

[< Previous](#)[Next >](#)

Get a Free SSL Certificate

The following Certificate Authorities provide free DV (Domain Validated) certificates.

1. Let's Encrypt
2. Cloudflare

Let's Encrypt

letsencrypt.org is a free, automated and open Certificate Authority operated by Internet Security Research Group (ISRG). The free DV certificates from letsencrypt.org are valid for 90 days and can be renewed easily and recognized by all the major browsers such as Firefox, Chrome and Internet Explorer. Learn how to get a free certificate from Let's Encrypt at [Getting started guide](#).

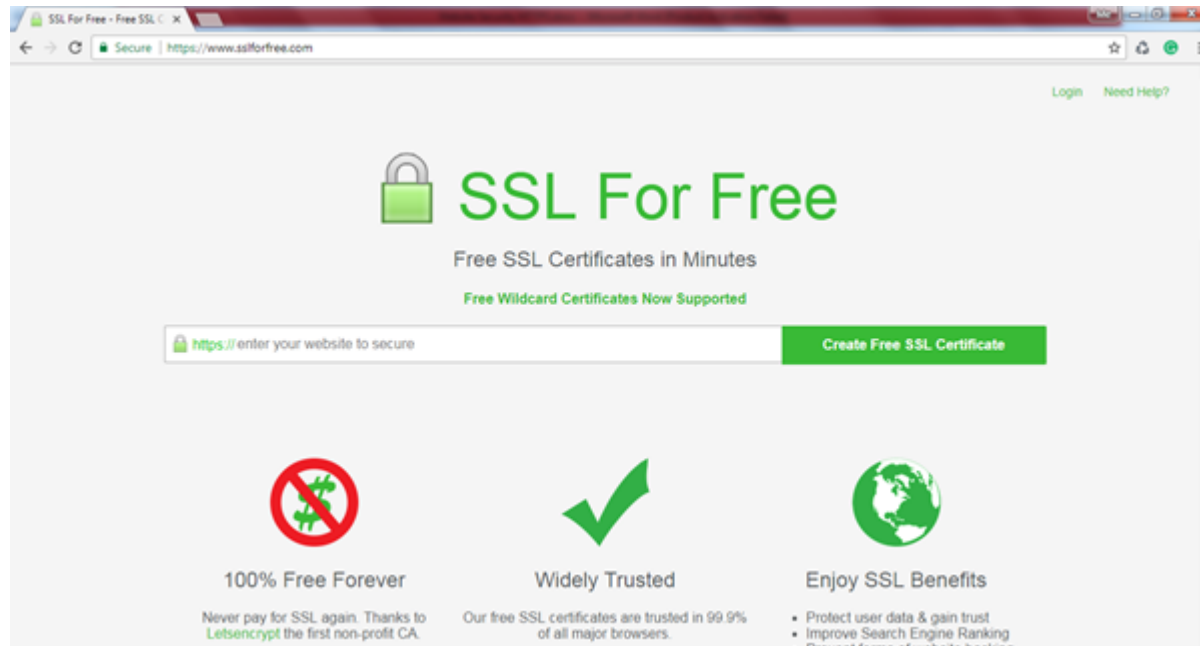
There are many web hosting providers who provide built-in support for the installation of a Let's Encrypt's certificate. Check out the [list of hosting providers who support let's encrypt](#).

If your hosting provider does not support a Let's Encrypt certificate and you find it difficult to get a certificate manually using Certbot, then you can go to sslforfree.com. This website generates a free certificate using Let's Encrypt's ACME server by using domain validation. It is 100% safe to get a free certificate from sslforfree.com. Let's

see how to get a free SSL certificate from [sslforfree.com](https://www.sslforfree.com).

