

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.

NOTES

Developers should be aware of the negative performance implications of calling these functions multiple times and should consider using **EVP_MD_fetch(3)** instead. See "Performance" in **crypto(7)** for further information.

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

Copyright 2017-2023 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>.