**What is different between Http, Https, SSL and TLS**

In address bar of a browser, have you noticed either *http://* or *https://* at the time of browsing a website? If neither of these are present then most likely, it’s *http://* Let’s find out the difference…

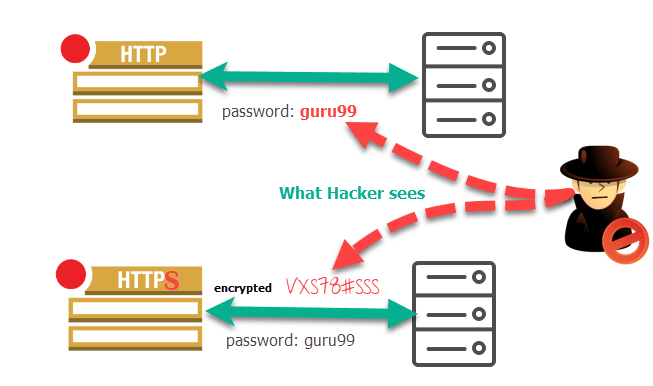
In short, both of these are protocols using which the information of a particular website is exchanged between Web Server and Web Browser. But what’s difference between these two? Well, extra *s* is present in *https* and that makes it secure! What a difference  A very short and concise difference between *http* and *https* is that *https* is much more secure compared to *http*

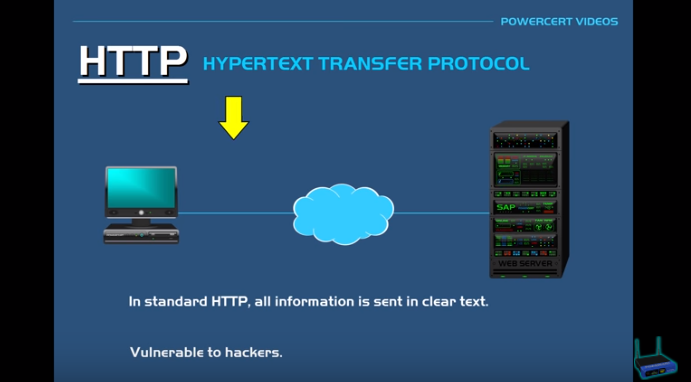
In fact, hyper-text exchanged using *http* goes as plain text i.e. anyone between the browser and server can read it relatively easy if one intercepts this exchange of data

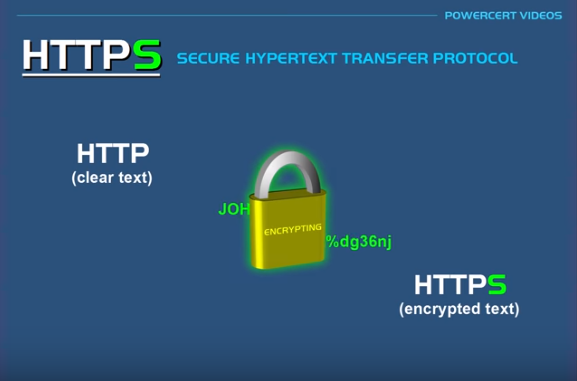
 Think of ‘Online shopping’ at Amazon or Flipkart. You might have noticed that as soon as we click on the Check-out on these online shopping portals, the address bar gets changed to use *https*. This is done so that the subsequent data transfer (i.e. financial transaction etc.) is made secure. And that’s why *https* was introduced so that a secure session is setup first between Server and Browser. In fact, cryptographic protocols such as SSL and/or TLS turn *http* into *https* i.e. **https** = **http** + **cryptographic protocols**.