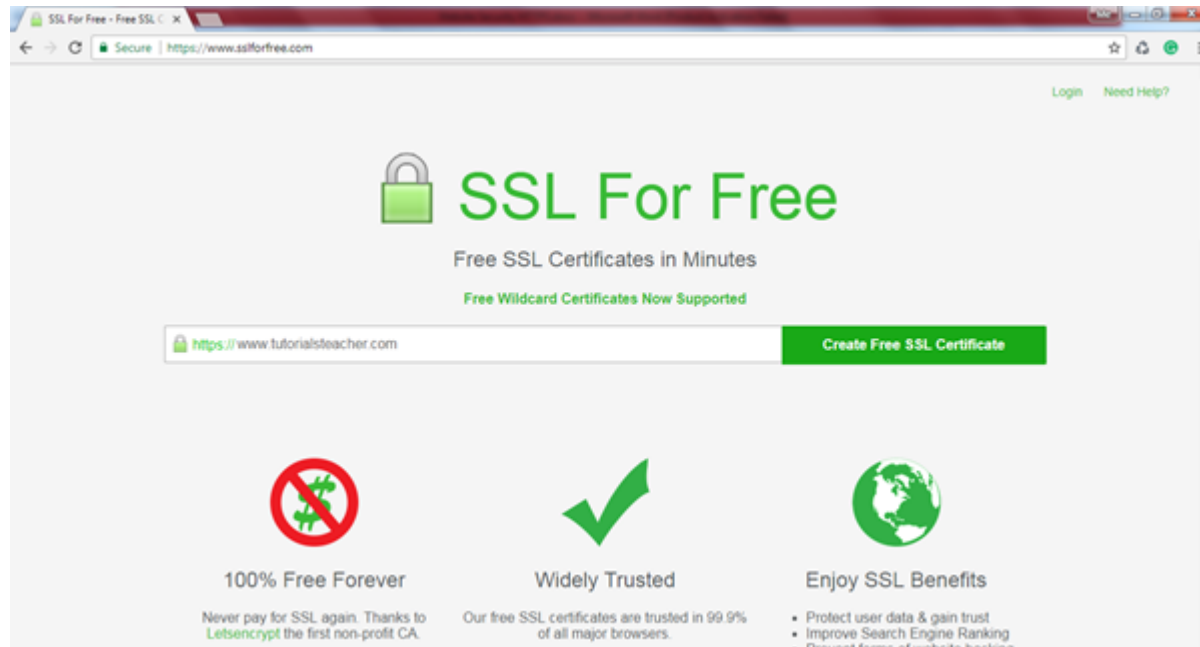
Create a Certificate on [sslforfree.com](https://www.sslforfree.com)

Open <https://www.sslforfree.com> in Google Chrome browser. It will display the web page as below.



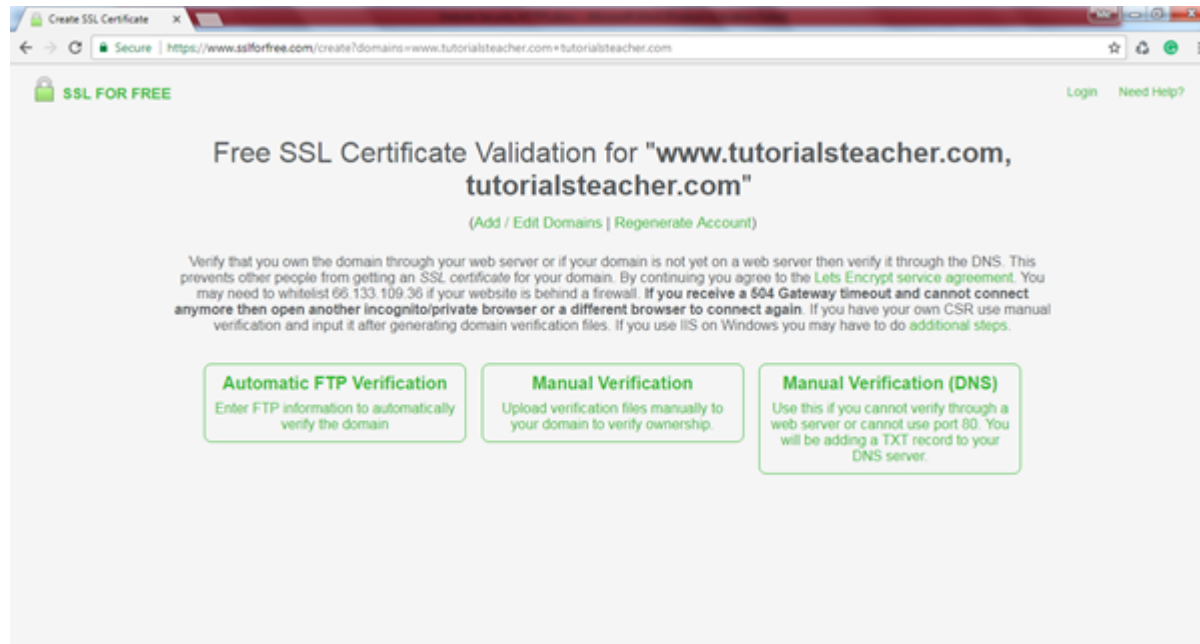
Get a Free SSL Certificate from [sslforfree.com](https://www.sslforfree.com)

