



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

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_MAC-BLAKE2SMAC.7ssl'***

***\$ man EVP\_MAC-BLAKE2SMAC.7ssl***

EVP\_MAC-BLAKE2(7SSL)                      OpenSSL                      EVP\_MAC-BLAKE2(7SSL)

**NAME**

EVP\_MAC-BLAKE2, EVP\_MAC-BLAKE2BMAC, EVP\_MAC-BLAKE2SMAC - The BLAKE2 EVP\_MAC implementations

**DESCRIPTION**

Support for computing BLAKE2 MACs through the EVP\_MAC API.

**Identity**

These implementations are identified with one of these names and properties, to be used with EVP\_MAC\_fetch():

"BLAKE2BMAC", "provider=default"

"BLAKE2SMAC", "provider=default"

**Supported parameters**

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

All these parameters can be set with EVP\_MAC\_CTX\_set\_params(). Furthermore, the "size" parameter can be retrieved with EVP\_MAC\_CTX\_get\_params(), or with EVP\_MAC\_CTX\_get\_mac\_size(). The length of the "size" parameter should not exceed that of a size\_t. Likewise, the "block-size" parameter can be retrieved with

EVP\_MAC\_CTX\_get\_params(), or with EVP\_MAC\_CTX\_get\_block\_size().

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

Sets the MAC key. It may be at most 64 bytes for BLAKE2BMAC or 32 for BLAKE2SMAC and at least 1 byte in both cases. Setting this parameter is identical to passing a key to EVP\_MAC\_init(3).

"custom" (OSSL\_MAC\_PARAM\_CUSTOM) <octet string>

Sets the custom value. It is an optional value of at most 16 bytes for BLAKE2BMAC or 8 for BLAKE2SMAC, and is empty by default.

"salt" (OSSL\_MAC\_PARAM\_SALT) <octet string>

Sets the salt. It is an optional value of at most 16 bytes for BLAKE2BMAC or 8 for BLAKE2SMAC, and is empty by default.

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

Sets the MAC size. It can be any number between 1 and 32 for EVP\_MAC\_BLAKE2S or between 1 and 64 for EVP\_MAC\_BLAKE2B. It is 32 and 64 respectively by default.

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

Gets the MAC block size. By default, it is 64 for EVP\_MAC\_BLAKE2S and 128 for EVP\_MAC\_BLAKE2B.

## SEE ALSO

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

## HISTORY

The macros and functions described here were added to OpenSSL 3.0.

## 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>>.

3.0.2

2024-02-16

EVP\_MAC-BLAKE2(7SSL)