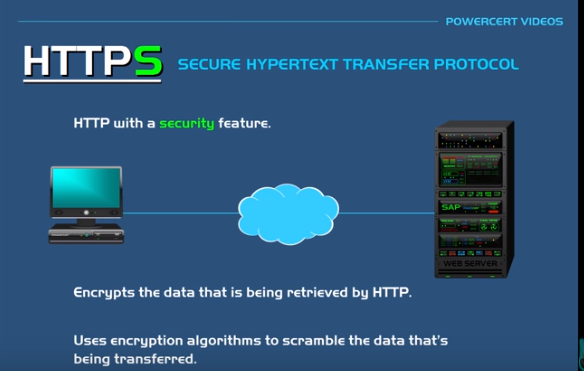
**Differences between HTTP and HTTPS**

* In HTTP, URL begins with “http://” whereas URL starts with “https://”
* HTTP uses port number 80 for communication and HTTPS uses 443
* HTTP is considered to be unsecure and HTTPS is secure
* HTTP Works at Application Layer and HTTPS works at Transport Layer
* No SSL certificates are required for HTTP, with HTTPS it is required that you have an SSL certificate and it is signed by a CA(certificate authority like Comodo, Symantec, Digicert, etc)
* HTTP doesn’t require domain validation, where as HTTPS requires at least domain validation and certain certificates even require legal document validation.
* In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above
* HTTP does not require any certificates and HTTPS needs SSL Certificates

