## NAME

openssl−mac − perform Message Authentication Code operations

## SYNOPSIS

**openssl mac** [**−help**] [**−cipher**] [**−digest**] [**−macopt**] [**−in** *filename*] [**−out** *filename*] [**−binary**] [**−provider** *name*] [**−provider−path** *path*] [**−propquery** *propq*] *mac_name*

## DESCRIPTION

The message authentication code functions output the MAC of a supplied input file.

## OPTIONS

**−help**

Print a usage message.

**−in** *filename*

Input filename to calculate a MAC for, or standard input by default. Standard input is used if the filename is '−'. Files are expected to be in binary format, standard input uses hexadecimal text format.

**−out** *filename*

Filename to output to, or standard output by default.

**−binary**

Output the MAC in binary form. Uses hexadecimal text format if not specified.

**−cipher** *name*

Used by CMAC and GMAC to specify the cipher algorithm. For CMAC it must be one of AES−128−CBC, AES−192−CBC, AES−256−CBC or DES−EDE3−CBC. For GMAC it should be a GCM mode cipher e.g. AES−128−GCM.

**−digest** *name*

Used by HMAC as an alphanumeric string (use if the key contains printable characters only). The string length must conform to any restrictions of the MAC algorithm. To see the list of supported digests, use `openssl list −digest−commands`.

**−macopt** *nm*:*v*

Passes options to the MAC algorithm. A comprehensive list of controls can be found in the EVP_MAC implementation documentation. Common parameter names used by **EVP_MAC_CTX_get_params()** are:

**key:***string*

Specifies the MAC key as an alphanumeric string (use if the key contains printable characters only). The string length must conform to any restrictions of the MAC algorithm. A key must be specified for every MAC algorithm.

**hexkey:***string*

Specifies the MAC key in hexadecimal form (two hex digits per byte). The key length must conform to any restrictions of the MAC algorithm. A key must be specified for every MAC algorithm.

**iv:***string*

Used by GMAC to specify an IV as an alphanumeric string (use if the IV contains printable characters only).

**hexiv:***string*

Used by GMAC to specify an IV in hexadecimal form (two hex digits per byte).

**size:***int*

Used by KMAC128 or KMAC256 to specify an output length. The default sizes are 32 or 64 bytes respectively.

**custom:***string*

Used by KMAC128 or KMAC256 to specify a customization string. The default is the empty string "".

**digest:***string*
This option is identical to the **−digest** option.

**cipher:***string*
This option is identical to the **−cipher** option.

**−provider** *name*
**−provider−path** *path*
**−propquery** *propq*
See ‘‘Provider Options’’ in **openssl** (1), **provider** (7), and **property** (7).

*mac_name*
Specifies the name of a supported MAC algorithm which will be used. To see the list of supported MAC’s use the command `openssl list −mac−algorithms`.

## EXAMPLES

To create a hex-encoded HMAC−SHA1 MAC of a file and write to stdout: \
openssl mac −digest SHA1 \
−macopt hexkey:000102030405060708090A0B0C0D0E0F10111213 \
−in msg.bin HMAC

To create a SipHash MAC from a file with a binary file output: \
openssl mac −macopt hexkey:000102030405060708090A0B0C0D0E0F \
−in msg.bin −out out.bin −binary SipHash

To create a hex-encoded CMAC−AES−128−CBC MAC from a file:\
openssl mac −cipher AES−128−CBC \
−macopt hexkey:77A77FAF290C1FA30C683DF16BA7A77B \
−in msg.bin CMAC

To create a hex-encoded KMAC128 MAC from a file with a Customisation String ’Tag’ and output length of 16: \
openssl mac −macopt custom:Tag −macopt hexkey:40414243444546 \
−macopt size:16 −in msg.bin KMAC128

To create a hex-encoded GMAC−AES−128−GCM with a IV from a file: \
openssl mac −cipher AES−128−GCM −macopt hexiv:E0E00F19FED7BA0136A797F3 \
−macopt hexkey:77A77FAF290C1FA30C683DF16BA7A77B −in msg.bin GMAC

## NOTES

The MAC mechanisms that are available will depend on the options used when building OpenSSL. Use `openssl list −mac−algorithms`to list them.

## SEE ALSO

**openssl** (1), **EVP_MAC** (3), **EVP_MAC−CMAC** (7), **EVP_MAC−GMAC** (7), **EVP_MAC−HMAC** (7), **EVP_MAC−KMAC** (7), **EVP_MAC−Siphash** (7), **EVP_MAC−Poly1305** (7)

## COPYRIGHT

Copyright 2018−2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the ‘‘License’’). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.