**Titles:**

**How Does SSL Works?**

**Understanding SSL: How Secure Connections Protect Your Data**

**The Mechanics of SSL: Ensuring Online Security and Privacy**

***Keywords***: how does ssl work, what is ssl, how does secure socket layer work,

What is ssl certificate?

**Introduction:**

SSL Certificate (Secure Socket Layer certificate): A digital certificate is used to establish a secure and encrypted connection between a web server and a client's browser. This means any unauthorized person cannot access the data being passed between the server and the user in transit. It protects any data traveling back and forth between the servers to a user; nobody can eavesdrop or alter it.

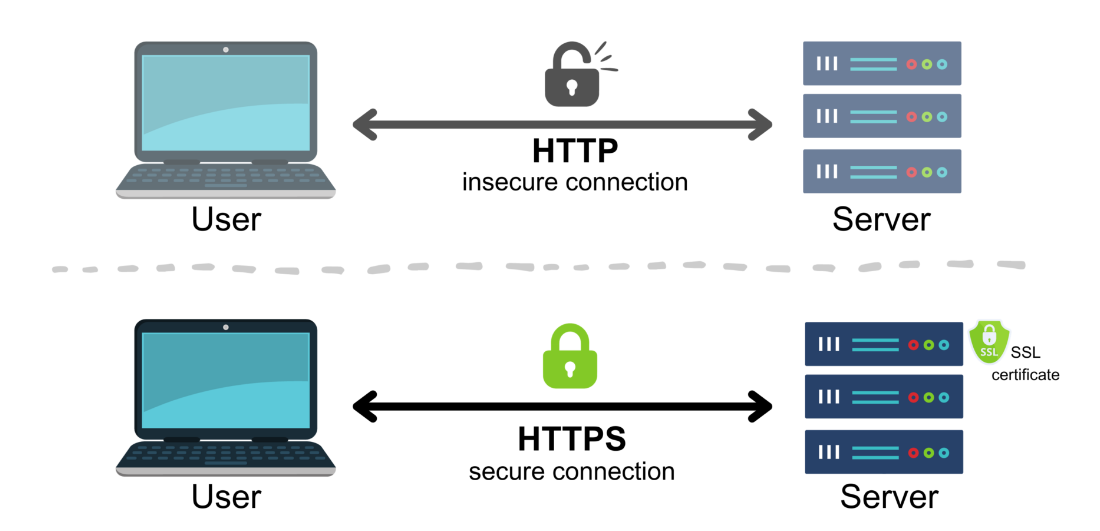
In an age where web security is the most critical thing. SSL Certificates are an essential part of web application security to secure your data transactions between server-to-server and client-to-server communication over a network connection.

**What is SSL?**

SSL protocol is a technology that protects data using strong encryption between the server and the client, such as a browser. It assures that the data being transmitted between these two endpoints remains private and secure.

**What is SSL Certificate?**

SSL certificate is a digital certificate that verifies the identity of a website and allows for an encrypted connection between your web server and users. When a site uses an SSL certificate, the URL begins with "https://," and most browsers display a little padlock in their address bar to show that your connection is secure. SSL Certificates are very important to secure personal information, build up user trust, and increase the reputation of a site.

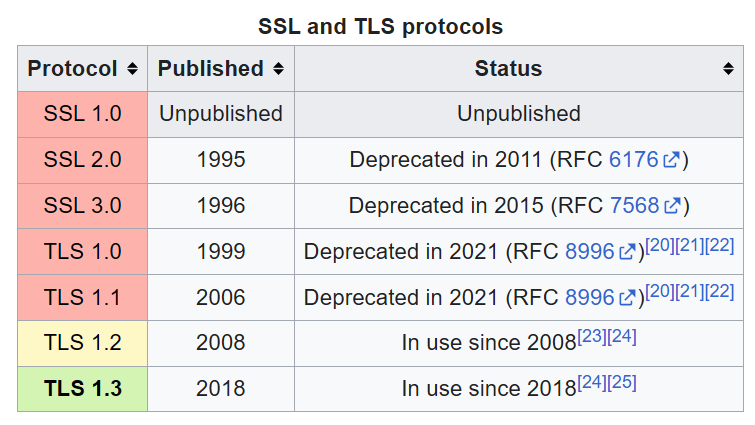


https://www.cloudns.net/blog/ssl-certificate/

**SSL timeline**

Below is a timeline for the evolution of SSL.

