NAME

SSL_get_peer_cert_chain, SSL_get0_verified_chain - get the X509 certificate chain of the peer

SYNOPSIS

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

 STACK_OF(X509) *SSL_get_peer_cert_chain(const SSL *ssl);
 STACK_OF(X509) *SSL_get0_verified_chain(const SSL *ssl);
```

DESCRIPTION

SSL_get_peer_cert_chain() returns a pointer to STACK_OF(X509) certificates forming the certificate chain sent by the peer. If called on the client side, the stack also contains the peer's certificate; if called on the server side, the peer's certificate must be obtained separately using **SSL_get_peer_certificate**(3). If the peer did not present a certificate, NULL is returned.

NB: **SSL_get_peer_cert_chain()** returns the peer chain as sent by the peer: it only consists of certificates the peer has sent (in the order the peer has sent them) it is **not** a verified chain.

SSL_get0_verified_chain() returns the **verified** certificate chain of the peer including the peer's end entity certificate. It must be called after a session has been successfully established. If peer verification was not successful (as indicated by **SSL_get_verify_result()** not returning X509_V_OK) the chain may be incomplete or invalid.

NOTES

If the session is resumed peers do not send certificates so a NULL pointer is returned by these functions. Applications can call **SSL_session_reused()** to determine whether a session is resumed.

The reference count of each certificate in the returned STACK_OF(X509) object is not incremented and the returned stack may be invalidated by renegotiation. If applications wish to use any certificates in the returned chain indefinitely they must increase the reference counts using **X509_up_ref()** or obtain a copy of the whole chain with **X509_chain_up_ref()**.

RETURN VALUES

The following return values can occur:

NULL

No certificate was presented by the peer or no connection was established or the certificate chain is no longer available when a session is reused.

Pointer to a STACK_OF(X509)

The return value points to the certificate chain presented by the peer.

SEE ALSO

ssl(7), **SSL_get_peer_certificate**(3), **X509_up_ref**(3), **X509_chain_up_ref**(3)

COPYRIGHT