# What is SSL certificate?

Ssl(secure socket layer) certificates are employed to encrypt the communication taking place between client and server

Ssl certificates encrypts data in to unreadable while transmitting like password abcdefgh to 1234567

CA(certificate authority will issue the ssl certificate)

3 types

* Domain Validation:( here domain ownership will be validated by CA it is entry level certificate used in small organizations)

a. SAN/ Multi-domain :- secure mutiple domain names using same ssl certificate ex:- domain1.com ,domain2.com

b. Wildcard: secure domains and unlimited subdomains

* Organization Validation:(here domain ownership and business is to be validated by CA this is medium level certificate used in mid level organizations)
* Extend Validation(This Is the highest level of thrust and validation it is used for banking ,ecom)

**Benefits of SSL**

* Eliminates phishing and cyber attacks
* Protects user sensitive info
* Eliminates browser warnings and alerts
* Increase reputation
* Secure communication from browser to server

What is certificate Authority?

A certificate authority is an third party entity that isuues digital certificates and manages the public keys and credentials for data encryption for end user

Ex :- Comodo

Symantec

Go Daddy

How to get SSL certificates?

* First we need to decide which certificate he need like DV OV or EV

And get ssl from authorities or from resellers

* Next we need to apply for certificate signing request (CSR) and CA will provide private key, need to store both CSR and private in server.
* Now CA has received request and user may need to provide documents to prove identit

### **Who should buy Domain Validated (DV) SSL?**

Small or medium level website owners who only wish to encrypt their domain should buy DV SSL certificate. Compared with organization validated (OV) & extended validated(EV) SSL certificate, the price of domain validated (DV) certificate is much lower.

Domain validation SSL certificates come up with alternative options such as ‘Wildcard SSL certificate’ and ‘Multi-domain certificate’. The wildcard SSL Certificate lets user secure the unlimited number of sub-domains whereas a Multi-domain (SAN) SSL certificate will allow the user to secure up to 100 multiple fully qualified domain names.

* **Lower Price** – The prices of the domain validated (DV) certificates are on the lower side compared to the organization validated (OV) & extended validated (EV) certificates.
* **Issued within minutes** – Certificate Authority Issues domain validated (DV) SSL certificates within minutes once the domain verification process is done.
* **No paperwork for validation** – Certificate Authority does not ask for any documents during domain name verification process.
* **Google Ranking Benefits** – Google recently announced to give ranking benefits to the SSL enabled websites. So, a DV SSL will help you increase your website traffic which can definitely give a boost to your business.
* **Increases user’s trust** – HTTPS and website seal are trust indicators which let the users know that the website is secured and their information is safe.

# Domain Validated SSL Validation Process

* **File based verification** – The certificate authority will provide you an html file knows as Authentication File (auth file) including a specific content (Hash Data), you just need to upload that file on your server directory. Once the finds the **auth file,** they will approve Certificate issuance request.
* **Domain Registrar Information (DNS Records)** – Certificate authority issues your certificate by domain registrar’s information. So if your domain registrar’s details are private, then you must turn it open.
* **Email Based Verification** – Certificate authority verify domain identity by email. They send an email to the domain administrator; included with a unique link and verification code, you just need to confirm that link and your certificate will be issued.

### **Domain Validated SSL Key Features:**

* 2048-bit SSL Certificate signature
* Robust encryption strength up to 256-bit
* Can secure both www and non-www domains
* Compatible with 99.9% of the web and mobile browsers
* Free certificate authority (CA) site seal
* Issuance within minutes
* No paperwork or documentation required for validation
* Free phishing detection alert service (Only offered by few certificate authorities)
* Can be reissued as many times as needed during the validity period
* Alternative options such as Wildcard and Multi-Domain feature

## OV SSL and Code Signing Certificate

Organization Validation SSL certificate is a high assurance SSL certificate which is used to validated a company/business/organization. The main purpose of OV SSL certificate is to encrypt website/business and user’s sensitive information which is being used for transactions.

It comes up with 2048-bit signature and powerful 256-bit encryption. It also displays the name of the organization in the site seal, which is a trust indicator that shows the business is legitimate and assures that the information shared remains confidential. It increases customer’s confidence therefore improving the conversation rate of the business.

OV SSL certificate secures the websites from phishing attacks and keeps hackers and attackers at bay.

Compared with the DV organization validated (OV) SSL is more trustworthy for online businesses.

### **1) Issuer’s Identify Verification**

**Issuer as Business**

If the SSL Issuer business is from a wide corporation, government agency, or a registered business; to verify issuer’s identity following documents are mandatory.

