## NAME

**claes** – conventional encryption tool interoperating with gpg and openssl

## SYNOPSIS

**claes [-debug] [-cms | -openssl [-128]] [OPTION] [FILE | -]**

## DESCRIPTION

**claes** encrypts or decrypts data in OpenPGP format, CMS format and OPENSSL format using files or standard input with a passphrase-based AES cipher. If no FILE or "-" is given, data is read from standard input. The size of any input data is limited to 150 MByte. The default mode of operation is **encryption** with the ciphertext stored base64-encoded in the OpenPGP format. To decrypt base64-encoded or binary input data the option "-decrypt" must be used.

All input data is processed AS IS and is treated internally as binary data with no changes. For every encryption or decryption a user-provided passphrase is read from the terminal in which claes is run. So claes always works interactively. There is deliberately no public-key-cryptography build into claes. If you need those, please use clrsa and clkeys.

## OPTIONS

**–help** display this help and exit

**–version**
output version information and exit

**–debug**
print debugging information to stderr

**–cms** produce CMS enveloped and encrypted data instead of OpenPGP (default)

**–openssl**
produce encrypted data using pbkdf2 in openssl format

**–128** forces the use of 128 bit AES keys in conjunction with -openssl (256 bits is the default)

**–decrypt**
decrypts an encrypted message (default is encrypt)

## 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.

## INTEROPERABILITY

**gpg2**

Without any options claes produces OpenPGP (base64-encoded) encrypted messages using AES-128. It can decrypt any messages (ascii or binary) produced by GnuPG with the following ciphers: AES, AES192, AES256, 3DES and CAST-128.

**openssl**

In OpenSSL mode claes writes (base64-encoded) encrypted messages in the proprietary OpenSSL format using AES256 as the default.

These messages can be decrypted with openssl :
**openssl aes-256-cbc -pbkdf2 -d -a -in FILE.asc**

The use of AES-128 can be forced by the additional option -128 both for encryption or decryption of OpenSSL messages.

**CMS**

In CMS mode claes produces PKCS#7 formated (base64-encoded) enveloped and encrypted messages.

## FILES

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

/lib64/libcl.so.3.4.6
The cryptlib library.

/usr/lib/python3.10/site-packages/cryptlib_py.so
Bindings to the cryptlib library used by python3.

## BUGS

Please report bugs to innovation@senderek.ie

## AUTHORS

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

## COPYRIGHT



## SEE ALSO

cryptlib, clrsa, clkeys