NAME

TS_VERIFY_CTX_set_certs, TS_VERIFY_CTS_set_certs - set certificates for TS response verification

SYNOPSIS

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

 STACK_OF(X509) *TS_VERIFY_CTX_set_certs(TS_VERIFY_CTX *ctx,
                                         STACK_OF(X509) *certs);
 STACK_OF(X509) *TS_VERIFY_CTS_set_certs(TS_VERIFY_CTX *ctx,
                                         STACK_OF(X509) *certs);
```

DESCRIPTION

The Time-Stamp Protocol (TSP) is defined by RFC 3161. TSP is a protocol used to provide long term proof of the existence of a certain datum before a particular time. TSP defines a Time Stamping Authority (TSA) and an entity who shall make requests to the TSA. Usually the TSA is denoted as the server side and the requesting entity is denoted as the client.

In TSP, when a server is sending a response to a client, the server normally needs to sign the response data - the TimeStampToken (TST) - with its private key. Then the client shall verify the received TST by the server's certificate chain.

TS_VERIFY_CTX_set_certs() is used to set the server's certificate chain when verifying a TST. **ctx** is the verification context created in advance and **certs** is a stack of **X509** certificates.

TS_VERIFY_CTS_set_certs() is a misspelled version of **TS_VERIFY_CTX_set_certs()** which takes the same parameters and returns the same result.

RETURN VALUES

TS_VERIFY_CTX_set_certs() returns the stack of **X509** certificates the user passes in via parameter **certs**.

SEE ALSO

OSSL_ESS_check_signing_certs(3)

HISTORY

The spelling of **TS_VERIFY_CTX_set_certs()** was corrected in OpenSSL 3.0.0. The misspelled version **TS_VERIFY_CTS_set_certs()** has been retained for compatibility reasons, but it is deprecated in OpenSSL 3.0.0.

COPYRIGHT