* Issuer’s legal creation, recognition or existence record from a government agency
* An Attestation Letter approved by Certificate Authority
* CA considers an updated third party database as legal data source for identification
* Website must be live, CA or Third party may visit it too…

**Officially approved data sources: QIIS (Qualified Independent Information Source)**

* <https://www.dnb.com/>
* <https://www.gov.uk/government/organisations/companies-house>

**Organization Address Verification**

* Legal business license with address issued by government
* Article of incorporation with address
* Recent bank statement
* Recent Telephone/Landline or Internet Bill
* Recent major utility bills (Electricity, water, etc…)
* Current lease agreement with address (optional)

**Issuer as Individual**

**Issuer’s address verification**

* Issuer’s passport, license or other copy
* Any utility paid for that organization (Telephone bill, electricity bill, tax bill, etc…)

### **2) Domain Registrar Verification**

* Require to verify WhoIs verification of that domain.

### **3) Domain Control Validation (DCV)**

### **4) Verification via Call**

* Certificate authority call back to the issuer on the given business phone number. But the phone number should follow below criteria.
  + Must be added in a third-party database
  + Must be added in government databases
  + Must be added in accountant letter or legal opinion letter.

One the certificate completes the above verification process and if they satisfy, they approve issuer’s request to approve the SSL Certificate.

### **Who should Buy OV SSL Certificate?**

You should definitely go for OV certificate if you have an online business which involves collecting sensitive information from your users. Social networking platforms, banking platforms, Facebook games & apps, Firefox Add-ons, Google Chrome extensions are highly recommended to adopt OV SSL certificate for security purposes.

**OV SSL Certificates** also come up with features such as wildcard & Multi-domain SSL feature. The wildcard SSL feature allows the users to validate business and to secure an unlimited number of sub-domains. Whereas the multi-domain feature allows the users to secure up to 100 fully qualified domain names.

Most certificate authorities (CAs) offer OV SSL Certificate with unlimited number of server licenses so that the user can install it on any number of servers and can be reissued any number of times.

### **Organization Validated SSL Key Features**

* Contains your authenticated organization details
* 2048 bit future proof SSL Certificates
* A single certificate secures both [www.domain.com](http://www.domain.com) and domain.com
* Universally works with 99.9% browsers, mobile phones, and devices
* SHA-2 signed certificates with 256-bit strong encryption
* Unlimited Server License and Reissuance

**Extended Validation SSL Certificates** offer top-notch level of safety and security which ultimately enhances the customer confidence. EV SSL certificate provide advanced level of security against phishing attacks, email fraud, and other cyber-attacks.

It displays green address bar with business name in URL which shows the users that the business is genuine and verified by a trusted SSL certificate authority (CA). This confidence eventually increases your website leading to rise in your business.

An EV SSL Certificate also comes up with Multi-domain security option, which lets user secure multiple domains (up to 100) under single EV Certificate. This certificate is called ‘EV Multi Domain SSL certificate’.

### **Who should Buy EV SSL Certificate?**

The business which deals with user’s payments details, sensitive information, etc. should apply for EV SSL certificate. Web security experts recommend adopting EV SSL Certificate for platforms such as E-commerce, Banking, Social Media, Health Care, Governmental and Insurance platforms. Not only large organizations, but small and medium level business can issue EV SSL certificates (given that they have all the documents which follow CA’s guidelines).

### **How to Know if a Website has EV SSL Certificate Enabled? – (EV SSL User Interface)**

EV supports all leading web browsers including Google chrome, Mozilla Firefox, Safari, Internet Explorer, Opera, etc. These browsers identify EV SSL certificate using the EV Identifiers preinstalled by the certificate authority (CA). Once the browser identifies the EV SSL certificate, it will display indicators suggesting that EV certificate is installed on the website.

The example of the EV SSL certificate interface is shown in the image below. In each browser, the Address Bar is green colored and Business Name (E.g. Thawte Inc. [US]) is displayed. which shows that business is genuine and been verified by the trusted certificate authority and customer do not have to free fearful about sharing his personal or financial details. This shows that your business is legitimate and encourages the customer to do business and make transactions without any concerns.

### **EV SSL Certificate Identifiers**

* HTTPS://
* Green Address Bar
* Organization name in URL
* CA’s name on Certificate information

## EV SSL Certificates Validation Process

Extended validation SSL Certificate delivers highest level of encryption which turn business to run via a tough validation & authentication process. The issuer must have to submit all the legal documents asked by the certificate authority.

