As companies are offering more online services, internet security has become a necessity. For better internet security, organizations need to have secure socket layer encryption (SSL encryption) certification to ensure secure transactions of customers. SSL certificates contain encrypted connections to build trust between users and the company. Trust is one of the foremost vital things for online businesses. When customers feel safe and secure about internet security and online transactions, they also show their loyalty to the company. They know that their account information such as credit card and debit card details are not in the wrong hands. SSL encryption certificates create this foundation of trust between customer and organization by building a secure connection.

**How does SSL encryption work?**

SSL encryption certificates have a private key and a public key. Both keys act together to set up an encrypted connection for the site. The certificate contains a subject as well, that is the name of the website or certificate owner. An SSL encrypted certificate verifies the organization’s identity. The browser also lets the customers know that the website is safe, and they can feel safe during browsing and sharing information for online transactions. There are a few steps to get your SSL encryption certificate:

* **Step 1:** We have to make the Certificate Signing Request (CSR) on our server. This step will create a public and a private key of the site. The CSR record sent to the Certificate Specialist (CA) has the public-key. The CSR file sent to the Certificate Authority (CA) contains the public-key. They use that file to match the private key. The private key is never visible to CA for internet security.
* **Step 2:** After we receive the SSL encryption certificate, we install it on our server. Installation steps are different depending on the type of the server. To establish the credibility of the certificate, we need another intermediate certificate.
* **Step 3:** In the Last step, it creates a chain between our server certificate, intermediate certificate, and CA’s root certificate.

Signature of a trusted Certificate Authority is the most important part of SSL encryption certificate. Nowadays, SSL certificate creation has become very common. However, browsers only accept certificates coming from their trusted certificate authorities list. Browsers come with their list of trusted certificate authorities called Trusted Root Certificate Authority store. To become the Certificate Authority, a company must satisfy all the standards created by the browsers. Before applying for an SSL certificate, make sure to verify the CA for internet security.