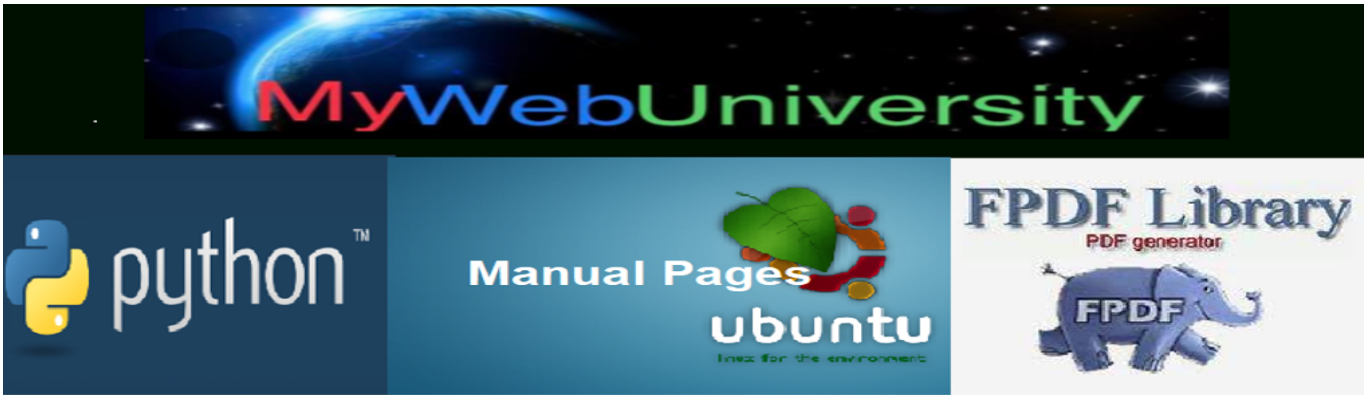

Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_MAC-HMAC.7ssl'

$ man EVP_MAC-HMAC.7ssl

NAME

EVP_MAC-HMAC - The HMAC EVP_MAC implementation

DESCRIPTION

Support for computing HMAC MACs through the EVP_MAC API.

This implementation uses EVP_MD functions to get access to the underlying digest.

Identity

This implementation is identified with this name and properties, to be used with EVP_MAC_fetch():

"HMAC", "provider=default" or "provider=fips"

Supported parameters

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

The following parameter can be set with EVP_MAC_CTX_set_params():

"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).

"digest" (OSSL_MAC_PARAM_DIGEST) <UTF8 string>

Sets the name of the underlying digest to be used.

"properties" (OSSL_MAC_PARAM_PROPERTIES) <UTF8 string>

Sets the properties to be queried when trying to fetch the underlying digest. This must be given together with the digest naming parameter ("digest", or OSSL_MAC_PARAM_DIGEST) to be considered valid.

"digest-noinit" (OSSL_MAC_PARAM_DIGEST_NOINIT) <integer>

A flag to set the MAC digest to not initialise the implementation specific data. The value 0 or 1 is expected.

"digest-oneshot" (OSSL_MAC_PARAM_DIGEST_ONESHOT) <integer>

A flag to set the MAC digest to be a one-shot operation. The value 0 or 1 is expected.

"tls-data-size" (OSSL_MAC_PARAM_TLS_DATA_SIZE) <unsigned integer>

The following parameter can be retrieved with EVP_MAC_CTX_get_params():

"size" (OSSL_MAC_PARAM_SIZE) <unsigned integer>

The "size" parameter can also be retrieved with EVP_MAC_CTX_get_mac_size(). The length of the "size" parameter is equal to that of an unsigned int.

"block-size" (OSSL_MAC_PARAM_SIZE) <unsigned integer>

Gets the MAC block size. The "block-size" parameter can also be retrieved with EVP_MAC_CTX_get_block_size().

SEE ALSO

EVP_MAC_CTX_get_params(3), EVP_MAC_CTX_set_params(3), "PARAMETERS" in EVP_MAC(3), OSSL_PARAM(3), HMAC(3)

COPYRIGHT