



*Full credit is given to the above companies including the OS that this PDF file was generated!*

### ***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_MAC-CMAC.7ossl'***

***\$ man EVP\_MAC-CMAC.7ossl***

EVP\_MAC-CMAC(7ossl)          OpenSSL          EVP\_MAC-CMAC(7ossl)

#### NAME

EVP\_MAC-CMAC - The CMAC EVP\_MAC implementation

#### DESCRIPTION

Support for computing CMAC MACs through the EVP\_MAC API.

This implementation uses EVP\_CIPHER functions to get access to the underlying cipher.

#### Identity

This implementation is identified with this name and properties, to be used with EVP\_MAC\_fetch():

"CMAC", "provider=default" or "provider=fips"

The general description of these parameters can be found in "PARAMETERS" in EVP\_MAC(3).

The following parameter can be set with EVP\_MAC\_CTX\_set\_params():

"key" (OSSL\_MAC\_PARAM\_KEY) <octet string>

Sets the MAC key. Setting this parameter is identical to passing a key to EVP\_MAC\_init(3).

"cipher" (OSSL\_MAC\_PARAM\_CIPHER) <UTF8 string>

Sets the name of the underlying cipher to be used.

"properties" (OSSL\_MAC\_PARAM\_PROPERTIES) <UTF8 string>

Sets the properties to be queried when trying to fetch the underlying cipher. This must be given together with the cipher naming parameter to be considered valid.

The following parameters can be retrieved with

EVP\_MAC\_CTX\_get\_params():

"size" (OSSL\_MAC\_PARAM\_SIZE) <unsigned integer>

The "size" parameter can also be retrieved with with EVP\_MAC\_CTX\_get\_mac\_size(). The length of the "size" parameter is equal to that of an unsigned int.

"block-size" (OSSL\_MAC\_PARAM\_SIZE) <unsigned integer>

Gets the MAC block size. The "block-size" parameter can also be retrieved with EVP\_MAC\_CTX\_get\_block\_size().

#### SEE ALSO

EVP\_MAC\_CTX\_get\_params(3), EVP\_MAC\_CTX\_set\_params(3), "PARAMETERS" in EVP\_MAC(3), OSSL\_PARAM(3)

## 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>.

3.0.7                    2023-07-13            EVP\_MAC-CMAC(7ossl)