

NAME

X509_sign, X509_sign_ctx, X509_REQ_sign, X509_REQ_sign_ctx, X509_CRL_sign, X509_CRL_sign_ctx - sign certificate, certificate request, or CRL signature

SYNOPSIS

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

```
int X509_sign(X509 *x, EVP_PKEY *pkey, const EVP_MD *md);
```

```
int X509_sign_ctx(X509 *x, EVP_MD_CTX *ctx);
```

```
int X509_REQ_sign(X509_REQ *x, EVP_PKEY *pkey, const EVP_MD *md);
```

```
int X509_REQ_sign_ctx(X509_REQ *x, EVP_MD_CTX *ctx);
```

```
int X509_CRL_sign(X509_CRL *x, EVP_PKEY *pkey, const EVP_MD *md);
```

```
int X509_CRL_sign_ctx(X509_CRL *x, EVP_MD_CTX *ctx);
```

DESCRIPTION

X509_sign() signs certificate *x* using private key *pkey* and message digest *md* and sets the signature in *x*. **X509_sign_ctx()** also signs certificate *x* but uses the parameters contained in digest context *ctx*.

X509_REQ_sign(), **X509_REQ_sign_ctx()**, **X509_CRL_sign()**, and **X509_CRL_sign_ctx()** sign certificate requests and CRLs, respectively.

NOTES

X509_sign_ctx() is used where the default parameters for the corresponding public key and digest are not suitable. It can be used to sign keys using RSA-PSS for example.

For efficiency reasons and to work around ASN.1 encoding issues the encoding of the signed portion of a certificate, certificate request and CRL is cached internally. If the signed portion of the structure is modified the encoding is not always updated meaning a stale version is sometimes used. This is not normally a problem because modifying the signed portion will invalidate the signature and signing will always update the encoding.

RETURN VALUES

All functions return the size of the signature in bytes for success and zero for failure.

SEE ALSO

ERR_get_error(3), **X509_NAME_add_entry_by_txt(3)**, **X509_new(3)**, **X509_verify_cert(3)**, **X509_verify(3)**, **X509_REQ_verify_ex(3)**, **X509_REQ_verify(3)**, **X509_CRL_verify(3)**

HISTORY

The **X509_sign()**, **X509_REQ_sign()** and **X509_CRL_sign()** functions are available in all versions of OpenSSL.

The **X509_sign_ctx()**, **X509_REQ_sign_ctx()** and **X509_CRL_sign_ctx()** functions were added in OpenSSL 1.0.1.

COPYRIGHT

Copyright 2015-2020 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>.