# OpenSSL - smime

Utilitaire smime

# OPTIONS

**-encrypt** Chiffrer un mail.

**-decrypt** Déchiffrer un mail

**-sign** Signer un mail

**-verify** Vérifier un mail signé

**-pk7out** Prend un message et le sort sous forme d'une structure PKCS#7 PEM

**-resign** Resigne un message

**-in filename** Ficher d'entrée

**-inform SMIME|PEM-DER** Format du fichier d'entrée

**-out filename** Fichier de sortie

**-outform SMIME|PEM|DER** Format du fichier de sortie

**-stream -indef** sont équivalent et activent le streaming I/O pour les opérations d'encodage. Permet de traiter en une seule passe sans maintenir toutes les données en mémoire.

**-noindef** Désactive le streaming I/O

**-content filename** Ficher contenant le contenu détaché. Utilisable si la structure PKCS#7 utilise la signature détachée, où le contenu n'est pas inclus.

**-text** Ajoute les en-têtes MIME en texte clair.

**-CAfile file** Fichier contenant la chaînes des certificats à truster, utilisé avec -verify

**-CApath dir** Répertoire contenant les certificats CA en 'hash form'

**-md digest** Algorithme de digest à utiliser pour signer ou resigner. (Défaut SHA1)

**-[cipher]** Algorithme de chiffrement à utiliser (défaut RC2 40bits)

**-nointern** Normalement lors de la vérification d'un message, les certificats inclus dans le message sont recherché pour valider la signature. Cette options utilise ceux spécifié avec -certfile.

**-noverify** Ne pas vérifier le certificat du signataire d'un message signé

**-nochain** Ne pas vérifier la chaîne de certificats des signataires.

**-nosigs** Ne tente pas de vérifier les signatures dans le message

**-nocerts** En signant un message, le certificat du signataire est normalement inclus. Cette option ne l'inclus pas.

**-noattr** Normalement un message signé inclus des attributs dont la date de signature et les algorithmes symmétriques supportés. Cette option ne les inclus pas.

**-binary** Normalement le message est convertit au format canonique utilisant CR et LF comme fin de ligne comme requis dans la spécification S/MIME. Avec cette option, aucune traduction n'est faite.

**-nodetach** En signant un message avec une signature opaque, plus résistant aux traductions par relais mais ne peuvent pas être lus pas des MTA qui ne supportent pas S/MIME. Avec cette option, aucune traduction n'est faite.

**-certfile file** Certificats PEM additionnels à inclure avec le message.

**-signer file** Certificats des signataires si un message est vérifié avec succès, ces certificats seront écris dans le fichier.

**-recip file** Certificat pour déchiffrer un message. Doit matcher un des bénéficiaires du message.

**-inkey file** La clé privée à utiliser pour signer ou déchiffrer. Peut être spécifié plusieurs fois.

**-passin arg** Source du mot de passe de la clé privée.

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

**cert.pem** Un ou plusieurs certificats utilisés pour chiffrer un message

**-to, -from, -subject** Champs d'en-tête du mail

**-purpose, -ignore_critical, -issuer_checks, -crl_check, -crl_check_all, -policy_check,**

**-extended_crl, -x509_strict, -policy -check_ss_sig** Diverses options de vérification de chaîne de certificat. voir verify

# Notes

Cette version ne permet qu'un seul signataire, mais permet de vérifier des messages contenant plusieurs signataires.

# Codes de sortie

**0** succès de l'opération

**1** Une erreur s'est produite en parsant les options

**2** Un des fichiers en entrée ne peut être lu

**3** Une erreur s'est produite en créant un fichier PKCS #7 ou en lisant un message SMIME

**4** Une erreur s'est produite en déchiffrant ou en vérifiant le message

**5** Le message a été vérifié correctement mais une erreur s'est produite en écrivant les certificats des signataires

# Exemples

Créer un message signé en texte clair :
**openssl smime -sign -in message.txt -text -out mail.msg -signer mycert.pem**
Créer un message signé opaque :
**openssl smime -sign -in message.txt -text -out mail.msg -nodetach -signer mycert.pem**
Créer un message signé, incluant des certificats additionnels et en lisant la clé privée depuis un autre fichier :
**openssl smime -sign -in in.txt -text -out mail.msg -signer mycert.pem -inkey mykey.pem -certfile mycerts.pem**
Créer un message signé par 2 signataires :
**openssl smime -sign -in message.txt -text -out mail.msg -signer mycert.pem -signer othercert.pem**
Envoyer un message signé à sendmail, incluant des en-têtes :
**openssl smime -sign -in in.txt -text -signer mycert.pem -from steve@openssl.org -to someone@somewhere -subject "Signed message" | sendmail someone@somewhere**
Vérifier un message et extraire le certificat du signataire :
**openssl smime -verify -in mail.msg -signer user.pem -out signedtext.txt**
Envoyer un message chiffré avec 3DES :
**openssl smime -encrypt -in in.txt -from steve@openssl.org -to someone@somewhere -subject "Encrypted message" -des3 user.pem -out mail.msg**
Signer et chiffrer un mail :
**openssl smime -sign -in ml.txt -signer my.pem -text | openssl smime -encrypt -out mail.msg -from steve@openssl.org -to someone@somewhere -subject "Signed and Encrypted message" -des3 user.pem**
Déchiffrer un mail :
**openssl smime -decrypt -in mail.msg -recip mycert.pem -inkey key.pem**
Créer un message chiffrer avec Camellia 128bits :
**openssl smime -encrypt -in plain.txt -camellia128 -out mail.msg cert.pem**
Ajouter un signataire à un message :
**openssl smime -resign -in mail.msg -signer newsign.pem -out mail2.msg**