What is SSL (Secure Sockets Layer)

It’s a protocol for encrypting and securing communications that take place on the Internet. It's now replaced by an updated protocol called TLS (Transport Layer Security) some time ago.

The main use case for SSL/TLS is securing communications between a client and a server, but it can also secure email, VoIP, and other communications over unsecured networks.

Why use SSL?

If information such as email IDs, user IDs, passwords, credit/debit card details, bank account details get transmitted over an unprotected protocol, there is a significant risk of such private information coming into the hands of cybercriminals. Such interception of data being transmitted is called a Man-in-the-middle (MITM) attack.

That’s the reason we need to protect this process of Data Transmission.

What is an SSL certificate?

An SSL certificate is a file installed on a website’s origin server. It’s simply a data file containing the public key and the identity of the website owner, along with other information. Basically the details of the party to whom the certificate has been issued.

Information includes-
Domain Name, Certificate Validity Period, Certificate Authority (CA) Details, Public Key, Key Algorithm, Certificate Signature Algorithm,
SSL/TLS Version, Thumbprint, Thumbprint Algorithm,
Name of the organization, Website owner, Address,
City, State, Country

Without an SSL certificate, a website's traffic can't be encrypted with TLS.

What Does an SSL Certificate Do?

The SSL protocol determines the encryption for both the link and the data being transmitted. Browsers can interact with secured web servers using the SSL security protocol, but to do that they need the SSL Certificate for establishing a secure connection. The most common use of SSL certificates is secure web browsing via the HTTPS protocol.

What Is Encryption?

As we know SSL certificates facilitate Encryption.

But what is that ??
If you send any data on an HTTPS-enabled website, that piece of information is converted into an unreadable string of characters. For example, if your password is 1234, then it might be converted into something like ^%jfdgrt5/*u. This makes it

virtually impossible for any hacker to interpret the information, even if they manage to intercept the data somehow.

How does SSL/TLS work?

Let’s understand it with a very simple example.

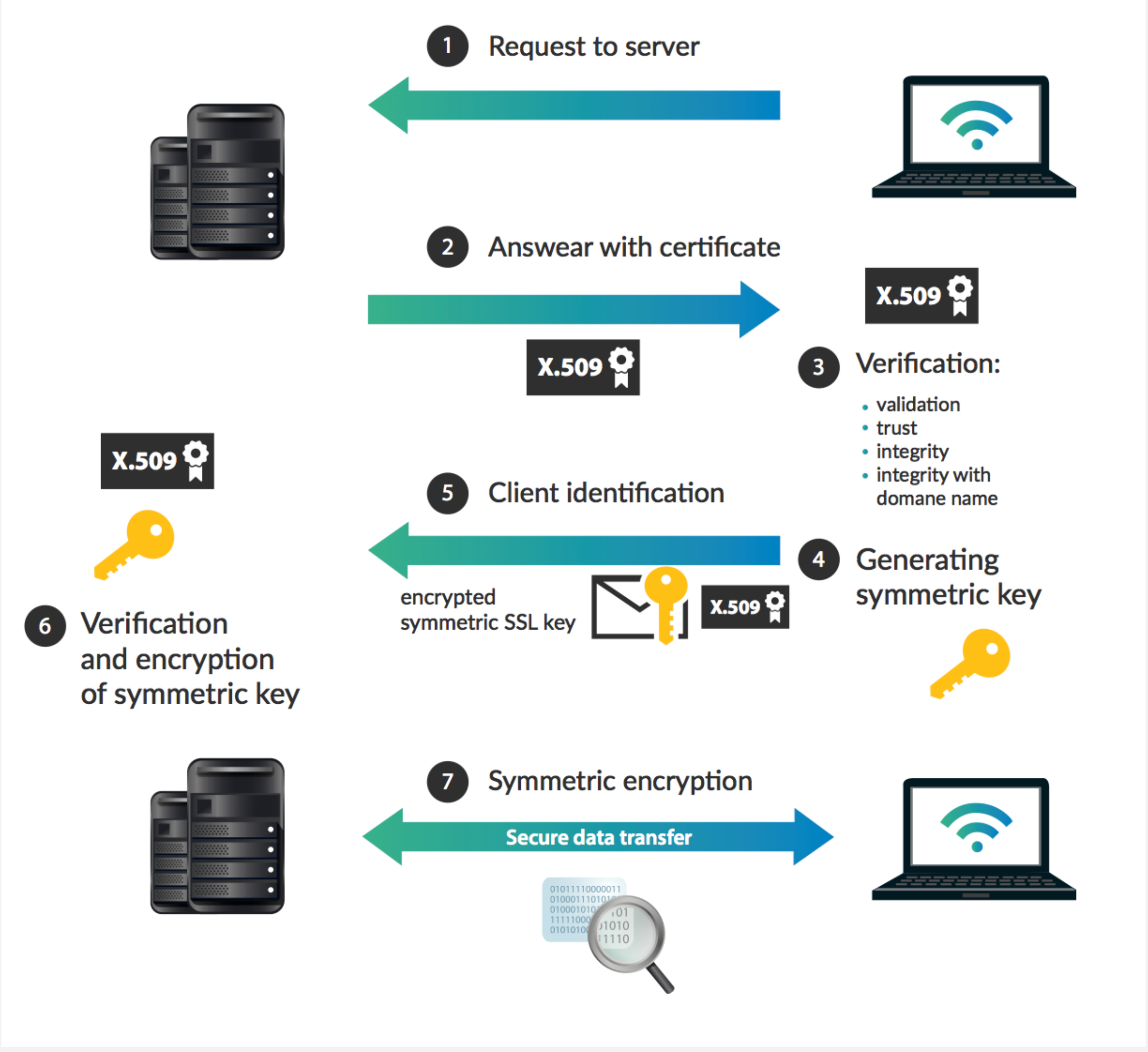
When you access a website, communication takes place between the web browser of your PC or mobile device and the webserver of the website. Information is then transferred from both sides.

