

NAME

SSL_CTX_add_extra_chain_cert, SSL_CTX_get_extra_chain_certs, SSL_CTX_get_extra_chain_certs_only, SSL_CTX_clear_extra_chain_certs - add, get or clear extra chain certificates

SYNOPSIS

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

```
long SSL_CTX_add_extra_chain_cert(SSL_CTX *ctx, X509 *x509);  
long SSL_CTX_get_extra_chain_certs(SSL_CTX *ctx, STACK_OF(X509) **sk);  
long SSL_CTX_get_extra_chain_certs_only(SSL_CTX *ctx, STACK_OF(X509) **sk);  
long SSL_CTX_clear_extra_chain_certs(SSL_CTX *ctx);
```

DESCRIPTION

SSL_CTX_add_extra_chain_cert() adds the certificate **x509** to the extra chain certificates associated with **ctx**. Several certificates can be added one after another.

SSL_CTX_get_extra_chain_certs() retrieves the extra chain certificates associated with **ctx**, or the chain associated with the current certificate of **ctx** if the extra chain is empty. The returned stack should not be freed by the caller.

SSL_CTX_get_extra_chain_certs_only() retrieves the extra chain certificates associated with **ctx**. The returned stack should not be freed by the caller.

SSL_CTX_clear_extra_chain_certs() clears all extra chain certificates associated with **ctx**.

These functions are implemented as macros.

NOTES

When sending a certificate chain, extra chain certificates are sent in order following the end entity certificate.

If no chain is specified, the library will try to complete the chain from the available CA certificates in the trusted CA storage, see **SSL_CTX_load_verify_locations(3)**.

The **x509** certificate provided to **SSL_CTX_add_extra_chain_cert()** will be freed by the library when the **SSL_CTX** is destroyed. An application **should not** free the **x509** object.

RESTRICTIONS

Only one set of extra chain certificates can be specified per **SSL_CTX** structure. Different chains for

different certificates (for example if both RSA and DSA certificates are specified by the same server) or different SSL structures with the same parent SSL_CTX cannot be specified using this function. For more flexibility functions such as **SSL_add1_chain_cert()** should be used instead.

RETURN VALUES

SSL_CTX_add_extra_chain_cert() and **SSL_CTX_clear_extra_chain_certs()** return 1 on success and 0 for failure. Check out the error stack to find out the reason for failure.

SEE ALSO

ssl(7), **SSL_CTX_use_certificate(3)**, **SSL_CTX_set_client_cert_cb(3)**,
SSL_CTX_load_verify_locations(3) **SSL_CTX_set0_chain(3)** **SSL_CTX_set1_chain(3)**
SSL_CTX_add0_chain_cert(3) **SSL_CTX_add1_chain_cert(3)** **SSL_set0_chain(3)** **SSL_set1_chain(3)**
SSL_add0_chain_cert(3) **SSL_add1_chain_cert(3)** **SSL_CTX_build_cert_chain(3)**
SSL_build_cert_chain(3)

COPYRIGHT

Copyright 2000-2018 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>>.