In the text box, enter the fully qualified domain name of your website e.g. www.tutorialsteacher.com.



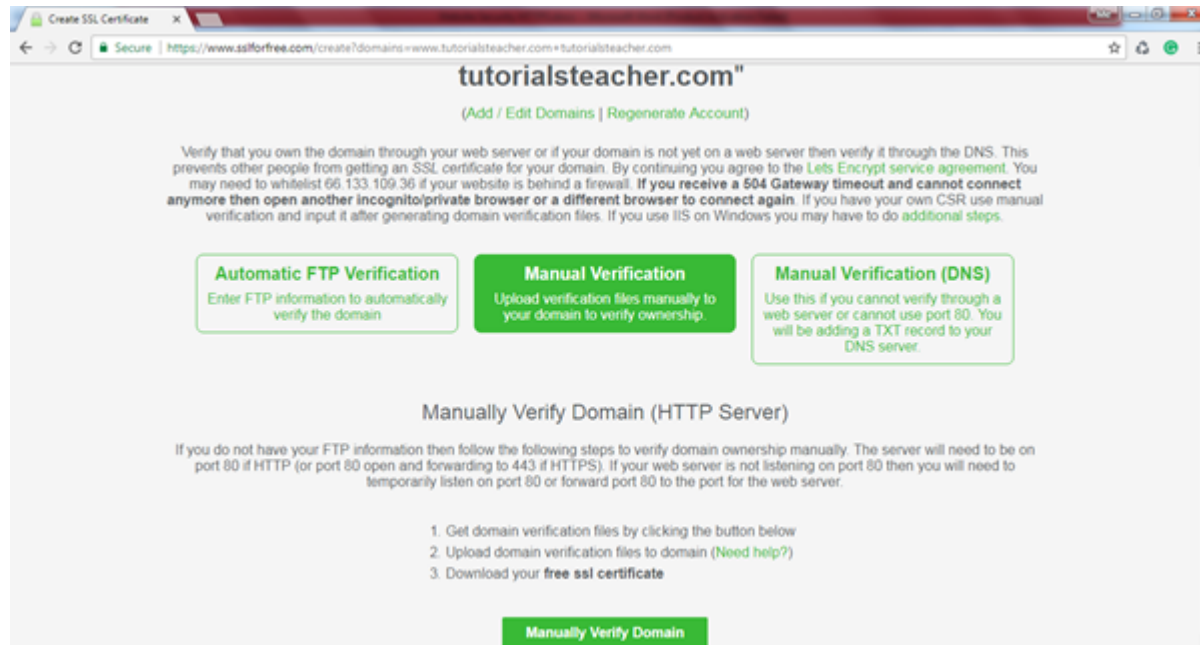
Enter Website Name

Click on the **Create Free SSL Certificate** button. This will go to the validation page where you need to verify that you control the specified domain, as shown below.



