[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@3d311baf80534aab8f4d526fc4e567e3?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**ref**[**https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate**](https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate)

**What is an SSL certificate – Definition and Explanation**



**What is an SSL certificate?**

An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for Secure  Sockets Layer, a security protocol that creates an encrypted link  between a web server and a web browser.

Companies and organizations need to add SSL certificates to their websites to  secure online transactions and keep customer information private and  secure.

In short: SSL keeps  internet connections secure and prevents criminals from reading or  modifying information transferred between two systems. When you see a  padlock icon next to the URL in the address bar, that means SSL protects the website you are visiting.

Since its inception about 25 years ago, there have been several versions of  SSL protocol, all of which at some point ran into security troubles. A  revamped and renamed version followed — TLS (Transport Layer Security),  which is still in use today. However, the initials SSL stuck, so the new version of the protocol is still usually called by the old name.

**How do SSL certificates work?**

SSL works by ensuring that any data transferred between users and websites, or between two systems, remains impossible to read. It uses encryption  algorithms to scramble data in transit, which prevents hackers from  reading it as it is sent over the connection. This data includes  potentially sensitive information such as names, addresses, credit card  numbers, or other financial details.

The process works like this:

1. A browser or server attempts to connect to a website (i.e., a web server) secured with SSL.
2. The browser or server requests that the web server identifies itself.
3. The web server sends the browser or server a copy of its SSL certificate in response.
4. The browser or server checks to see whether it trusts the SSL certificate. If it does, it signals this to the webserver.
5. The web server then returns a digitally signed acknowledgment to start an SSL encrypted session.
6. Encrypted data is shared between the browser or server and the webserver.

This process is sometimes referred to as an "SSL handshake." While it sounds like a lengthy process, it takes place in milliseconds.

When a website is secured by an SSL certificate, the acronym HTTPS (which  stands for HyperText Transfer Protocol Secure) appears in the URL.  Without an SSL certificate, only the letters HTTP – i.e., without the S  for Secure – will appear. A padlock icon will also display in the URL  address bar. This signals trust and provides reassurance to those  visiting the website.

To view an SSL certificate's details, you can click on the padlock symbol  located within the browser bar. Details typically included within SSL  certificates include:

* The domain name that the certificate was issued for
* Which person, organization, or device it was issued to
* Which Certificate Authority issued it
* The Certificate Authority's digital signature
* Associated subdomains
* Issue date of the certificate
* The expiry date of the certificate
* The public key (the private key is not revealed)

**Why you need an SSL certificate**

Websites need SSL certificates to keep user data secure, verify ownership of the website, prevent attackers from creating a fake version of the site,  and convey trust to users.

If a website is asking users to sign in, enter personal details such as  their credit card numbers, or view confidential information such as  health benefits or financial information, then it is essential to keep  the data confidential. SSL certificates help keep online interactions  private and assure users that the website is authentic and safe to share private information with.

More relevant to businesses is the fact that an SSL certificate is required  for an HTTPS web address. HTTPS is the secure form of HTTP, which means  that HTTPS websites have their traffic encrypted by SSL. Most browsers  tag HTTP sites – those without SSL certificates – as "not secure." This  sends a clear signal to users that the site may not be trustworthy –  incentivizing businesses who have not done so to migrate to HTTPS.

An SSL certificate helps to secure information such as:

* Login credentials
* Credit card transactions or bank account information
* Personally identifiable information — such as full name, address, date of birth, or telephone number
* Legal documents and contracts
* Medical records
* Proprietary information

**Types of SSL certificate**

There are different types of SSL certificates with different validation levels. The six main types are:

1. Extended Validation certificates (EV SSL)
2. Organization Validated certificates (OV SSL)
3. Domain Validated certificates (DV SSL)
4. Wildcard SSL certificates
5. Multi-Domain SSL certificates (MDC)
6. Unified Communications Certificates (UCC)

**Extended Validation certificates (EV SSL)**

This is the highest-ranking and most expensive type of SSL certificate. It  tends to be used for high profile websites which collect data and  involve online payments. When installed, this SSL certificate displays  the padlock, HTTPS, name of the business, and the country on the browser address bar. Displaying the website owner's information in the address  bar helps distinguish the site from malicious sites. To set up an EV SSL certificate, the website owner must go through a standardized identity  verification process to confirm they are authorized legally to the  exclusive rights to the domain.

**Organization Validated certificates (OV SSL)**

This version of SSL certificate has a similar assurance similar level to the EV SSL certificate since to obtain one; the website owner needs to  complete a substantial validation process. This type of certificate also displays the website owner's information in the address bar to  distinguish from malicious sites. OV SSL certificates tend to be the  second most expensive (after EV SSLs), and their primary purpose is to  encrypt the user's sensitive information during transactions. Commercial or public-facing websites must install an OV SSL certificate to ensure  that any customer information shared remains confidential.

