Understanding SSL Certificates and Certificate Validation Levels

Most people realize that SSL is something that helps users stay secure while they're online. However, not everyone realizes what this certificate actually does, or the differences between types of certificates. This article explains the different kinds of SSL certificates and the certificate validation levels.

What is a Certificate For, And Do I Need One?

In short? Absolutely. SSL certificates are used to provide a secure, encrypted connection for visitors to your domain. Because certificates are only issued to the owners of a domain, or to their authorized representatives, they also allow visitors to be confidant that their connection has been secured by the domain they are visiting rather than someone impersonating them so long as they correctly enter the web address for their intended domain. Browser manufacturers have taken great pains to ensure that trusted certificate authorities are able to issue valid certificates, making it necessary to purchase a certificate rather than generating one yourself. A certificate also effects search rankings.

Lastly, browser manufacturers have begun making sites that are not secured by a certificate as 'insecure', which has a significant impact on visitor confidence.

The Different Kinds of SSL Certificate Types

SSL Certificates come in a few different types, and the certificate you choose will be dependent on what you need to provide SSL encryption for.

- Single-Site Certificate - These certificates are intended for when you have only a handful of domains you need to secure. A single-site certificate will cost significantly less than a similar certificate of one of the other types, but only covers one domain, so for example, www.example.com, or mail.example.com, but not both. The exception to this is that most brands will include coverage for the root of a domain if you purchase a certificate for the www subdomain, so for example, a certificate purchased for www.example.com will also provide protection for example.com.

- Wildcard Certificate - A Wildcard certificate provides protection for all subdomains at a single root domain, so for example, a Wildcard certificate purchased for *.example.com would provide protection for mail.example.com, www.example.com, blog.example.com, and any other similar addresses. Wildcard certificates are more costly than a Single-Site certificate, so this option is best when you either have several subdomains that need to be secured.

- Multi-Domain (SAN/UCC) Certificate - A Multi-Domain certificate secures multiple different domains. These certificates are best for situations where you are hosting several different domains in a single location, or when you want to manage all of your domains with only one certificate. For example, a Multi-Domain certificate could be used to secure www.site.com, www.example.com, mail.page.net, and shop.example.org. These certificates usually come with three domains by default, and additional domains must be added to the certificate for additional costs, so consider this when comparing with pricing for the other options. Note that unlike the Single-Site certificate, a Multi-Domain certificate will not provide encryption for the root of a domain unless you explicitly include it, so to get www.example.com and example.com, you must include that as a covered domain.

The Different Kinds of SSL Validation

There are three different kinds of SSL certificate validation classifications, each kind corresponds to how thoroughly the SSL certificate vendor - for example GeoTrust, Thawte, Comodo, Symantec, etc - has validated the request is coming from the owner, or an authorized agent of the owner, of the site before issuing the SSL to whomever is purchasing it.

The job of the SSL provider is to make sure that SSL's are only granted to people who own the site that the SSL is being purchased for, rather than someone else who may be trying to impersonate the site. The amount at which an SSL vendor validates the site and its owner is broken down into the following three levels:

- Domain Validation (DV) - For a DV SSL, the only thing that's checked is that the person requesting the SSL certificate has control over the domain that the SSL is being issued to. This validation is done by sending a confirmation email to a specific address, or by checking for the presence of a specific file on the website. The entire process is almost always fully automated.

- Organization Validated (OV) - For OV SSL, an actual human almost always checks your business records with those from a reliable source, like state or other government records. During the order process, you will be asked for things like your business tax ID number or other official documents so that they can be verified.

- Extended Validation (EV) - EV SSL are the most stringently checked SSL certificates that we have currently. Not only are your government records checked, but other aspects of your business are also verified.