

**NAME**

RSA\_private\_encrypt, RSA\_public\_decrypt - low-level signature operations

**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_private_encrypt(int flen, unsigned char *from,  
                        unsigned char *to, RSA *rsa, int padding);
```

```
int RSA_public_decrypt(int flen, unsigned char *from,  
                      unsigned char *to, RSA *rsa, int padding);
```

**DESCRIPTION**

Both of the functions described on this page are deprecated. Applications should instead use **EVP\_PKEY\_sign\_init\_ex(3)**, **EVP\_PKEY\_sign(3)**, **EVP\_PKEY\_verify\_recover\_init(3)**, and **EVP\_PKEY\_verify\_recover(3)**.

These functions handle RSA signatures at a low-level.

**RSA\_private\_encrypt()** signs the **flen** bytes at **from** (usually a message digest with an algorithm identifier) using the private key **rsa** and stores the signature in **to**. **to** must point to **RSA\_size(rsa)** bytes of memory.

**padding** denotes one of the following modes:

**RSA\_PKCS1\_PADDING**

PKCS #1 v1.5 padding. This function does not handle the **algorithmIdentifier** specified in PKCS #1. When generating or verifying PKCS #1 signatures, **RSA\_sign(3)** and **RSA\_verify(3)** should be used.

**RSA\_NO\_PADDING**

Raw RSA signature. This mode should *only* be used to implement cryptographically sound padding modes in the application code. Signing user data directly with RSA is insecure.

**RSA\_public\_decrypt()** recovers the message digest from the **flen** bytes long signature at **from** using the signer's public key **rsa**. **to** must point to a memory section large enough to hold the message digest (which is smaller than **RSA\_size(rsa) - 11**). **padding** is the padding mode that was used to sign the data.

**RETURN VALUES**

**RSA\_private\_encrypt()** returns the size of the signature (i.e., `RSA_size(rsa)`). **RSA\_public\_decrypt()** returns the size of the recovered message digest.

On error, -1 is returned; the error codes can be obtained by **ERR\_get\_error(3)**.

**SEE ALSO**

**ERR\_get\_error(3)**, **RSA\_sign(3)**, **RSA\_verify(3)**, **EVP\_PKEY\_sign(3)**, **EVP\_PKEY\_verify\_recover(3)**

**HISTORY**

Both 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>.