SSL Offloading:

SSL offloading is the process of removing the SSL based encryption from incoming traffic that a web server receives to reduce its work from decryption of data. SSL traffic is intensive since it requires encryption and decryption of traffic. The processing is offloaded to a separate server designed specifically to perform SSL termination

SSL Self signed certificate:

To establish the required level of trust and eliminate the use of rogue certificates impersonating legitimate companies, SSL certificates need to be signed and validated by a trusted Certificate Authority (CA). A self-signed certificate is one that is not signed by a CA at all – neither private nor public. In this case, the certificate is signed with its own private key, instead of requesting it from a public or a private CA.

Advantages:

- Fast and easy to use
- Flexible
- Useful for test environments

Disadvantages:

- It’s virtually impossible to keep track of self-signed certificates
- Security risks

Third party SSL certificate:

In this, a trusted third party verifies the identification information contained in your SSL certificate, assuring customers that your site is actually your site