|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **OpenSSL** | | | | | | |
| **DESC** | Secure Socket Layer | | | | | |
| **CLI** | | | | | | |
| **GENERALE** | | | | | | |
| **openssl** | version | | | Version OpenSSL | | |
|  | List-standard-commands | | |  | | |
|  | List-cipher-commands | | |  | | |
|  | ciphers | | | != protocoles available (sym, asym, hash) | | |
|  | speed | | | Test des protocoles par le système | | |
|  |  | | |  | | |
| **CHIFFREMENT/DECHIFFREMENT SYMETRIQUE** | | | | | | |
| **openssl** | Enc –base64 | | | n’importe quel algorithme  Choix de l’algorithme de chiffrement/déchiffrement dans la  List-cipher-commands | | | |
|  |  | | -in <file> | |  | |
|  |  | | -out <file> | |  | |
|  |  | | -d | | Déchiffrement  Chiffrement si –d absent | |
|  |  | | -pass pass :mdp | |  | |
| **GENERATION CLEFS ASYMETRIQUES** | | | | | | |
| **openssl** | Genrsa [Opts] 1024 | | Génère un fichier contenant les 2 clefs pub/priv | | | |
|  |  | | -out <file> | | |  |
| **MANAGEMENT CLEFS ASYMETRIQUES** | | | | | | |
| **openssl** | Rsa –des3 | | Chiffrement de la clef privée en symétrique avec/sans passphrase | | | |
|  |  | | -in <file> | | |  |
|  |  | | -out <file> | | |  |
|  | Rsa -pubout | | Extraction de la clef publique à partir du fichier contenant les 2 clefs | | | |
|  |  | | -in <file> | | |  |
|  |  | | -out <file> | | |  |
| **CHIFFREMENT/DECHIFFREMENT ASYMETRIQUE** | | | | | | |
| **openssl** | Rsautl -encrypt | |  | | |  |
|  |  | | -in <file> | | | Fichier à chiffrer |
|  |  | | -inkey  -pubin | | | Fichier contenant uniquement pub+priv  Fichier contenant uniquement pub |
|  |  | | -out <file> | | |  |
| **HASH** | | | | | | |
| **openssl** | Dgst -algo <file> | | Génération d’un hash à partir de file | | | |
|  |  | | -out <file> | | |  |
|  | passwd | | Création d’un hash | | | |
| **CERTIFICATS** | | | | | | |
| **openssl** | ca |  | | | | |
|  | X509 |  | | | | |
| **Comments :** | | | | | | |