

---

# OpenSSL - dhparam

Génération et manipulation de paramètre DH

## OPTIONS

- inform DER|PEM** Format du fichier d'entrée
- outform DER|PEM** Format du fichier de sortie
- in filename** Fichier d'entrée
- out filename** Fichier de sortie
- dsaparam** Si spécifié, les paramètres DSA sont lus ou créé au lieu de paramètres DH; ils sont convertis au format DH. Sinon, les premiers 'fort' seront utilisé pour la génération de paramètres DH.
- check** Vérifie si les paramètres sont valides
- 2, -5** Générateur à utiliser. Si présent, le fichier d'entrée est ignoré et les paramètres sont générés. Défaut : 2
- rand file(s)** Fichiers contenant des données aléatoires utilisée pour le générateur de nombre aléatoire, ou un socket EGD.
- numbits** Spécifie le nombre de bit à utiliser. Doit être la dernière option. Défaut : 2048
- noout** Inhibe la sortie de la version encodée des paramètres
- text** Affiche les paramètres DH au format lisible
- C** Convertis les paramètres en code C. Les paramètres peuvent ainsi être chargés en appelant `get_dhNNNN()`
- engine id** dhparam va tenter d'obtenir une référence fonctionnelle du moteur spécifié.

## Notes

Le programme dhparam combine les fonctionnalités des programmes dh et gendh dans les versions précédentes de OpenSSL. Les programmes dh et gendh sont retenus pour d'autres utilisations dans le future.

Les paramètres DH au format PEM utilisent les en-tête et pied de page suivant :

```
---BEGIN DH PARAMETERS---  
---END DH PARAMETERS---
```

Openssl supporte actuellement l'ancien PKCS#3 DH, pas le nouveau X9.42 DH.