OpenSSL - pkcs12

Utilitaire pkcs #12

Options de lecture

-in filename Fichier pkcs#12 à lire

-out filename Fichier où écrire les certificats et clé privée au format PEM.

-pass arg, -passin arg passphrase pour chiffrer les clés privées

-noout Ne sort pas les clé et certificats dans le fichier de sortie.

-clcerts sort uniquement les certificats clients (pas de certificat CA)

-cacerts sort uniquement les certificats CA

-nocerts Ne sort pas les certificats

-nokeys Ne sort pas les clés privées

-info Affiche des informations additionnelles sur la structure du fichier PKCS#12

-des|-des3|-idea|-aes128|-aes192|-aes256|-camellia128|-camellia192|-camellia256 Algorithme à utiliser pour chiffrer la clé privée.(défaut : des3)

-nodes Ne chiffre pas les clés privées

-nomacver Ne tente pas de vérifier l'intégrité MAC avant de lire le fichier

-twopass Séparer l'intégrité et le chiffrement du mot de passe. Peut rendre le fichier illisible.

Options de création

-export Spécifie une création de fichier PKCS#12

-out filename Nom du fichier PKCS#12 à créer

-in filename Fichier à lire contenant les certificats et clé privées au format PEM

-inkey filename fichier contenant la clé privée à lire.

-name friendlyname 'friendly name' pour le certificat et sa clé privée.

-certfile filename Fichier où lire les certificats additionnels

-caname friendlyname friendly name' pour les autres certificats. Peut-être spécifié plusieurs fois

-pass arg, -passout arg source du mot de passe pour le fichier de sortie.

-passin password Source du mot de passe pour déchiffrer la clé privée.

-chain Tente d'inclure toute la chaîne de certificat

-descert Chiffre le certificat en utilisant 3des (défaut : des3 pour la clé privée et RC2-40bits pour le certificat)

-keypbe alg, -certpbe alg Algorithme utilisé pour chiffrer la clé et les certificats. peut-être un algorithme PKCS#15 ou PKCS#12 PBE.

-keyex|-keysig Spécifie que la clé privée doit être utilisé pour un échange de clé ou juste signer. Uniquement interprété par MSIE et logiciels MS.

-macalg digest Spécifie l'algorithme digest MAC (défaut : SHA1)

-nomaciter, -noiter Affecte le compteur d'itération dans les algorithmes de clé et MAC.(défaut : 2048)

-maciter Inclus pour compatibilité avec les versions précédentes.

-nomac Ne tente pas de fournir l'intégrité MAC.

-rand file(s) fichier(s) contenant les données aléatoire utilisé par le générateur de nombre aléatoire.

-CAfile file Fichier de la CA

-CAptah dir Répertoire contenant les certificats CA.

-CSP name Ecrit le nom sous la forme Microsoft CSP name.

Exemples

Lire un fichier PKCS #12 et le sortir dans un fichier :
openssl pkcs12 -in file.p12 -out file.pem
Sortie seulement les certificats clients dans un fichier :
openssl pkcs12 -in file.p12 -clcerts -out file.pem
Sortir uniquement la clé privée dans un fichier :
openssl pkcs12 -in file.p12 -nocerts -out file.pem
Ne pas chiffrer la clé privée :
openssl pkcs12 -in file.p12 -out file.pem -nodes
Afficher des informations sur le fichier PKCS #12 :
openssl pkcs12 -in file.p12 -info -noout
Créer un fichier PKCS #12 :
openssl pkcs12 -export -in file.pem -out file.p12 -name "My Certificate"
Inclure des certificats supplémentaires :
openssl pkcs12 -export -in file.pem -out file.p12 -name "My Certificate" -certfile othercerts.pem