* [Community](https://community.sap.com/)
* [Topics](https://community.sap.com/topics)
* [Answers](https://answers.sap.com/index.html)
* [Blogs](https://blogs.sap.com/)
* [Events](https://community.sap.com/events)
* [Programs](https://community.sap.com/programs)
* [Resources](https://community.sap.com/resources)
* [What's New](https://community.sap.com/resources/what-is-new)
* [Home](https://www.sap.com/)
* [Community](https://community.sap.com/)
* [Blogs](https://blogs.sap.com/)
* [Ask a Question](https://answers.sap.com/questions/ask.html)
* [Write a Blog Post](https://blogs.sap.com/wp-admin/post-new.php)
* [Login / Sign-up](https://blogs.sap.com/wp-login.php?redirect_to=%2F2021%2F09%2F08%2Fdemystifying-ssl-tls%2F)

Personal Insights

[](https://people.sap.com/nitshukla28)

[NITISH KUMAR SHUKLA](https://people.sap.com/nitshukla28)

September 8, 2021 4 minute read

Demystifying SSL/TLS

065,470

As a critical component in integrations, We regularly use terms like SSL and TLS but recently i got a chance to dig deep into the basics and functioning of Secure Socket Layer (SSL) / Transport Layer Security (TLS).

In this blog post, we will be discussing about terminologies such as SSL, TLS, HTTPS, Certificates, Certification Authority etc. along with steps followed for the great SSL-TLS handshake between client and Server systems.

What are these?

**SSL –** This is the standard protocol/process for maintaining secure communication between two systems, safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, This is deprecated now.

**TLS –** This is a more secure and updated version to SSL. Its purpose is to provide security in communication between two or multiple parties.  Several versions of the protocol are widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible. This runs in Application layer in internet and is totally different from TCP (not to be confused with, which is a transport layer protocol). Latest version is TLS 1.3 defined in Aug, 2018.

**HTTPS –** This in simplest terms is, HTTP + S, which means addition of Security (S) to the ever-existing HTTP (Hyper Text transfer protocol).

Note: We’ll be using SSL for certificates terminology here for convenience as this is most commonly referenced term.

Why is security needed for communication?

1. **Server authentication issue –** As I believe, you would never be interested in talking to any great personality’s lookalike. On similar terms, any Client system (C-Ac) would never be interested in talking to a Server system which is not the actual system (S-Ac) itself and is instead a mal-intentioned Server (S-Ms) trying to mimic the actual server (S-Ac). Question arises – how to ensure that target system communicating is the authentic server and not a mimic server. Note: Proxy servers are not actual servers, but instead authentic servers entrusted by actual server to communicate on its behalf. Example – a banking site can easily be mimicked by any hacker and they get access to all the communications/actions intended for bank.
2. **Communication secrecy issue –** Again, no one likes a third person to be listening into the conversation taking place between two persons. Similarly, communication between C-Ac (Actual Client) and S-Ac (Actual Server) must be made in a manner that S-Ms/C-Ms don’t get to know what is being communicated between C-Ac and S-Ac. Example – what if hackers don’t get card details directly by snooping in between the communication intended for bank.

How is this security ensured?

Let’s think about point 2 from above first. To resolve secrecy issue, we need to ensure that data transfer between two parties employed in communication is encrypted while in the transit. For this communication process, Public Key encryption is used, and to communicate public key to client system (C-Ac) – SSL certificates are used. Additional benefit of using SSL certificates – only an authentic server will be in possession of a valid certificate. This is wrong, right? – yes it is, S-Ms can also keep same certificate as S-Ac since it is publicly available but that certificate will only be having public key as specified in certificate but not corresponding private key which is the responsibility of S-Ac to preserve, safeguard and ensure no compromise (point 1). This ensures both server authentication (Private key of certificate is available only to S-Ac) and security throughout communication (the great Public key encryption).  So, unless hackers can break public key encryption algorithm used and get corresponding private key, communication is safe.

