1 FAQ

**General SSL Knowledge**

#### [What is SSL?](javascript:;)

SSL, which stands for Secure Sockets Layer, is a cyber-security protocol that digitally encrypts information sent from a browser to a server. SSL certificates are used to [**protect sensitive information**](https://www.thesslstore.com/products/ssl.aspx) like credit card numbers, usernames, passwords, email addresses, and more. A website with an SSL certificate is identified using a number of trust indicators, like "https" and the padlock icon in the browser bar, a site seal from a reputable Certificate Authority (CA), and a green bar that wraps around the URL on more premium certificates.

#### [What is a Domain Validated (DV) SSL Certificate?](javascript:;)

A Domain Validated (DV) SSL certificate is a [**quick and easy way to secure a domain**](https://www.thesslstore.com/products/cheap-ssl-certificates.aspx), as the Certificate Authority (CA) issuing the certificate only requires verification that the recipient actually owns the domain they wish to cover. This verification process can typically be completed in a matter of minutes. However, these certificates offer little in the way of SSL recognition, so they are recommended for websites where visitor trust is not of high importance and information like usernames, passwords, or credit card information is not required.

#### [What is an Organization Validated (OV) SSL Certificate?](javascript:;)

An Organization Validated (OV) SSL certificate requires that a business complete a light vetting process by the Certificate Authority before being issued. These certificates are a nice middle-ground between DV and EV certificates, as they aren't as expensive as EV options but still offer more SSL and trust indications than basic [**between DV and EV certificates**](https://www.thesslstore.com/products/high-assurance-certificates.aspx). These certificates typically take between 2-3 days to be issued.

#### [What is an Extended Validation (EV) SSL Certificate?](javascript:;)

EV stands for Extended Validation and is the most premium type of SSL certificate available. These certificates are identified on websites mainly by the [**green address bar**](https://www.thesslstore.com/extended-validation-ssl-certificates.aspx), the most universally recognized symbol of trust on the web. EV certificates are becoming more and more commonplace in the industry, especially amongst ecommerce sites, as they are used by some of the most trusted sites in the world like Bank of America, Twitter, Paypal, and more. These certificates require that a company complete a thorough vetting process before being issued.

#### [How can I get a Green Address Bar for my website?](javascript:;)

The only way to get the green address bar on your website is with an [**Extended Validation (EV) certificate**](https://www.thesslstore.com/extended-validation-ssl-certificates.aspx). These are the only type of SSL certificate that come with the green address bar.

#### [Can I qualify for an EV certificate?](javascript:;)

The main criteria for qualifier for an EV certificate would be that your business is an official company registered with a [**government authority**](https://www.thesslstore.com/ev/making-ev-application-fast-and-easy.aspx). Also, if you're a Sole Proprietor or a Partnership registered in the U.K., you cannot qualify for any EV SSL certificate.

#### [What certificates offer www and non-www coverage?](javascript:;)

[**All major SSL Brands**](https://www.thesslstore.com/brands.aspx) like GeoTrust, RapidSSL, Symantec, Thawte & Comodo offers coverage for www and non-www on single-domain certificates. However, multi-domain certificates may require each domain that you need to secure to be included as an additional domain and will not automatically cover any domain name. Please contact our support team if you need any help picking the best certificate for your needs!

#### [What is a Wildcard SSL certificate?](javascript:;)

Wildcard SSL certificates can cover one main domain name (www.domain.com) and an [**unlimited amount of subdomains**](https://www.thesslstore.com/wildcardssl-certificates.aspx) (mail.domain.com, login.domain.com, test.domain.com, etc.).

#### [What is a Multi-domain or SAN certificate?](javascript:;)

Multi-domain or SAN (Secure Alternate Name) SSL certificates can cover [**multiple domain names on just one certificate**](https://www.thesslstore.com/san-ssl-certificates.aspx). For example, Symantec and Thawte multi-domain certificates can cover up to 250 domains, whereas Comodo certificates can cover up to 250 domains with just a single SSL certificate. GeoTrust multi-domain certificates can cover anywhere from 25 to 250 domains, depending on the type of certificate you order.

#### [What is the difference between Wildcard and SAN/Multi-Domain functionality?](javascript:;)

Wildcard SSL certificates can cover one main domain (www.domain.com) and an [**unlimited amount of subdomains**](https://www.thesslstore.com/wildcardssl-certificates.aspx) (mail.domain.com, login.domain.com, test.domain.com, etc.). Multi-domain (SAN) SSL certificates can cover [**multiple domains on just one certificate**](https://www.thesslstore.com/san-ssl-certificates.aspx). For example, Symantec and Thawte multi-domain certificates can cover up to 250 domains, whereas Comodo certificates can cover up to 250 domains with just a single SSL certificate. GeoTrust multi-domain certificates can cover anywhere from 25 to 250 domains, depending on the type of certificate you order.

#### [How can I use 256-bit encryption?](javascript:;)

256-bit encryption is a server configuration. This has nothing to do with the certificate itself, it is based on your server configuration. To learn this, you should seek information provided by your webhosting platform or operating system. They will inform you how to set this encryption strength up.

#### [What is the difference between 1024- and 2048-bit key lengths?](javascript:;)

These key lengths refer to the strength of the private key. You can think of it as the size of the cypher being used to encode your messages. Obviously, 2048-bit private keys are exponentially more secure than 1024-bit ones and are the new standard across the industry and are required during the generation process.

