difference between http to https

Security:

HTTP: HTTP is not secure by default. Data transmitted over HTTP is sent in plain text, making it susceptible to interception and eavesdropping. This lack of encryption means that sensitive information, such as login credentials, credit card numbers, and personal data, can be easily intercepted by malicious actors.

HTTPS: HTTPS, on the other hand, is designed to provide a secure and encrypted connection between the user's browser and the web server. It uses protocols like SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt data, ensuring that it cannot be easily intercepted or tampered with in transit. This encryption helps protect the confidentiality and integrity of the data being transmitted.

Data Integrity:

HTTP: HTTP does not provide any mechanism for ensuring data integrity during transmission. Data can be modified or corrupted without detection.

HTTPS: HTTPS ensures data integrity through cryptographic hashing. If data is tampered with during transmission, it will be detected, and the connection may be terminated.

Authentication:

HTTP: HTTP does not provide strong authentication of the web server, making it vulnerable to man-in-the-middle attacks. Users can't be sure that they are connecting to the intended website.

HTTPS: HTTPS provides authentication through digital certificates issued by trusted Certificate Authorities (CAs). When you visit a website using HTTPS, your browser checks the certificate to verify the identity of the server. This helps users trust that they are connecting to the correct website.

Trust and SEO:

HTTP: Modern web browsers may flag HTTP websites as "Not Secure," which can erode trust with users. Additionally, search engines like Google may penalize HTTP sites in search rankings.

HTTPS: HTTPS websites are considered more trustworthy by users and search engines. Google, for example, has used HTTPS as a ranking factor, so HTTPS can positively impact SEO.

In summary, the key difference between HTTP and HTTPS is the level of security and privacy they offer. HTTPS is the recommended choice for websites, especially those that handle sensitive information, to protect data and provide a secure and trusted browsing experience for users.


http://www.example.com
password: abc123
Helen
HTTP
Without password encryption
Hacker see "abc123"


https://www.example.com
password: abc123
Carol
HTTPS
With password encryption
Hacker see "xyaerXzabc"

How Server Connect to HTTPS Web?

A server connects to an HTTPS (Hypertext Transfer Protocol Secure) website through a series of steps to establish a secure and encrypted connection. Here's a simplified overview of the process:

1. Client Hello: When a client (typically a web browser) initiates a connection to an HTTPS website, it sends a "Client Hello" message to the server. This message contains information about the client's capabilities and supported encryption algorithms.

2. Server Hello: The web server responds with a "Server Hello" message, selecting the best encryption algorithm and other parameters from the client's list. It also sends its digital certificate, which includes its public key.

3. Certificate Verification: The client checks the server's digital certificate to ensure it's valid and signed by a trusted Certificate Authority (CA). This step establishes trust in the server's identity.

4. Key Exchange: The client generates a random symmetric encryption key and encrypts it using the server's public key from the certificate. This key will be used to encrypt and decrypt data during the session. This process is known as the key exchange.

5. Session Key: Both the client and server now have a shared secret session key, which is used to encrypt and decrypt the data exchanged during the session. This ensures data confidentiality and integrity.

