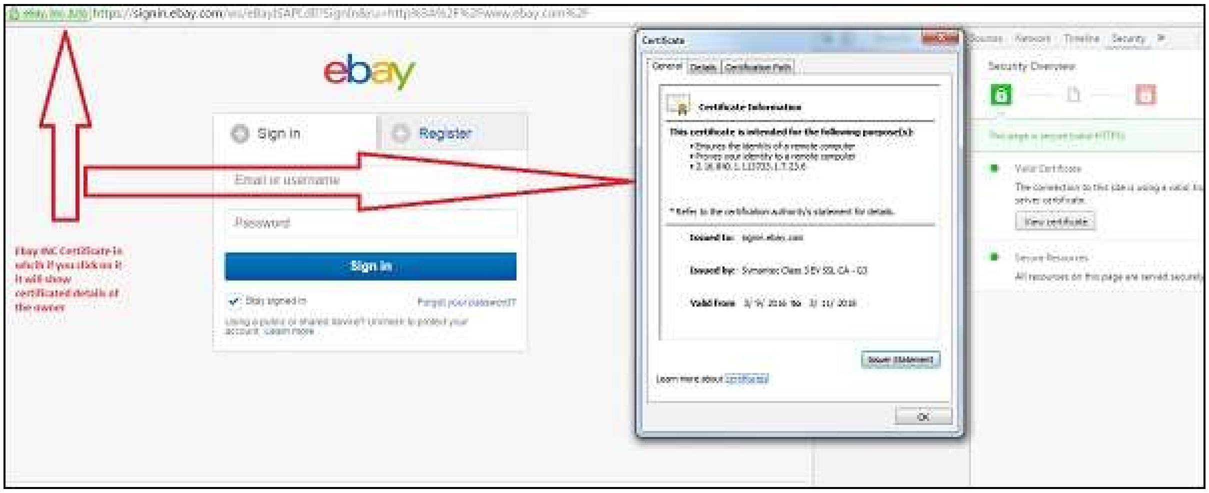
Public Authority Certificates

Digital Certificates are a standard of **security for establishing an encrypted link** between a server and a client. This is generally between a mail server or a webserver that protects data in transitions by encrypting them. A Digital Certificate is also a Digital ID or a passport which is issued by a Third-party authority, which verifies the identity of the server's owner.

For example, the following screenshot shows the eBay public certificate.



Ebay INC Certificate in which if you click on it it will show certificated details of the owner

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.113733.1.7.23.6

* Refer to the certification authority's statement for details.

Issued to: signin.ebay.com

Issued by: Symantec Class 3 EV SSL CA - G3

Valid from 3/ 9/ 2016 to 3/ 11/ 2018

Learn more about certificates

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a valid, trusted server certificate.

Secure Resources

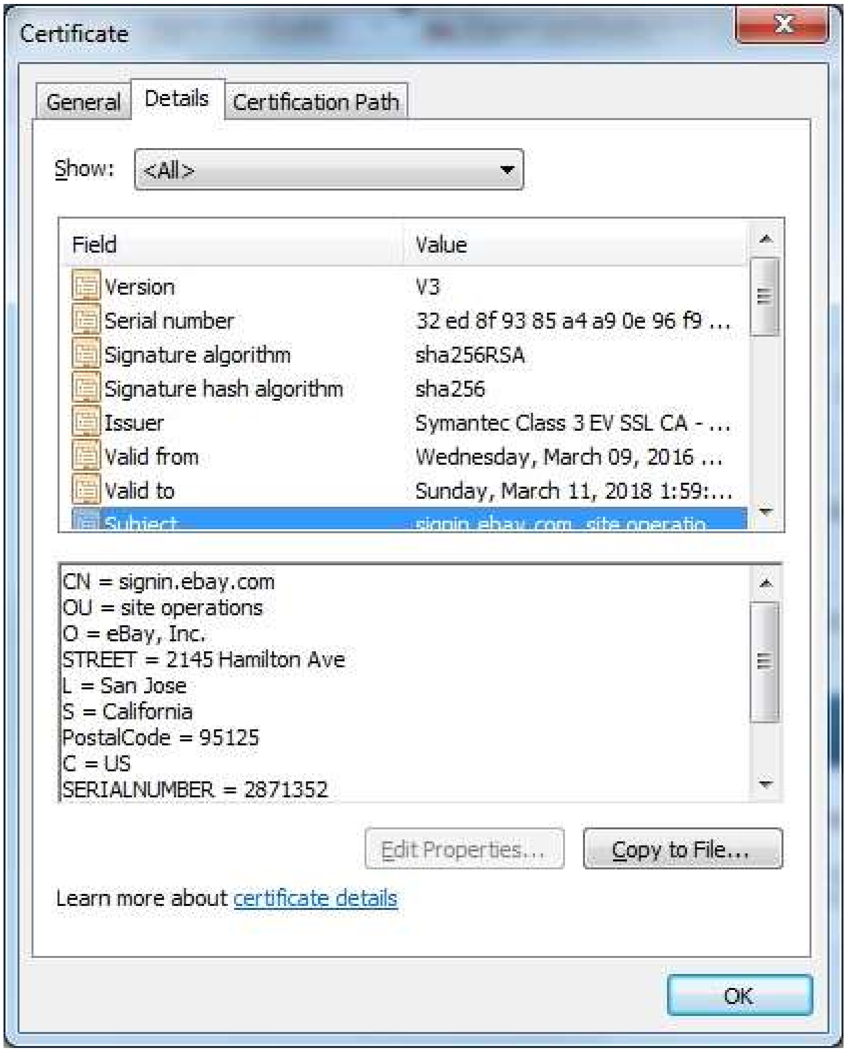
All resources on this page are served securely

