



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

## ***Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP\_MAC-Siphash.7oss1' command***

***\$ man EVP\_MAC-Siphash.7oss1***

EVP\_MAC-SIPHASH(7oss1)      OpenSSL      EVP\_MAC-SIPHASH(7oss1)

### 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>.

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