**Domain Validated certificates (DV SSL)**

The validation process to obtain this SSL certificate type is minimal, and  as a result, Domain Validation SSL certificates provide lower assurance  and minimal encryption. They tend to be used for blogs or informational  websites – i.e., which do not involve data collection or online  payments. This SSL certificate type is one of the least expensive and  quickest to obtain. The validation process only requires website owners  to prove domain ownership by responding to an email or phone call. The  browser address bar only displays HTTPS and a padlock with no business  name displayed.

**Wildcard SSL certificates**

Wildcard SSL certificates allow you to secure a base domain and unlimited  sub-domains on a single certificate. If you have multiple sub-domains to secure, then a Wildcard SSL certificate purchase is much less  expensive than buying individual SSL certificates for each of them.  Wildcard SSL certificates have an asterisk \* as part of the common name, where the asterisk represents any valid sub-domains that have the same  base domain. For example, a single Wildcard certificate for \*website can be used to secure:

* payments.yourdomain.com
* login.yourdomain.com
* mail.yourdomain.com
* download.yourdomain.com
* anything.yourdomain.com

**Multi-Domain SSL Certificate (MDC)**

A Multi-Domain certificate can be used to secure many domains and/or  sub-domain names. This includes the combination of completely unique  domains and sub-domains with different TLDs (Top-Level Domains) except  for local/internal ones.

For example:

* www.example.com
* example.org
* mail.this-domain.net
* example.anything.com.au
* checkout.example.com
* secure.example.org

Multi-Domain certificates do not support sub-domains by default. If you need to  secure both www.example.com and example.com with one Multi-Domain  certificate, then both hostnames should be specified when obtaining the  certificate.

**Unified Communications Certificate (UCC)**

Unified Communications Certificates (UCC) are also considered Multi-Domain SSL  certificates. UCCs were initially designed to secure Microsoft Exchange  and Live Communications servers. Today, any website owner can use these  certificates to allow multiple domain names to be secured on a single  certificate. UCC Certificates are organizationally validated and display a padlock on a browser. UCCs can be used as EV SSL certificates to give website visitors the highest assurance through the green address bar.

It is essential to be familiar with the different types of SSL  certificates to obtain the right type of certificate for your website.

**How to obtain an SSL certificate**

SSL certificates can be obtained directly from a Certificate Authority  (CA). Certificate Authorities – sometimes also referred to as  Certification Authorities – issue millions of SSL certificates each  year. They play a critical role in how the internet operates and how  transparent, trusted interactions can occur online.

The cost of an SSL certificate can range from free to hundreds of dollars,  depending on the level of security you require. Once you decide on the  type of certificate you require, you can then look for Certificate  Issuers, which offer SSLs at the level you require.

Obtaining your SSL involves the following steps:

* Prepare by getting your server set up and ensuring your [WHOIS](https://www.whois.net/) record is updated and matches what you are submitting to the  Certificate Authority (it needs to show the correct company name and  address, etc.)
* Generating a Certificate Signing Request (CSR) on your server. This is an action your hosting company can assist with.
* Submitting this to the Certificate Authority to validate your domain and company details
* Installing the certificate they provide once the process is complete.

Once obtained, you need to configure the certificate on your web host or on your own servers if you host the website yourself.

How quickly you receive your certificate depends on what type of  certificate you get and which certificate provider you procure it from.  Each level of validation takes a different length of time to complete. A simple Domain Validation SSL certificate can be issued within minutes  of being ordered, whereas Extended Validation can take as long as a full week.

**Can an SSL certificate be used on multiple servers?**

It is possible to use one SSL certificate for multiple domains on the same server. Depending on the vendor, you can also use one SSL certificate  on multiple servers. This is because of Multi-Domain SSL certificates,  which we discussed above.

As  the name implies, Multi-Domain SSL Certificates work with multiple  domains. The number is left up to the specific issuing Certificate  Authority. A Multi-Domain SSL Certificate is different from a Single  Domain SSL Certificate, which – again, as the name implies – is designed to secure a single domain.

To make matters confusing, you may hear Multi-Domain SSL Certificates,  also referred to as SAN certificates. SAN stands for Subject Alternative Name. Every multi-domain certificate has additional fields (i.e.,  SANs), which you can use to list additional domains that you want to  cover under one certificate.

Unified Communications Certificates (UCCs) and Wildcard SSL Certificates also  allow for multi-domains and, in the latter case, an unlimited number of  subdomains.

**What happens when an SSL certificate expires?**

SSL certificates do expire; they don't last forever. [The Certificate Authority/Browser Forum](https://cabforum.org/), which serves as the de facto regulatory body for the SSL industry, states that SSL certificates should have a lifespan of [no more than 27 months](https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.0.pdf). This essentially means two years plus you can carry over up to three  months if you renew with time remaining on your previous SSL  certificate.

SSL certificates expire because, as with any form of authentication, information needs  to be periodically re-validated to check it is still accurate. Things  change on the internet, as companies and also websites are bought and  sold. As they change hands, the information relevant to SSL certificates also changes. The purpose of the expiry period is to ensure that the  information used to authenticate servers and organizations is as  up-to-date and accurate as possible.