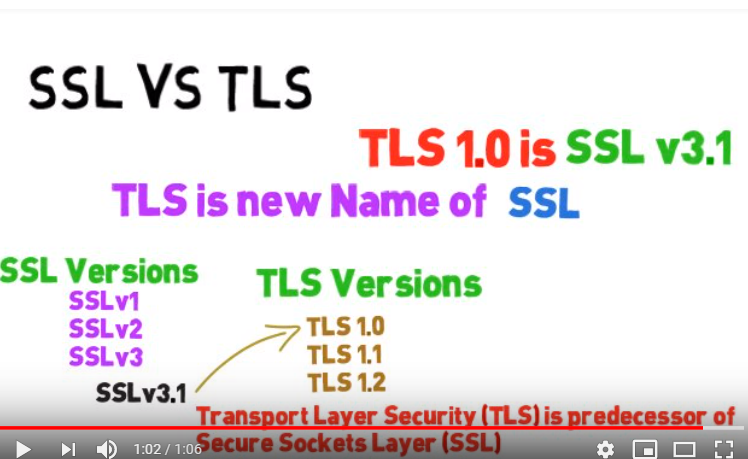


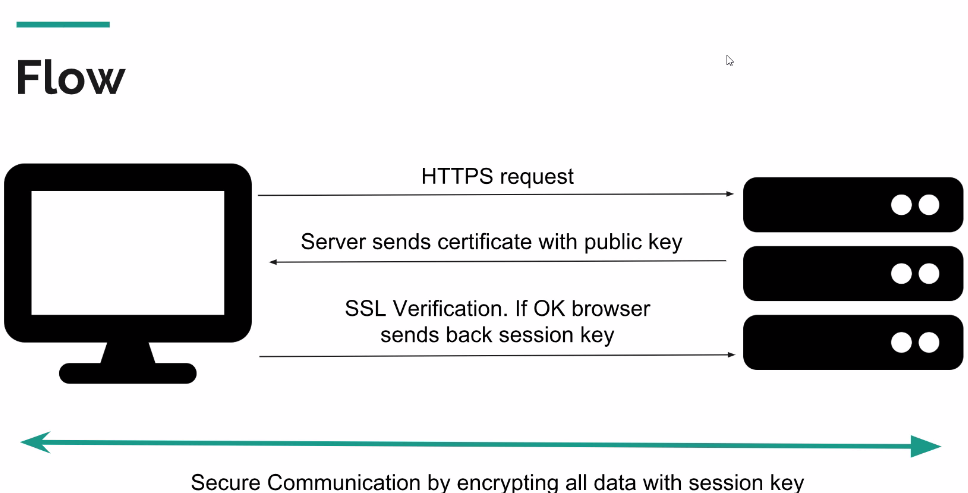


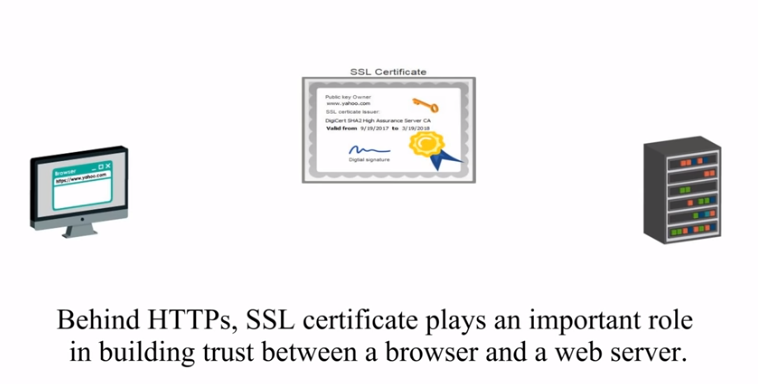








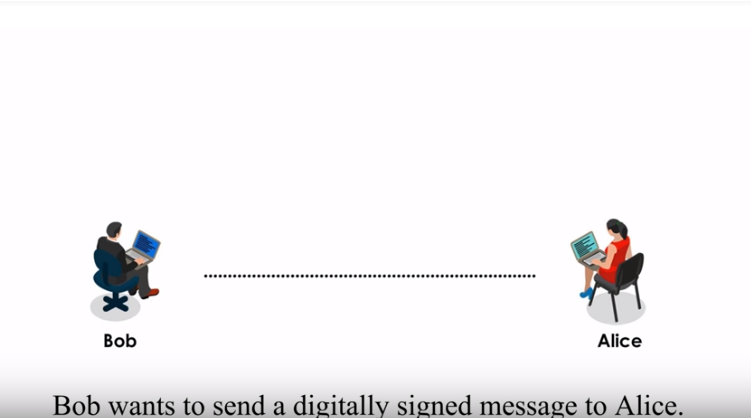


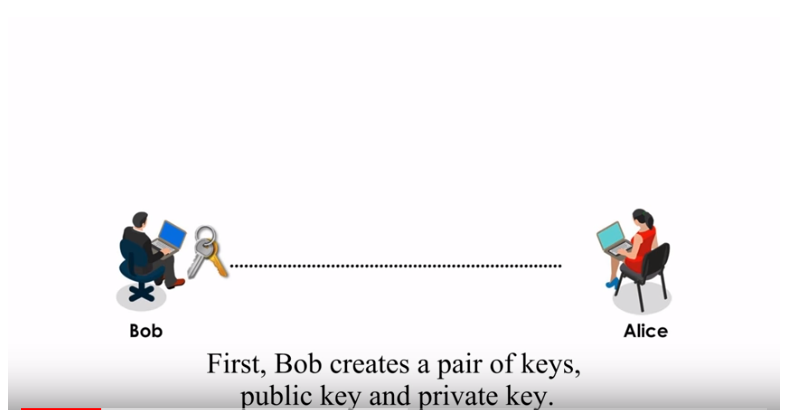


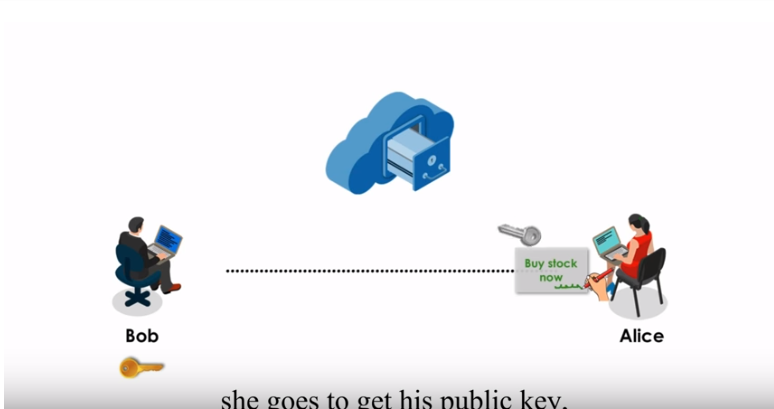
