

NAME

RSA_sign, RSA_verify - RSA signatures

SYNOPSIS

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

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining **OPENSSL_API_COMPAT** with a suitable version value, see **openssl_user_macros(7)**:

```
int RSA_sign(int type, const unsigned char *m, unsigned int m_len,  
             unsigned char *sigret, unsigned int *siglen, RSA *rsa);
```

```
int RSA_verify(int type, const unsigned char *m, unsigned int m_len,  
              unsigned char *sigbuf, unsigned int siglen, RSA *rsa);
```

DESCRIPTION

All of the functions described on this page are deprecated. Applications should instead use **EVP_PKEY_sign_init(3)**, **EVP_PKEY_sign(3)**, **EVP_PKEY_verify_init(3)** and **EVP_PKEY_verify(3)**.

RSA_sign() signs the message digest **m** of size **m_len** using the private key **rsa** using RSASSA-PKCS1-v1_5 as specified in RFC 3447. It stores the signature in **sigret** and the signature size in **siglen**. **sigret** must point to **RSA_size(rsa)** bytes of memory. Note that PKCS #1 adds meta-data, placing limits on the size of the key that can be used. See **RSA_private_encrypt(3)** for lower-level operations.

type denotes the message digest algorithm that was used to generate **m**. If **type** is **NID_md5_sha1**, an SSL signature (MD5 and SHA1 message digests with PKCS #1 padding and no algorithm identifier) is created.

RSA_verify() verifies that the signature **sigbuf** of size **siglen** matches a given message digest **m** of size **m_len**. **type** denotes the message digest algorithm that was used to generate the signature. **rsa** is the signer's public key.

RETURN VALUES

RSA_sign() returns 1 on success and 0 for failure. **RSA_verify()** returns 1 on successful verification and 0 for failure.

The error codes can be obtained by **ERR_get_error(3)**.

CONFORMING TO

SSL, PKCS #1 v2.0

SEE ALSO

ERR_get_error(3), **RSA_private_encrypt(3)**, **RSA_public_decrypt(3)**

HISTORY

All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2000-2021 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>](https://www.openssl.org/source/license.html).