OpenSSL - ec

Outil de traitement de clé EC

OPTIONS

-inform DER|NET|PEM Format du fichier d'entrée.
-outform DER|NET|PEM Format du fichier de sortie
-in filename Fichier d'entrée
-passin arg source du mot de passe du fichier d'entrée
-out filename Fichier de sortie où écrire la clé
-passout password source du mot de passe du fichier de sortie
-des|-des3|-idea Chiffre la clé privée avec DES, triple DES ou IDEA, ou un autre chiffrement supporté
-text Affiche des infos sur les clés privée et publique
-noout N'affiche pas la version encodée de la clé
-modulus Affiche la valeur du modulo de la clé
-pubin Lit une clé publique en entrée plutôt qu'une clé privée
-pubout Sort une clé publique plutôt qu'une clé privée
-engine id ec va tenter d'obtenir une référence fonctionnelle de ce moteur.
-conv_form Spécifie comment les points sur la courbe elliptique sont convertis en chaîne d'octets (compressed, uncompressed ou hybrid).
-param_enc arg Spécifie comment les paramètres de courbe elliptique sont encodés. **named_curve** ou **explicit**

Notes

la forme PEM de la clé privée contient :

```
---BEGIN EC PRIVATE KEY---
---END EC PRIVATE KEY---
```

Exemples

Chiffrer une clé privée avec 3DES :
openssl ec -in key.pem -des3 -out keyout.pem
Convertir une clé privée PEM en DER :
openssl ec -in key.pem -outform DER -out keyout.der
Afficher les composants d'une clé privée sur stdout :
openssl ec -in key.pem -text -noout
Afficher la partie publique d'une clé privée :
openssl ec -in key.pem -pubout -out pubkey.pem
Changer les paramètres d'encodage à explicit :
openssl ec -in key.pem -param_enc explicit -out keyout.pem
Changer la conversion de point à compressed :
openssl ec -in key.pem -conv_form compressed -out keyout.pem