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 64 bits consists of a counter in little-endian order followed by a 64 bit nonce. For example a nonce of:

0000000000000002

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

2a00000000000000000000000000000002

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.

NOTES

Developers should be aware of the negative performance implications of calling these functions multiple times and should consider using **EVP_CIPHER_fetch**(3) instead. See "Performance" in **crypto**(7) for further information.

RFC 7539 <https://www.rfc-editor.org/rfc/rfc7539.html#section-2.4> uses a 32 bit counter and a 96 bit nonce for the IV.

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