Rocky Enterprise Linux 9.2 Manual Pages on command 'i2d_re_X509_tbs.3ossl'

$ man i2d_re_X509_tbs.3ossl

I2D_RE_X509_TBS(3ossl) OpenSSL I2D_RE_X509_TBS(3ossl)

NAME

d2i_X509_AUX, i2d_X509_AUX, i2d_re_X509_tbs, i2d_re_X509_CRL_tbs,

i2d_re_X509_REQ_tbs - X509 encode and decode functions

SYNOPSIS

#include <openssl/x509.h>

X509 *d2i_X509_AUX(X509 **px, const unsigned char **in, long len);

int i2d_X509_AUX(const X509 *x, unsigned char **out);

int i2d_re_X509_tbs(X509 *x, unsigned char **out);

int i2d_re_X509_CRL_tbs(X509_CRL *crl, unsigned char **pp);

int i2d_re_X509_REQ_tbs(X509_REQ *req, unsigned char **pp);

DESCRIPTION

The X509 encode and decode routines encode and parse an X509 structure,

which represents an X509 certificate.

d2i_X509_AUX() is similar to d2i_X509(3) but the input is expected to

consist of an X509 certificate followed by auxiliary trust information.

This is used by the PEM routines to read "TRUSTED CERTIFICATE" objects.

This function should not be called on untrusted input.

i2d_X509_AUX() is similar to i2d_X509(3), but the encoded output contains both the certificate and any auxiliary trust information. This is used by the PEM routines to write "TRUSTED CERTIFICATE" objects. Note that this is a non-standard OpenSSL-specific data format.

i2d_re_X509_tbs() is similar to i2d_X509(3) except it encodes only the TBSCertificate portion of the certificate. i2d_re_X509_CRL_tbs() and i2d_re_X509_REQ_tbs() are analogous for CRL and certificate request, respectively. The "re" in i2d_re_X509_tbs stands for "re-encode", and ensures that a fresh encoding is generated in case the object has been modified after creation (see the BUGS section).

The encoding of the TBSCertificate portion of a certificate is cached in the X509 structure internally to improve encoding performance and to ensure certificate signatures are verified correctly in some certificates with broken (non-DER) encodings.

If, after modification, the X509 object is re-signed with X509_sign(), the encoding is automatically renewed. Otherwise, the encoding of the TBSCertificate portion of the X509 can be manually renewed by calling i2d_re_X509_tbs().

RETURN VALUES

d2i_X509_AUX() returns a valid X509 structure or NULL if an error occurred.

i2d_X509_AUX() returns the length of encoded data or -1 on error.

i2d_re_X509_tbs(), i2d_re_X509_CRL_tbs() and i2d_re_X509_REQ_tbs() return the length of encoded data or 0 on error.

SEE ALSO

ERR_get_error(3) X509_CRL_get0_by_serial(3), X509_get0_signature(3), X509_get_ext_d2i(3), X509_get_extension_flags(3), X509_get_pubkey(3), X509_get_subject_name(3), X509_get_version(3), X509_NAME_add_entry_by_txt(3), X509_NAME_ENTRY_get_object(3), X509_NAME_get_index_by_NID(3), X509_NAME_print_ex(3), X509_new(3), X509_sign(3), X509V3_get_d2i(3), X509_verify_cert(3)

COPYRIGHT