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.7ossl' command

$ man EVP_MAC-Siphash.7ossl

EVP_MAC-SIPHASH(7ossl) OpenSSL EVP_MAC-SIPHASH(7ossl)

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