**OpenSSL**

|  |  |
| --- | --- |
| **DESC** | |
| Secure Socket Layer | |
| **FILES** | |
| /etc/pki/tls/openssl.cnf | Configuration |
| **QUICK START** | |
| * Openssl genrsa pour générer le fichier contenant les 2 clefs * Openssl rsa pour extraire la clef privée et publique de ce fichier | |

**Généralités :**

* PKI : Public key infrastructure (contient la CA, le fonctionnement…etc)
* CA atteste que la clef publique est la bonne en émettant des certificats.
* Pour obtenir un certificat d’une CA, on doit générer préalablement un CSR (certificate signing request) = infos + clef publique
* Digest = résultats d’une fonction de hash
* Passphrase : pour chiffrer la clef privée

**Certificats signés:**

* Pays
* Ville
* Localité
* Organisation
* Site
* Email
* Clef publique
* Date de création du certificat
* Date de révocation du certificat
* Signature de tous les éléments hashés au-dessus