Then the process of SSL/TLS handshake comes into the picture. TLS handshakes occur after a TCP connection has been opened via a TCP handshake. A TLS handshake also happens whenever any other communications use HTTPS, including API calls and DNS over HTTPS queries.

What is an SSL/TLS handshake?

TLS communication sessions begin with a TLS handshake.

Browser connects to the server, secured with SSL/TLS (https).
The server sends a copy of the SSL certificate, including the public key.
The browser checks the certificate and if it is valid it creates, encrypts, and sends back a symmetric session key using the server’s public key.
Server decrypts the symmetric session key using its private key and sends back an encrypted session key to start the encrypted session.


1 Request to server
2 Answear with certificate
X.509
X.509
3 Verification:
• validation
• trust
• integrity
• integrity with domane name
X.509
5 Client identification
encrypted symmetric SSL key
X.509
4 Generating symmetric key
6 Verification and encryption of symmetric key
7 Symmetric encryption
Secure data transfer

How does a website get an SSL certificate?

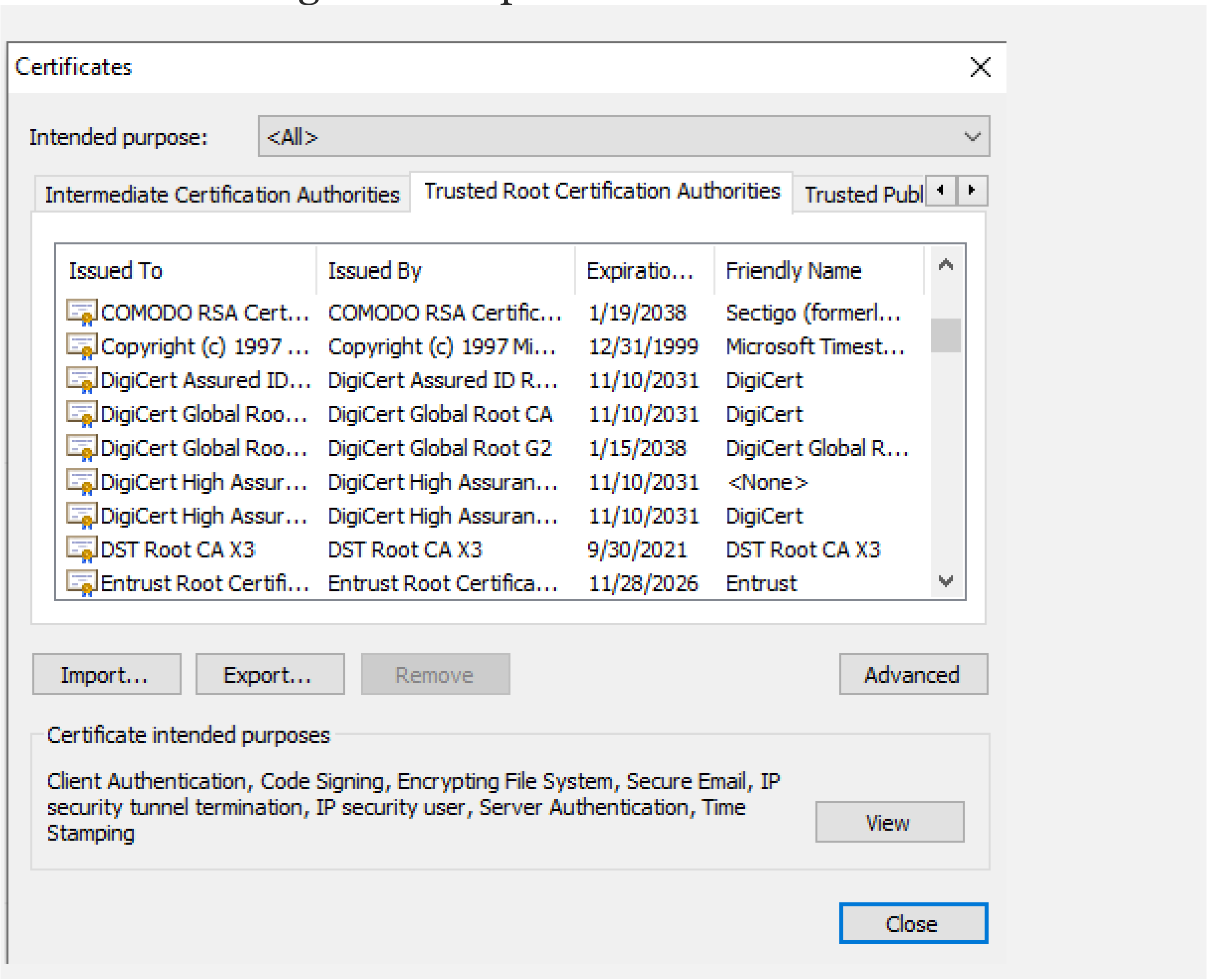
Website owners need to obtain an SSL certificate from a certificate authority, and then install it on their web server (often a web host can handle this process). A certificate authority is an outside party who can confirm that the website owner is who they say they are. They keep a copy of the certificates they issue.

What is the difference between HTTP and HTTPS?

The S in “HTTPS” stands for “secure.” HTTPS is just HTTP with SSL/TLS. A website with an HTTPS address has a legitimate SSL certificate issued by a certificate authority, and traffic to and from that website is authenticated and encrypted with the SSL/TLS protocol.

