OpenSSL - ecparam

Manipulation et génération de paramètre 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

-out filename fichier de sortie où écrire les paramètres

-text Affiche des infos sur les clés privée et publique

-noout n'affiche pas la version encodée des paramètres

-C Convertis les paramètres EC en code C.

-check Valide les paramètres de courbe elliptique

-name arg Utilise les paramètres EC avec le nom court spécifié.

-list_curves Affiche la liste de tous les paramètres EC implémentés.

-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**

-no_seed Inhibe que le 'seed' pour la génération de paramètre soit inclus dans la structure ECParameters

-genkey Génère une clé privée EC en utilisant les paramètres spécifiés

-rand file Un ou plusieurs fichiers contenant des données aléatoires.

-engine id ecparam va tenter d'obtenir une référence fonctionnelle de ce moteur.

Notes

la forme PEM des paramètres EC utilisent la forme :

```
---BEGIN EC PARAMETERS---
---END EC PARAMETERS---
```

Exemples

Créer des paramètres EC avec le groupe 'prime192v1' :
openssl ecparam -out ec_param.pem -name prime192v1
Créer des paramètres EC avec les paramètres explicites :
openssl ecparam -out ec_param.pem -name prime192v1 -param_enc explicit
Valider les paramètres EC donnés :
openssl ecparam -in ec_param.pem -check
Créer des paramètres EC et une clé privée :
openssl ecparam -out ec_key.pem -name prime192v1 -genkey
Changer l'encodage des points à compressed :

openssl ecparam -in ec_in.pem -out ec_out.pem -conv_form compressed
Afficher les paramètres EC :
openssl ecparam -in ec_param.pem -noout -text