#### **NAME**

```
ssl_ct_validation_cb, SSL_enable_ct, SSL_CTX_enable_ct, SSL_disable_ct, SSL_CTX_disable_ct, SSL_set_ct_validation_callback, SSL_CTX_set_ct_validation_callback, SSL_ct_is_enabled, SSL_CTX_ct_is_enabled - control Certificate Transparency policy
```

### **SYNOPSIS**

## **DESCRIPTION**

SSL\_enable\_ct() and SSL\_CTX\_enable\_ct() enable the processing of signed certificate timestamps (SCTs) either for a given SSL connection or for all connections that share the given SSL context, respectively. This is accomplished by setting a built-in CT validation callback. The behaviour of the callback is determined by the validation\_mode argument, which can be either of SSL\_CT\_VALIDATION\_PERMISSIVE or SSL\_CT\_VALIDATION\_STRICT as described below.

If validation\_mode is equal to SSL\_CT\_VALIDATION\_STRICT, then in a full TLS handshake with the verification mode set to SSL\_VERIFY\_PEER, if the peer presents no valid SCTs the handshake will be aborted. If the verification mode is SSL\_VERIFY\_NONE, the handshake will continue despite lack of valid SCTs. However, in that case if the verification status before the built-in callback was X509\_V\_OK it will be set to X509\_V\_ERR\_NO\_VALID\_SCTS after the callback. Applications can call SSL\_get\_verify\_result(3) to check the status at handshake completion, even after session resumption since the verification status is part of the saved session state. See SSL\_set\_verify(3), <SSL\_get\_verify\_result(3)>, SSL\_session\_reused(3).

If validation mode is equal to SSL CT VALIDATION PERMISSIVE, then the handshake continues,

and the verification status is not modified, regardless of the validation status of any SCTs. The application can still inspect the validation status of the SCTs at handshake completion. Note that with session resumption there will not be any SCTs presented during the handshake. Therefore, in applications that delay SCT policy enforcement until after handshake completion, such delayed SCT checks should only be performed when the session is not resumed.

SSL\_set\_ct\_validation\_callback() and SSL\_CTX\_set\_ct\_validation\_callback() register a custom callback that may implement a different policy than either of the above. This callback can examine the peer's SCTs and determine whether they are sufficient to allow the connection to continue. The TLS handshake is aborted if the verification mode is not SSL\_VERIFY\_NONE and the callback returns a non-positive result.

An arbitrary callback data argument, **arg**, can be passed in when setting the callback. This will be passed to the callback whenever it is invoked. Ownership of this context remains with the caller.

If no callback is set, SCTs will not be requested and Certificate Transparency validation will not occur.

No callback will be invoked when the peer presents no certificate, e.g. by employing an anonymous (aNULL) cipher suite. In that case the handshake continues as it would had no callback been requested. Callbacks are also not invoked when the peer certificate chain is invalid or validated via **DANE-TA(2)** or **DANE-EE(3)** TLSA records which use a private X.509 PKI, or no X.509 PKI at all, respectively. Clients that require SCTs are expected to not have enabled any aNULL ciphers nor to have specified server verification via **DANE-TA(2)** or **DANE-EE(3)** TLSA records.

**SSL\_disable\_ct()** and **SSL\_CTX\_disable\_ct()** turn off CT processing, whether enabled via the built-in or the custom callbacks, by setting a NULL callback. These may be implemented as macros.

**SSL\_ct\_is\_enabled()** and **SSL\_CTX\_ct\_is\_enabled()** return 1 if CT processing is enabled via either **SSL\_enable\_ct()** or a non-null custom callback, and 0 otherwise.

### **NOTES**

When SCT processing is enabled, OCSP stapling will be enabled. This is because one possible source of SCTs is the OCSP response from a server.

The time returned by **SSL\_SESSION\_get\_time**() will be used to evaluate whether any presented SCTs have timestamps that are in the future (and therefore invalid).

### RESTRICTIONS

Certificate Transparency validation cannot be enabled and so a callback cannot be set if a custom client extension handler has been registered to handle SCT extensions

3.0.11 2023-09-19 SSL\_CTX\_SF

 $(TLSEXT\_TYPE\_signed\_certificate\_timestamp).$ 

## **RETURN VALUES**

SSL\_enable\_ct(), SSL\_CTX\_enable\_ct(), SSL\_CTX\_set\_ct\_validation\_callback() and SSL\_set\_ct\_validation\_callback() return 1 if the callback is successfully set. They return 0 if an error occurs, e.g. a custom client extension handler has been setup to handle SCTs.

SSL\_disable\_ct() and SSL\_CTX\_disable\_ct() do not return a result.

**SSL\_CTX\_ct\_is\_enabled()** and **SSL\_ct\_is\_enabled()** return a 1 if a non-null CT validation callback is set, or 0 if no callback (or equivalently a NULL callback) is set.

### **SEE ALSO**

```
ssl(7), <SSL_get_verify_result(3)>, SSL_session_reused(3), SSL_set_verify(3), SSL_CTX_set_verify(3), SSL_SESSION_get_time(3)
```

# **COPYRIGHT**

Copyright 2016-2020 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 <a href="https://www.openssl.org/source/license.html">https://www.openssl.org/source/license.html</a>>.

3.0.11 2023-09-19 SSL\_CTX\_SF