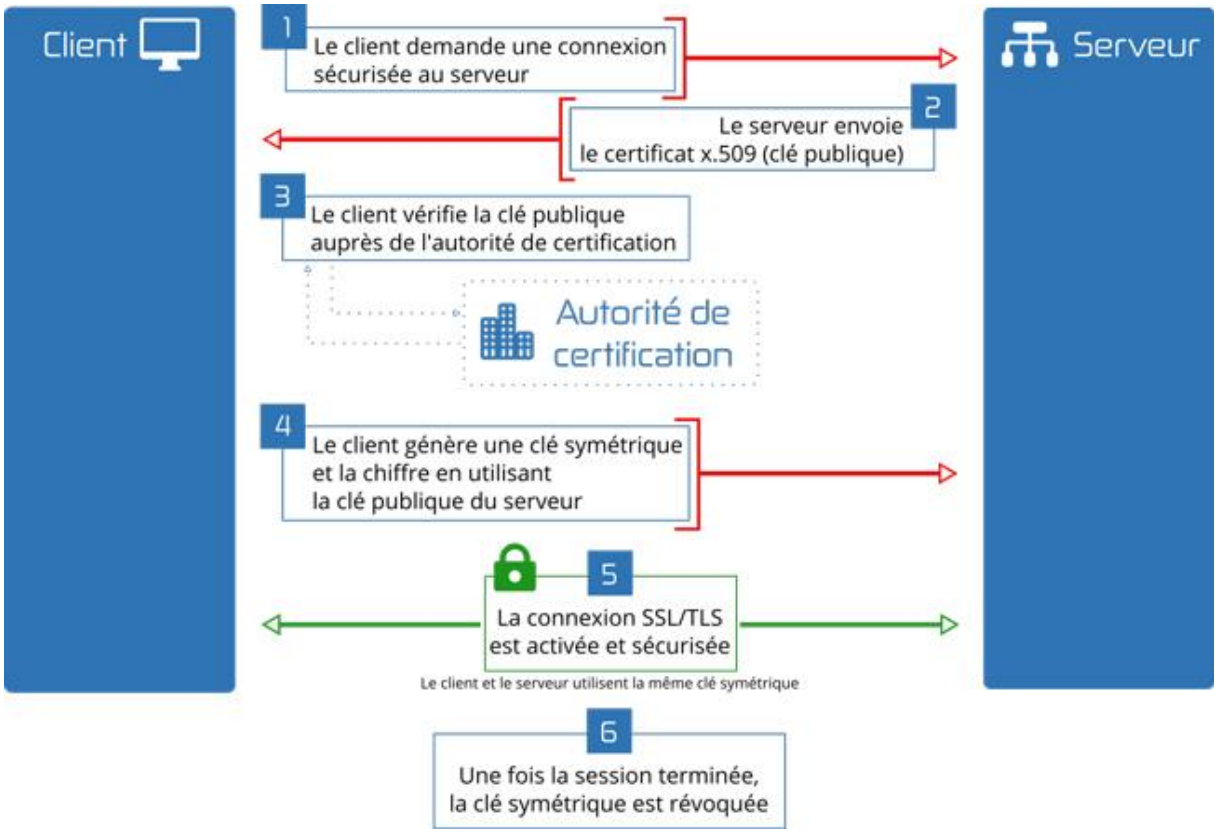
# Certificat SSL

## Principe de fonctionnement

Le certificat SSL est un certificat numérique qui assure l'authenticité d'un site WEB et permet de sécuriser les échanges d'informations grâce à un cryptage des informations.

La technologie est intégrée à tous les navigateurs WEB, le certificat est hébergé sur le serveur WEB du site visité et est utilisé par le protocole HTTPS.

Le schéma ci-dessous permet de visualiser le déroulé de l'échange.




## Principe d'asymétrie/symétrie

Il existe 2 types de clé dans le chiffrement SSL. Les clés asymétriques et symétrique.

**La clé symétrique** est une seule clé pour verrouiller et déverrouiller l'échange. La même clé est utilisée des deux côtés, entre l'expéditeur et le destinataire.

**La clé asymétrique** est un système de deux clés. La clé publique est utilisée pour chiffrer et la clé privée correspondante est utilisée pour déchiffrer. Seul le serveur sur lequel nous tentons de nous connecter dispose de cette la clé privée.