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-BLAKE2.7ossl' command

$ man EVP_MAC-BLAKE2.7ossl

EVP_MAC-BLAKE2(7ossl) OpenSSL EVP_MAC-BLAKE2(7ossl)

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