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-Poly1305.7ossl' command

$ man EVP_MAC-Poly1305.7ossl

EVP_MAC-POLY1305(7ossl) OpenSSL EVP_MAC-POLY1305(7ossl)

NAME

EVP_MAC-Poly1305 - The Poly1305 EVP_MAC implementation

DESCRIPTION

Support for computing Poly1305 MACs through the EVP_MAC API.

Identity

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

"POLY1305", "provider=default"

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).

The following parameters can be retrieved with
EVP_MAC_CTX_get_params():

"size" (OSSL_MAC_PARAM_SIZE) <unsigned integer>
Gets the MAC size.

The "size" parameter can also be retrieved with with
EVP_MAC_CTX_get_mac_size(). The length of the "size" parameter should
not exceed that of an unsigned int.

NOTES

The OpenSSL implementation of the Poly 1305 MAC corresponds to RFC
7539.

It is critical to never reuse the key. The security implication noted
in RFC 8439 applies equally to the OpenSSL implementation.

SEE ALSO

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

COPYRIGHT