Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_chacha20_poly1305.3ossl'

$ man EVP_chacha20_poly1305.3ossl

EVP_CHACHA20(3ossl) OpenSSL EVP_CHACHA20(3ossl)

NAME

EVP_chacha20, EVP_chacha20_poly1305 - EVP ChaCha20 stream cipher

SYNOPSIS

#include <openssl/evp.h>

const EVP_CIPHER *EVP_chacha20(void);

const EVP_CIPHER *EVP_chacha20_poly1305(void);

DESCRIPTION

The ChaCha20 stream cipher for EVP.

EVP_chacha20()

The ChaCha20 stream cipher. The key length is 256 bits, the IV is

128 bits long. The first 32 bits consists of a counter in little-

endian order followed by a 96 bit nonce. For example a nonce of:

00000000000000000000002

With an initial counter of 42 (2a in hex) would be expressed as:

2a000000000000000000000000000002

EVP_chacha20_poly1305()

Authenticated encryption with ChaCha20-Poly1305. Like EVP_chacha20(), the key is 256 bits and the IV is 96 bits. This supports additional authenticated data (AAD) and produces a 128-bit authentication tag. See the "AEAD Interface" in EVP_EncryptInit(3) section for more information.

RETURN VALUES

These functions return an EVP_CIPHER structure that contains the implementation of the symmetric cipher. See EVP_CIPHER_meth_new(3) for details of the EVP_CIPHER structure.

SEE ALSO

evp(7), EVP_EncryptInit(3), EVP_CIPHER_meth_new(3)

COPYRIGHT