

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.

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 180-4.

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>.