Sécurité :

La sécurité c'est un élément primordial pour la réussite d'une application web ou autre, pour notre application on peut définir deux niveaux de sécurité :

- Sécurité d'accès à l'application.
- Sécurisé des transactions (technologie HTTPS).

1 Sécurité d'accès à l'application :

- L'utilisation de mécanisme d'authentification
- L'utilisation des sessions

2. Technologie HTTPS :

2.1 HTTPS :

HTTPS est un protocole réseau utilisé pour la navigation sécurisée sur le web.Il apporte des possibilités d'authentification et de chiffrement pour les sites web demandant un certain niveau de sécurité dans leurs échanges avec les navigateurs web. HTTPS qui signifie Hypertext Transfer Protocol Secure n'est en faite que l'encapsulation du protocole HTTP au travers du protocole SSL.

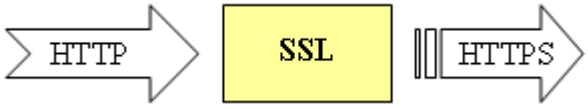

Figure A.13 : protocole HTTPS

HTTPS est utilisé de nos jours sur le très grand réseau mondial qu'est Internet mais aussi sur les réseaux Intranet nécessitant une confidentialité des données.

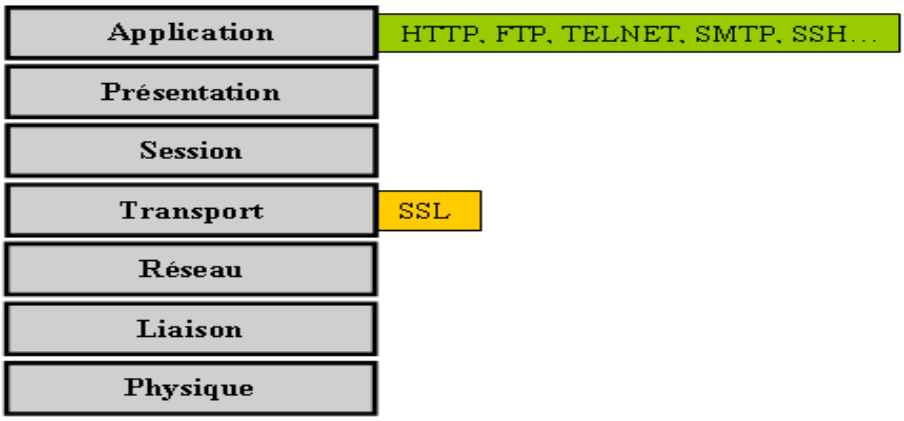

Figure A.14 : SSL & les couches réseau

Etant basé sur un protocole de couche inférieure qu'est SSL, d'autres standards peuvent utilisé le même modèle. Nous avons ainsi entre autre:

HTTP ☐ HTTPS
FTP ☐ FTPS
SMTP ☐ SMTPS
IMAP ☐ IMAPS
POP3 ☐ POP3S
TELNET ☐ TELNETS

Les principaux avantages que peut procurer HTTPS par rapport à HTTP sont les suivants :

- ☐ Cryptage des données.
- ☐ Intégrité des données.
- ☐ Confidentialité des données.
- ☐ Garantie d'avoir un hôte récepteur de confiance.

Quand on dit que la quasi totalité des navigateurs supportent ce protocole, en faite ici, on parle de support du protocole SSL. Généralement signalé par un petit cadenas dans la barre d'état du navigateur, les adresses commencent toujours par *https://*

2.2 SSL

SSL abrégé de Secure Sockets Layers est un standard permettant de sécuriser des transactions qui a été développé par Netscape en collaboration avec des sociétés tel quel Bank of America.

Le principe repose sur un procédé cryptographique par clefs publique qui procure une plus grande sécurité.

SSL est basé sur l'utilisation de certificat utilisant différents algorithmes cryptographiques tel que:

- chiffrement: DES, 3DES, RC2, RC4, AES
- hachage: MD5, SHA
- signature: RSA

2.3 Les étapes SSL:

1. Le client se connecte au serveur indique la version de SSL qu'il utilise.
2. Le serveur répond à son tour avec ses informations.
3. Le client peut vérifier auprès d'une autorité tiers pour savoir si c'est réellement le serveur avec qui il communique.
4. Le client s'authentifie auprès du serveur qui vérifie par l'intermédiaire du certificat du client.
5. Les échanges de certificat qui comprend la clé de session commencent.
6. Arrivé à ce stade nous avons un réseau de confiance opérationnel entre 2 entités. Les échanges de messages chiffrés et signés peuvent commencer.
7. A la fin de communication, les clés sont détruites.

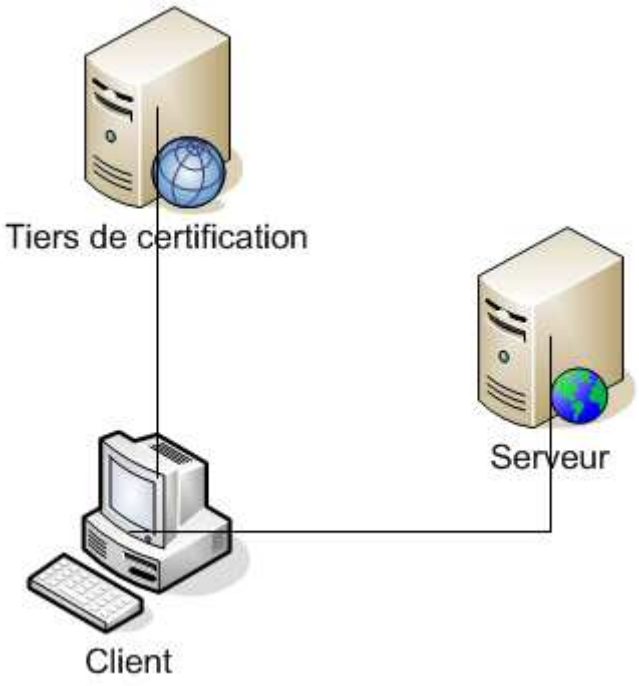

Figure A.15 : les étapes de transaction SSL