Contents of an SSL certificate –

* The domain name that the certificate was issued for.
* Which person, organization, or device it was issued to.
* Which certificate authority issued it.
* The certificate authority’s digital signature.
* Associated subdomains.
* Issue date of the certificate.
* Expiration date of the certificate.
* The public key (the private key is kept secret)

Steps in this communication – The great SSL/TLS handshake –

Scenario – Client C-Ac requesting access to information on Server S-Ac/ communication is bi-directional.

**Step 1 –** Client C-Ac sends a hello message to Server S-Ac. This message includes SSL/TLS Version, Supported Encryption algorithms and Supported data compression algorithms.

**Step 2 –** Server S-Ac sends a hello message back to Client C-Ac. This message includes encryption algorithm, Digital/SSL Certificate having Public Key (Pub key) and Session ID.

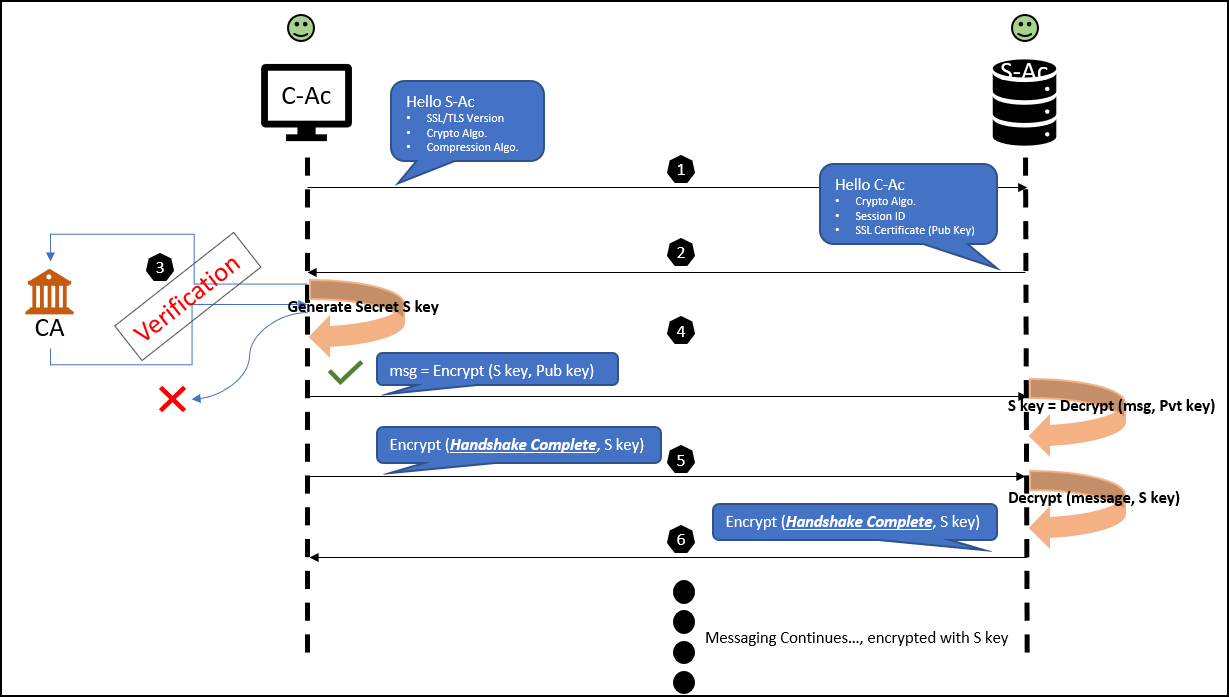
**Step 3 –** Client verifies SSL Certificate with its certifying authority (CA) to ascertain if the received digital certificate is valid and is generated by it. If CA acknowledges, The CA’s digital certificate establishes trust that the Server authenticating is authentic S-Ac.

**Step 4 –** Client C-Ac will generate a secret key (S Key), encrypt this key with public key (Pub key) received from Server SSL certificate (Step 2) and send it to Server S-Ac.

**Step 5 –** Client will send handshake completion message encrypted by secret key (S Key).

**Step 6 –** Server S-Ac will decrypt Client message using Private key corresponding to Public key (Pub key) and read the handshake completion message. Server S-Ac will send out handshake completion message encrypted with secret key (S Key) and send to Client.

Secret Key (S Key) is to be used for all further communications taking place in the session.



