Network And Security

Chapter 1 SSL, Security Certificate, HTTS

1.1 SSL

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.To be able to create an SSL connection a web server requires an SSL Certificate.

1.2 SSL Certificate

Step 1: When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

Step2: Then you should apply a SSL certificate from Certification Authority. The Public Key is placed into a Certificate Signing Request (CSR) - a data file also containing your details. You should then submit the CSR.

Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

Step3: When you use your certificate,browsers provide clients with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals.

1.3 Wildcard certificate

There are lots of scams and bad intentions that now take place online. For people who have two or more sub-domains, they must strive to have wild card certificate. It is one of the cheapest and most famous secure certificates that are known for its advantages but one must have sufficient knowledge on how to handle it properly in order for you to reap all of its benefits.

There are different types of SSL or secure socket layer certificates available which you can choose from. The secure certificates types are company validated certificates, shared certificates, domain validated certificates, multi-domain certificates and wildcard certificates. All of these types are deliberately created for security purposes. However, they differ in terms of their functions. One of the best and the cheapest among those types is the wildcard certificate. It is well-known because of its great advantages when it comes to security aside from it less expensive price.

What is wildcard certificate? The wildcard SSL is another type of secure certificates that helps to enable the SSL encryption on your several sub domains with the use of one certificate, unless the domains are still in control by the similar organization and they are sharing same domain second-level name. Like, for example, a wildcard certificate released to SSL Company using the same name like “SSL.com” will be used to keep it secure with the following possible domains such as “login.ssl.com”, “support.ssl.com” or “payment.ssl.com” and more. A wildcard notification consists of asterisk then a period before the chosen domain name. These are wildcards to broaden the SSL encryption to its sub domains. In case of [www.ssl.com](http://www.ssl.com/) as example, the \*.ssl.com will also secure its other sub domains such as “login.ssl.com” and more.

1.4 A formal step to create SSL certificate

This is how SSL.com create SSL certificate for you.

1. You generate the csr (some tools)
2. You summit csr
3. Ssl.com validate your request by letting you reply an email or put some validation file in your domain.
4. You can your certificate from email.
5. You install your certificate on your server.

1.5 Types of SSL certificates

All [SSL certificates](https://www.ssl.com/certificates/) use similar methods to protect and validate your data, a useful way to categorize them is by validation method. Any certificate must be verified by the issuing Certificate Authority (or CA) to ensure that it is covering the correct, authorized site. This verification confirms at a minimum control of the domain. However, more steps can be taken to also confirm the existence of the requesting company or organization (for OV certificates) or to establish even more trust through extended vetting (for EV certificates).

DV: domain validated certificate

OV: Organization validated or OV certificates require more validation than DV certificates, but provide more trust.

EV: Extended validation or EV certificates provide the maximum amount of trust to visitors, and also require the most effort by the CA to validate.

1.6 SSL installation

SSL can be installed in IIS, Zimbra,Exchange, Microsoft Azure/CLOUD web app/web site.

SSL is a security protocol. Protocols describe how algorithms should be used. In this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted. Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

Here is a simple steps cited from godaddy to install the SSL in apache,

#### **To Install SSL and Intermediate Certificates**

1/ Copy your SSL certificate file and the certificate bundle file to your Apache server. You should already have a key file on the server from when you generated your certificate request.

2/ Locate the following directives in either your httpd.conf or ssl.conf file (which files you use depends on how you configured Apache). If one or more of them are currently commented out, uncomment them by removing the # character from the beginning of the line. Set the values of these directives to the absolute path and filename of the appropriate file, based on your version of Apache:

|  |  |
| --- | --- |
| **Apache Version < 2.4.8** | |
| **Directive** | **Path to Enter** |
| SSLCertificateFile | Certificate file path |
| SSLCertificateKeyFile | Key file path |
| SSLCertificateChainFile | Intermediate bundle path |
| **Apache Version 2.4.8+** | |
| **Directive** | **Path to Enter** |
| SSLCertificateFile | Certificate file path |
| SSLCertificateKeyFile | Key file path |
| SSLCACertificatePath | Intermediate bundle path |

3/ Save your configuration file and restart Apache.

4/ Restart your server. The procedure to restart Apache will depend heavily on your OS platform. On Unix-like platforms (Linux, Solaris, HP-UX, etc.) you will typically run a script to stop and restart the httpd daemon. On Windows, you will typically stop and restart the Apache service in the Services administrative console. Please consult your OS vendor's documentation or the [Apache documentation](http://httpd.apache.org/docs/).

Your SSL Certificate is installed. If you have problems, please see [Test your SSL's configuration](https://www.godaddy.com/help/test-your-ssls-configuration-6015) to help diagnose issues.

1.7 Is My Certificate SSL or TLS ?

The SSL protocol has always been used to encrypt and secure transmitted data. Each time a new and more secure version was released, only the version number was altered to reflect the change (e.g., SSLv2.0). However, when the time came to update from SSLv3.0, instead of calling the new version SSLv4.0, it was renamed TLSv1.0. We are currently on TLSv1.2.

1.8 How SSL works

1/ A browser or server attempts to connect to a Website, a.k.a. Web server, secured with SSL. The browser/server requests that the Web server identify itself.

2/ The Web server sends the browser/server a copy of its SSL certificate.

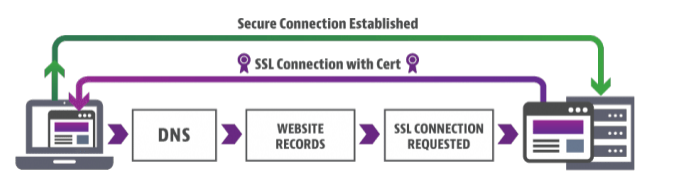
3/ The browser/server checks to see whether or not it trusts the SSL certificate. If so, it sends a message to the Web server.

4/ The Web server sends back a digitally signed acknowledgement to start an SSL encrypted session.

Encrypted data is shared between the browser/server and the Web server.

There are many benefits to using SSL Certificates. Namely, SSL customers:

* Get HTTPs which elicits a stronger Google ranking
* Create safer experiences for your customers
* Build customer trust and improve conversions
* Protect both customer and internal data
* Encrypt browser-to-server and server-to-server communication
* Increase security of your mobile and cloud apps



Chapter 2 OSI and TCP IP