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_md5.3ossl' command

$ man EVP_md5.3ossl

EVP_MD5(3ossl) OpenSSL EVP_MD5(3ossl)

NAME

EVP_md5, EVP_md5_sha1 - MD5 For EVP

SYNOPSIS

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

const EVP_MD *EVP_md5(void);
const EVP_MD *EVP_md5_sha1(void);
```

DESCRIPTION

MD5 is a cryptographic hash function standardized in RFC 1321 and designed by Ronald Rivest.

The CMU Software Engineering Institute considers MD5 unsuitable for further use since its security has been severely compromised.

EVP_md5()

The MD5 algorithm which produces a 128-bit output from a given input.

EVP_md5_sha1()

A hash algorithm of SSL v3 that combines MD5 with SHA-1 as described in RFC 6101.

WARNING: this algorithm is not intended for non-SSL usage.

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

IETF RFC 1321.

SEE ALSO

evp(7), EVP_DigestInit(3)

COPYRIGHT