Le certificat SSL

[sommaire]

1. **Objectif**

- Connaitre Le certificat SSL

- **Présentation**

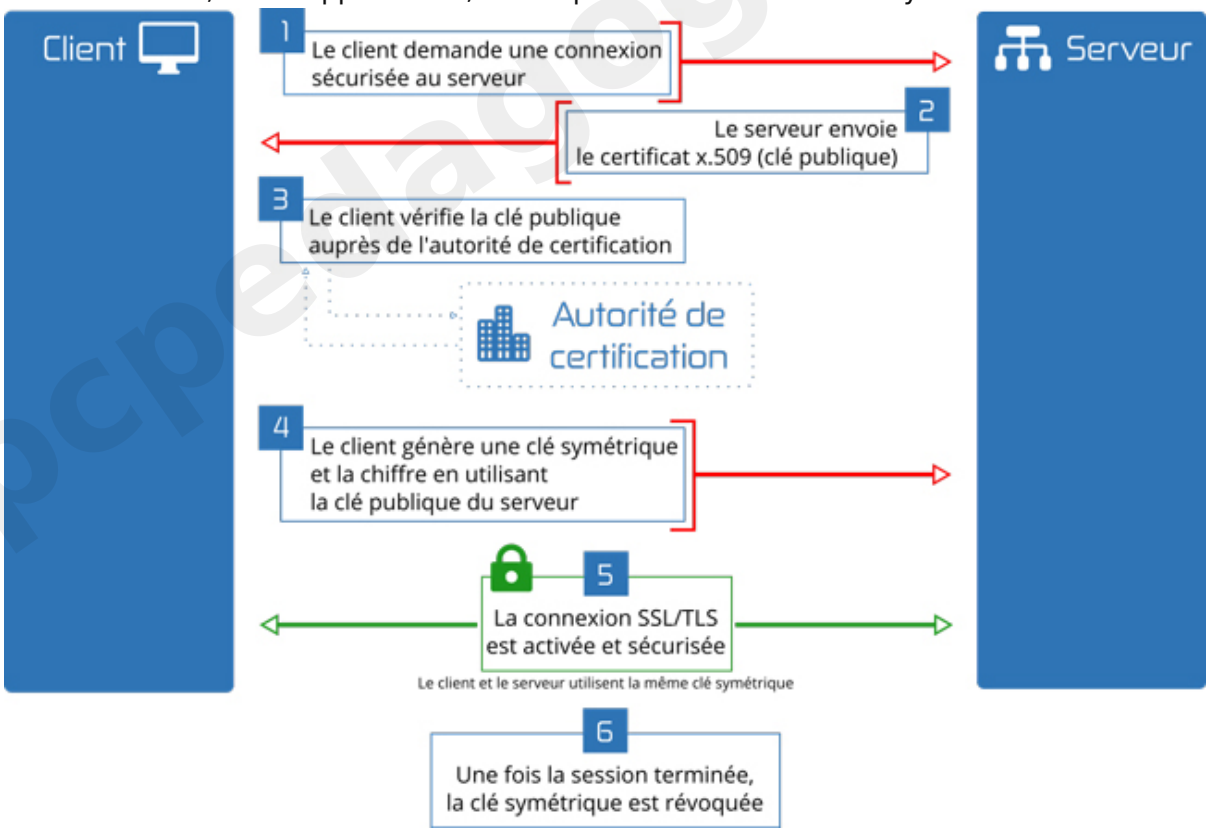


- Le **SSL** (**S**ecure **S**ocket **L**ayer) aussi connu sous le nom de TLS (Transport Layer Security), est un certificat qui permet de sécuriser la connexion entre le visiteur et le serveur d'un site internet à l'aide d'un cryptage très élevé.
- Le **SSL** (**S**ecure **S**ocket **L**ayer), ou TLS (Transport Layer Security), est un protocole de chiffrement des données qui permet de sécuriser les échanges d'informations transitant entre deux machines connectées sur un réseau.
- Un certificat SSL (appelé également certificat électronique ou certificat numérique) est l'équivalent d'une carte d'identité numérique.
- Un certificat SSL est un fichier de données qui lie une clé cryptographique aux informations d'une organisation ou d'un individu. Installé sur un serveur, le certificat active le cadenas et le protocole « https » (via le port 443) dans les navigateurs, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur.
- Généralement, le SSL est utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions, telles que les noms d'utilisateur et les mots de passe.
- Cette technologie peut être utilisée pour fiabiliser la plupart des flux de données sur Internet. Son but est de sécuriser les pages, les formulaires (...) qui affichent ou transmettent des données sensibles ou confidentielles. Il peut s'agir, selon les cas, de numéros de carte

apcpedagogie.com

bancaires ou de données privées (renseignements médicaux, coordonnées personnelles, mots de passe, informations confidentielles, etc.).

- **Pourquoi utiliser un certificat SSL ?**
  - Un certificat SSL permet de sécuriser le transport des données pour les applications suivantes :
    - transactions bancaires en ligne.
    - connexions et échanges d'informations confidentielles.
    - applications et les messageries web.
    - trafics intranet dans les organisations.
    - flux de production, les applications de virtualisation et les plates-formes sur le Cloud.
    - connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
    - transferts de fichiers au travers de services "https" et FTP, lors des mises à jour des sites internet.
    - connexions aux panneaux de contrôle et les activités d'hébergement.
    - connexions aux réseaux et aux trafics de réseaux utilisant les VPNs SSL comme VPN Access Servers, et les applications, telles que Citrix Access Gateway.



- **Les différents types de certificats**

- **Certificats SSL fournis en marge des organismes certificateurs**
  - Ils sont généralement développés de façon à garantir la sécurité des échanges à l'intérieur d'une entreprise, d'une structure ou d'une organisation (dans un intranet par exemple).
- **Certificats SSL fournis par un organisme certificateur**
- L'organisme certificateur est une autorité reconnue qui tient lieu de tiers de confiance.
  En fonction des niveaux de garanties demandés, l'autorité de certification peut garantir :
  - L'authentification des flux de données transitant entre un serveur et un navigateur internet (ou un logiciel FTP, un client SSH, un client mail...) ;
  - La prise en charge d'un ou plusieurs algorithmes de chiffrement ;
  - L'identité d'un site internet (le contenu que vous affichez dans le navigateur n'a pas pu être intercepté et modifié par un tiers entre votre navigateur et le serveur web) ;
  - L'identité du propriétaire d'un site internet (dans le cas d'un certificat de validation étendue, la barre d'adresse du navigateur est verte) ;
  - Une garantie financière des transactions bancaires (si une carte bancaire est débitée frauduleusement par un hack du cryptage garanti par le certificat) ;
  - Un service d'évaluation des vulnérabilités et une détection quotidienne des logiciels malveillants sur le site protégé ;
  - Un taux de compatibilité avec les navigateurs entre 97 et 99% en fonction des autorités de certification.

- ## Les différents niveaux de certification

Sources

- Livre: Sécurité informatique Laurent Bloch, Christoph Wolfhugel
- https://www.icodia.com/fr/solutions/certificats-ssl/en-savoir-plus-certificats-ssl.html

---

Cours le commerce électronique

Source : https://apcpedagogie.com/le-certificat-ssl · téléchargé le 03/11/2026 · © APC Pédagogie · apcpedagogie.com