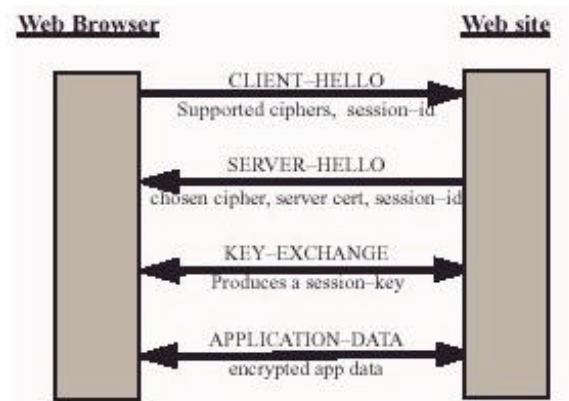


Protocoles Sécurisés sur Internet: SSL (Secure Sockets Layer)

Les différentes phases d'une connexion sécurisée:



"SSL Handshake"

CLIENT-HELLO: Le client initialise la demande en envoyant la liste des algorithmes de compression supportés.

SERVER-HELLO: Le serveur renvoie l'algorithme choisi et fournit un certificat qui permet son authentification ainsi qu'une "session-id".

KEY-EXCHANGE: Le client et le serveur négocient une "session-key", clé qui sera utilisée ensuite pour crypter la session.

"Application-Data"

Echange des données cryptées par la "session-key".

L'échange de clés SSL étant basé sur une cryptographie utilisant des clés publiques, cela nécessite des ressources CPU importantes sur le serveur. Afin de réduire le nombre "SSL Handshake", le protocole SSL prévoit la phase "SSL Resume" qui supprime la négociation d'une nouvelle "session-key".

"SSL Resume"

CLIENT-HELLO: Le client envoie la "session-id" précédente et la liste des algorithmes de compression supportés.

SERVER-HELLO: Si cette "session-id" est toujours valide au niveau du serveur, celui-ci confirme la phase "Resume".

La phase "KEY-EXCHANGE" n'est plus nécessaire.

"Application-Data"

Echange des données cryptées par la "session-key".