

NAME

`d2i_RSAPublicKey`, `i2d_RSAPublicKey`, `d2i_RSAPrivateKey`, `i2d_RSAPrivateKey`,
`d2i_RSA_PUBKEY`, `i2d_RSA_PUBKEY`, `i2d_Netscape_RSA`, `d2i_Netscape_RSA` - RSA public
and private key encoding functions.

SYNOPSIS

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

```
RSA * d2i_RSAPublicKey(RSA **a, const unsigned char **pp, long length);
```

```
int i2d_RSAPublicKey(RSA *a, unsigned char **pp);
```

```
RSA * d2i_RSA_PUBKEY(RSA **a, const unsigned char **pp, long length);
```

```
int i2d_RSA_PUBKEY(RSA *a, unsigned char **pp);
```

```
RSA * d2i_RSAPrivateKey(RSA **a, const unsigned char **pp, long length);
```

```
int i2d_RSAPrivateKey(RSA *a, unsigned char **pp);
```

```
int i2d_Netscape_RSA(RSA *a, unsigned char **pp, int (*cb)());
```

```
RSA * d2i_Netscape_RSA(RSA **a, const unsigned char **pp, long length, int (*cb)());
```

DESCRIPTION

`d2i_RSAPublicKey()` and `i2d_RSAPublicKey()` decode and encode a PKCS#1 `RSAPublicKey` structure.

`d2i_RSA_PUBKEY()` and `i2d_RSA_PUBKEY()` decode and encode an RSA public key using a `SubjectPublicKeyInfo` (certificate public key) structure.

`d2i_RSAPrivateKey()`, `i2d_RSAPrivateKey()` decode and encode a PKCS#1 `RSAPrivateKey` structure.

`d2i_Netscape_RSA()`, `i2d_Netscape_RSA()` decode and encode an RSA private key in NET format.

The usage of all of these functions is similar to the `d2i_X509()` and `i2d_X509()` described in the [d2i_X509\(3\)](#) manual page.

NOTES

The `RSA` structure passed to the private key encoding functions should have all the PKCS#1 private key components present.

The data encoded by the private key functions is unencrypted and therefore offers no private key security.

The NET format functions are present to provide compatibility with certain very old software. This format has some severe security weaknesses and should be avoided if possible.

SEE ALSO

[d2i_X509\(3\)](#)

HISTORY

TBA