



Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'MDC2.3ossl'

\$ man MDC2.3ossl

MDC2_INIT(3ossl) OpenSSL MDC2_INIT(3ossl)

NAME

MDC2, MDC2_Init, MDC2_Update, MDC2_Final - MDC2 hash function

SYNOPSIS

```
#include <openssl/mdc2.h>
```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining OPENSSL_API_COMPAT with a suitable version value, see openssl_user_macros(7):

```
unsigned char *MDC2(const unsigned char *d, unsigned long n,  
                  unsigned char *md);
```

```
int MDC2_Init(MDC2_CTX *c);
```

```
int MDC2_Update(MDC2_CTX *c, const unsigned char *data,  
              unsigned long len);
```

```
int MDC2_Final(unsigned char *md, MDC2_CTX *c);
```

DESCRIPTION

All of the functions described on this page are deprecated.

Applications should instead use `EVP_DigestInit_ex(3)`,
`EVP_DigestUpdate(3)` and `EVP_DigestFinal_ex(3)`.

MDC2 is a method to construct hash functions with 128 bit output from block ciphers. These functions are an implementation of MDC2 with DES.

`MDC2()` computes the MDC2 message digest of the `n` bytes at `d` and places it in `md` (which must have space for `MDC2_DIGEST_LENGTH == 16` bytes of output). If `md` is `NULL`, the digest is placed in a static array.

The following functions may be used if the message is not completely stored in memory:

`MDC2_Init()` initializes a `MDC2_CTX` structure.

`MDC2_Update()` can be called repeatedly with chunks of the message to be hashed (`len` bytes at `data`).

`MDC2_Final()` places the message digest in `md`, which must have space for `MDC2_DIGEST_LENGTH == 16` bytes of output, and erases the `MDC2_CTX`.

Applications should use the higher level functions `EVP_DigestInit(3)` etc. instead of calling the hash functions directly.

RETURN VALUES

`MDC2()` returns a pointer to the hash value.

`MDC2_Init()`, `MDC2_Update()` and `MDC2_Final()` return 1 for success, 0 otherwise.

CONFORMING TO

ISO/IEC 10118-2:2000 Hash-Function 2, with DES as the underlying block cipher.

SEE ALSO

EVP_DigestInit(3)

HISTORY

All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2000-2021 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>.

3.0.7

2023-07-13

MDC2_INIT(3ossl)