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 'EVP_shake128.3ossl' command

$ man EVP_shake128.3ossl

EVP_SHA3_224(3ossl) OpenSSL EVP_SHA3_224(3ossl)

NAME

EVP_sha3_224, EVP_sha3_256, EVP_sha3_384, EVP_sha3_512, EVP_shake128, EVP_shake256 - SHA-3 For EVP

SYNOPSIS

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

const EVP_MD *EVP_sha3_224(void);
const EVP_MD *EVP_sha3_256(void);
const EVP_MD *EVP_sha3_384(void);
const EVP_MD *EVP_sha3_512(void);

const EVP_MD *EVP_shake128(void);
const EVP_MD *EVP_shake256(void);
```

DESCRIPTION

SHA-3 (Secure Hash Algorithm 3) is a family of cryptographic hash functions standardized in NIST FIPS 202, first published in 2015. It is based on the Keccak algorithm.

EVP_sha3_224(), EVP_sha3_256(), EVP_sha3_384(), EVP_sha3_512()

The SHA-3 SHA-3-224, SHA-3-256, SHA-3-384, and SHA-3-512 algorithms respectively. They produce 224, 256, 384 and 512 bits of output from a given input.

EVP_shake128(), EVP_shake256()

The SHAKE-128 and SHAKE-256 Extendable Output Functions (XOF) that can generate a variable hash length.

Specifically, EVP_shake128 provides an overall security of 128 bits, while EVP_shake256 provides that of 256 bits.

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 202.

SEE ALSO

evp(7), EVP_DigestInit(3)

COPYRIGHT