Components of a digital certificate

All these components can be found in the certificate details −

- **Serial Number** − Used to uniquely identify the certificate.
- **Subject** − The person or entity identified.
- **Signature Algorithm** − The algorithm used to create the signature.
- **Signature** − The actual signature to verify that it came from the issuer.
- **Issuer** − The entity that verified the information and issued the certificate.
- **Valid-From** − The date a certificate is first valid from.
- **Valid-To** − The expiration date.
- **Key-Usage** − Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- **Public Key** − The public key.
- **Thumbprint Algorithm** − The algorithm used to hash the public key certificate.

- **Thumbprint** − The hash itself, used as an abbreviated form of the public key certificate.



Field	Value
Version	V3
Serial number	32 ed 8f 93 85 a4 a9 0e 96 f9 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Symantec Class 3 EV SSL CA - ...
Valid from	Wednesday, March 09, 2016 ...
Valid to	Sunday, March 11, 2018 1:59:...
Subject	signin.ebay.com, site operatio

CN = signin.ebay.com
OU = site operations
O = eBay, Inc.
STREET = 2145 Hamilton Ave
L = San Jose
S = California
PostalCode = 95125
C = US
SERIALNUMBER = 2871352

Types of Validations

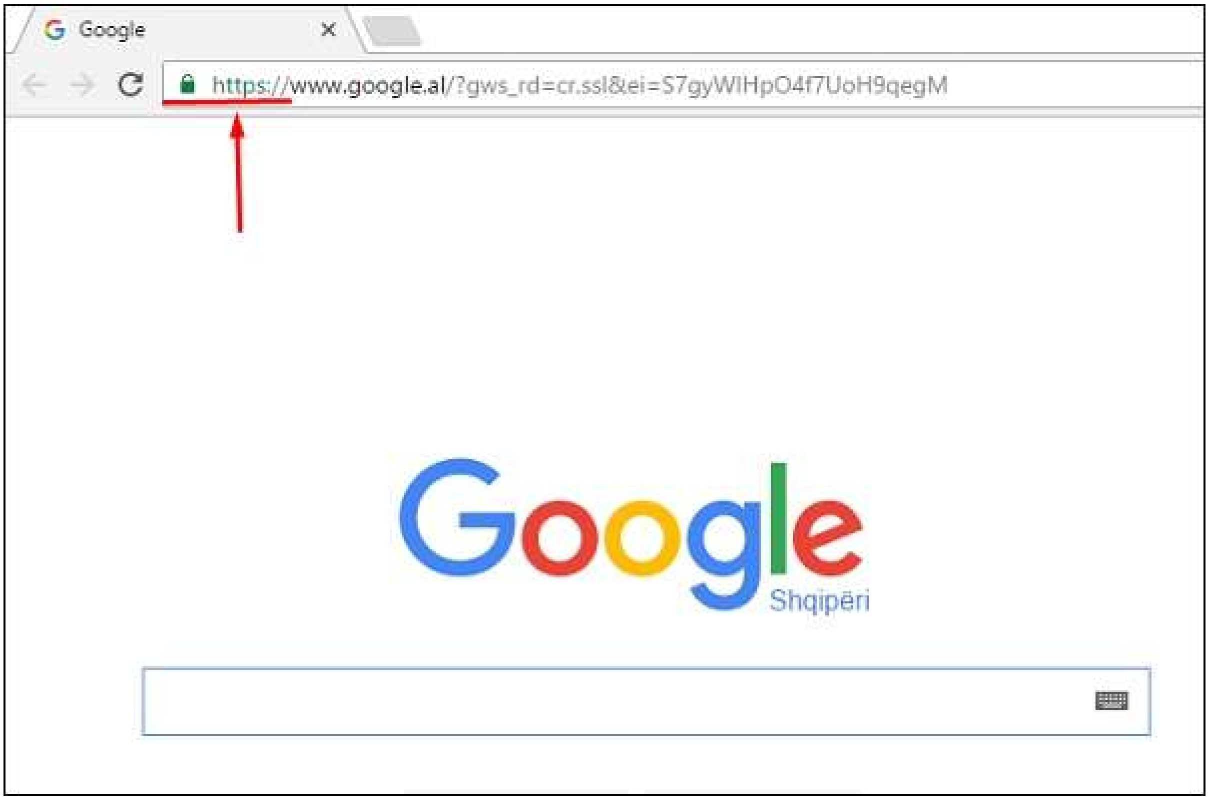
There are three types of validations, which are as follows −

