Content-type: text/html

OPENSSL

Section: OpenSSL (1)
Updated: 0.9.6a
Index Return to Main Contents

NOM

openssl - OpenSSL - Outil de ligne de commande

SYNOPSIS

openssl *commande* [*options_commande*] [*arguments_commande*]

openssl [**commandes-standard-liste**|**commandes-signature-messages-liste**|**commande-chiffrement-liste**]

openssl no-*XXX* [*options arbitraires*]

DESCRIPTION

OpenSSL est un utilitaire cryptographique qui implémente les protocoles réseau Secure Sockets Layer (SSL v2/v3, Couche de sockets sécurisés) et Transport Layer Security (TLS v1, sécurité pour la couche de transport) ainsi que les standards cryptographiques liés dont ils ont besoin.

Le programme **openssl** est un outil de ligne de commande pour utiliser les différentes fonctions cryptographiques de la librairie **crypto** d'OpenSSL à partir du shell. Il peut être utilisé pour

- Création de paramètres des clefs RSA, DH et DSA
- Création de certificats X.509, CSRs et CRLs
- Calcul de signature de messages
- Chiffrement et Déchiffrement
- Tests SSL/TLS client et server
- Gestion de mail S/MIME signé ou chiffrés

RESUME DES COMMANDES

Le programme **openssl** fournit une variété de commandes (*commande* dans le SYNOPSIS ci-dessus), dont chacune possède de nombreuses options et arguments. (*options-commande* et *arguments-commande* dans la SYNOPSIS).

Les commandes-pseudo **commandes-standard-liste**, **commandes-signature-message-liste**, et **commande-chiffrement-liste** génèrent une liste (une entrée par ligne) des noms de toutes les commandes standards, commandes de signature de messages (NdT ex : MD5) ou commandes de chiffrement, respectivement, qui sont disponible dans le présent utilitaire **openssl**.

La commande-pseudo **no-***XXX* teste si une commande du nom donné existe. Si aucune commande nommée *XXX* n'existe, le retour vaut 0 (succès) et l'affichage **no-***XXX* ; sinon le retour vaut 1 et l'affichage *XXX*. Dans les deux cas, la sortie est dirigée vers **stdout** (NdT : Sortie standard) et le flux **stderr** n'est pas utilisé. Les arguments de ligne de commande supplémentaires sont ignorés. Comme pour chaque chiffrement, il existe une commande portant le même nom, ceci fournit aux scripts shell une façon simple de tester la disponibilité des chiffrements dans le programme **openssl**. (**no-***XXX* n'est pas capable de détecter des pseudo-commandes telles que **quit**, **list-**...**-commands**, ou **no-***XXX* lui-même.)

COMMANDES STANDARDS

asn1parse
: Traitement d'une séquence ASN.1.

ca
: Gestion Certificate Authority (CA).

ciphers
: Détermination de la description de la suite de chiffrement.

crl
: Gestion Certificate Revocation List (CRL).

crl2pkcs7
: Conversion CRL vers PKCS#7.

dgst
: Calcul signature message (MD5).

dh
: Gestion des paramètres Diffie-Hellman. Obsolète par **dhparam**.

dsa
: Gestion données DSA.

dsaparam
: Génération paramètres DSA.

enc
: Chiffrement.

errstr
: Conversion numéro d'erreur vers descriptif texte (String).

dhparam
: Génération et gestion de paramètres Diffie-Hellman.

gendh
: Génération de paramètres Diffie-Hellman. Obsolète par **dhparam**.

gendsa

Génération de paramètres DSA.

genrsa

Génération de paramètres RSA.

passwd

Génération de mots de passe hashés.

pkcs7

Gestion données PKCS#7.

rand

Génère octets pseudo-aléatoires.

req

Gestion X.509 Certificate Signing Request (CSR).

rsa

Gestion données RSA.

rsautl

Utilitaire RSA pour signature, vérification, chiffrement, et déchiffrement.

s_client

Ceci fournit un client SSL/TLS générique qui sait établir une connexion transparente avec un serveur distant parlant SSL/TLS. ётant seulement prévu pour des propos de test, il n'offre qu'une interface fonctionnelle rudimentaire tout en utilisant en interne la quasi-totalité des fonctionnalités de la librairie **ssl** d'OpenSSL.