**What digital signature**

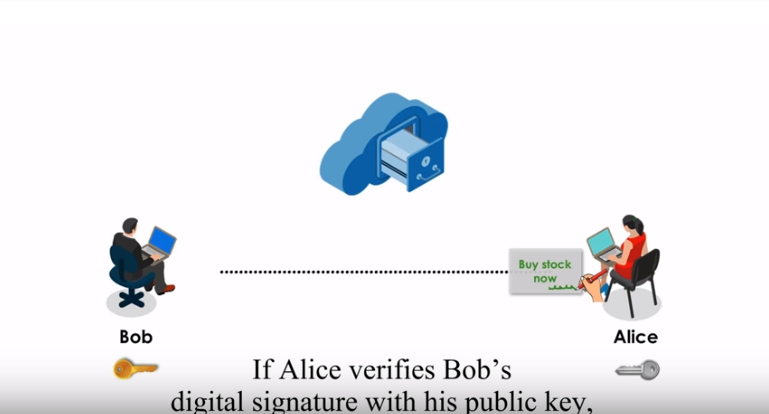
**A digital signature nothing is equivalent to handwritten signature.**

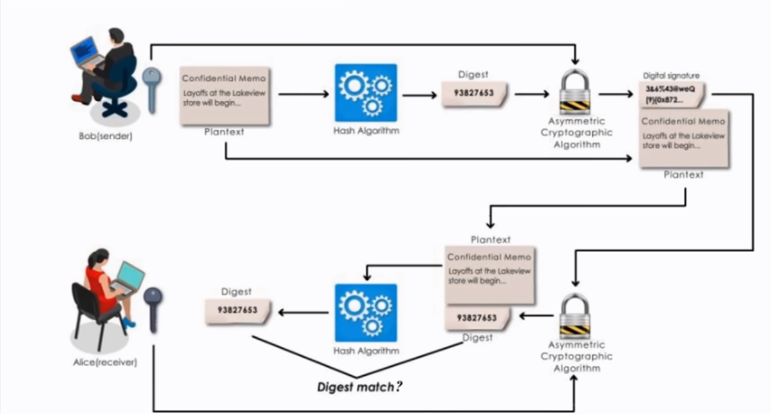
**It is electronic verification of sender.**