- Domain validation SSL Certificate.
- Organization Validated SSL Certificates.
- Extended Validation SSL Certificates.

Let us now discuss each of them in detail.

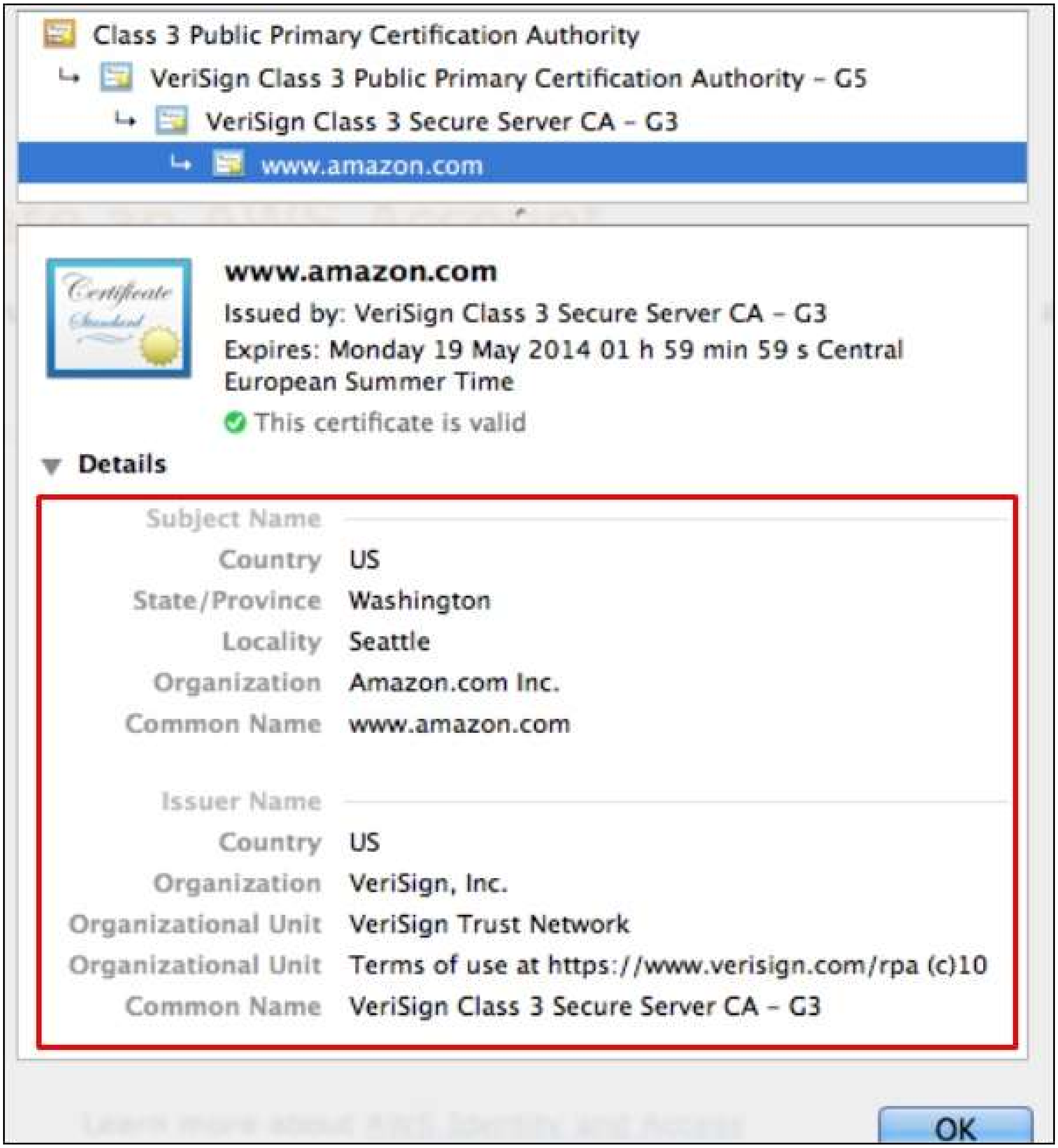
Domain validation SSL certificate

It validates the domain that is registered by a system administrator and he has the administrator rights (authorization or permission) to approve the certificate request. This validation is generally done by an email request or by DNS record.