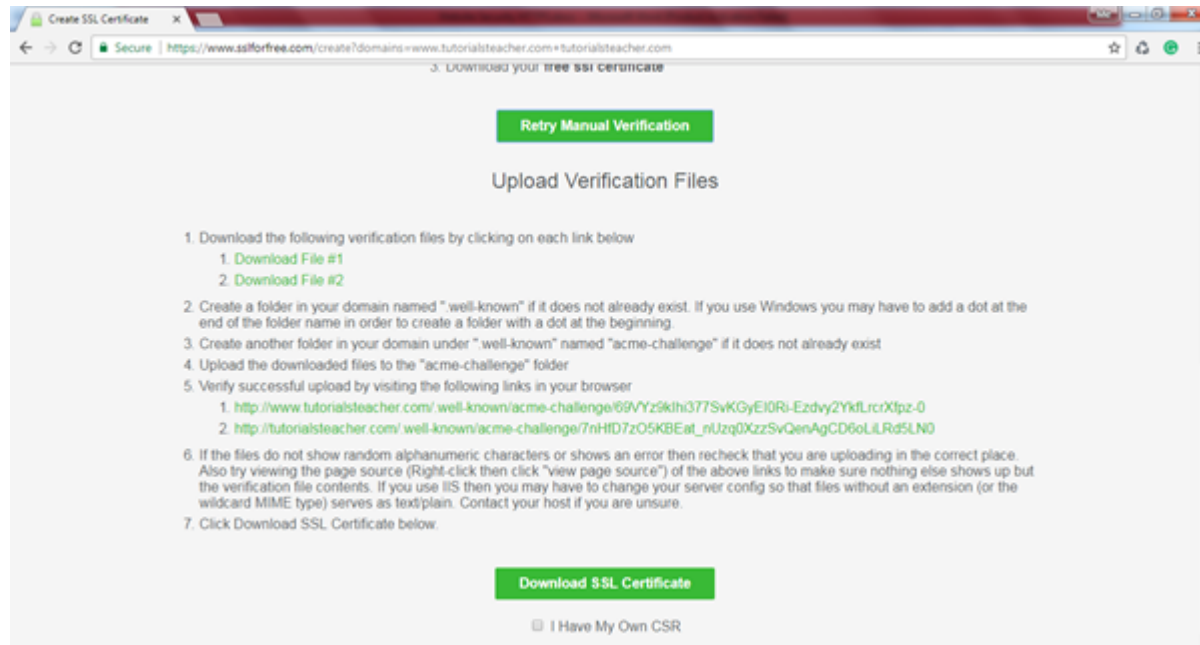
Select Verification Method

Your domain can be validated in three ways: Automatic FTP Verification, Manual Verification by uploading verification file to your domain or Manual Verification by adding TXT records to your DNS server. Select a feasible method to validate your domain. For example, select the Manual Verification method where you need to upload verification files, as shown below.