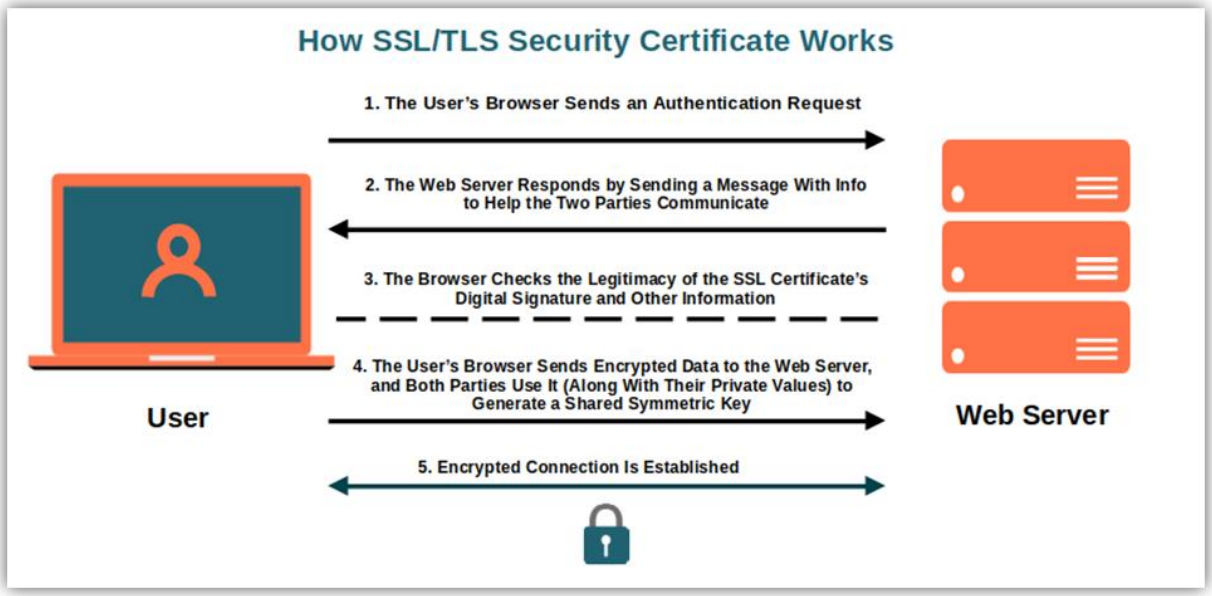
6. Encrypted Data Transfer: All data exchanged between the client and server is encrypted using the session key. This encryption prevents unauthorized access to the data while it's in transit.

7. Secure Data Transfer: With the secure connection established, the client and server can communicate securely, and the web page's content is sent over this encrypted connection.

8. Data Decryption: On the client side, the received data is decrypted using the session key, making it accessible to the user's browser.

9. Page Rendering: The web browser renders the web page for the user to interact with, ensuring that the content remains confidential and unaltered during transmission.

This process ensures the security and privacy of data exchanged between the client and server, protecting against eavesdropping and tampering by malicious actors. It's essential for secure online transactions, sensitive information transfer, and maintaining user trust on the internet.


How SSL/TLS Security Certificate Works
1. The User's Browser Sends an Authentication Request
2. The Web Server Responds by Sending a Message With Info to Help the Two Parties Communicate
3. The Browser Checks the Legitimacy of the SSL Certificate's Digital Signature and Other Information
4. The User's Browser Sends Encrypted Data to the Web Server, and Both Parties Use It (Along With Their Private Values) to Generate a Shared Symmetric Key
5. Encrypted Connection Is Established
User
Web Server

HTTPS encryption with SSL?

HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP, the protocol used for transmitting data over the internet. It ensures that the data exchanged between a user's web browser and a website is encrypted and secure. SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are cryptographic protocols used to establish secure communication channels over the internet.

Here's how HTTPS encryption works with SSL/TLS:

1. Handshake: When you connect to a website using HTTPS, your browser and the web server perform a handshake. During this process, they agree on encryption methods and exchange encryption keys.

2. Encryption: Once the handshake is complete, all data exchanged between your browser and the web server is encrypted. This means that even if someone intercepts the data, they cannot read it without the encryption key.

