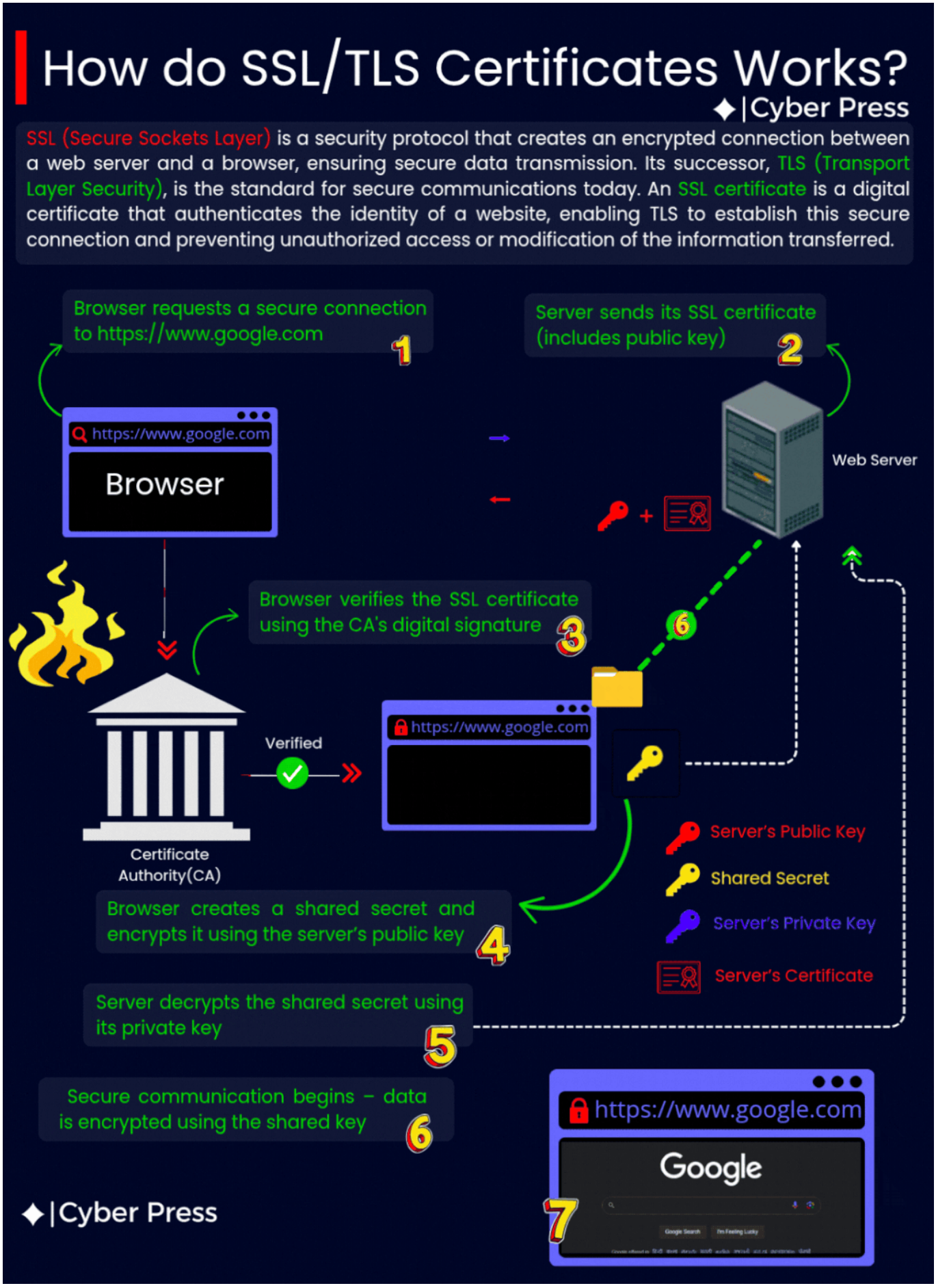
SSL - TLS


How do SSL/TLS Certificates Works?
✦|Cyber Press
SSL (Secure Sockets Layer) is a security protocol that creates an encrypted connection between a web server and a browser, ensuring secure data transmission. Its successor, TLS (Transport Layer Security), is the standard for secure communications today. An SSL certificate is a digital certificate that authenticates the identity of a website, enabling TLS to establish this secure connection and preventing unauthorized access or modification of the information transferred.
Browser requests a secure connection to https://www.google.com
1
Server sends its SSL certificate (includes public key)
2
https://www.google.com
Browser
Web Server
Browser verifies the SSL certificate using the CA's digital signature
3
Verified
Certificate Authority(CA)
https://www.google.com
6
Server's Public Key
Shared Secret
Server's Private Key
Server's Certificate
Browser creates a shared secret and encrypts it using the server's public key
4
Server decrypts the shared secret using its private key
5
Secure communication begins – data is encrypted using the shared key
6
https://www.google.com
Google
7
✦|Cyber Press

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/ssltls

Last update: **2026/09/08 13:34**