Manual Verification

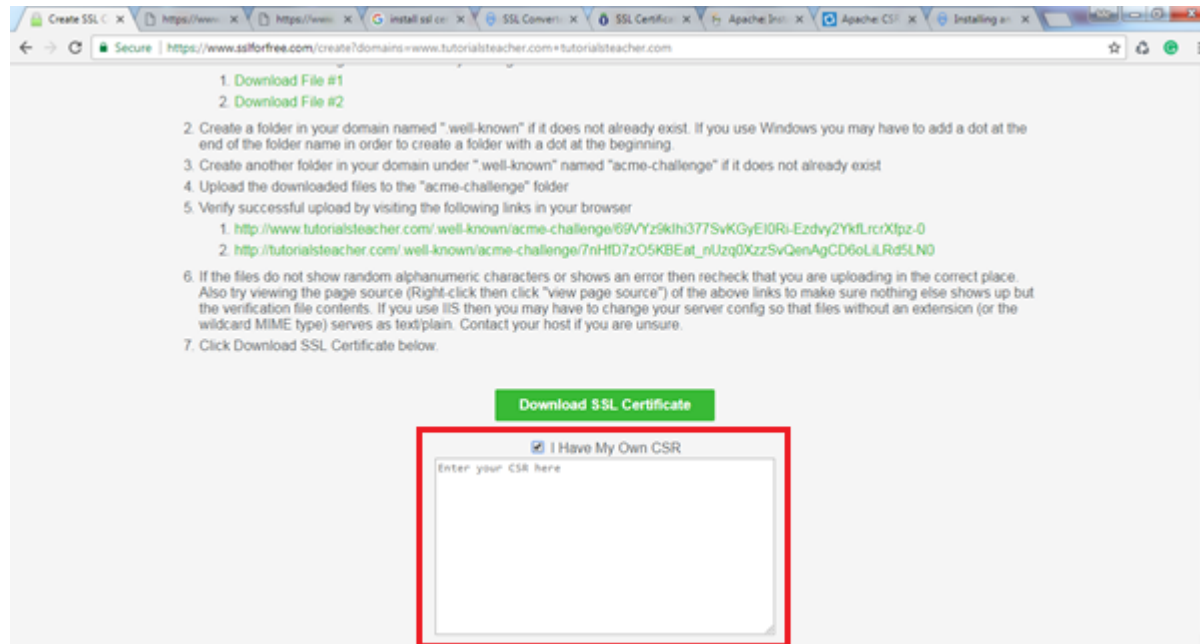
Once you selected the verification method, select the **Manually Verify Domain** button. This will display further information on how to download and upload verification files to your hosting server, as shown below.



Verification

After you successfully completed the verification process listed above, you can download the SSL certificate by clicking on the **Download SSL Certificate** button.

If you have a generated CSR from your web server, then select the **I Have My Own CSR** checkbox. This will display a textbox to copy and paste your CSR and then click on **Download SSL Certificate** button.



1. Download File #1
2. Download File #2

3. Create a folder in your domain named "well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning

4. Create another folder in your domain under "well-known" named "acme-challenge" if it does not already exist

5. Upload the downloaded files to the "acme-challenge" folder

6. Verify successful upload by visiting the following links in your browser

1. <http://www.tutorialsteacher.com/well-known/acme-challenge/69VYz5kth377SvKGyE10Ri-Ezdvy2YkLrcrXtpz-0>
2. http://tutorialsteacher.com/well-known/acme-challenge/7nHID7zO5KBEat_nUzq0XzzSvQenAgCD6oLILRd5LND

