

**NAME**

EVP\_md2 - MD2 For EVP

**SYNOPSIS**

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

```
const EVP_MD *EVP_md2(void);
```

**DESCRIPTION**

MD2 is a cryptographic hash function standardized in RFC 1319 and designed by Ronald Rivest. This implementation is only available with the legacy provider.

**EVP\_md2()**

The MD2 algorithm which 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**

IETF RFC 1319.

**SEE ALSO**

**evp(7)**, **provider(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>>.