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

$ man SSL_get_privatekey.3ossl

SSL_GET_CERTIFICATE(3ossl) OpenSSL SSL_GET_CERTIFICATE(3ossl)

NAME

SSL_get_certificate, SSL_get_privatekey - retrieve TLS/SSL certificate and private key

SYNOPSIS

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

X509 *SSL_get_certificate(const SSL *s);
EVP_PKEY *SSL_get_privatekey(const SSL *s);
```

DESCRIPTION

SSL_get_certificate() returns a pointer to an X509 object representing a certificate used as the local peer's identity.

Multiple certificates can be configured; for example, a server might have both RSA and ECDSA certificates. The certificate which is returned

by SSL_get_certificate() is determined as follows:

? If it is called before certificate selection has occurred, it returns the most recently added certificate, or NULL if no certificate has been added.

? After certificate selection has occurred, it returns the certificate which was selected during the handshake, or NULL if no certificate was selected (for example, on a client where no client certificate is in use).

Certificate selection occurs during the handshake; therefore, the value returned by SSL_get_certificate() during any callback made during the handshake process will depend on whether that callback is made before or after certificate selection occurs.

A specific use for SSL_get_certificate() is inside a callback set via a call to SSL_CTX_set_tlsext_status_cb(3). This callback occurs after certificate selection, where it can be used to examine a server's chosen certificate, for example for the purpose of identifying a certificate's OCSP responder URL so that an OCSP response can be obtained.

SSL_get_privatekey() returns a pointer to the EVP_PKEY object corresponding to the certificate returned by SSL_get_certificate(), if any.

RETURN VALUES

These functions return pointers to their respective objects, or NULL if no such object is available. Returned objects are owned by the SSL object and should not be freed by users of these functions.

SEE ALSO

ssl(7), SSL_CTX_set_tlsext_status_cb(3)

COPYRIGHT