7. Click Download SSL Certificate below.

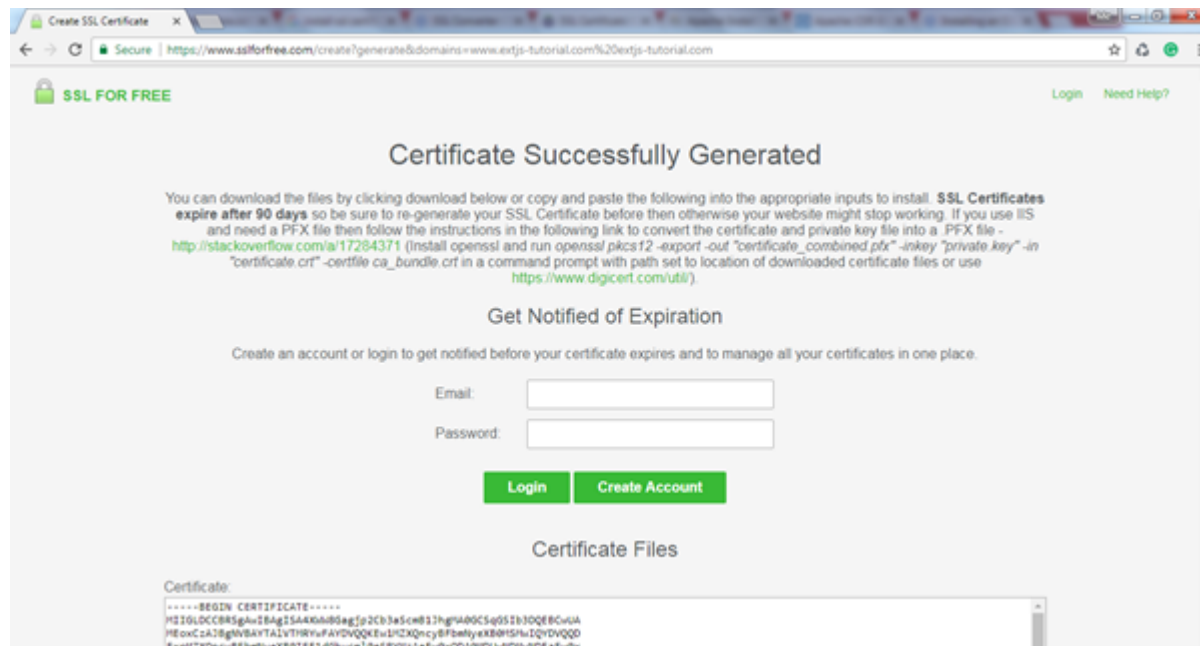
Download SSL Certificate

☒ I Have My Own CSR

Enter your CSR here

Enter CSR

This will generate the certificates and display the page shown below.



SSL FOR FREE Login Need Help?

Certificate Successfully Generated

You can download the files by clicking download below or copy and paste the following into the appropriate inputs to install **SSL Certificates** **expire after 90 days** so be sure to re-generate your SSL Certificate before then otherwise your website might stop working. If you use IIS and need a PFX file then follow the instructions in the following link to convert the certificate and private key file into a PFX file - <http://stackoverflow.com/a/17284371> (install openssl and run `openssl pkcs12 -export -out "certificate_combined.pfx" -inkey "private.key" -in "certificate.crt" -certfile ca_bundle.crt` in a command prompt with path set to location of downloaded certificate files or use <https://www.digicert.com/util/>).

Get Notified of Expiration

Create an account or login to get notified before your certificate expires and to manage all your certificates in one place.

Email:

Password:

