NAME

RSA_size, RSA_bits, RSA_security_bits - get RSA modulus size or security bits

SYNOPSIS

#include <openssl/rsa.h>

int RSA_bits(const RSA *rsa);

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_size(const RSA *rsa);

int RSA_security_bits(const RSA *rsa);

DESCRIPTION

RSA_bits() returns the number of significant bits.

rsa and **rsa->n** must not be **NULL**.

The remaining functions described on this page are deprecated. Applications should instead use **EVP_PKEY_get_size**(3), **EVP_PKEY_get_bits**(3) and **EVP_PKEY_get_security_bits**(3).

RSA_size() returns the RSA modulus size in bytes. It can be used to determine how much memory must be allocated for an RSA encrypted value.

RSA_security_bits() returns the number of security bits of the given **rsa** key. See **BN_security_bits**(3).

RETURN VALUES

RSA_bits() returns the number of bits in the key.

RSA_size() returns the size of modulus in bytes.

RSA_security_bits() returns the number of security bits.

SEE ALSO

BN_num_bits(3)

HISTORY

The **RSA_size()** and **RSA_security_bits()** functions were deprecated in OpenSSL 3.0.

The **RSA_bits()** function was added in OpenSSL 1.1.0.

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>.