

NAME

SSL_get_peer_tmp_key, SSL_get_server_tmp_key, SSL_get_tmp_key - get information about temporary keys used during a handshake

SYNOPSIS

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

```
long SSL_get_peer_tmp_key(SSL *ssl, EVP_PKEY **key);
```

```
long SSL_get_server_tmp_key(SSL *ssl, EVP_PKEY **key);
```

```
long SSL_get_tmp_key(SSL *ssl, EVP_PKEY **key);
```

DESCRIPTION

SSL_get_peer_tmp_key() returns the temporary key provided by the peer and used during key exchange. For example, if ECDHE is in use, then this represents the peer's public ECDHE key. On success a pointer to the key is stored in ***key**. It is the caller's responsibility to free this key after use using **EVP_PKEY_free(3)**.

SSL_get_server_tmp_key() is a backwards compatibility alias for **SSL_get_peer_tmp_key()**. Under that name it worked just on the client side of the connection, its behaviour on the server end is release-dependent.

SSL_get_tmp_key() returns the equivalent information for the local end of the connection.

RETURN VALUES

All these functions return 1 on success and 0 otherwise.

NOTES

This function is implemented as a macro.

SEE ALSO

ssl(7), **EVP_PKEY_free(3)**

COPYRIGHT

Copyright 2017-2018 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>>.