Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_sha512_256.3ossl'

$ man EVP_sha512_256.3ossl

EVP_SHA224(3ossl) OpenSSL EVP_SHA224(3ossl)

NAME

EVP_sha224, EVP_sha256, EVP_sha512_224, EVP_sha512_256, EVP_sha384,

EVP_sha512 - SHA-2 For EVP

SYNOPSIS

#include <openssl/evp.h>

const EVP_MD *EVP_sha224(void);

const EVP_MD *EVP_sha256(void);

const EVP_MD *EVP_sha512_224(void);

const EVP_MD *EVP_sha512_256(void);

const EVP_MD *EVP_sha384(void);

const EVP_MD *EVP_sha512(void);

DESCRIPTION

SHA-2 (Secure Hash Algorithm 2) is a family of cryptographic hash

functions standardized in NIST FIPS 180-4, first published in 2001.

EVP_sha224(), EVP_sha256(), EVP_sha512_224, EVP_sha512_256, EVP_sha384(), EVP_sha512()

The SHA-2 SHA-224, SHA-256, SHA-512/224, SHA512/256, SHA-384 and SHA-512 algorithms, which generate 224, 256, 224, 256, 384 and 512 bits respectively of output from a given input.

The two algorithms: SHA-512/224 and SHA512/256 are truncated forms of the SHA-512 algorithm. They are distinct from SHA-224 and SHA-256 even though their outputs are of the same size.

RETURN VALUES

These functions return a EVP_MD structure that contains the implementation of the message digest. See EVP_MD_meth_new(3) for details of the EVP_MD structure.

CONFORMING TO

NIST FIPS 180-4.

SEE ALSO

evp(7), EVP_DigestInit(3)

COPYRIGHT