* SSL protocol, developed by Netscape in the 1990s, made digital conversation more manageable and secure. SSL v1.0 was never fixed, so it did not have a release.
* SSL v2 was released by Netscape in 1995. This version still needed improvement and had many flaws.
* SSL v3.0 was released in 1996, and it has corrected the flaws of SSL v2.0. The feature has since seen incredible enhancements and changed the way the internet works. As of 2015, up to SSL version 3.0 has been deprecated due to the introduction of TLS versions.



https://en.wikipedia.org/wiki/Transport\_Layer\_Security

* The Internet Engineering Task Force (IETF) developed the TLS protocol as an upgrade to SSL. It was released in 1999, based on SSL v3.0, with fewer changes.
* TLS v1. However, the second version (TLS 1) also came out in 2006. However, it was replaced by TLS v2.0 in 2008. Finally, 11 years later, TLS v1.3 is in practice now, and it was released in 2018.
* In March 2020, browser authorities like Google, Mozilla, Apple, and Microsoft deprecated TLS 1.0 and 1.1 versions. At present, TLS 1.2 and 1.3 are active versions.

**Why SSL is important?**

SSL certificate is essential for several reasons, as it offers data integrity, authenticity, and confidentiality.

An SSL certificate is required to maintain the security of user data, prove website ownership, protect against unauthorized data access, and convey trust to users.

Websites, when asking users to sign in and enter financial or personal details, should need an SSL certificate to keep their data secret. SSL certificates keep online communications confidential and give users confidence that the website is genuine to protect their information.

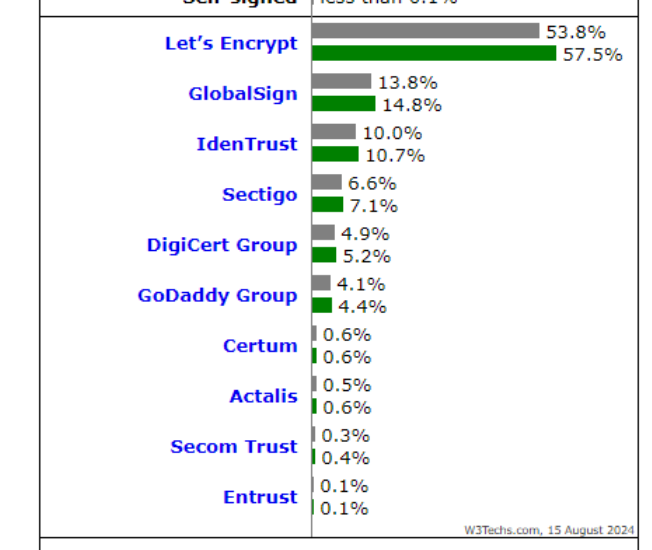


<https://www.globalsign.com/en/blog/the-difference-between-http-and-https>

You need an SSL certificate for a HTTPS web address. In essence, HTTPS is an abbreviation for the secure version of HTTP, which makes all data on such websites encrypted via SSL. Most browsers now mark HTTP sites as 'not secure' when there is no SSL certificate installed on the site. It communicates clearly to users that a site might not be legitimate and suggests businesses switch to HTTPS.

Let us look at **a few** [**statistics**](https://sslinsights.com/ssl-certificates-statistics/#:~:text=317%2C772%2C074%20SSL%20Certificates%20Detected%20on,with%20nearly%2014%20million%20certificates) **about SSL certificates** that show how essential SSL certificates are.

* There are 317 million SSL certificates installed across the world.
* The USA holds the highest number of SSL certificates, 34 million, whereas Germany is second with 14 million.
* Almost 90% of SSL certificates are issued by the six top certificate authorities.
* The global market of certificate authorities will reach $282 million by 2028 year.

