NAME

X509_get0_signature, X509_REQ_set0_signature, X509_REQ_set1_signature_algo, X509_get_signature_nid, X509_get0_tbs_sigalg, X509_REQ_get0_signature, X509_REQ_get_signature_nid, X509_CRL_get0_signature, X509_CRL_get_signature_nid, X509_get_signature_info, X509_SIG_INFO_get, X509_SIG_INFO_set - signature information

SYNOPSIS

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

void X509_get0_signature(const ASN1_BIT_STRING **psig,
                         const X509_ALGOR **palg,
                         const X509 *x);
void X509_REQ_set0_signature(X509_REQ *req, ASN1_BIT_STRING *psig);
int X509_REQ_set1_signature_algo(X509_REQ *req, X509_ALGOR *palg);
int X509_get_signature_nid(const X509 *x);
const X509_ALGOR *X509_get0_tbs_sigalg(const X509 *x);

void X509_REQ_get0_signature(const X509_REQ *crl,
                             const ASN1_BIT_STRING **psig,
                             const X509_ALGOR **palg);
int X509_REQ_get_signature_nid(const X509_REQ *crl);

void X509_CRL_get0_signature(const X509_CRL *crl,
                             const ASN1_BIT_STRING **psig,
                             const X509_ALGOR **palg);
int X509_CRL_get_signature_nid(const X509_CRL *crl);

int X509_get_signature_info(X509 *x, int *mdnid, int *pknid, int *secbits,
                            uint32_t *flags);

int X509_SIG_INFO_get(const X509_SIG_INFO *siginf, int *mdnid, int *pknid,
                      int *secbits, uint32_t *flags);
void X509_SIG_INFO_set(X509_SIG_INFO *siginf, int mdnid, int pknid,
                       int secbits, uint32_t flags);
```

DESCRIPTION

X509_get0_signature() sets ***psig** to the signature of **x** and ***palg** to the signature algorithm of **x**. The values returned are internal pointers which **MUST NOT** be freed up after the call.

X509_set0_signature() and **X509_REQ_set1_signature_algo()** are the equivalent setters for the two values of **X509_get0_signature()**.

X509_get0_tbs_sigalg() returns the signature algorithm in the signed portion of **x**.

X509_get_signature_nid() returns the NID corresponding to the signature algorithm of **x**.

X509_REQ_get0_signature(), **X509_REQ_get_signature_nid()** **X509_CRL_get0_signature()** and **X509_CRL_get_signature_nid()** perform the same function for certificate requests and CRLs.

X509_get_signature_info() retrieves information about the signature of certificate **x**. The NID of the signing digest is written to ***mdnid**, the public key algorithm to ***pknid**, the effective security bits to ***secbits** and flag details to ***flags**. Any of the parameters can be set to **NULL** if the information is not required.

X509_SIG_INFO_get() and **X509_SIG_INFO_set()** get and set information about a signature in an **X509_SIG_INFO** structure. They are only used by implementations of algorithms which need to set custom signature information: most applications will never need to call them.

NOTES

These functions provide lower level access to signatures in certificates where an application wishes to analyse or generate a signature in a form where **X509_sign()** et al is not appropriate (for example a non standard or unsupported format).

The security bits returned by **X509_get_signature_info()** refers to information available from the certificate signature (such as the signing digest). In some cases the actual security of the signature is less because the signing key is less secure: for example a certificate signed using SHA-512 and a 1024 bit RSA key.

RETURN VALUES

X509_get_signature_nid(), **X509_REQ_get_signature_nid()** and **X509_CRL_get_signature_nid()** return a NID.

X509_get0_signature(), **X509_REQ_get0_signature()** and **X509_CRL_get0_signature()** do not return values.

X509_get_signature_info() returns 1 if the signature information returned is valid or 0 if the information is not available (e.g. unknown algorithms or malformed parameters).

X509_REQ_set1_signature_algo() returns 0 on success; or 1 on an error (e.g. null ALGO pointer). X509_REQ_set0_signature does not return an error value.

SEE ALSO

d2i_X509(3), **ERR_get_error**(3), **X509_CRL_get0_by_serial**(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)

HISTORY

The **X509_get0_signature()** and **X509_get_signature_nid()** functions were added in OpenSSL 1.0.2.

The **X509_REQ_get0_signature()**, **X509_REQ_get_signature_nid()**, **X509_CRL_get0_signature()** and **X509_CRL_get_signature_nid()** were added in OpenSSL 1.1.0.

The **X509_REQ_set0_signature()** and **X509_REQ_set1_signature_algo()** were added in OpenSSL 1.1.1e.

COPYRIGHT

Copyright 2015-2021 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>.