OpenSSL - rsa

Traitement des clés rsa

OPTIONS

-inform DER|NET|PEM Format du fichier d'entrée.

-outform DER|NET|PEM Format du fichier de sortie

-in filename Fichier d'entrée

-passin arg source du mot de passe du fichier d'entrée

-out filename Fichier de sortie où écrire la clé

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

-sgckey Utilisé pour l'algorithme modifié NET utilisé avec certaines versions de Microsoft IIS et les clé SGC.

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

-text Affiche des infos sur les clés privée et publique

-noout N'affiche pas la version encodée de la clé

-modulus Affiche la valeur du modulo de la clé

-check Vérifie la consistance de la clé privée RSA

-pubin Lit une clé publique en entrée plutôt qu'une clé privée

-pubout Sort une clé publique plutôt qu'une clé privée

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

Notes

la forme PEM de la clé privée contient :

```
---BEGIN RSA PRIVATE KEY---
---END RSA PRIVATE KEY---
```

la forme PEM de la clé publique contient :

```
---BEGIN PUBLIC KEY---
---END PUBLIC KEY---
```

Exemples

Supprimer le passphrase d'une clé privée :
openssl rsa -in key.pem -out keyout.pem
Chiffrer une clé privée avec triple DES :
openssl rsa -in key.pem -des3 -out keyout.pem
Convertir une cléprivée PEM en DER :
openssl rsa -in key.pem -outform DER -out keyout.der

Afficher les composantes de la clé privée :
openssl rsa -in key.pem -text -noout
Afficher la partie publique de la clé privée :
openssl rsa -in key.pem -pubout -out pubkey.pem