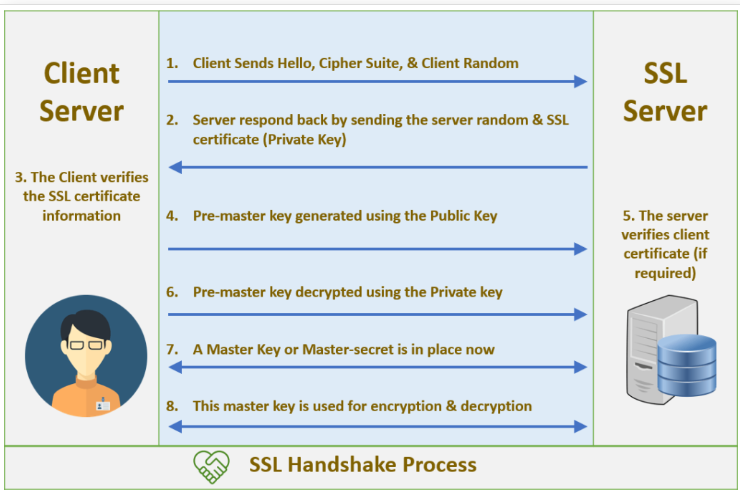


<https://sslinsights.com/ssl-certificates-statistics/#:~:text=317%2C772%2C074%20SSL%20Certificates%20Detected%20on,with%20nearly%2014%20million%20certificates>.

**How Does SSL work?**

SSL offers assurance about data integrity, confidentiality, and authentication by encrypting the data sent between the server and the browser. Many people have questions about how the secure socket layer works. Here is the answer.

* When a browser is trying to start a secure connection, it sends a "ClientHello" message to the server in the first stage (ClientHello). On the other hand, it covers all the vital details; one of them is the SSL/TLS version, which can support cipher suites that can be used.
* Next, the server sends a "ServerHello” message, providing the highest SSL/TLS version and cipher suite that the two parties support.



[How SSL/TLS Handshake Works? | Jian Huang](https://ijianhuang.wordpress.com/2020/04/18/how-ssl-tls-handshake-works/)

* The server then shows its digital certificate, which a Certificate Authority (CA) has verified as a fact of authenticity.
* Then, the browser then verifies the server’s certificate. Once it verifies, it uses the server’s public key to encode a ‘premaster secret’ (a unique session key) and send them back to the server.
* Finally, the server takes its private key and decrypts this premaster secret. Therefore, the server and the client calculate the session key to use symmetric encryption for all future communications.

**Types of SSL Validations:**

Each SSL certificate is made for specific use cases and is suitable for different websites or blogs.

**Domain Validation:**

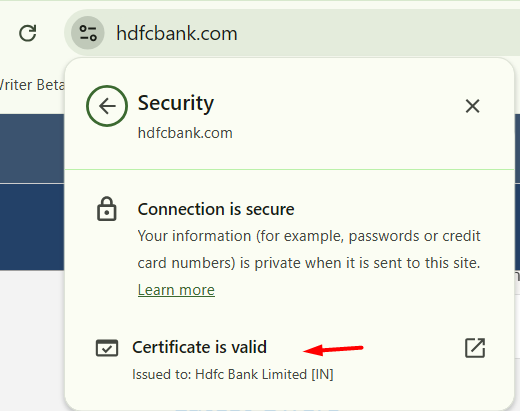
Domain ownership verification (DV) is the simplest form of SSL certificate validation and is only applicable for validating domain ownership by email validation, file-based validation, or CNAME-based authentication. This is usually done through email verification. No further investigation is required on behalf of the certificate authority. In addition, it is the cheapest and fastest way to obtain an SSL certificate.

**Organization Validation:**

Organization Validation is one-step ahead when it comes to validation. The CA (Certificate Authority) will also validate your domain and ensure that your business is legitimate. For that, the CA can contact you or your business. However, the CA makes sure that you own the domain and that it relates to a legally registered business. The CA can perform telephone verification for further verification. OV certificates are seen by all as very reliable.

