## NAME

SSL_CTX_set_max_cert_list, SSL_CTX_get_max_cert_list, SSL_set_max_cert_list, SSL_get_max_cert_list - manipulate allowed size for the peer's certificate chain

## SYNOPSIS

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

long SSL_CTX_set_max_cert_list(SSL_CTX *ctx, long size);
long SSL_CTX_get_max_cert_list(SSL_CTX *ctx);

long SSL_set_max_cert_list(SSL *ssl, long size);
long SSL_get_max_cert_list(SSL *ctx);
```

## DESCRIPTION

**SSL_CTX_set_max_cert_list()** sets the maximum size allowed for the peer's certificate chain for all SSL objects created from **ctx** to be <size> bytes. The SSL objects inherit the setting valid for **ctx** at the time **SSL_new**(3) is being called.

**SSL_CTX_get_max_cert_list()** returns the currently set maximum size for **ctx**.

**SSL_set_max_cert_list()** sets the maximum size allowed for the peer's certificate chain for **ssl** to be <size> bytes. This setting stays valid until a new value is set.

**SSL_get_max_cert_list()** returns the currently set maximum size for **ssl**.

## NOTES

During the handshake process, the peer may send a certificate chain. The TLS/SSL standard does not give any maximum size of the certificate chain. The OpenSSL library handles incoming data by a dynamically allocated buffer. In order to prevent this buffer from growing without bounds due to data received from a faulty or malicious peer, a maximum size for the certificate chain is set.

The default value for the maximum certificate chain size is 100kB (30kB on the 16-bit DOS platform). This should be sufficient for usual certificate chains (OpenSSL's default maximum chain length is 10, see **SSL_CTX_set_verify**(3), and certificates without special extensions have a typical size of 1-2kB).

For special applications it can be necessary to extend the maximum certificate chain size allowed to be sent by the peer, see e.g. the work on "Internet X.509 Public Key Infrastructure Proxy Certificate Profile" and "TLS Delegation Protocol" at http://www.ietf.org/ and http://www.globus.org/ .

Under normal conditions it should never be necessary to set a value smaller than the default, as the

buffer is handled dynamically and only uses the memory actually required by the data sent by the peer.

If the maximum certificate chain size allowed is exceeded, the handshake will fail with a SSL_R_EXCESSIVE_MESSAGE_SIZE error.

## RETURN VALUES

**SSL_CTX_set_max_cert_list()** and **SSL_set_max_cert_list()** return the previously set value.

**SSL_CTX_get_max_cert_list()** and **SSL_get_max_cert_list()** return the currently set value.

## SEE ALSO

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

## COPYRIGHT

Copyright 2001-2020 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>.