

NAME

SSL_get_current_cipher, SSL_get_cipher_name, SSL_get_cipher, SSL_get_cipher_bits, SSL_get_cipher_version, SSL_get_pending_cipher - get SSL_CIPHER of a connection

SYNOPSIS

```
#include <openssl/ssl.h>
```

```
const SSL_CIPHER *SSL_get_current_cipher(const SSL *ssl);  
const SSL_CIPHER *SSL_get_pending_cipher(const SSL *ssl);
```

```
const char *SSL_get_cipher_name(const SSL *s);  
const char *SSL_get_cipher(const SSL *s);  
int SSL_get_cipher_bits(const SSL *s, int *np);  
const char *SSL_get_cipher_version(const SSL *s);
```

DESCRIPTION

SSL_get_current_cipher() returns a pointer to an SSL_CIPHER object containing the description of the actually used cipher of a connection established with the **ssl** object. See **SSL_CIPHER_get_name(3)** for more details.

SSL_get_cipher_name() obtains the name of the currently used cipher. **SSL_get_cipher()** is identical to **SSL_get_cipher_name()**. **SSL_get_cipher_bits()** is a macro to obtain the number of secret/algorithm bits used and **SSL_get_cipher_version()** returns the protocol name.

SSL_get_pending_cipher() returns a pointer to an SSL_CIPHER object containing the description of the cipher (if any) that has been negotiated for future use on the connection established with the **ssl** object, but is not yet in use. This may be the case during handshake processing, when control flow can be returned to the application via any of several callback methods. The internal sequencing of handshake processing and callback invocation is not guaranteed to be stable from release to release, and at present only the callback set by **SSL_CTX_set_alpn_select_cb()** is guaranteed to have a non-NULL return value. Other callbacks may be added to this list over time.

RETURN VALUES

SSL_get_current_cipher() returns the cipher actually used, or NULL if no session has been established.

SSL_get_pending_cipher() returns the cipher to be used at the next change of cipher suite, or NULL if no such cipher is known.

NOTES

SSL_get_cipher, SSL_get_cipher_bits, SSL_get_cipher_version, and SSL_get_cipher_name are

implemented as macros.

SEE ALSO

ssl(7), **SSL_CIPHER_get_name**(3)

COPYRIGHT

Copyright 2000-2022 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>.