

# What kind of SSL/TLS certificate do you need?

Protect your website with SSL/TLS certificates

## What Are SSL/TLS Certificates?

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) certificates are cryptographic protocols that secure communication between web servers and clients (such as web browsers or applications). They provide encryption, authentication, and data integrity to prevent unauthorized access, data breaches, and cyberattacks.

TLS is the successor to SSL, with enhanced security features. Though the term "SSL" is commonly used, most modern implementations use TLS.

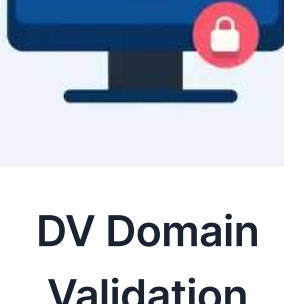
## Types of SSL/TLS certificates

SSL/TLS certificates come in different types based on validation levels and domain coverage.



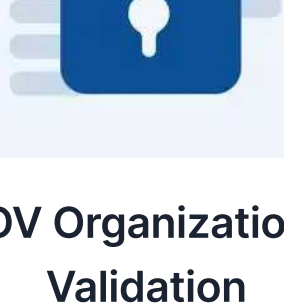
### 1. Validation-based classification

SSL/TLS certificates are categorized based on the level of validation required before issuance. The three primary validation types are DV, OV and EV.




#### DV Domain Validation

- Provides basic encryption and is validated by proving domain ownership.
- Ideal for personal websites, blogs, and small businesses.
- Quick issuance, usually within minutes or hours.



#### OV Organization Validation

- Requires verification of the business entity behind the website.
- Includes company details in the certificate, offering more trust.
- Suitable for business and organization websites.

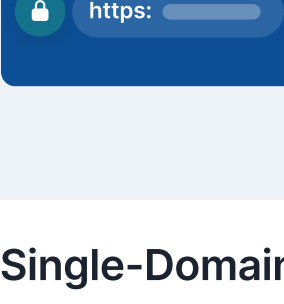


#### EV Extended Validation

- The highest level of validation, requiring thorough vetting of the business.
- Displays the company name in the browser address bar (on some browsers).
- Best for e-commerce, banking, and high-trust sites.

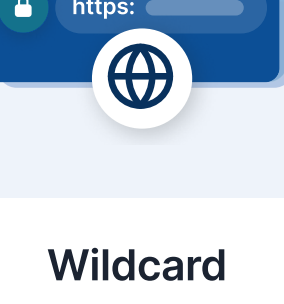
### 2. Domain coverage-based classification

SSL/TLS certificates can also be classified based on the number of domains they secure



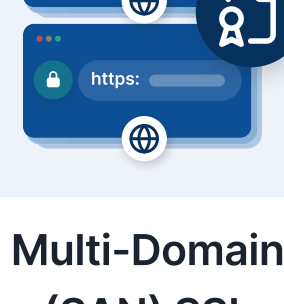
#### Single-Domain SSL

- Secures one specific domain.
- Example: example.com



#### Wildcard SSL


- Covers a domain and all its subdomains.
- Example: \*.example.com (secures blog.example.com, store.example.com, etc.)



#### Multi-Domain (SAN) SSL


- Secures multiple different domains under one certificate.
- Example: example.com, example.net, example.org

## How SSL/TLS certificates work




#### 1. Handshake and encryption

- When a user visits a website with SSL/TLS, the server and browser perform a **handshake** to establish a secure connection.
- The server presents its SSL certificate to the browser.
- The browser verifies the certificate with a trusted Certificate Authority (CA).
- A secure, encrypted session is created using asymmetric (public/private key) and symmetric encryption.



#### 2. Data Integrity and authentication

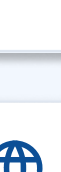
- SSL/TLS certificates prevent data tampering by ensuring that messages are not altered in transit.
- Authentication verifies the website owner's identity, reducing the risk of phishing attacks.



#### 3. HTTPS implementation


- Websites using SSL/TLS certificates display "HTTPS" in the URL instead of "HTTP".
- Some browsers show a padlock symbol, signifying secure connections.

## Importance of SSL/TLS for online security




#### Encryption of sensitive data

- Protects user information such as login credentials, credit card details, and personal data from hackers.




#### Authentication and trust

- Visitors trust websites with SSL/TLS certificates, increasing credibility.
- Google and other search engines give ranking preference to HTTPS-secured sites.




#### Protection against cyber threats

- Helps prevent **Man-in-the-Middle (MitM) attacks**, where attackers intercept communication.
- Defends against **phishing attacks** by verifying legitimate website ownership.



#### Compliance with industry standards

- Essential for businesses to comply with regulations such as GDPR, PCI DSS (for payment processing), and HIPAA (for healthcare data).




#### Boosts SEO and user confidence

- Google penalizes non-HTTPS sites with lower search rankings.
- Browsers like Chrome mark HTTP sites as "Not Secure," deterring visitors.



## How Openprovider enhances SSL/TLS security

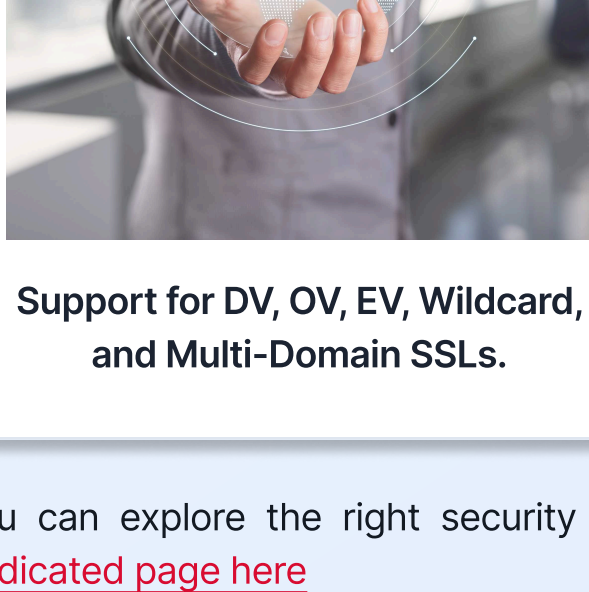
As a provider of **Sectigo** SSL certificates, Openprovider offers:



#### Affordable SSL options for resellers, IT service providers, and agencies.



#### Automated issuance and management via API integration.



#### Support for DV, OV, EV, Wildcard, and Multi-Domain SSLs.



#### Dedicated account management for seamless SSL deployment.

You can explore the right security solution for your business by [accessing our dedicated page here](#)



**Openprovider Memberships, allow to purchase domains at wholesale pricing and unlimited discounted SSL certificates.**

[Get your membership](#)