NAME

X509_verify, X509_self_signed, X509_REQ_verify_ex, X509_REQ_verify, X509_CRL_verify - verify certificate, certificate request, or CRL signature

SYNOPSIS

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

int X509_verify(X509 *x, EVP_PKEY *pkey);
int X509_self_signed(X509 *cert, int verify_signature);

int X509_REQ_verify_ex(X509_REQ *a, EVP_PKEY *pkey, OSSL_LIB_CTX *libctx,
                       const char *propq);
int X509_REQ_verify(X509_REQ *a, EVP_PKEY *r);
int X509_CRL_verify(X509_CRL *a, EVP_PKEY *r);
```

DESCRIPTION

X509_verify() verifies the signature of certificate *x* using public key *pkey*. Only the signature is checked: no other checks (such as certificate chain validity) are performed.

X509_self_signed() checks whether certificate *cert* is self-signed. For success the issuer and subject names must match, the components of the authority key identifier (if present) must match the subject key identifier etc. The signature itself is actually verified only if **verify_signature** is 1, as for explicitly trusted certificates this verification is not worth the effort.

X509_REQ_verify_ex(), **X509_REQ_verify()** and **X509_CRL_verify()** verify the signatures of certificate requests and CRLs, respectively.

RETURN VALUES

X509_verify(), **X509_REQ_verify_ex()**, **X509_REQ_verify()** and **X509_CRL_verify()** return 1 if the signature is valid and 0 if the signature check fails. If the signature could not be checked at all because it was ill-formed, the certificate or the request was not complete or some other error occurred then -1 is returned.

X509_self_signed() returns the same values but also returns 1 if all respective fields match and **verify_signature** is 0.

SEE ALSO

d2i_X509(3), **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_ENTRY_get_object**(3),

X509_NAME_get_index_by_NID(3), **X509_NAME_print_ex**(3), **X509V3_get_d2i**(3), **X509_verify_cert**(3), **OSSL_LIB_CTX**(3)

HISTORY

The **X509_verify()**, **X509_REQ_verify()**, and **X509_CRL_verify()** functions are available in all versions of OpenSSL.

X509_REQ_verify_ex(), and **X509_self_signed()** were added in OpenSSL 3.0.

COPYRIGHT