Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'DSA_do_verify.3ossl' command

$ man DSA_do_verify.3ossl

DSA_DO_SIGN(3ossl) OpenSSL DSA_DO_SIGN(3ossl)

NAME

DSA_do_sign, DSA_do_verify - raw DSA signature operations

SYNOPSIS

#include <openssl/dsa.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):

DSA_SIG *DSA_do_sign(const unsigned char *dgst, int dlen, DSA *dsa);

int DSA_do_verify(const unsigned char *dgst, int dgst_len,
DSA_SIG *sig, DSA *dsa);

DESCRIPTION

All of the functions described on this page are deprecated.

Applications should instead use EVP_PKEY_sign_init(3), EVP_PKEY_sign(3), EVP_PKEY_verify_init(3) and EVP_PKEY_verify(3).

DSA_do_sign() computes a digital signature on the len byte message

digest dgst using the private key dsa and returns it in a newly allocated DSA_SIG structure.

DSA_sign_setup(3) may be used to precompute part of the signing operation in case signature generation is time-critical.

DSA_do_verify() verifies that the signature sig matches a given message digest dgst of size len. dsa is the signer's public key.

RETURN VALUES

DSA_do_sign() returns the signature, NULL on error. DSA_do_verify() returns 1 for a valid signature, 0 for an incorrect signature and -1 on error. The error codes can be obtained by ERR_get_error(3).

SEE ALSO

DSA_new(3), ERR_get_error(3), RAND_bytes(3), DSA_SIG_new(3), DSA_sign(3)

HISTORY

All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT