|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 -<ciphername> | | | | | n’importe quel algorithme symétrique | | | | | | | |
|  |  | | | | | -in <file> | | | | Stdin par défaut | | | |
|  |  | | | | | -out <file> | | | | Stdout par défaut | | | |
|  |  | | | | | -d | | | | Déchiffrement | | | |
|  |  | | | | | -pass pass :mdp | | | | Password à utiliser pour chiffrement | | | |
|  |  | | | | | -a | | | | Base64 appliqué après chiffrement | | | |
|  | Enc help | | | | | Liste des ciphers disponibles pour cette version | | | | | | | |
| **GENERATION CLEFS ASYMETRIQUES** | | | | | | | | | | | | | |
| **openssl** | genpkey | | | | Génération clefs RSA, DSA…  Rend genrsa et gendsa obsolète | | | | | | | | |
|  | -out <file> | | | | Stdout par défaut | | | | | | | | |
|  | -outform DER|PEM | | | | Format de sortie | | | | | | | | |
|  | -pass pass :hello | | | | passphrase | | | | | | | | |
|  | -<ciphername> | | | | Chiffrement symétrique de la clef privée | | | | | | | | |
|  | -algorithm <alg> | | | | RSA|DSL|DH | | | | | | | | |
|  | -pkeyopt | | | | Rsa\_keygen\_bits :2048 | | | | | | | | Taille clef |
|  | Genrsa [Opts] 2048 | | | | Génération d’une paire de clés RSA (publique + privée) 2048 bits  au format PEM | | | | | | | | |
|  |  | | | | -out <file> | | | | | |  | | |
| **MANAGEMENT CLEFS ASYMETRIQUES** | | | | | | | | | | | | | |
| **openssl** | Rsa | -<ciphername> | | | | | Chiffrement de la clef privée en symétrique | | | | | | |
|  |  | -out <file> | | | | |  | | | | | | |
|  |  | -pubout <file> | | | | | Extraction de la clef publique | | | | | | |
|  |  | -in <file> | | | | | Lecture clef privée+publique | | | | | | |
|  |  | -pubin <file> | | | | | Lecture clef publique | | | | | | |
|  |  | -inform | | | | | DER|NET|PEM | | | | | | |
|  |  | -outform | | | | | DER|NET|PEM | | | | | | |
| **CHIFFREMENT/DECHIFFREMENT RSA** | | | | | | | | | | | | | |
| **openssl** | Rsautl | |  | | | | |  | | | | | |
|  |  | | -in <file> | | | | | Fichier à chiffrer | | | | | |
|  |  | | -out <file> | | | | |  | | | | | |
|  |  | | -inkey | | | | | Fichier contenant la clef privée | | | | | |
|  |  | | -pubin | | | | | Fichier contenant uniquement pub | | | | | |
|  |  | | -sign | | | | | Signature des données en entrée | | | | | |
|  |  | | -encrypt | | | | |  | | | | | |
|  |  | | -decrypt | | | | |  | | | | | |
| **HASH** | | | | | | | | | | | | | |
| **openssl** | Dgst | | Génération d’un hash à partir de file | | | | | | | | | | |
|  |  | | <file> | | | | | Fichier à hasher, stdin par défaut | | | | | |
|  |  | | -out <file> | | | | |  | | | | | |
|  |  | | -algo <file> | | | | |  | | | | | |
|  |  | | -sign <filename> | | | | | Signature du digest via la clef privée dans filename | | | | | |
|  | passwd | | Création d’un hash de mdp | | | | | | | | | | |
| **CREATION CSR ET CERTIFICATS X509** | | | | | | | | | | | | | |
| **openssl** | req | Création certificat | | | | | | | | | | | |
|  |  | -inform | | | | | | DER|PEM | | | | | |
|  |  | -outform | | | | | | DER|PEM | | | | | |
|  |  | -in <filename> | | | | | | Uniquement si -new et -newkey non spécifiés | | | | | |
|  |  | -out <filename> | | | | | |  | | | | | |
|  |  | -new | | | | | | New CSR (requête de certificat) | | | | | |
|  |  | -x509 | | | | | | New certificat auto-signé | | | | | |
|  |  | -days X | | | | | | Validité du certificat | | | | | |
|  |  | -key <file> | | | | | | Fichier contenant clef publique + privée | | | | | |
|  |  | -newkey [Opts] | | | | | | Création de clefs si besoin | | | | | |
|  |  |  | | | | | | rsa :1024 | | | |  | |
| **MANAGEMENT CERTIFICATS** | | | | | | | | | | | | | |
| **openssl** | X509 | | |  | | | | | | | | | |
| **SIGNATURE CERTIFICAT** | | | | | | | | | | | | | |
| **openssl** | ca | | |  | | | | | | | | | |
|  |  | | | -in <cert> | | | | | CSR | | | | |
|  |  | | | -out <cert> | | | | |  | | | | |
|  |  | | | -cert <cert> | | | | | Certificat CA | | | | |
|  |  | | | -keyfile <key> | | | | | Clef privée CA | | | | |
| **Comments :**  Ca – certificats  Crl – certificats  Dhparam – paramètres diffie hellman | | | | | | | | | | | | | |