****

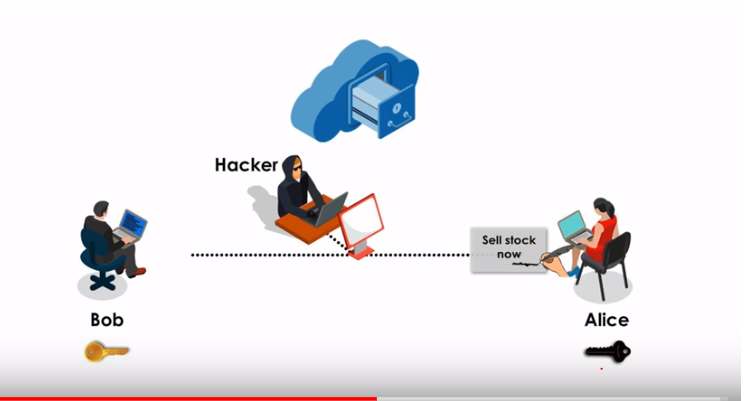
****

****

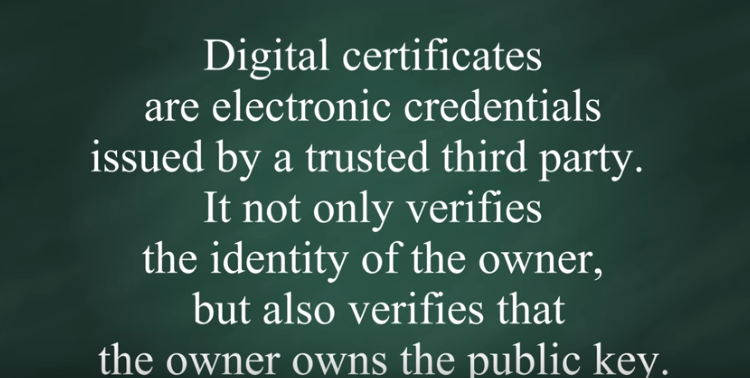
****



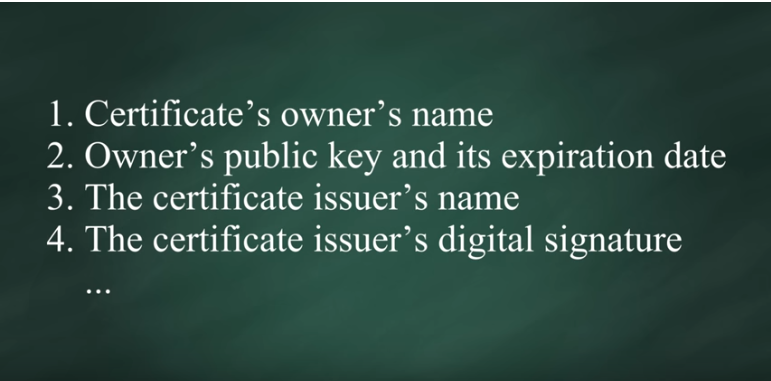
Digital signature is some problem , while sending hacker create pair of key and place the public key public place



