OpenSSL - x509

Utilitaire de manipulation de certificat

OPTIONS

-inform DER|PEM|NET Format du fichier x509 en entrée
-outform DER|PEM|NET Format du fichier en sortie
-in filename Fichier en entrée
-out filename Fichier de sortie
-md2|-md5|-sha1|-mdc2 Message digest à utiliser
-engine id x509 va tenter d'obtenir une référence fonctionnelle du moteur spécifié.

Options d'affichage

-text Affiche le certificat au format texte.
-certopt option Personnalise la sortie utilisée avec -text liste d'options à afficher. Peut être spécifié plusieurs fois
-noout N'affiche pas la version encodée de la requête
-pubkey Affiche le block SubjectPublicKeyInfo du certificat au format PEM
-modulus Affiche la valeur du modulo de la clé publique contenue dans le certificat
-serial Affiche le numéro de série du certificat
-subject_hash Affiche le hash du nom du certificat
-issuer_hash Affiche le hash de l'issuer du certificat
-hash idem à -subject_hash
-subject_hash_old Affiche le hash du nom du certificat en utilisant l'ancien algorithme pré v1
-issuer_hash_old Affiche le hash de l'issuer du certificat en utilisant l'ancien algorithme pré v1
-subject Affiche le sujet
-issuer Affiche le fournisseur
-nameopt option Détermine comment le sujet et l'issuer sont affichés (voir options de nom)
-email Affiche les adresses email
-ocsp_uri Affiche les adresses de répondeur OCSP
-startdate Affiche la date de début de validité du certificat
-enddate Affiche la date de fin de validité du certificat
-dates Affiche la date de début et d'expiration du certificat
-fingerprint Affiche le digest de la version encodé DER du certificat
-C Affiche le certificat sous la forme d'un source C

Paramètres de confiance

-trustout Sort un certifcat de confiance.

-setalias arg Définis l'alias du certificat

-alias Affiche l'alias du certificat, s'il existe

-clrtrust Efface toutes les utilisations de confiance et permises du certificat

-clrreject Efface toutes les utilisations rejetée ou interdites du certificat

-addtrust arg Ajoute une utilisation de certifiaction de confiance. (clientAuth, serverAuth, emailProtection)

-addreject arg Ajoute une utilisation interdite. Accèpte lesmême valeurs que -addtrust

-purpose Effectue des tests sur les extensions du certificat et affiche le résultat (voir les extensions de certificat)

Options de signature

-signkey filename Signe le fichier en entrée avec la clé privée spécifiée. Si l'entrée est une requête de certificat, génère un certificat auto-signé

-clrext Supprime des extensions d'un certificat

-keyform PEM|DER Format de la clé privée

-days arg Spécifie le nombre de jours pour créer une validité pour le certificat

-x509toreq Convertit un certificat en une requête

-req L'entrée est une requete au lieu d'un certificat

-set_serial n Numéro de série à utiliser en décimal ou hexa

-CA filename Certificat de la CA à utiliser pour signer le certificat

-CAkey filename Clé privée de la CA

-CAserial filename Définis le fichier de numéro de série à utiliser

-CAcreateserial Créé le fichier de numéro de série s'il n'existe pas

-extfile filename Fichier contenant les extensions à utiliser

-extensions section Section où se trouvent les extensions à ajouter

Options de nommage

compat Utiliser l'ancien formats, équivalent à ne spécifier aucune option de nommage

RFC2253 Affiche les noms compatibles avec la rfc2253 equivalent à spécifier : **esc_2253, esc_ctrl, esc_msb, utf8, dump_nostr, dump_unknown, dump_der, sep_comma_plus, dn_rev et sname**

oneline Format oneline, plus lisible que rfc2253. equivalent à spécifier : **esc_2253, esc_ctrl, esc_msb, utf8, dump_nostr, dump_der, use_quote, sep_comma_plus_space, space_eq et sname**

multiline Format multiligne. équivalent à spécifier : **esc_ctrl, esc_msb, sep_multiline, space_eq, lname et align**.

esc_2253 Échappe les caractères spéciaux (,+"<>;#) requis par la rfc2253

esc_ctrl Échappe les caractères de contrôle d'échappement

esc_msb Echappe les caractères avec le MSB mis, c'est à dire les valeurs ASCII > 127

use_quote Échappe certains caractères en les plaçant entre "" au lieu de \

utf8 Convertit toutes les chaînes en UTF8

no_type Ne tente pas d'interpréter les caractères multi-octets

show_type Affiche le type de chaîne caractère ASN1

dump_der Dump en encodé DER les champs qui doivent être dumpé en hexa

dump_nostr Dump les types de chaînes non caractères

dump_all Dump tous les champs

dump_unknown Dump les champs dont l'OID n'est pas reconnus par openssl

sep_comma_plus
sep_comma_plus_space
sep_semi_plus_space
sep_multiline Déterminent les séparateurs de champs
dn_rev Renverse les champs d'un DN
nofname
sname
lname
oid Altère la manière dont le nom des champs est affiché
align Aligne les valeurs de champs
space_eq Met des espace autour du caractère '='

