



*Full credit is given to the above companies including the OS that this PDF file was generated!*

## **Red Hat Enterprise Linux Release 9.2 Manual Pages on 'i2d\_re\_X509\_REQ\_tbs.3ossl' command**

**\$ man i2d\_re\_X509\_REQ\_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

Copyright 2002-2021 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>>.

