SSL/TLS (Secure Sockets Layer / Transport Layer Security)

1. Définition

- **SSL (Secure Sockets Layer)** : SSL est l'ancien protocole de sécurisation des échanges sur Internet utilisé.
- **TLS (Transport Layer Security)** : TLS lui est le remplaçant moderne de SSL, plus sécurisé et toujours utilisé.

Le but de ce protocole est de chiffrer les communications entre deux machines (souvent client-serveur) pour garantir :

Confidentialité : Les données sont chiffrées donc un attaquant ne peut pas les lire.,

Intégrité : Aucune modification des données n'est possible pendant le transfert.

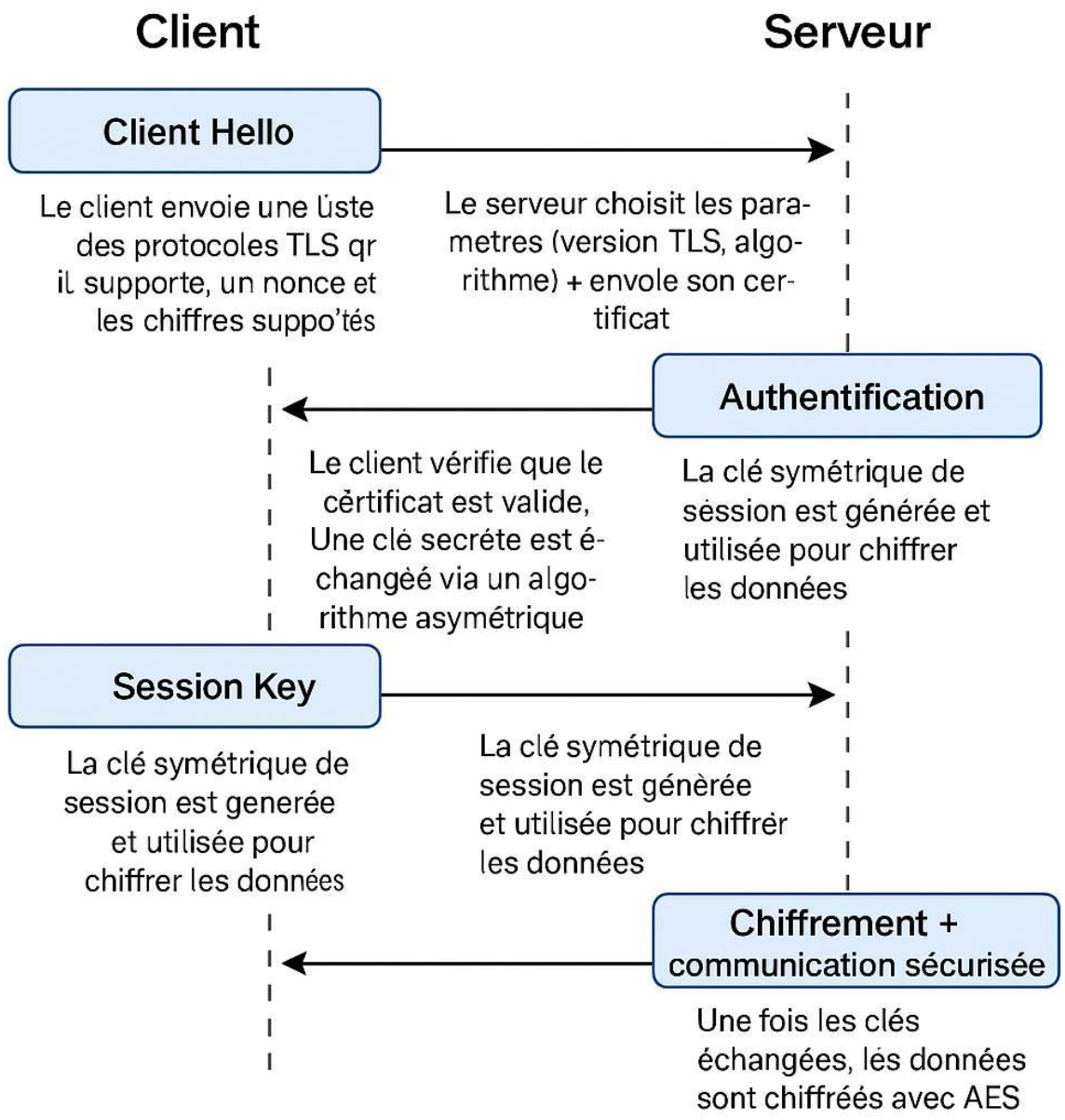
Authenticité : On vérifie l'identité du serveur (et parfois du client) via un certificat.

Voici le fonctionnement du handshake TLS

But global : Permet à un client (ex. navigateur) et un serveur (ex. site web) de **s'**authentifier mutuellement, d'échanger une clé de session de manière sécurisée, puis de chiffrer les communications avec cette clé.

Client ↔ Serveur (ex : navigateur ↔ site web)

1. **Client** :
   - Le client envoie une liste des protocoles TLS qu'il supporte (ex. TLS 1.2 ou 1.3).
   - Il envoie aussi un nonce (valeur aléatoire) servant plus tard à la génération des clés et ses chiffres (algorithmes) supportés**.**
2. **Serveur** :
   - Le serveur choisit les paramètres (TLS version, algorithme négociée à partir de celles proposées par le client) + son propre nonce (autre valeur aléatoire) + envoie son certificat (signé par une autorité de certification CA, comme Let's Encrypt, Comodo… valide dans le temps, correspondant au nom du domaine demandé.
3. **Authentification + Clé** :
   - Le client vérifie que le certificat est valide via une chaîne de confiance.
   - Une **clé secrète** (ou pré-master key) est échangée via un algorithme asymétrique (ex : RSA, Diffie-Hellman).
4. **Session Key** :
   - La clé symétrique de session est générée et utilisée pour chiffrer les données.
5. **Chiffrement + communication sécurisée** :
   - Une fois les clés échangées, les données sont chiffrées avec AES ou ChaCha20.



SSL	**TLS**
Ancien protocole	Nouveau protocole
Moins sécurisé	+ Sécurisé
SSL 2.0/3.0 obsolètes	TLS 1.2 / TLS 1.3 sont les versions actuelles
Utilise RC4 (faible)	Utilise AES, ChaCha20

⚠ **SSL est aujourd'hui obsolète et vulnérable (ne pas utiliser).**

Le Certificat SSL/TLS

- Format X.509
- Délivré par une autorité de certification (CA) comme Let’s Encrypt, DigiCert, etc.
- Contient :
    - Nom du domaine
    - Clé publique du serveur
    - Signature de la CA
    - Date de validité