

**NAME**

RSA\_sign\_ASN1\_OCTET\_STRING, RSA\_verify\_ASN1\_OCTET\_STRING - 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_ASN1_OCTET_STRING(int dummy, unsigned char *m,
                               unsigned int m_len, unsigned char *sigret,
                               unsigned int *siglen, RSA *rsa);
```

```
int RSA_verify_ASN1_OCTET_STRING(int dummy, 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 APIs.

**RSA\_sign\_ASN1\_OCTET\_STRING()** signs the octet string **m** of size **m\_len** using the private key **rsa** represented in DER using PKCS #1 padding. It stores the signature in **sigret** and the signature size in **siglen**. **sigret** must point to **RSA\_size(rsa)** bytes of memory.

**dummy** is ignored.

The random number generator must be seeded when calling **RSA\_sign\_ASN1\_OCTET\_STRING()**. If the automatic seeding or reseeding of the OpenSSL CSPRNG fails due to external circumstances (see **RAND(7)**), the operation will fail.

**RSA\_verify\_ASN1\_OCTET\_STRING()** verifies that the signature **sigbuf** of size **siglen** is the DER representation of a given octet string **m** of size **m\_len**. **dummy** is ignored. **rsa** is the signer's public key.

**RETURN VALUES**

**RSA\_sign\_ASN1\_OCTET\_STRING()** returns 1 on success, 0 otherwise.

**RSA\_verify\_ASN1\_OCTET\_STRING()** returns 1 on successful verification, 0 otherwise.

The error codes can be obtained by **ERR\_get\_error(3)**.

RSA\_SIGN\_ASN1\_OCTET\_STRING(3openssl) OpenSSL RSA\_SIGN\_ASN1\_OCTET\_STRING(3openssl)

## **BUGS**

These functions serve no recognizable purpose.

## **SEE ALSO**

**ERR\_get\_error(3)**, **RAND\_bytes(3)**, **RSA\_sign(3)**, **RSA\_verify(3)**, **RAND(7)**

## **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>.