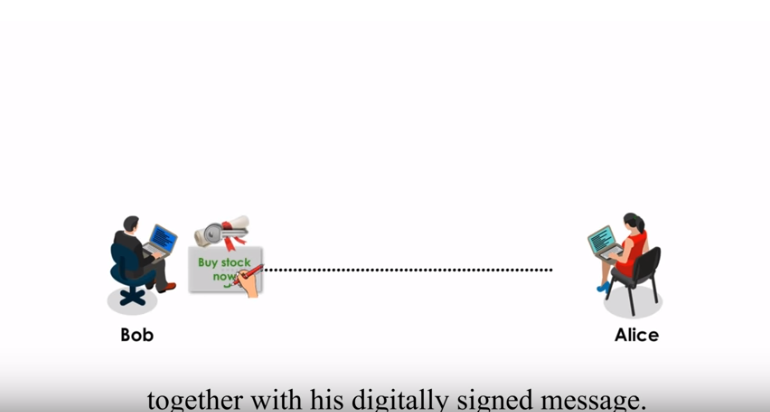
**Digital certificate:**



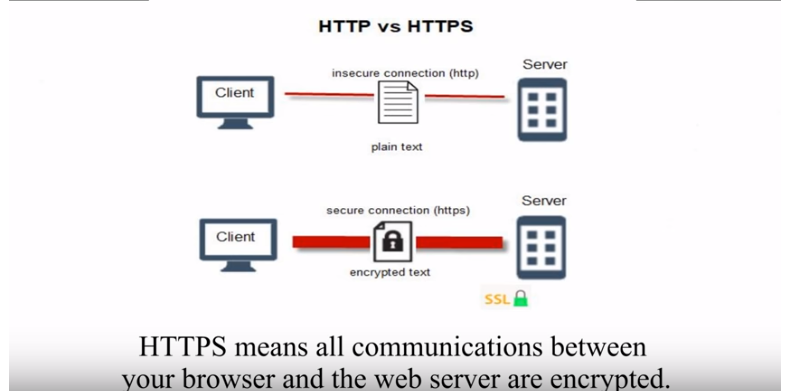
Certificate contain inside info

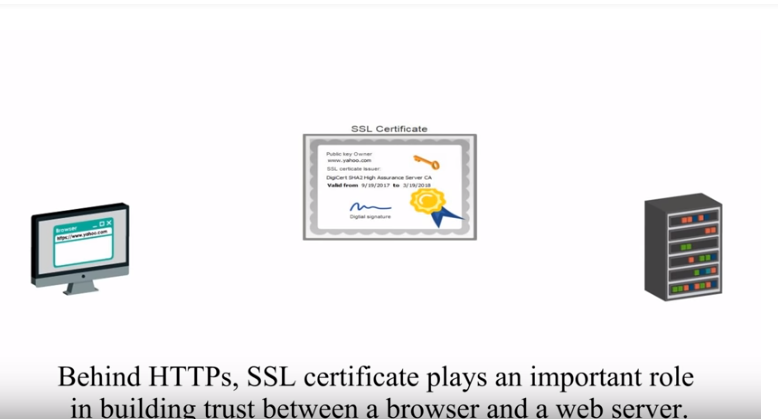


In this cars sender is not place public key in center place, sender send certificate along with public key

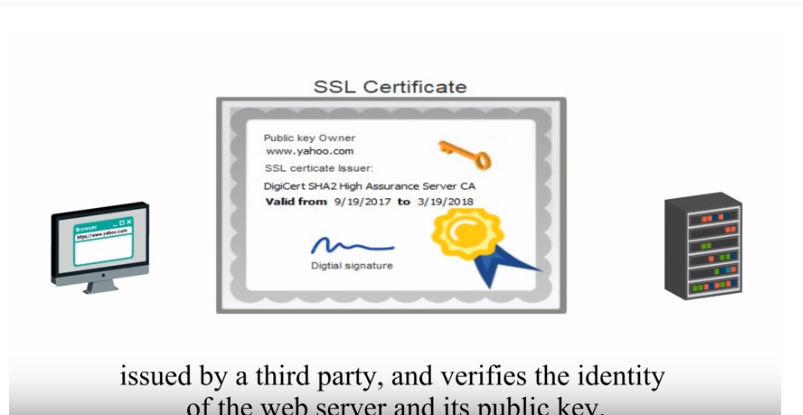


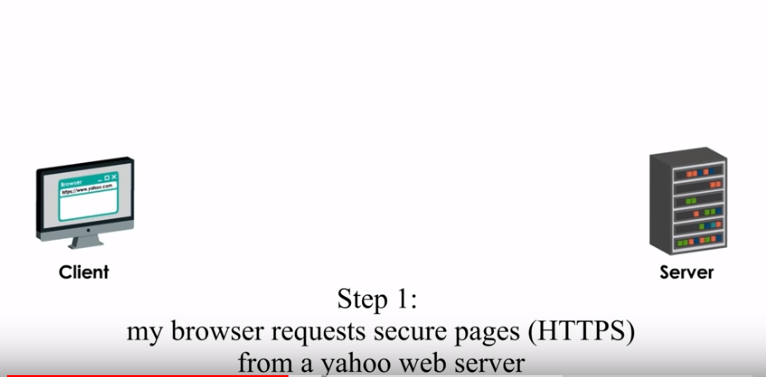
How to does SSL work.



