NAME

ct − Certificate Transparency

SYNOPSIS

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

DESCRIPTION

This library implements Certificate Transparency (CT) verification for TLS clients, as defined in RFC 6962. This verification can provide some confidence that a certificate has been publicly logged in a set of CT logs.

By default, these checks are disabled. They can be enabled using **SSL_CTX_enable_ct**(3) or **SSL_enable_ct**(3).

This library can also be used to parse and examine CT data structures, such as Signed Certificate Timestamps (SCTs), or to read a list of CT logs. There are functions for: − decoding and encoding SCTs in DER and TLS wire format. − printing SCTs. − verifying the authenticity of SCTs. − loading a CT log list from a CONF file.

SEE ALSO

d2i_SCT_LIST(3), **CTLOG_STORE_new**(3), **CTLOG_STORE_get0_log_by_id**(3), **SCT_new**(3), **SCT_print**(3), **SCT_validate**(3), **SCT_validate**(3), **CT_POLICY_EVAL_CTX_new**(3), **SSL_CTX_set_ct_validation_callback**(3)

HISTORY

The ct library was added in OpenSSL 1.1.0.

COPYRIGHT