NAME

RSA_sign_ASN1_OCTET_STRING, RSA_verify_ASN1_OCTET_STRING - RSA signatures

SYNOPSIS

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

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

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 prior to calling *RSA_sign_ASN1_OCTET_STRING()*.

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)* .

BUGS

These functions serve no recognizable purpose.

SEE ALSO

ERR_get_error(3) , *rand(3)* , *RSA_sign(3)* , *RSA_verify(3)*

COPYRIGHT