



*Full credit is given to the above companies including the OS that this PDF file was generated!*

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_chacha20\_poly1305.3oss1'***

***\$ man EVP\_chacha20\_poly1305.3oss1***

EVP\_CHACHA20(3oss1)            OpenSSL            EVP\_CHACHA20(3oss1)

**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:

00000000000000000000000000000002

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

Copyright 2017-2020 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.