#### [What is the difference between SHA-1 and SHA-2?](javascript:;)

SHA stands for [**Signature Hashing Algorithm**](https://www.thesslstore.com/sha/sha-2-google-next-steps.aspx). It's a mathematical hash that proves the authenticity of the certificate. SHA-1 is an older version of the algorithm that is no longer seen as secure by industry experts and major browsers and is not allowed to be used during the generation process any longer by the industry. SHA-2 is the latest version that is widely accepted and viewed as secure by all major browsers and industry experts. The hashing algorithm of your CSR has no relevance to what hashing algorithm is used on the certificate.

#### [I'm a Sole Proprietor, can I still qualify for an OV/EV certificate?](javascript:;)

Sole Proprietors outside of the U.K. can qualify for both OV and EV certificates. However, Sole Proprietors located in the United Kingdom or UK Partnerships cannot qualify for EV certificates, but are eligible for OV certificates, with additional documentation required.

#### [What is a Certificate Authority and what is your relationship to them?](javascript:;)

A Certificate Authority (CA) is the company that actually issues the SSL certificates. Symantec, Thawte, GeoTrust, RapidSSL, and Comodo are all CAs, for example. We are a reseller of these CAs, meaning that we are able to offer the exact same certificate that you would get from buying direct, but at much lower prices. We are hooked up to the API of these CAs, which is how we are able to offer the exact same products. Because we buy in bulk, we are able to offer them at the significant discounts that you see. We also offer dedicated SSL support for every certificate we offer and can help walk you through the entire process, from purchasing to generation to issuance to installation and more.

#### [Which SSL brands are most trusted & secure?](javascript:;)

All of the Certificate Authorities (CAs) that we carry are leaders in the industry and trusted across the world. Symantec is the [**largest CA in the world**](https://www.thesslstore.com/symantec/the-number-one-brand.aspx), and their Norton Trust Seal is the most recognized symbol of trust across the web. Their name definitely adds the most value of any CA in the industry. Additionally, GeoTrust, Thawte, RapidSSL, and Comodo are all trusted and secure CAs.

#### [Can I see which Certification Authorities have their own Trusted CA root present in browsers?](javascript:;)

Yes, the brands that we provide all have their roots included in modern devices and browsers. They all feature 99% or better compatibility, or browser ubiquity.

#### [What is the SSL certificate warranty?](javascript:;)

An SSL certificate warranty covers any damages that you may incur as a result of a data breach or hack that was caused due to a flaw in the certificate. The warranties range in value, which means that the higher value certificates come with more extensive warranties.

#### [What is browser ubiquity or browser recognition?](javascript:;)

Browser ubiquity or browser recognition basically means how many browsers recognize an SSL certificate and properly display the trust indicators. So, the higher the browser ubiquity of an SSL certificate, the more browsers that recognize and accept it.

#### [How long are your SSL certificates valid for?](javascript:;)

Our SSL certificates can be valid from anywhere to 1-2 years, depending on the certificate you choose to purchase. Per the Certificate Authority/Browser (CA/B) Forum, the governing body of the SSL industry, EV certificates can only be issued for a maximum of 2 years. DV and OV certificates from Symantec, GeoTrust, Thawte, Comodo, and RapidSSL can be issued for a maximum of 2 years.

#### [What is an Intermediate certificate?](javascript:;)

An intermediate certificate is a file that helps the web browser identify who issued your SSL certificate. It is not required, but it is HIGHLY recommended that you install it along with your server SSL certificate in order to have full compatibility with all browsers and mobile devices.

#### [Where do I get my Intermediate certificate?](javascript:;)

#### [Can I use SSL to cover an internal domain?](javascript:;)

You can use SSL to cover an internal domain if it is an officially registered domain (a publically available FQDN). If the internal domain is not a delegated and registered domain, the certificate will not be issued.

#### [What if I can only use one certificate file?](javascript:;)

If your hosting platform or company tells you that you can only use one certificate file, then you can combine your server certificate with the intermediate file.

#### [What is the difference between 128- and 256-bit security?](javascript:;)

That is the difference between the key lengths used once an SSL connection has been established in the browser. 256-bit security is indeed a bigger key however that does not necessarily mean it is more secure. Experts and research agrees that 128-bit is equally secure for the foreseeable future. The only reason 256-bit security is needed is if it's specifically required by your industry or company policy.

All our certificates have the ability to use either bit-length, which one you use is a matter of server configuration, NOT certificate support.

#### [How many domains can I secure with a Multi-Domain SSL Certificate?](javascript:;)

This largely depends on the type of Multi-Domain SSL certificate that you purchase. Comodo Multi-Domain certificates can cover up to [**250 additional domains**](https://www.thesslstore.com/comodo/comodo-multi-domain-ssl.aspx). Symantec and Thawte certificates can cover up to 25 additional domains. GeoTrust Multi-Domain certificates can cover anywhere between 25-250 additional domains, depending on the certificate.

#### [What is a UC Certificate (UCC)?](javascript:;)

UC stands for [**Unified Communications**](https://www.thesslstore.com/comodo/comodo-ucc-ssl.aspx) and is a newer type of SSL certificate that is designed and primarily used for securing Microsoft Exchange 2007 and Microsoft Office Communications Server 2007 products. The main difference between a UCC SSL and a standard Multi-Domain certificate is that a UCC can secure both internal network names and external domain names as well.