Google
https://www.google.al/?gws_rd=cr.ssl&ei=S7gyWIHpO4f7UoH9qegM
Google
Shqipëri

Organization Validated SSL Certificates

It validates the domain ownership and business information like the official name, City, Country. Validation is done also by email or DNS record entering. The certificate authority also needs some genuine documents to verify your Identity. The Organization Validated SSL Certificates display the company information in the certificate details as shown in the following screenshot.



Class 3 Public Primary Certification Authority

↳ VeriSign Class 3 Public Primary Certification Authority – G5

↳ VeriSign Class 3 Secure Server CA – G3

↳ www.amazon.com

www.amazon.com

Issued by: VeriSign Class 3 Secure Server CA – G3

Expires: Monday 19 May 2014 01 h 59 min 59 s Central European Summer Time

✓ This certificate is valid

▼ **Details**

Subject Name

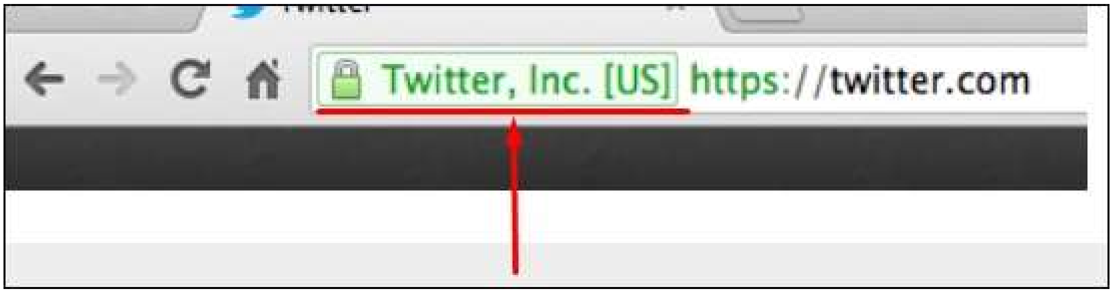
Country	US
State/Province	Washington
Locality	Seattle
Organization	Amazon.com Inc.
Common Name	www.amazon.com

Issuer Name

Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Common Name	VeriSign Class 3 Secure Server CA – G3

Extended Validation SSL Certificates

It validates the domain ownership, organization information and the legal existence of the organization. It also validates that the organization is aware of the SSL certificate request and approves it. The validation requires documentation to certify the company identity plus a set of additional steps and checks. The Extended Validation SSL Certificates are generally identified with a green address bar in the browser containing the company name like the one shown in screenshot below.



Useful Video Courses

Create A WordPress Website In 24 Hours Or Less Guaranteed

23 Lectures 1.5 hours

Zach Miller

More Detail

The Ultimate Guide To Building Your WordPress Website

45 Lectures 2 hours

Zach Miller

More Detail

Google Maps SEO: The 4 Pillars To Rank Your Website Page 1

21 Lectures 2.5 hours

Zach Miller

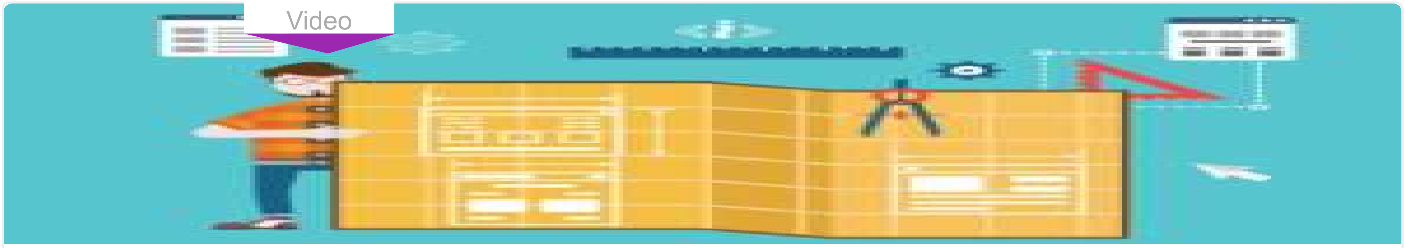
More Detail

Complete CSS Flexbox Course & A Real World Website Project

21 Lectures 2.5 hours

DigiFisk (Programming Is Fun)

More Detail



CSS Grid - Build Modern Real World Websites Fast (+Projects)

52 Lectures 4 hours

DigiFisk (Programming Is Fun)

More Detail

E Commerce Website Development In PHP With PDO

100 Lectures 34 hours

Azaz Patel

More Detail