NAME

x509 - X.509 certificate handling

SYNOPSIS

#include <openssl/x509.h>

DESCRIPTION

An X.509 certificate is a structured grouping of information about an individual, a device, or anything one can imagine. An X.509 CRL (certificate revocation list) is a tool to help determine if a certificate is still valid. The exact definition of those can be found in the X.509 document from ITU-T, or in RFC3280 from PKIX. In OpenSSL, the type X509 is used to express such a certificate, and the type X509_CRL is used to express a CRL.

A related structure is a certificate request, defined in PKCS#10 from RSA Security, Inc, also reflected in RFC2896. In OpenSSL, the type X509_REQ is used to express such a certificate request.

To handle some complex parts of a certificate, there are the types X509_NAME (to express a certificate name), X509_ATTRIBUTE (to express a certificate attribute), X509_EXTENSION (to express a certificate extension) and a few more.

Finally, there's the supertype X509_INFO, which can contain a CRL, a certificate and a corresponding private key.

X509_*XXX*, **d2i_X509**_*XXX*, and **i2d_X509**_*XXX* functions handle X.509 certificates, with some exceptions, shown below.

X509_CRL_*XXX*, **d2i_X509_CRL**_*XXX*, and **i2d_X509_CRL**_*XXX* functions handle X.509 CRLs.

X509_REQ_*XXX*, **d2i_X509_REQ**_*XXX*, and **i2d_X509_REQ**_*XXX* functions handle PKCS#10 certificate requests.

X509_NAME_*XXX* functions handle certificate names.

X509_ATTRIBUTE_*XXX* functions handle certificate attributes.

X509_EXTENSION_*XXX* functions handle certificate extensions.

SEE ALSO

X509_NAME_ENTRY_get_object(3), **X509_NAME_add_entry_by_txt**(3), **X509_NAME_add_entry_by_NID**(3), **X509_NAME_print_ex**(3), **X509_NAME_new**(3),

PEM_X509_INFO_read(3), **d2i_X509**(3), **d2i_X509_ALGOR**(3), **d2i_X509_CRL**(3), **d2i_X509_NAME**(3), **d2i_X509_REQ**(3), **d2i_X509_SIG**(3), **crypto**(7)

COPYRIGHT

Copyright 2003-2021 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>.