NAME

SSL_get_peer_certificate, SSL_get0_peer_certificate, SSL_get1_peer_certificate - get the X509 certificate of the peer

SYNOPSIS

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

X509 *SSL_get_peer_certificate(const SSL *ssl);
X509 *SSL_get0_peer_certificate(const SSL *ssl);
X509 *SSL_get1_peer_certificate(const SSL *ssl);
```

DESCRIPTION

These functions return a pointer to the X509 certificate the peer presented. If the peer did not present a certificate, NULL is returned.

NOTES

Due to the protocol definition, a TLS/SSL server will always send a certificate, if present. A client will only send a certificate when explicitly requested to do so by the server (see **SSL_CTX_set_verify**(3)). If an anonymous cipher is used, no certificates are sent.

That a certificate is returned does not indicate information about the verification state, use **SSL_get_verify_result**(3) to check the verification state.

The reference count of the X509 object returned by **SSL_get1_peer_certificate()** is incremented by one, so that it will not be destroyed when the session containing the peer certificate is freed. The X509 object must be explicitly freed using **X509_free()**.

The reference count of the X509 object returned by **SSL_get0_peer_certificate()** is not incremented, and must not be freed.

SSL_get_peer_certificate() is an alias of **SSL_get1_peer_certificate()**.

RETURN VALUES

The following return values can occur:

NULL
: No certificate was presented by the peer or no connection was established.

Pointer to an X509 certificate
: The return value points to the certificate presented by the peer.

SEE ALSO

ssl(7), **SSL_get_verify_result**(3), **SSL_CTX_set_verify**(3)

HISTORY

SSL_get0_peer_certificate() and **SSL_get1_peer_certificate()** were added in 3.0.0.
SSL_get_peer_certificate() was deprecated in 3.0.0.

COPYRIGHT