SSL is an encryption protocol that has become an important aspect of website security to provide secure exchange of information. The term stands for Secure Sockets Layer and is used to transfer data or use it for storage. The use of SSL has become mandatory for the security of websites. Moreover, Google considers SSL certificates as an important ranking factor in search results.

**What are SSL Certificates?**

A lot of online portals require the user to enter personal information which is submitted to the author. Before this information reaches the concerned personnel, it can be intercepted by a hacker. An attack of this type is known as a man-in-the-middle attack. Companies that are storing sensitive customer information such as bank details, their address, etc. should have SSL certificates to ensure the safety of their customer's data. Moreover, website owners who are distributing codes or other content should use [code signing certificates](http://codesigningstore.com/)to authenticate their data and make online data exchanges more secure.

**How do SSL Certificates Secure Your Website?**

Let’s try to understand SSL in terms of URLs - have you noticed that some URLs begin with http:// while others begin with https://? The extra ‘s’ is what SSL stands for and is the magic key to maintaining security on your site. Technically speaking, SSL certificates are data files that are placed to establish a link between the server and the browser. This link ensures that all data exchanged remains private.

So, how exactly does SSL make a website more secure? On a website that is encrypted through an SSL certificate, the first thing your browser does is form a secure connection with the server. The connection ensures that only the website owner and the user can access the information that is being typed. This connection happens almost immediately after you visit a website that has SSL.

**SSL Certificates and their Level of Encryption**

The different types of SSL certificates are classified according to the level of encryption they provide or based on the number of domains that are registered under the SSL certificate. Below is a list of different SSL certificates that are found.

1. **Domain Validation (DV) Certificate**

This certificate is probably the cheapest kind of SSL certificate. Unsurprisingly, the kind of encryption it provides is also a low level. If you are running your blog or a website that does not require the user to fill out private information then this is the SSL certificate that you need to apply for. The validation process is also quite simple and only requires a few hours at most.

1. **Organization Validation (OV) Certificate**

If you find DV certificates too basic then you can go ahead and apply for Organization Validation Certificates. These are mostly for those website owners that require only basic encryption for their customer data. Validation for OV certificates takes longer than DV certificates since they need to be validated by certificate authorities.

1. **Extended Validation (EV) Certificate**

An EV certificate provides high-level encryption. It is one of the most commonly used SSL certifications. Moreover, the process to validate EV is much stricter as compared to DV or OV certificates.

1. **Wildcard SSL certificates**

These certificates fall under the domain and subdomain category. You can use these certificates to encrypt several subdomains under one single domain. This is a cheaper option for those companies that want to purchase several domains.

1. **Single domain SSL certificates**

A single domain SSL certification will help you protect only one domain at one time. Unlike the case in Wildcard certificates, you cannot protect multiple domains under a single-domain SSL certificate.

**The Bottom Line**

Getting an SSL certificate for your website is extremely important from a security point of view. Even if your website is not taking [payment details](http://www.cardzgroup.com/ContactSmartCard.html) – data is still exchanged and is vulnerable to hackers. However, the type of SSL certificate depends on the level of security that your website requires and the number of subdomains that come under your website. Once you have decided which SSL certificate you need for your website you can install it on your server. Other than security, SSL certificates also improve the SEO of your webpage and help improve the ranking on Google SERPs.