entity has properly authorized the issuance of the EV Certificate**

EV Certificates are used for all types of businesses, including government entities and both incorporated & unincorporated businesses. Takes about 10 days to issue.

A second set of guidelines are for the actual CA and it establishes the criteria to which a CA needs to be audited before being allowed to issue an EV Certificate. It is called, the EV Audit Guidelines, and they are always done every year to ensure the integrity of the issuance process.

Organization Validation (OV) SSL Certificates are issued only when a Certification Authority (CA) checks to make sure that the applicant actually has the right to the specific domain name **plus** the CA does some vetting (investigation) of the said organization. This additional vetted company info is displayed to customers when the Secure Site Seal is clicked on, this gives enhanced visibility to who is behind the site which in turn gives enhanced trust in the site. Takes about 2 days to issue.

Domain Validation (DV) SSL Certificates are issued when the CA checks to make sure that the applicant actually has the right to the specific domain name. No company identity information is vetted and no information is displayed other than encryption information within the Secure Site Seal. DV certs can be issued immediately.