



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-Siphash.7ssl'

\$ man EVP_MAC-Siphash.7ssl

EVP_MAC-SIPHASH(7SSL) OpenSSL EVP_MAC-SIPHASH(7SSL)

NAME

EVP_MAC-Siphash - The Siphash EVP_MAC implementation

DESCRIPTION

Support for computing Siphash MACs through the EVP_MAC API.

Identity

This implementation is identified with this name and properties, to be used with

EVP_MAC_fetch():

"SIPHASH", "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.

"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)`.

"size" (`OSSL_MAC_PARAM_SIZE`) <unsigned integer>

Sets the MAC size.

"c-rounds" (`OSSL_MAC_PARAM_C_ROUNDS`) <unsigned integer>

Specifies the number of rounds per message block. By default this is 2.

"d-rounds" (`OSSL_MAC_PARAM_D_ROUNDS`) <unsigned integer>

Specifies the number of finalisation rounds. By default this is 4.

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>>.