NAME

clsmime − S/MIME public key encryption tool interoperating with Thunderbird, Evolution, Outlook and OpenSSL

SYNOPSIS

clsmime [OPTIONS] encrypt messagefile certificate

clsmime [OPTIONS] decrypt encrypted_message KeysetName

clsmime [OPTIONS] sign messagefile KeysetName

clsmime [OPTIONS] verify signed_message [CArootCertificate]

clsmime [OPTIONS] list [<NumLines>] MessageFile

DESCRIPTION

clsmime encrypts text or binary data with a RSA **public key** stored in a recipients's certificate file.

clsmime decrypts or signs S/MIME data with a RSA **private key** stored in a *.p15 keyset file. RSA public and private keys stored in *.p15 keyset file can be generated and managed with **clkeys**.

clsmime verifies S/MIME signatures with enclosed certificates. The signer's certificate will be checked against an optional issuer CA certificate. This CA certificate will be considered as a trusted CA root certificate.

The resulting encrypted and/or signed S/MIME message files can be exchanged with either OpenSSL or Email clients that support the processing of S/MIME messages (like Thunderbird, Evolution or MS Outlook).

OPTIONS

−help   display this help and exit

−version

output version information and exit

−debug

print debugging information to stderr

−detach

generate a detached signature in S/MIME format as multipart/signed
(default is a signature including the enclosed text message)

-integritycheck

forces integrity protection while encrypting data.
The cryptogram is enveloped in a authEnvelopedData object that cannot be decrypted with OpenSSL.
Use this option when the output data is processed with **clsmime**.

−binary

do not change the input bytes (default is **text mode**)

in **text mode** all '\n' are replaced by '\r\n' and a Content-Type header is added in front of the input bytes before the message is signed. When clsmime verifies a signed message, the Content-Type header and the additional '\r' characters are removed after verification. Thus the verification bytes that are stored into the file system match the original text message.

−certchain

write the certificate chain to the file system during verification of a S/MIME signature.

INTEROPERABILITY

S/MIME capable E-mail clients (Thunderbird, Evolution, Outlook)

Thunderbird or Evolution: Import the CA certificate (into the CA section) before you import a user's certificate (into the person section).

Microsoft Outlook: Use the contacts tab to enter the Common Name and the email address and finally click on the 'certificate button' to import the contact's certificate stored in a *.cer file.

OpenSSL

The following OpenSSL commands can be used to exchange message files with **clsmime** :

Encryption :
openssl smime -encrypt -aes-256-cbc -in message -binary -out message.smime certfile

Decryption :
openssl smime -decrypt -in message -out message.clear -recip cert -inkey RSAkey

Signing   :
openssl smime -sign -in message -text -signer cert -inkey RSAkey -out message.sig

Verification :
openssl smime -verify -in message -out message.verified -inkey certfile -CAfile CAcert

CertChains can be examined with:
sed -i ´s/CERTIFICATE CHAIN/PKCS7/´ certchain ; openssl pkcs7 -in certchain -text -print_certs

NOTES
Full documentation <https://senderek.ie/cryptlib/tools>

This program depends on two packages providing the cryptlib shared object library and the python3-bindings to this library.

You can download both packages in RPM or DEB format at https://senderek.ie/cryptlib/downloads

Using FEDORA, you can install the packages cryptlib and cryptlib-python3 directly from the repository.

In addition the program /bin/systemd-ask-password is needed to read sensible data from stdin. This program is part of the systemd package.

FILES
/usr/bin/systemd-ask-password
        This program is used to provide the passphrase based on a user's input.

/usr/bin/dumpasn1
        This program is used to list the ASN1 structure of output files.

/lib64/libcl.so.3.4.8
        The cryptlib library.

/usr/lib/python3.1x/site-packages/cryptlib_py.so
Bindings to the cryptlib library used by python3.

BUGS
Please report bugs to innovation@senderek.ie

AUTHORS
clsmime is written by Ralf Senderek <innovation@senderek.ie>.
Cryptlib is written and maintained by Peter Gutmann <pgut001@cs.auckland.ac.nz>

COPYRIGHT
Copyright © 2024 - 2025 Ralf Senderek. All rights reserved.

License BSD-3-Clause: <https://senderek.ie/cryptlib/bsd.html>.
This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

SEE ALSO
cryptlib, clkeys, claes, clrsa