

Different types of SSL Certificates (DV / OV / EV explained)

Question: What types of SSL Certificates exist?

There are several types of SSL certificates available, each with their own set of features and use cases. The main types of SSL certificates include Single Domain, Multi Domain and Wildcard certificates.

Single Domain SSL Certificate:

A Single Domain SSL certificate, as the name suggests, is designed to secure a single domain, such as example.com. Single Domain SSL certificates are ideal for websites that only have one primary domain and do not require protection for subdomains or additional domains.

Multi-Domain SSL Certificate:

A Multi-Domain SSL certificate, also known as a SAN (Subject Alternative Name) certificate, is designed to secure multiple domains and subdomains on a single certificate in the same validation process. Multi-Domain SSL offer more flexibility as you can reissue the SSL and change the domains covered by this SSL (except for the common name) and can provide cost savings compared to purchasing individual certificates for each domain.

Wildcard SSL Certificate:

A Wildcard SSL certificate is designed to secure a main domain and all of its subdomains under a single certificate. For example, a Wildcard SSL certificate for *.example.com would secure example.com, www.example.com, blog.example.com, mail.example.com, and any other

subdomains of example.com. Wildcard SSL certificates are ideal for websites that have multiple subdomains that need SSL protection, as they can provide cost savings and simplify certificate management, as you do not need to know all the subdomains yet, at the moment of requesting the SSL. You can secure an unlimited number of subdomains using a wildcard SSL certificate.

It will **NOT** cover:

- Nested subdomains (e.g., sub2.sub1.example.com)
- Different domains (e.g., example.net or example.org)

Alternative SSL certificates *S/MIME* and *Code Signing SSL* are described [here](#).

Besides the type of SSL, you can also choose the level of Validation;

1. **Domain Validated (DV)** SSL Certificates: DV SSL certificates are the most basic type of SSL certificate, and are typically the least expensive. They only verify that the person or organization requesting the certificate has control over the domain in question. DV SSL certificates do not provide any additional information about the website or organization that operates it.
Click [here](#) to read how DV certificates can be validated.
2. **Organization Validated (OV)** SSL Certificates: OV SSL certificates require a more rigorous verification process than DV certificates. In addition to verifying domain ownership, the certificate authority (CA) will also verify the organization's identity a phone validation. Therefore it is very important that the information provided during the request are valid and up to date. OV SSL certificates can provide more information about the website or organization that operates it, which can help to establish trust with visitors.
Click [here](#) to read how OV certificates can be validated.
3. **Extended Validation (EV)** SSL Certificates: EV SSL certificates are the highest level of SSL certificate available. They require the most rigorous verification process, which includes the same steps as the DV and OV, but adds 1 more step, a signed agreement with the CA itself. This is done via digital signature.
EV SSL certificates provide the most information about the website or organization that operates it, and can help to establish the highest level of trust with visitors. Websites that use EV SSL certificates typically display a green address bar in the browser, which indicates that the website is secure and has been verified by a trusted third party. **Note:** EV SSL certificates are not available with the wildcard option; they are only offered for single-domain or multi-domain configurations.
Click [here](#) to read how EV certificates can be validated.

Object

Single domain

Protect one domain

"WWW"

included for free

◆ mysite.nl

Mult-domain

Protect several domain under one name

◆ mysite.com

◆ mysite.ch

◆ mysite.fi

Wildcard

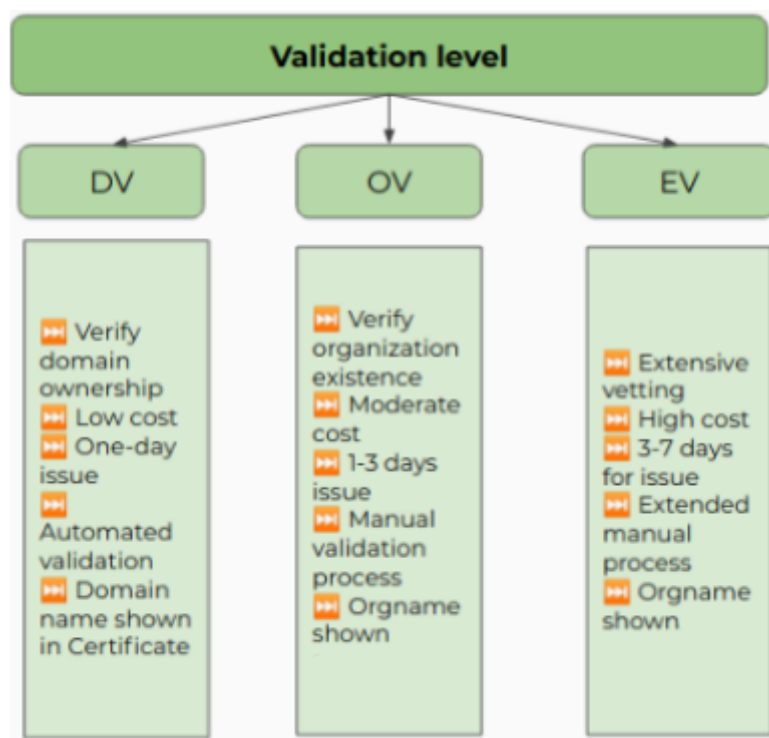
Protects Main domain + Subdomains of the main domain.

◆ mysite.nl

◆ a.mysite.nl

◆ b.mysite.nl

◆ c.mysite.nl



It's important to note that the type of SSL certificate you choose will depend on your specific needs and use case. If you're running a personal blog or website, a DV SSL certificate may be sufficient. However, if you're running an e-commerce site or other website that deals with sensitive information, you may want to consider an OV or EV SSL certificate, which can provide additional assurance and establish greater trust with your visitors.

REMEMBER

The certificate will be on the name of the company for which the request has been done. If you are a reseller and are ordering a SSL Certificate for your client, you need to select that client as SSL owner. In most cases, the client will have to perform the validation.

If you request it for the organization HostingExampleLTD with the domains domain1.de, domain2.fr, and domain3.ch, all 3 domains will show the organization HostingExampleLTD in the certificate.

Each certificate can only be requested for one company, regardless of the domains inside the order.

It is not possible to put multiple companies in a one request.

See these FAQ articles for additional information

[Is "www" automatically included in my SSL order?](#)

[Can I add a wildcard in a multidomain ssl?](#)

Revision #2

Created 2026-08-07 14:27:51 UTC by Sarath

Updated 2026-08-07 15:45:27 UTC by Sarath