**Extended Validation**:

Extended validation is more than a domain validation certificate; it validates a business entity with a strict process. A validated company name can be seen when a user clicks on a padlock. Users gain more trust, and it establishes authenticity towards your website. The CA verifies operational existence, physical address verification, telephone verification, and domain authentication to issue an Extended Validation certificate.



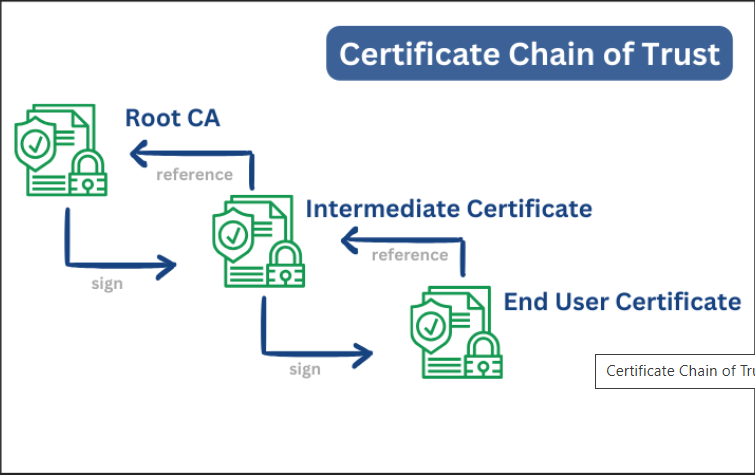
<https://www.hdfcbank.com/>

**Chain of trust**

A chain of trust in an SSL certificate protects the authenticity and integrity of a website’s identity when linked through a chain of trust to a trusted root CA. This chain allows browsers and operating systems to authenticate the origin of sites and determine if a site is legitimate and trustworthy. The chain of trust works through a hierarchical structure with three main components:

**1. Root Certificate Authority (Root CA)**

The Root CA is a trusted entity that signs and issues certificates. These are Self-Signed, meaning they can self-validate their certificates. Operating systems and browsers have preinstalled root certificates, creating a foundation of trust.



<https://sslinsights.com/what-is-the-certificate-chain-of-trust/>

**2. Intermediate Certificate Authority (Intermediate CA)**

The Root CA does not directly issue certificates to end entities. Therefore, it assigns this task to Intermediate CAs.

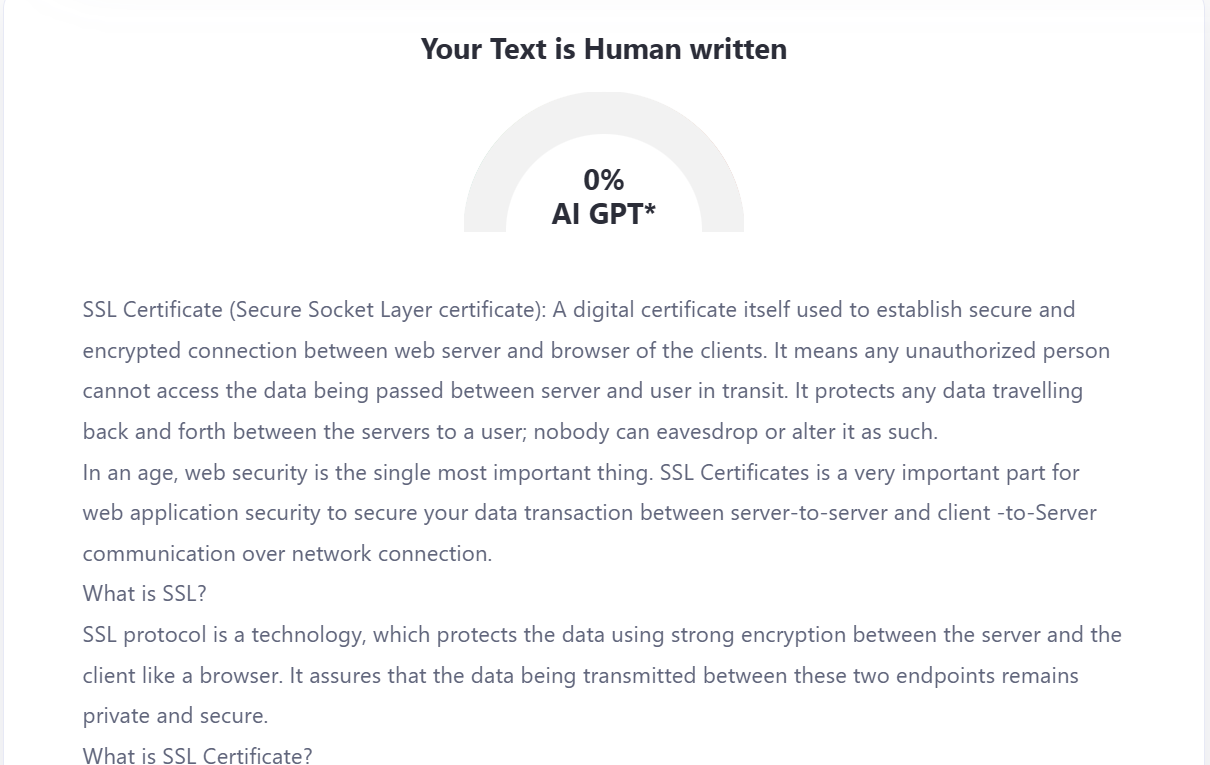
A Root CA is the trust one for issuing certificates to the intermediate CAs, which are then trusted to sign server certificates.