Options de texte

compatible Utiliser l'ancien formats, équivalent à ne spécifier aucune option de sortie
no_header N'affiche pas les en-têtes
no_version N'affiche pas le numéro de version
no_serial N'affiche pas le numéro de série
no_signame N'affiche pas l'algorithme de signature utilisé
no_validity N'affiche pas la validité
no_subject N'affiche pas le sujet
no_issuer N'affiche pas l'issuer
no_pubkey N'affiche pas la clé publique
no_sigdump Ne dump par la signature du certificat
no_aux N'affiche pas les informations de trust du certificat
no_extensions N'affiche pas les extensions X509v3
ext_default Tente d'afficher les extensions de certificat non supportés
ext_error Affiche une erreur pour les extensions de certificat non supportés
ext_parse Parse en ASN1 les extensions non supportés
ext_dump Dumps en hexa les extensions non supportés
ca_default Valeur utilisé par l'utilitaire ca. equivalent à **o_issuer, no_pubkey, no_header, no_version, no_sigdump et no_signame**

Exemples

Afficher le contenu d'un certificat :
openssl x509 -in cert.pem -noout -text
Afficher le numérode série d'un certificat :
openssl x509 -in cert.pem -noout -serial
Affiche le sujet d'un certificat :
openssl x509 -in cert.pem -noout -subject
Afficher le sujet du certificat sous la forme RFC2253 :
openssl x509 -in cert.pem -noout -subject -nameopt RFC2253
Afficher le sujet du certificat en une ligne et en utf8 :
openssl x509 -in cert.pem -noout -subject -nameopt oneline,-esc_msb
Affiche l'empreinte MD5 du certificat :
openssl x509 -in cert.pem -noout -fingerprint
Affiche l'empreinte SHA1 du certificat :

openssl x509 -sha1 -in cert.pem -noout -fingerprint
Convertir un certificat PEM en DER :
openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
Convertit un certificat en requête :
openssl x509 -x509toreq -in cert.pem -out req.pem -signkey key.pem
Convertit une requête en un certificat auto-signé utilisant des extensions :
openssl x509 -req -in careq.pem -extfile openssl.cnf -extensions v3_ca -signkey key.pem -out cacert.pem
Signer une requête en utilisant le certificat d'un CA et en ajoutant des extensions utilisateur :
openssl x509 -req -in req.pem -extfile openssl.cnf -extensions v3_usr -CA cacert.pem -CAkey key.pem -CAcreateserial
Définis un certificat à truster pour un client SSL et changer son alias en "Steve's Class 1 CA" :
openssl x509 -in cert.pem -addtrust clientAuth -setalias "Steve's Class 1 CA" -out trust.pem

Notes

Le format PEM utilise les élements suivants :

```
---BEGIN CERTIFICATE---
---END CERTIFICATE---
```

ou :

```
---BEGIN X509 CERTIFICATE---
---END X509 CERTIFICATE---
```

Les certificats trustés auronts les lignes :

```
---BEGIN TRUSTED CERTIFICATE---
---END TRUSTED CERTIFICATE---
```

Extensions de certificat

l'option **-purpose** vérifie les extensions de certificat et détermine l'utilisation du certificat.

basicContraints (Bool)Cette extension est utilisé pour déterminer si le certificat peut être utilisé comme CA.

keyUsage Cette extension contient des restrictions sur l'utilisation du certificat. Un certificat CA doit avoir le but keyCertSign mis si cette extension est présente.

Description de chaque tests

SSL Client L'extension d'utilisation de clé doit être absent ou inclure l'OID web client authentication. keyUsage doit être absent ou avoir le bit digitalSignature mis.

SSL Client CA L'extension d'utilisation de clé doit être absent ou inclure l'OID web client authentication.

SSL Server L'extension d'utilisation de clé doit être absent ou inclure l'OID web server authentication et/ou un OID SGC. keyUsage doit être absent ou avoir le bit digitalSignature et/ou keyEncipherment mis.

SSL Server CA L'extension d'utilisation de clé doit être absent ou inclure l'OID web server authentication et/ou un OID SGC.

Netscape SSL Server Pour que les clients Netscape se connectent à un serveur SSL il doitavoir le bit keyEncipherment mis si keyUsage est présent

Common S/MIME Client Tests L'extension d'utilisation de clé doit être absent ou inclure l'OID email protection.

S/MIME Signing idem, et test le bit digitalSignature sur keyUsage est présent

S/MIME Encryption idem et test le bit keyEncipherment sur keyUsage est présent

S/MIME CA L'extension d'utilisation de clé doit être absent ou inclure l'OID email protection.

CRL Signing KeyUsage doit être absent ou avoir le bit CRL Signing mis.

CRL Signing CA Test normal CA, excepté que l'extention basicContraints ne doit pas être présent