Where to find trusted certificate authority details on a Browser?

Here I am taking the example of Chrome on Windows ->



Certificates

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
COMODO RSA Cert...	COMODO RSA Certific...	1/19/2038	Sectigo (formerl...
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/31/1999	Microsoft Timest...
DigiCert Assured ID...	DigiCert Assured ID R...	11/10/2031	DigiCert
DigiCert Global Roo...	DigiCert Global Root CA	11/10/2031	DigiCert
DigiCert Global Roo...	DigiCert Global Root G2	1/15/2038	DigiCert Global R...
DigiCert High Assur...	DigiCert High Assuran...	11/10/2031	<None>
DigiCert High Assur...	DigiCert High Assuran...	11/10/2031	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	DST Root CA X3
Entrust Root Certifi...	Entrust Root Certifica...	11/28/2026	Entrust

Certificate intended purposes

Client Authentication, Code Signing, Encrypting File System, Secure Email, IP security tunnel termination, IP security user, Server Authentication, Time Stamping

Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
View
Close

How does my browser inherently trust a CA?

Your browser (and possibly your OS) ships with a list of trusted CAs. These pre-installed certificates serve as trust anchors to derive all further trust from. When visiting an HTTPS website, your browser verifies that the trust chain presented by the server during the TLS handshake ends at one of the locally trusted root certificates.

Does root certificates Expire?

Root certificates do expire, but they tend to have exceptionally long validity times (often about 20 years). You can expect that with an update of your browser or OS, you will get fresh root certificates before the old ones expire.