

## NAME

X509\_cmp, X509\_NAME\_cmp, X509\_issuer\_and\_serial\_cmp, X509\_issuer\_name\_cmp, X509\_subject\_name\_cmp, X509\_CRL\_cmp, X509\_CRL\_match - compare X509 certificates and related values

## SYNOPSIS

```
#include <openssl/x509.h>
```

```
int X509_cmp(const X509 *a, const X509 *b);
int X509_NAME_cmp(const X509_NAME *a, const X509_NAME *b);
int X509_issuer_and_serial_cmp(const X509 *a, const X509 *b);
int X509_issuer_name_cmp(const X509 *a, const X509 *b);
int X509_subject_name_cmp(const X509 *a, const X509 *b);
int X509_CRL_cmp(const X509_CRL *a, const X509_CRL *b);
int X509_CRL_match(const X509_CRL *a, const X509_CRL *b);
```

## DESCRIPTION

This set of functions are used to compare X509 objects, including X509 certificates, X509 CRL objects and various values in an X509 certificate.

The **X509\_cmp()** function compares two **X509** objects indicated by parameters *a* and *b*. The comparison is based on the **memcmp** result of the hash values of two **X509** objects and the canonical (DER) encoding values.

The **X509\_NAME\_cmp()** function compares two **X509\_NAME** objects indicated by parameters *a* and *b*. The comparison is based on the **memcmp** result of the canonical (DER) encoding values of the two objects using **i2d\_X509\_NAME(3)**. This procedure adheres to the matching rules for Distinguished Names (DN) given in RFC 4517 section 4.2.15 and RFC 5280 section 7.1. In particular, the order of Relative Distinguished Names (RDNs) is relevant. On the other hand, if an RDN is multi-valued, i.e., it contains a set of AttributeValueAssertions (AVAs), its members are effectively not ordered.

The **X509\_issuer\_and\_serial\_cmp()** function compares the serial number and issuer values in the given **X509** objects *a* and *b*.

The **X509\_issuer\_name\_cmp()**, **X509\_subject\_name\_cmp()** and **X509\_CRL\_cmp()** functions are effectively wrappers of the **X509\_NAME\_cmp()** function. These functions compare issuer names and subject names of the objects, or issuers of **X509\_CRL** objects, respectively.

The **X509\_CRL\_match()** function compares two **X509\_CRL** objects. Unlike the **X509\_CRL\_cmp()** function, this function compares the whole CRL content instead of just the issuer name.

## RETURN VALUES

The **X509** comparison functions return **-1**, **0**, or **1** if object *a* is found to be less than, to match, or be greater than object *b*, respectively.

**X509\_NAME\_cmp()**, **X509\_issuer\_and\_serial\_cmp()**, **X509\_issuer\_name\_cmp()**, **X509\_subject\_name\_cmp()**, **X509\_CRL\_cmp()**, and **X509\_CRL\_match()** may return **-2** to indicate an error.

## NOTES

These functions in fact utilize the underlying **memcmp** of the C library to do the comparison job. Data to be compared varies from DER encoding data, hash value or **ASN1\_STRING**. The sign of the comparison can be used to order the objects but it does not have a special meaning in some cases.

**X509\_NAME\_cmp()** and wrappers utilize the value **-2** to indicate errors in some circumstances, which could cause confusion for the applications.

## SEE ALSO

**i2d\_X509\_NAME(3)**, **i2d\_X509(3)**

## COPYRIGHT

Copyright 2019-2021 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>>.