**3. Server Certificate**

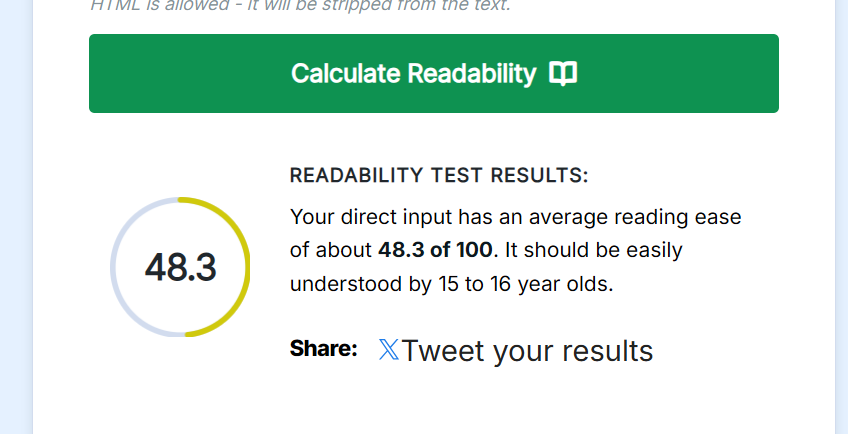
It is issued to the server itself (for the site) in order to set up the encrypted SSL/TLS connection, and an Intermediate CA signs it.

**Conclusion**:

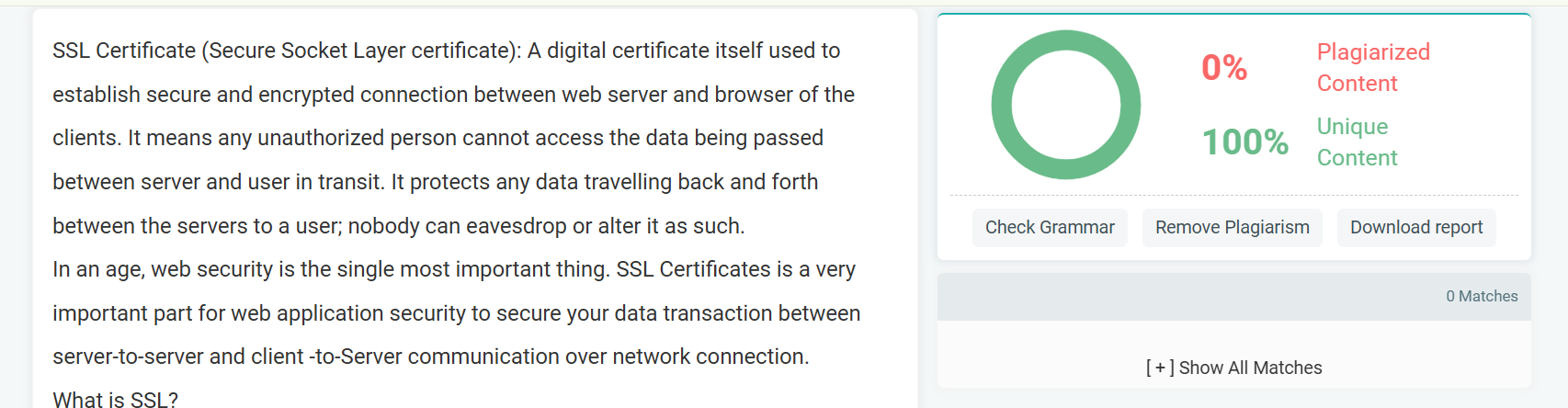
SSL secures communication over the web with a robust encryption. This article explains how SSL works, which we wish would help for knowledge seekers. Today, SSL has been replaced by TLS but its principles remain the same.



