

NAME

EVP_sm3 - SM3 for EVP

SYNOPSIS

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

```
const EVP_MD *EVP_sm3(void);
```

DESCRIPTION

SM3 is a cryptographic hash function with a 256-bit output, defined in GB/T 32905-2016.

EVP_sm3()

The SM3 hash function.

NOTES

Developers should be aware of the negative performance implications of calling this function 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

GB/T 32905-2016 and GM/T 0004-2012.

SEE ALSO

evp(7), **EVP_DigestInit(3)**

COPYRIGHT

Copyright 2017-2023 The OpenSSL Project Authors. All Rights Reserved. Copyright 2017 Ribose Inc. 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>>.