

NAME

X509_get_pubkey, X509_get0_pubkey, X509_set_pubkey, X509_get_X509_PUBKEY, X509_REQ_get_pubkey, X509_REQ_get0_pubkey, X509_REQ_set_pubkey, X509_REQ_get_X509_PUBKEY - get or set certificate or certificate request public key

SYNOPSIS

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

```
EVP_PKEY *X509_get_pubkey(X509 *x);  
EVP_PKEY *X509_get0_pubkey(const X509 *x);  
int X509_set_pubkey(X509 *x, EVP_PKEY *pkey);  
X509_PUBKEY *X509_get_X509_PUBKEY(const X509 *x);
```

```
EVP_PKEY *X509_REQ_get_pubkey(X509_REQ *req);  
EVP_PKEY *X509_REQ_get0_pubkey(X509_REQ *req);  
int X509_REQ_set_pubkey(X509_REQ *x, EVP_PKEY *pkey);  
X509_PUBKEY *X509_REQ_get_X509_PUBKEY(X509_REQ *x);
```

DESCRIPTION

X509_get_pubkey() attempts to decode the public key for certificate **x**. If successful it returns the public key as an **EVP_PKEY** pointer with its reference count incremented: this means the returned key must be freed up after use. **X509_get0_pubkey()** is similar except it does **not** increment the reference count of the returned **EVP_PKEY** so it must not be freed up after use.

X509_get_X509_PUBKEY() returns an internal pointer to the **X509_PUBKEY** structure which encodes the certificate of **x**. The returned value must not be freed up after use.

X509_set_pubkey() attempts to set the public key for certificate **x** to **pkey**. The key **pkey** should be freed up after use.

X509_REQ_get_pubkey(), **X509_REQ_get0_pubkey()**, **X509_REQ_set_pubkey()** and **X509_REQ_get_X509_PUBKEY()** are similar but operate on certificate request **req**.

NOTES

The first time a public key is decoded the **EVP_PKEY** structure is cached in the certificate or certificate request itself. Subsequent calls return the cached structure with its reference count incremented to improve performance.

RETURN VALUES

X509_get_pubkey(), **X509_get0_pubkey()**, **X509_get_X509_PUBKEY()**, **X509_REQ_get_pubkey()**

and **X509_REQ_get_X509_PUBKEY()** return a public key or **NULL** if an error occurred.

X509_set_pubkey() and **X509_REQ_set_pubkey()** return 1 for success and 0 for failure.

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_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)**

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>.