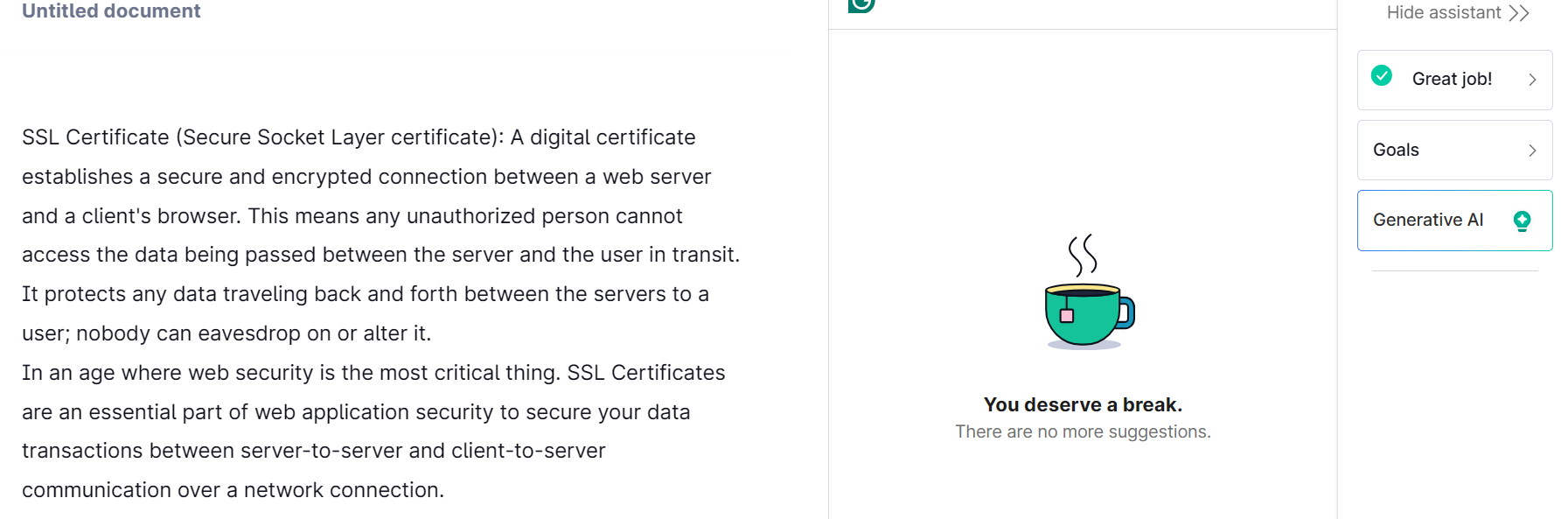
[**https://www.zerogpt.com/**](https://www.zerogpt.com/)



[**https://www.webfx.com/**](https://www.webfx.com/)



[**https://www.prepostseo.com/plagiarism-checker**](https://www.prepostseo.com/plagiarism-checker)



**Grammarly.com**