NAME

X509_check_private_key, X509_REQ_check_private_key - check the consistency of a private key with the public key in an X509 certificate or certificate request

SYNOPSIS

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

int X509_check_private_key(X509 *x, EVP_PKEY *k);

int X509_REQ_check_private_key(X509_REQ *x, EVP_PKEY *k);
```

DESCRIPTION

X509_check_private_key() function checks the consistency of private key **k** with the public key in **x**.

X509_REQ_check_private_key() is equivalent to **X509_check_private_key()** except that **x** represents a certificate request of structure **X509_REQ**.

RETURN VALUES

X509_check_private_key() and **X509_REQ_check_private_key()** return 1 if the keys match each other, and 0 if not.

If the key is invalid or an error occurred, the reason code can be obtained using **ERR_get_error**(3).

BUGS

The **check_private_key** functions don’t check if **k** itself is indeed a private key or not. It merely compares the public materials (e.g. exponent and modulus of an RSA key) and/or key parameters (e.g. EC params of an EC key) of a key pair. So if you pass a public key to these functions in **k**, it will return success.

SEE ALSO

ERR_get_error(3)

COPYRIGHT