Previously, SSL certificates could be issued for as long as five years, which was  subsequently reduced to three and most recently to two years plus a  potential extra three months. In 2020, Google, Apple, and Mozilla  announced [they would enforce one-year SSL certificates](https://techbeacon.com/security/google-apple-mozilla-enforce-1-year-max-security-certifications), despite this proposal being voted down by the Certificate Authority  Browser Forum. This took effect from September 2020. It is possible that in the future, the length of validity will reduce still further.

When an SSL certificate expires, it makes the site in question unreachable.  When a user's browser arrives at a website, it checks the SSL  certificate's validity within milliseconds (as part of the SSL  handshake). If the SSL certificate has expired, visitors will receive a  message to the effect of — "This site is not secure. Potential risk  ahead".

While users do have  the option to proceed, it is not advisable to do so, given the  cybersecurity risks involved, including the possibility of [malware](https://www.kaspersky.com/resource-center/threats/malware-protection). This will significantly impact bounce rates for website owners, as users rapidly click off the homepage and go elsewhere.

Keeping on top of when SSL certificates expire presents a challenge for larger businesses. While smaller and [medium-sized businesses (SMEs)](https://www.kaspersky.com/small-to-medium-business-security) may have one or only a few certificates to manage, [enterprise-level organizations](https://www.kaspersky.com/enterprise-security) that potentially transact across markets – with numerous websites and  networks – will have many more. At this level, allowing an SSL  certificate to expire is usually the result of oversight rather than  incompetence. The best way for larger businesses to stay on top of when  their SSL certificates expire is by using a certificate management  platform. There are various products on the market, which you can find  using an online search. These allow enterprises to see and manage  digital certificates across their entire infrastructure. If you do use  one of these platforms, it is important to log in regularly so you can  be aware of when renewals are due.

If you allow a certificate to expire, the certificate becomes invalid, and you will no longer be able to run secure transactions on your website.  The Certification Authority (CA) will prompt you to renew your SSL  certificate before the expiration date.

Whichever Certificate Authority or SSL service you use to obtain your SSL  certificates from will send you expiration notifications at set  intervals, usually starting at 90 days out. Try to ensure that these  reminders are being sent to an email distribution list — rather than a  single individual, who may have left the company or moved to another  role by the time the reminder is sent. Think about which stakeholders in your company are on this distribution list to ensure the right people  see the reminders at the right time.

**How to tell if a site has an SSL certificate**

The easiest way to see if a site has an SSL certificate is by looking at the address bar in your browser:

* If the URL begins with HTTPS instead of HTTP, that means the site is secured using an SSL certificate.
* Secure sites show a closed padlock emblem, which you can click on to see  security details – the most trustworthy sites will have green padlocks  or address bars.
* Browsers also show warning signs when a  connection is not secure — such as a red padlock, a padlock which is not closed, a line going through the website's address, or a warning  triangle on top of the padlock emblem.

**How to ensure your online session is safe**

**Only submit your personal data and online payment details to websites with EV or OV certificates**. DV certificates are not suitable for eCommerce websites. You can tell  if a site has an EV or OV certificate by looking at the address bar. For an EV SSL, the organization's name will be visible in the address bar  itself. For an OV SSL, you can see the organization's name's details by  clicking on the padlock icon. For a DV SSL, only the padlock icon is  visible.

**Read the website's privacy policy**. This enables you to see how your data will be used. Legitimate  companies will be transparent about how they collect your data and what  they do with it.

**Look out for trust signals or indicators on websites**.  
 As well as SSL certificates, these include reputable logos or badges  which show the website meets specific security standards. Other signs  that can help you determine if a site is real or not include checking  for a physical address and telephone number, checking their returns or  refunds policy, and making sure prices are believable and not too good  to be true.

**Stay alert to phishing scams**.  
 Sometimes cyber attackers create websites that mimic existing websites  to trick people into purchasing something or logging in to their  phishing site. It is possible for a [phishing](https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips) site to obtain an SSL certificate and therefore encrypt all the traffic that flows between you and it. A growing proportion of phishing scams  occur on HTTPS sites — deceiving users who feel reassured by the padlock icon's presence.

To avoid these kinds of attacks:

* Always examine the domain of the site you are on and ensure it is spelled  correctly. The URL of a fake site might differ by only one character –  e.g., amaz0n.com instead of amazon.com. If in doubt, type the domain  directly into your browser to make sure you are connecting to the  website you intend to visit.
* Never enter logins, passwords,  banking credentials, or any other personal information on the site  unless you are sure of its authenticity.
* Always consider what a particular site is offering, whether it looks suspicious, and whether you really need to register on it.
* Make sure your devices are well protected: [Kaspersky Internet Security](https://www.kaspersky.com/internet-security)checks URLs against an extensive database of phishing sites, and it detects scams regardless of how "safe" the resource looks.

Cybersecurity risks continue to evolve but understanding the types of SSL  certificates to look out for and how to distinguish a safe site from a  potentially dangerous one will help internet users avoid scams and  protect their personal data from cybercriminals.