

Introduction à **SSL & TLS**





SSL et TLS kézako ?

- « *Secure Sockets Layer* » et « Transport Layer Security »
- Prévus pour utiliser TCP en tant que service bout-en-bout sécurisé
- SSL & TLS = mêmes protocoles avec différents algorithmes
- TLS = SSLv3.1
- -> **authentification** (serveur), **confidentialité**, **intégrité**



SSL et TLS

- 3 phases :
- Négociations portant sur l'algorithme à employer (chiffrement, échange de clés...Etc)
- Échange de clés et authentification
- Chiffrement symétrique et authentification du message