Rocky Enterprise Linux 9.2 Manual Pages on command 'DH_security_bits.3ossl'

$ man DH_security_bits.3ossl

DH_SIZE(3ossl) OpenSSL DH_SIZE(3ossl)

NAME

DH_size, DH_bits, DH_security_bits - get Diffie-Hellman prime size and security bits

SYNOPSIS

#include <openssl/dh.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 DH_bits(const DH *dh);

int DH_size(const DH *dh);

int DH_security_bits(const DH *dh);

DESCRIPTION

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

DH_bits() returns the number of significant bits.

dh and dh->p must not be NULL.

DH_size() returns the Diffie-Hellman prime size in bytes. It can be used to determine how much memory must be allocated for the shared secret computed by DH_compute_key(3).

DH_security_bits() returns the number of security bits of the given dh key. See BN_security_bits(3).

RETURN VALUES

DH_bits() returns the number of bits in the key, or -1 if dh doesn't hold any key parameters.

DH_size() returns the prime size of Diffie-Hellman in bytes, or -1 if dh doesn't hold any key parameters.

DH_security_bits() returns the number of security bits, or -1 if dh doesn't hold any key parameters.

SEE ALSO

EVP_PKEY_get_bits(3), DH_new(3), DH_generate_key(3), BN_num_bits(3)

HISTORY

All functions were deprecated in OpenSSL 3.0.

COPYRIGHT