Comunicacions segures

- HTTPS=HTTP + TLS
- El protocol TLS engloba un conjunt de tecnologies criptogràfiques tant simètriques com asimètriques que permeten assegurar la confidencialitat, integritat i autenticació de la informació transmesa
- Concepte de certificat: clau pública signada per (idealment) un tercer. Útil en el pas d'autenticació i assegurament de la connexió

Com crear un certificat autosignat amb clau privada mitjançant la suite OpenSSL

openssl req -new -x509 -newkey rsa:2048 -nodes -keyout clauPriv.key -out cert.crt

Com configurar Apache per a què faci servir el certificat i clau privada anteriors

- Cal afegir les directives *SSLEngine on*, *SSLCertificateFile* i *SSLCertificateKeyFile* a la configuració del VH en qüestió
- Cal activar el mòdul "ssl"

En qualsevol cas, l'opció assequible (gratis) més "professional" és Let's encrypt (`https://letsencrypt.org`) però es necessita tenir un nom DNS registrat a Internet per a què funcioni.