OpenSSL - présentation

Utilitaire cryptographique

OpenSSL est un utilitaire cryptographique implémentant SSL v2/v3 et TLS v1 et les standards cryptographiques liés. Il permet de :

- Crée des paramètres de clé RSA, DH et DSA
- Créer des certificats X.509, CSR et CRL
- Calculer les digests de messages
- Crypter et décrypter avec chiffrement
- Tests client/serveur SSL/TLS
- Manipuler les mails signé ou chiffré S/MIME

Sommaire des commandes

list-standard-commands Affiche la liste des commandes standards
list-message-digest-commands Affiche la liste des commandes Digest standard
list-cipher-commands Affiche la liste des commandes de chiffrement standard
list-public-key-algorithms Liste les algorithmes de clé publique supportés.
no-<commande> test si une commande est disponible. (Sort 0 si la commande existe, 1 sinon)

Commandes standards

asn1parse Parse une séquence ASN.1
ca Gestion de CA
ciphers Détermine le Cipher Suite Description
cms Utilitaire CMS
crl Gestion de CRL
crl2pkcs7 Conversion de CRL vers pkcs7
dgst Calcul de Message Digest
dh Gestion des paramètre Diffie Hellman
dhparam Génération et gestion des paramètres Diffie Hellman
dsa Gestion des données DSA
dsaparam Génération des paramètres DSA
ec Traitement de clé EC
ecparam Génération et manipulation de paramètres EC
enc Encodage avec Chiffrement
engine Information et manipulation du moteur
errstr Conversion des numéro d'erreur en message d'erreur
gendh Génération des paramètres Diffie Hellman
gendsa Génération des paramètres DSA

genrsa Génération des paramètres RSA
genpkey Génération des clés privée ou paramètres
nseq Créer ou examiner une séquence de certificat Netscape
ocsp Utilitaire pour le protocole Online Certificate Status
passwd Génération de hash de mot de passe
pkcs12 Gestion des données PKCS #12
pkcs7 Gestion des données PKCS #7
pkey Gestion de clé publique et privée
pkeyparam Gestion des paramètres d'algorithme de clé publique
pkeyutl Utilitaire pour les opérations cryptographique de clé publique
rand Génère des octets pseudo-aléatoire
req Gestion des CSR
rsa Gestion des données RSA
rsautil Utilitaire RSA pour signer, vérifier, chiffrer et déchiffrer
s_client Implémente un client générique SSL/TLS pour établir une connexion transparente à un serveur distant.
s_server Implémente un serveur SSL/TLS qui accepte les connections depuis des clients distant.
s_time Timer de connexion SSL
sess_id Gestion de données de session SSL
smime Traitement des mail S/MIME
speed Mesure de vitesse des algorithmes
spkac Utilitaire de génération et d'affichage SPKAC
ts Outil client/serveur d'autorité TimeStamping
verify Vérification de certificats X.509
version Information de version d'openssl
x509 Gestion des données des certificats x509

Commandes Digest Standards

md2 digest md2
md5 Digest md5
mdc2 digest mdc2
rmd160 digestion RMD-160
sha digest sha
sha1 digest sha-1
sha224 digest sha-224
sha256 digest sha-256
sha384 digest sha-384
sha512 digest sha-512

Commandes d'encodage et de chiffrement

base64 Encodage en base64
bf bf-cbc bf-cfb bf-ecb bf-ofb Chiffrement blowfish
cast cast-cbc Chiffrement CAST

cast5-cbc cast5-cfb cast5-ecb cast5-ofb Chiffrement CAST5

des des-cbc des-cfb des-ecb des-ede des-ebe-cbc des-ebe-cfb des-ebe-ofb des-ofb Chiffrement DES

des3 desx des-ede3 des-ede3-cdc des-ede3-cfb des-ede3-ofb Chiffrement TRIPLE-DES

idea idea-cbc idea-cfb idea-ecb idea-ofb Chiffrement IDEA

rc2 rc2-cbc rc2-ecb rc2-ofb Chiffrement RC2

rc4 Chiffrement rc4

rc5 rc5-cbc rc5-cfb rc5-ecb rc5-ofb Chiffrement rc5

Arguments de pass-phrase

pass :password Le mot de passe actuel est password.

env :var Obtenir le mot de pass depuis la variable d'environnement var

file :pathname La première ligne du fichier est le mot de passe. Si ce même fichier est spécifié à -passin et -passout, la première ligne est pour l'entrée la ligne suivante est pour la sortie

fd :number Lit le mot de passe depuis le descripteur de fichier spécifié

stdin Lit le mot de passe depuis l'entrée standard