OpenSSL - dsa

Traitement des clés dsa. Utilise le format compatible SSLeay pour le chiffrement des clés privées, les applications devraient utiliser pkcs8, plus sécure.

OPTIONS

-inform DER|PEM Format du fichier d'entrée. DER avec une clé privée utilise une forme encodée ASN1 DER d'une séquence ASN.1 consistant de valeurs de version (0 actuellement), p, q, g, les clés publique et privée en tant qu'entier ASN.1.

-outform DER|PEM Format de la sortie.

-in filename Fichier contenant la clé à lire

-passing arg Source du mot de passe du fichier d'entrée.

-out filename fichier de sortie où écrire une clé.

-passout arg source du mot de passe du fichier de sortie

-des|des3|-idea Algorithme utilisé pour chiffrer la clé privée.

-text Affiche la clé privée, publique et les paramètres

-noout n'affiche pas la sortie encodée de la clé

-modulus Affiche la valeur de la composante clé publique de la clé

-pubin Par défaut, la clé privée est lue depuis le fichier d'entrée. Cette option lit une clé publique à la place.

-pubout Par défaut, une clé privée est sortie. Avec cette option, une clé publique est sortie.

-engine id dsa va tenter d'obtenir une référence fonctionnelle au moteur spécifié.

Notes

Le format de clé privée PEM utilise :
—–BEGIN DSA PRIVATE KEY—–
—–END DSA PRIVATE KEY—–
Le format de clé publique PEM utilise :
—–BEGIN PUBLIC KEY—–
—–END PUBLIC KEY—–

Exemples

Supprimer une passphrase d'une clé privée DSA :
openssl dsa -in key.pem -out keyout.pem
Chiffrer une clé privée en utilisant 3DES :
openssl dsa -in key.pem -des3 -out keyout.pem
Convertir une clé privée PEM en DER :
openssl dsa -in key.pem -outform DER -out keyout.der
Afficher les composants d'une clé privée sur stdout :
openssl dsa -in key.pem -text -noout
Affiche la partie publique d'une clé privée :
openssl dsa -in key.pem -pubout -out pubkey.pem