3. Data Transmission: Encrypted data is transmitted securely over the internet.

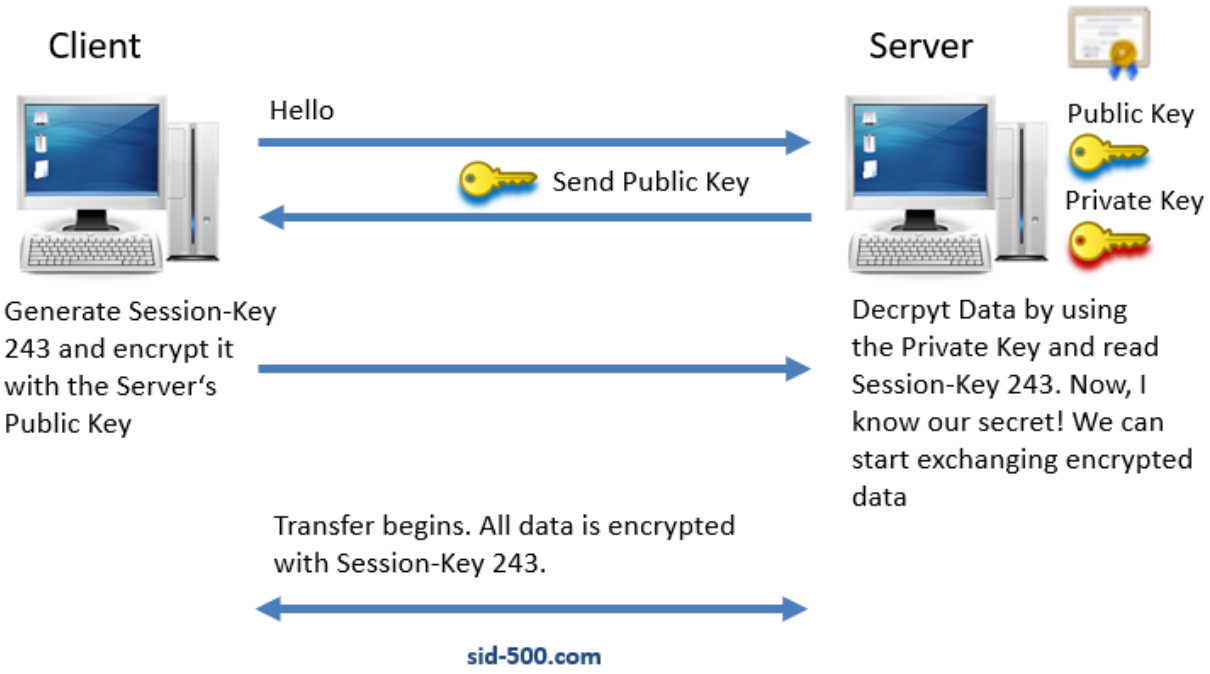
4. Decryption: When the data reaches the web server, it is decrypted using the encryption key. This ensures that the server can understand and process the data.

This encryption process provides confidentiality and integrity for the data transmitted between your browser and the website. It helps protect sensitive information like login credentials, credit card numbers, and personal data from being intercepted by malicious actors.

SSL/TLS certificates, issued by trusted Certificate Authorities (CAs), are essential for establishing the authenticity of the website and ensuring that the encryption is trustworthy. When you visit a website with HTTPS, your browser checks the website's SSL/TLS certificate to verify its authenticity.

In summary, HTTPS encryption with SSL/TLS is crucial for securing online communication and protecting sensitive information. It's widely used to ensure data privacy and security on the internet.

SSL Encryption (HTTPS)



Has the ssl certificate expired and the site has become vulnerable?

If an SSL certificate for a website expires, it can potentially make the site vulnerable in several ways:

1. **Loss of Encryption**: The primary purpose of an SSL certificate is to encrypt the data exchanged between a user's browser and the website's server. When the certificate expires, this encryption is no longer in place. As a result, any data transmitted between the user and the site becomes vulnerable to interception by malicious actors.

2. **Browser Warnings**: Most modern web browsers will display a warning message to users when they visit a site with an expired SSL certificate. This warning may deter visitors from accessing the site, as it suggests potential security risks.

3. **Loss of Trust**: SSL certificates also serve as a trust indicator. They confirm the identity of the website, indicating that it is operated by a legitimate entity. An expired certificate can erode user trust, as it raises questions about the site's authenticity.

4. **Search Engine Impact**: Search engines like Google may penalize websites with expired SSL certificates in their search rankings. This can lead to a decrease in organic traffic to the site.

To mitigate these risks, website owners should regularly monitor and renew their SSL certificates before they expire. Many certificate authorities offer notifications and auto-renewal options to help with this. Additionally, it's essential to keep SSL certificates up to date to maintain the security and trustworthiness of the website.

If you encounter a site with an expired SSL certificate, it's advisable not to enter sensitive information on that site, and you should exercise caution when interacting with it.