s_server

Ceci fournit un client SSL/TLS générique qui accepte des connexions transparentes provenant de clients qui parlent SSL/TLS. ётant seulement prévu pour des propos de test, il n'offre qu'une interface fonctionnelle rudimentaire tout en utilisant en interne la quasi-totalité des fonctionnalités de la librairie **ssl** d'OpenSSL. Il fournit à la fois son propre protocole orienté commandes en ligne pour le test de fonctions SSL et une facilité de réponse simple HTTP pour émuler un serveur internet qui gère SSL/TLS.

s_time

Horlogeur de connections SSL.

sess_id

Gestion des données de session SSL.

smime

Traitement mails S/MIME.

speed

Mesure la vitesse de l'algorithme.

verify

Vérification du certificat X.509.

version

Information sur la version d'OpenSSL.

x509

Gestion de données pour le certificat X.509.

COMMANDES DE SIGNATURE DE MESSAGE

md2

Signature MD2

md5

Signature MD5

mdc2

Signature MDC2

rmd160

Signature RMD-160

sha

Signature SHA

sha1

Signature SHA-1

COMMANDES D'ENCODAGE ET DE CHIFFREMENT

base64

Chiffrement 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-ede-cbc des-ede-cfb des-ede-ofb des-ofb

Chiffrement DES

des3 desx des-ede3 des-ede3-cbc des-ede3-cfb des-ede3-ofb

Chiffrement Triple-DES

idea idea-cbc idea-cfb idea-ecb idea-ofb

Chiffrement IDEA

rc2 rc2-cbc rc2-cfb rc2-ecb rc2-ofb

Chiffrement RC2

rc4

Chiffrement RC4

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

Chiffrement RC5

ARGUMENTS DE PHRASE DE PASSE

Certaines commandes acceptent des arguments de mot de passe, typiquement en utilisant **-passin** et **-passout** pour les mots de passe d'entrée et de sortie respectivement. Ceux-ci permettent d'obtenir le mot de passe à partir de plusieurs sources. Les deux options prennent un seul argument dont le format est décrit ci-dessous. Si aucun argument de mot de passe n'est donné alors qu'il est requis, l'utilisateur doit en fournir un : typiquement, cette requête est lancée sur le terminal avec l'écho désactivé (NdT : pas d'affichage des caractères tapés).

pass:motdepasse

Le mot de passe utilisé est **motdepasse**. Comme le mot de passe est visible à des utilitaires externes (tels que `ps' sous Unix), cette forme ne devrait être employé lorsque la sécurité n'est pas importante.

env:var
: Obtenir le mot de passe de la variable d'environnement **var**. Comme l'environnement d'autres processus est visible sur certaines plates-formes (ex : ps sous certaines versions d'Unix) cette option devrait être utilisé avec précaution.

file:pathname
: La première ligne de **pathname** est le mot de passe. Si le même **pathname** est donné pour les arguments **-passin** et **-passout**, alors la première ligne sert pour le mot de passe d'entrée et la suivante pour celui de sortie. **pathname** n'est pas obligatoirement un fichier régulier : il peut par exemple faire référence à un périphérique logique ou encore un tuyau nommé.

fd:number
: lit le mot de passe du descripteur de fichier **number**. Ceci peut être utilisé pour envoyer les données via un tuyau par exemple.

stdin
: lecture sur l'entrée standard.

VOIR AUSSI

asn1parse(1), ca(1), config(5), crl(1), crl2pkcs7(1), dgst(1), dhparam(1), dsa(1), dsaparam(1), enc(1), gendsa(1), genrsa(1), nseq(1), openssl(1), passwd(1), pkcs12(1), pkcs7(1), pkcs8(1), rand(1), req(1), rsa(1), rsautl(1), s_client(1), s_server(1), smime(1), spkac(1), verify(1), version(1), x509(1), crypto(3), ssl(3)

HISTORIQUE

La page de man *openssl*(1) est apparue dans la version 0.9.2 d'OpenSSL. Les pseudo-commandes **list-*XXX*-commands** ont été ajoutées pour la version 0.9.3 d'OpenSSL ; La pseudo-commande **no-*XXX*** a été ajoutée pour la version 0.9.5a d'OpenSSL. Pour des remarques concernant la disponibilité d'autres commandes, regarder les pages de manuel correspondantes.

Index

This document was created by man2html, using the manual pages.
Time: 20:41:58 GMT, July 10, 2005