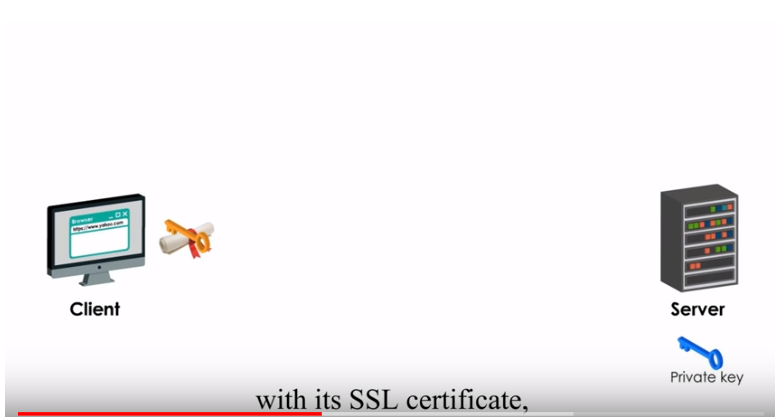


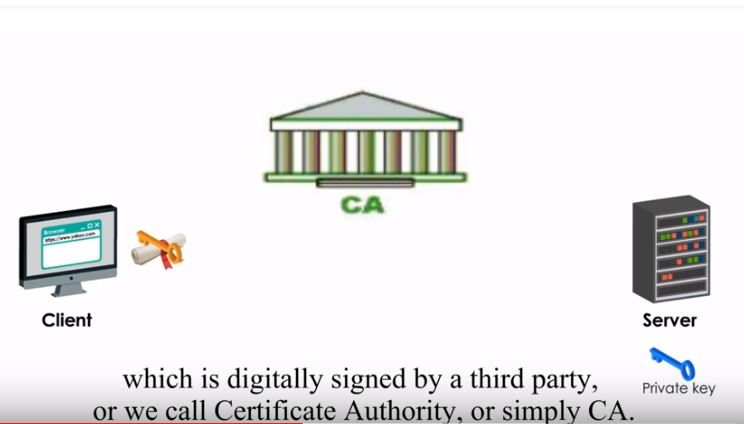


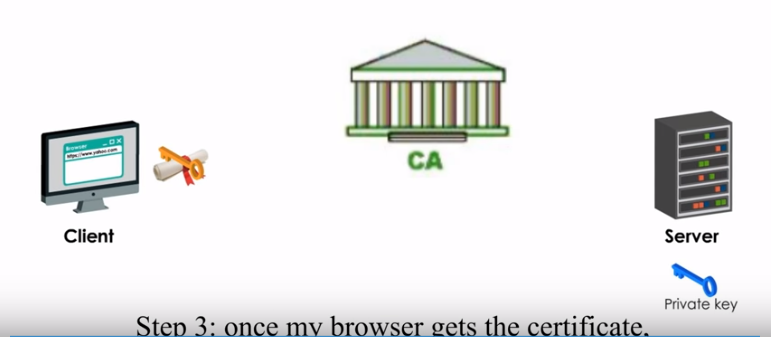




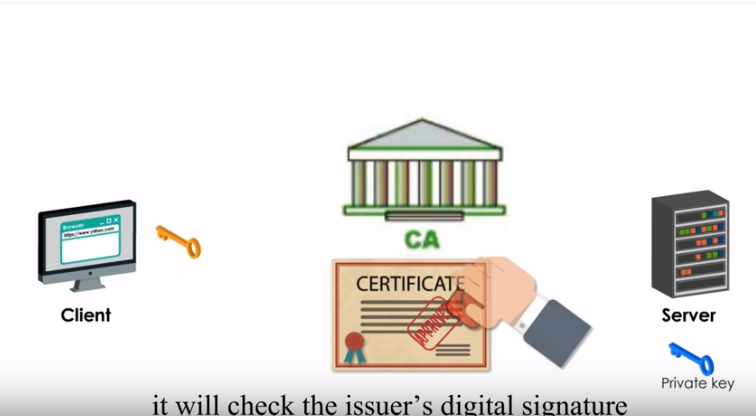
Yahoo server send public with ssl certificate

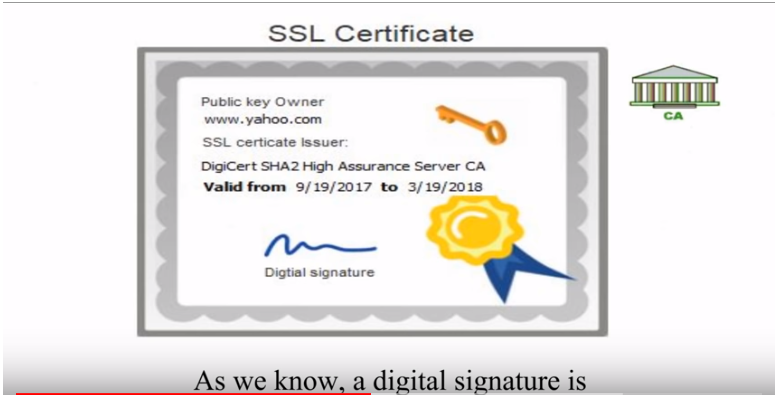






It will check certificate in CA





Created by Ca private key

