



Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP_mdc2.3oss1' command

\$ man EVP_mdc2.3oss1

EVP_MDC2(3oss1) OpenSSL EVP_MDC2(3oss1)

NAME

EVP_mdc2 - MDC-2 For EVP

SYNOPSIS

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

```
const EVP_MD *EVP_mdc2(void);
```

DESCRIPTION

MDC-2 (Modification Detection Code 2 or Meyer-Schilling) is a cryptographic hash function based on a block cipher. This implementation is only available with the legacy provider.

EVP_mdc2()

The MDC-2DES algorithm of using MDC-2 with the DES block cipher. It produces a 128-bit output from a given input.

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

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

SEE ALSO

evp(7), provider(7), EVP_DigestInit(3)

COPYRIGHT

Copyright 2017-2022 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 EVP_MDC2(3ossl)