Potential Breach attempts and how SSL prevents them –

* S-Ms receives request in Step 1 and send backs a certificate of its own. CA will reject this in verification Step 3.
* S-Ms receives request in Step 1 and send back digital certificate having its own Public Key, Pub-Ms Key. CA will reject this request as the certificate is corrupt or not a valid one anymore.
* S-Ms receives request in Step 1 and send back a certificate of S-Ac. CA will authenticate this request, but S-Ms won’t be able to receive S Key since it doesn’t possess Pvt Key corresponding to Pub key.
* S-Ms cannot get Secret Key (S Key) because this is encrypted by Pub Key, for which only S-Ac has the Pvt key.
* S-Ms cannot access information in message since it doesn’t possess Secret Key (S Key).

I hope you found this post helpful in understanding the basics of SSL/TLS. Feel free to provide your valuable feedback and suggestions to this blog post in comments section. In case you have any questions with respect to SSL/TLS, post a comment.

Stay tuned or follow profile for further similar blogs.

References:

1. [TLS – Wiki](https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0)
2. [TLS Handshake – YouTube](https://www.youtube.com/watch?v=sEkw8ZcxtFk)
3. [SSL – Verisign](https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml)
4. [SSL – CloudFlare](https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/)
5. [SSL/TLS – Digicert](https://www.websecurity.digicert.com/en/in/security-topics/what-is-ssl-tls-https)
6. [SSL – Oracle](https://docs.oracle.com/cd/E18686_01/coh.37/e18681/ssl.htm#COHSG5421)

FollowLikeRSS Feed

Alert Moderator

**Assigned tags**

* [Cloud Integration](https://blogs.sap.com/tags/67837800100800006801/)
* [SAP Integration Suite](https://blogs.sap.com/tags/73554900100800003241/)
* [SAP Process Integration](https://blogs.sap.com/tags/01200615320800000719/)

Similar Blog Posts

* [JMS Adapter ActiveMQ (AMQ) with SSL/TLS on PI 7.4](https://blogs.sap.com/?p=375503)

By [Former Member](https://people.sap.com/former.member)Sep 30, 2016

* [How to check supported outbound cipher suites](https://blogs.sap.com/2016/09/29/how-to-check-supported-outbound-cipher-suites/)

By [Markus Schalk](https://people.sap.com/markus.schalk)Sep 29, 2016

* [Believe it or not, SSL Enabling for your PI 7.31 EHP1(Java only) is a cake walk now.](https://blogs.sap.com/?p=84945)

By [Anil Veepuri](https://people.sap.com/anil.veepuri)May 13, 2013

Related Questions

* [SCPI - authentication header](https://answers.sap.com/questions/13464981/scpi-authentication-header.html)

By [Morten Nielsen](https://people.sap.com/morten.nielsen_danfoss.com)Aug 25, 2021

* [org.apache.commons.net.ftp.FTPConnectionClosedException: Connection closed without indication.](https://answers.sap.com/questions/13399784/orgapachecommonsnetftpftpconnectionclosedexception.html)

By [Sweta Gohil](https://people.sap.com/swetagohil)Jun 03, 2021

* [SSL certificate of Successfactor required in SAP CPI?](https://answers.sap.com/questions/13313529/ssl-certificate-of-successfactor-required-in-sap-c.html)

By [Aarti Kumari](https://people.sap.com/aarti.a.kumari)Mar 08, 2021

Be the first to leave a comment

You must be [Logged on](https://blogs.sap.com/wp-login.php?redirect_to=2021/09/08/demystifying-ssl-tls) to comment or reply to a post.

Find us on

* [Privacy](http://sap.com/about/legal/privacy.html)
* [Terms of Use](http://sap.com/corporate/en/legal/terms-of-use.html)
* [Legal Disclosure](http://sap.com/about/legal/impressum.html)
* [Copyright](http://sap.com/about/legal/copyright.html)
* [Trademark](http://sap.com/about/legal/trademark.html)
* Cookie Preferences
* [Newsletter](https://www.sap.com/cmp/nl/sap-community-voice/index.html)
* [Support](mailto:sapnetwork@sap.com)