Login **Create Account**

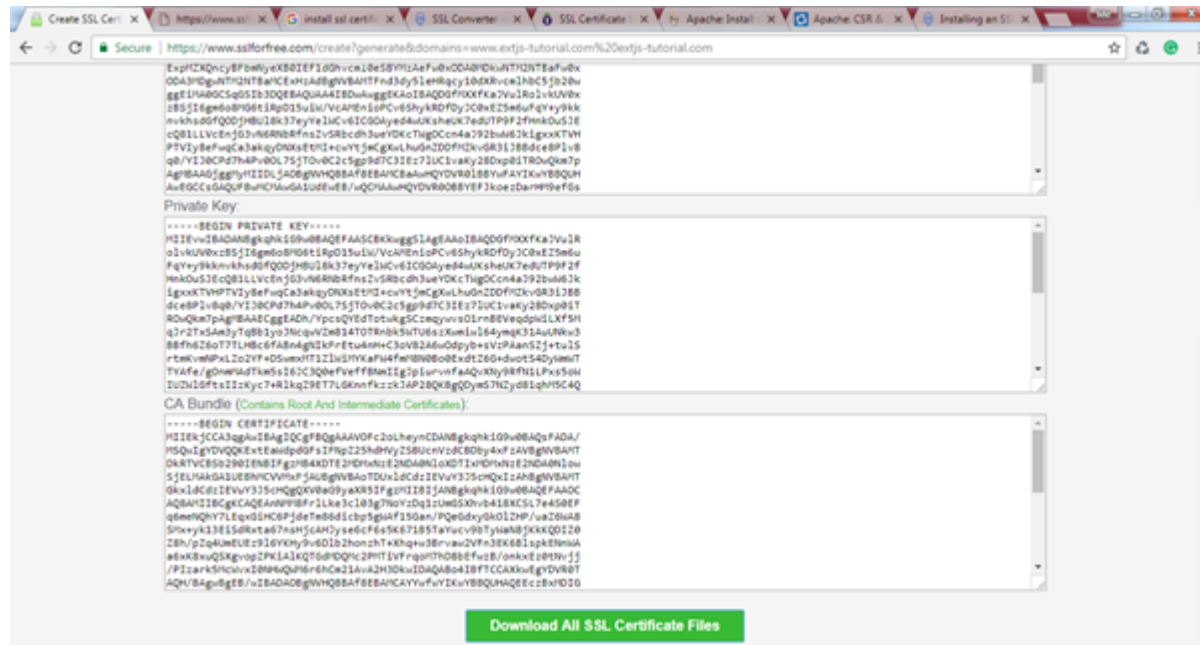
Certificate Files

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDCCBRGAwIBAgISAAKAAQAgMjE2b3A5cml81h9V40CSq052b3Q08CvUA
HEoxCzA3BglvbkYALVTRVYvPAYDVQ0EeU1h2XQncyBfbeflyeXB05b3Q0VQ0Q
Exo1Ck0ncvBfbeflyeXB05b3Q0VQ0EeU1h2XQncyBfbeflyeXB05b3Q0VQ0Q
-----END CERTIFICATE-----
```

SSL Certificates




Scroll down to see your certificate, private key and CA bundle (root and intermediate certificates), as shown below.



Certificate, Private Key & CA Bundle


Click on the **Download All SSL Certificate Files** button to download a zip file which contains all the certificates.

Unzip sslforfree.zip and you will see the following three files:

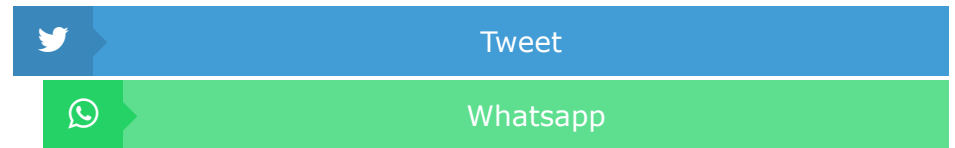
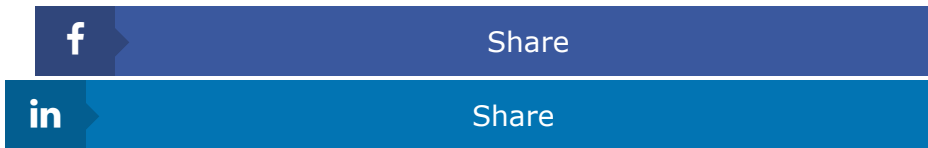
Name	Type	Size
 ca_bundle.crt	Security Certificate	2 KB
 certificate.crt	Security Certificate	3 KB
 private.key	KEY File	2 KB

Certificate Files

As you can see above, your certificate and intermediate certificate are issued in .crt files and the private key in a .key file.

Once you get your certificate, you need to install it on your web server. The installation of an SSL certificate on the web server depends on the OS and the web server you are using. Before the installation, you need to understand the [certificate formats and file extensions](#) .

Learn how to buy an SSL certificate in the next chapter.



[< Previous](#)[Next >](#)

TutorialsTeacher.com is optimized for learning web technologies step by step. Examples might be simplified to improve reading and basic understanding. While using this site, you agree to have read and accepted our terms of use and [privacy policy](#).

✉ feedback@tutorialsteacher.com

TUTORIALS

- > [ASP.NET Core](#)
- > [ASP.NET MVC](#)
- > [IoC](#)
- > [Web API](#)
- > [C#](#)
- > [LINQ](#)
- > [Entity Framework](#)
- > [AngularJS 1](#)
- > [Node.js](#)
- > [D3.js](#)
- > [JavaScript](#)
- > [jQuery](#)
- > [Sass](#)
- > [Https](#)

E-MAIL LIST

Subscribe to TutorialsTeacher email list and get latest updates, tips & tricks on C#, .Net, JavaScript, jQuery, AngularJS, Node.js to your inbox.

We respect your privacy.

[HOME](#) [PRIVACY POLICY](#) [TERMS OF USE](#) [ADVERTISE WITH US](#)

© 2020 TutorialTeacher.com. All Rights Reserved.