
OpenSSL - pkey

Outil de traitement de clé privée ou publique

OPTIONS

- inform DER|PEM** Format du fichier d'entrée
- outform DER|PEM** Spécifie le format de sortie
- in filename** Fichier à lire
- out filename** Fichier à écrire
- passin arg** source du mot de passe du fichier d'entrée
- passout password** source du mot de passe du fichier de sortie.
- cipher** Chiffre la clé privée avec le chiffrement spécifié
- text** Affiche les composant de clé privée ou publique en texte clair en plus de la version encodée.
- text_pub** Affiche uniquement la composante clé publique.
- noout** Ne sort pas la version encodée 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 écrite en sortie. Cette option sort une clé publique.
- engine id** pkey va tenter d'obtenir une référence fonctionnelle de ce moteur.

Exemples

Enlever un passphrase d'une clé RSA :

openssl pkey -in key.pem -out keyout.pem

Chiffrer une clé publique avec 3DES :

openssl pkey -in key.pem -des3 -out keyout.pem

Convertir une clé privée PEM en DER :

openssl pkey -in key.pem -outform DER -out keyout.der

Afficher les composants de clé privée :

openssl pkey -in key.pem -text -noout

Afficher les composants publics d'une clé privée :

openssl pkey -in key.pem -text_pub -noout

Sortie la partie publique d'une clé privée :

openssl pkey -in key.pem -pubout -out pubkey.pem