Retour au glossaire

Certificat SSL

Un certificat SSL (Secure Sockets Layer) est un fichier numérique qui lie une clé cryptographique à une organisation. Il est utilisé pour sécuriser les communications sur Internet en établissant une connexion chiffrée entre un client (comme un navigateur web) et un serveur (comme un site web). Les certificats SSL sont émis par des autorités de certification (CA) de confiance et sont essentiels pour garantir la sécurité et la confidentialité des données échangées en ligne.

SSL

SSL (Secure Sockets Layer) est un protocole de sécurité utilisé pour établir des communications sécurisées sur Internet. Il a été développé par Netscape dans les années 1990 et a depuis été remplacé par son successeur, TLS (Transport Layer Security). Cependant, le terme SSL est encore couramment utilisé pour désigner à la fois SSL et TLS. Les principales fonctions du SSL sont :

- **Chiffrement** : Les données échangées entre le client et le serveur sont chiffrées, ce qui les rend illisibles pour quiconque intercepterait la communication (c'est le HTTPS des navigateur).
- **Authentification** : SSL/TLS utilise des certificats numériques pour authentifier l'identité du serveur (et parfois du client). Ces certificats sont émis par des autorités de certification (CA) de confiance.
- **Intégrité des Données** : SSL/TLS assure que les données ne sont pas altérées pendant le transit en utilisant des techniques de hachage et de vérification d'intégrité.

Voir aussi

- La procédure Proc#156 - Création et renouvellement des certificats SSL

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
https://wiki-logeas.fr/certif/doku.php?id=glossaire:certificatssl

Last update: **2025/08/27 07:16**