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.

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

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