OpenSSL - genpkey

Génération de clé privée

OPTIONS

-out filename Nom du fichier de sortie

-outform PEM|DER Format du fichier de sortie

-pass arg Source du mot de passe du fichier de sortie

-cipher Algorithme à utiliser pour chiffrer la clé privée.

-engine id genpkey va tenter d'obtenir une référence fonctionnelle pour le moteur spécifié.

-algorithm alg Algorithme de clé publique à utiliser tel que RSA, DSA ou DH. Doit précéder -pkeyopt

-pkeyopt opt :value Définis une option pour l'algorithme de clé publique.

-genparam Génère un jeu de paramètres au lieu d'une clé privée. Doit précéder -algorithm, -paramfile ou -pkeyopt

-paramfile filename Fichier contenant les paramètres à utiliser pour générer la clé privée. Doit précéder -pkeyopt.

-text Affiche une représentation texte des clés publique et privée et des paramètres.

Options de génération de clé

Les options prises en charge par chaque algorithme et même chaque mise en œuvre d'un algorithme peut varier.

Options de génération de clé RSA

rsa_keygen_bits :numbits Nombre de bits dans la clé générée. (défaut : 1024)

rsa_keygen_pubexp :value Valeur d'exposant publique RSA, en décimal ou hexa (défaut : 65537)

Options de génération de clé DSA

dsa_paramgen_bits :numbits Nombre de bits dans les paramètres générés (défaut 1024)

Options de génération de paramètres DH

dh_paramgen_prime_len :numbits Nombre de bits dans le paramètre p

dh_paramgen_generator :value valeur à utiliser pour le générateur g

dh_rfc5114 :num Applique les paramètres RFC5114. num peut être (1 : groupe de 1024 avec sous-groupe 160bits, 2 : groupe de 2048 avec sous-groupe 224bits ,3 : groupe de 2048 avec sous-groupe 256bits).

Options de génération de paramètres EC

ec_paramgen_curve :curve La courbe EC à utiliser

Options de paramètres et de génération de clé GOST2001

paramset :name Spécifie le paramètre GOST R 34.10-2001 en accord avec la RFC 4357. Les paramètres suivants sont supportés

paramset OID Usage

```
A 1.2.643.2.2.35.1 Signature
B 1.2.643.2.2.35.2 Signature
C 1.2.643.2.2.35.3 Signature
XA 1.2.643.2.2.36.0 Key exchange
XB 1.2.643.2.2.36.1 Key exchange
test 1.2.643.2.2.35.0 Test purposes
```

Exemples

Générer une clé privée RSA en utilisant les paramètres par défaut :
openssl genpkey -algorithm RSA -out key.pem
Chiffrer une clé privée en utilisant AES128 et la passphrase 'hello' :
openssl genpkey -algorithm RSA -out key.pem -aes-128-cbc -pass pass :hello
Générer une clé RSA 2048bits et un exposant publique 3 :
openssl genpkey -algorithm RSA -out key.pem -pkeyopt rsa_keygen_bits :2048 -pkeyopt rsa_keygen_pubexp :3
Générer des paramètres DSA 1024bits :
openssl genpkey -genparam -algorithm DSA -out dsap.pem -pkeyopt dsa_paramgen_bits :1024
Générer une clé DSA depuis des paramètres :
openssl genpkey -paramfile dsap.pem -out dsakey.pem
Générer des paramètres DH 1024bits :
openssl genpkey -genparam -algorithm DH -out dhp.pem -pkeyopt dh_paramgen_prime_len :1024
sortir des paramètres DH RFC5114 type 2 :
openssl genpkey -genparam -algorithm DH -out dhp.pem -pkeyopt dh_rfc5114 :2
Générer une clé DH depuis des paramètres :
openssl genpkey -paramfile dhp.pem -out dhkey.pem