



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 'EVP_blake2b512.3oss1'

\$ man EVP_blake2b512.3oss1

EVP_BLAKE2B512(3oss1) OpenSSL EVP_BLAKE2B512(3oss1)

NAME

EVP_blake2b512, EVP_blake2s256 - BLAKE2 For EVP

SYNOPSIS

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

```
const EVP_MD *EVP_blake2b512(void);
```

```
const EVP_MD *EVP_blake2s256(void);
```

DESCRIPTION

BLAKE2 is an improved version of BLAKE, which was submitted to the NIST SHA-3 algorithm competition. The BLAKE2s and BLAKE2b algorithms are described in RFC 7693.

EVP_blake2s256()

The BLAKE2s algorithm that produces a 256-bit output from a given

input.

EVP_blake2b512()

The BLAKE2b algorithm that produces a 512-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

RFC 7693.

NOTES

While the BLAKE2b and BLAKE2s algorithms supports a variable length digest, this implementation outputs a digest of a fixed length (the maximum length supported), which is 512-bits for BLAKE2b and 256-bits for BLAKE2s.

SEE ALSO

`evp(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>.