### **Entities which can apply to issue EV SSL certificate**

* Small/Medium/Large Corporations
* Government Agencies
* General Partnerships
* Sole Proprietorships
* Unincorporated Associations

### **Documents required for EV SSL Certificate Validation**

### **1) Organization Authentication documents**

Certificate authority ask for following organization authentication documents

* Official Government Agency Records included with
  + Registration number.
  + Date of Registration or Incorporation.
  + Business Address.
* If the business address is not added in a governmental agency’s records, the issuer can submit any non-governmental data sources.
  + Approved Data Sources are
    - dnb.com
    - hoovers.com
    - [http://www.companieshouse.gov.uk/](https://www.gov.uk/government/organisations/companies-house)

### **2) Domain Authentication Documents**

Domain registration details must me matched with the registered organization name to issue an EV SSL Certificate. Issuer must have right to use the domain name and layer’s opinion letter is also required. Following domain authentication criteria must be followed to issue EV SSL.

* IANA or ICANN registrar domain is mandatory, others will be disapproved.
* Admin must need to keep domain registrar information must keep open, private mode will be rejected.
* Issuer must have the information about the domain name, CA may also go with phone call verification.

### **3) Authentication Documents of Organization’s Certificate Approver**

The certificate issuer must be the owner or employee of that organization and he must have the authorities to access and use the Extended Validated SSL Certificate.

*Important notes*

1. *In case the certificate issuer is listed on some governmental official records as CEO, CIO, Director, Secretary, COO, President, CFO, CSO, etc. then certificate authority will accept issuer’s authentication without verifying any other information described below.*
2. *Issuer’s information will not be verified by company’s website.*

CA will ask for following documents to verify the Issuer

* Issuer’s identify including title & employment document by company
* As the issuer must have rights to access the EV SSL certificate, following documents are mandatory.
  + Opinion letter from lawyer
  + Business Resolution
  + CA will contact CEO, COO, CIO, etc. directly to verify issue’s information; if no one available or not been able to contact, CA will ask to Human Resource department.

### **4) Phone call Verification**

CA must contact the issuer via phone call to verify all the SSL certificate details with following ways.

* Via number provided on Layer’s opinion letter
* Via official website
* Via third party business directories or online databases.

**Following information will verify by certificate authority over the phone conversation**

* Issuer’s name and authority to access the EV SSL Certificate
* Issuer’s knowledge for that business and access to use the domain name which was request for EV Certificate.
* Approval of the EV SSL Certificate request.
* Acknowledgement of signature of Certificate Authority Subscriber Agreement that is added with all EV SSL terms and conditions.

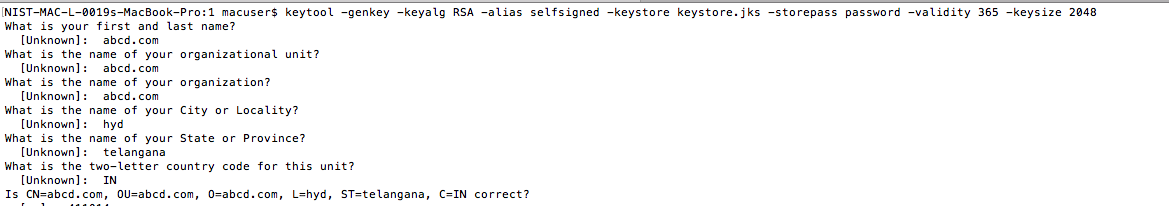
### **Extended Validated SSL Features**

* Extended Validation triggers the green address bar in the browsers.
* Displays **Organization Name** in URL.
* Mostly issued within 3-7 business days.
* Full business Validation.
* Adds Encryption up to **256-bit.**
* Supports two encryption algorithms, namely RSA and DSA.
* Increases transaction **conversion rates.**
* Lowers shopping cart abandonment.
* **99.9%** web and mobile browser support.
* Unlimited number of server licenses.
* Protects from phishing attacks.

# How to Create a Self Signed Certificate using Java Keytool

**Step 1.** Open the command console

**Step 2.** Run this command (Where indicate the number of days for which the certificate will be valid)  
keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass password -validity 365 -keysize 2048



**Step 3.** Enter a password for the keystore. Note this password as you require this for configuring the server

**Step 4.** When prompted for first name and last name, enter the domain name of the server. For example, myserver or myserver.mycompany.com.

**Step 5.** Enter the other details, such as Organizational Unit, Organization, City, State, and Country.

**Step 6.** When prompted with Enter key password for , press Enter to use the same password as the keystore password

**Step 7.** Run this command to verify the contents of the keystore  
keytool -list -v -keystore selfsigned.jks

**Step 8.** When prompted, enter the keystore password note in Step 3. The basic information about the generated certificate is displayed. Verify that the Owner and Issuer are the same. Also, you should see the information you provided in Step 4 and 5.