NAME

EVP_sha1 - SHA-1 For EVP

SYNOPSIS

#include <openssl/evp.h>

const EVP_MD *EVP_sha1(void);

DESCRIPTION

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function standardized in NIST FIPS 180-4. The algorithm was designed by the United States National Security Agency and initially published in 1995.

EVP_sha1()

The SHA-1 algorithm which produces a 160-bit output from a given input.

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

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>.