

NAME

EVP_MD-common - The OpenSSL EVP_MD implementations, common things

DESCRIPTION

All the OpenSSL EVP_MD implementations understand the following **OSSL_PARAM(3)** entries that are gettable with **EVP_MD_get_params(3)**, as well as these:

"blocksize" (**OSSL_DIGEST_PARAM_BLOCK_SIZE**) <unsigned integer>

The digest block size. The length of the "blocksize" parameter should not exceed that of a **size_t**.

This value can also be retrieved with **EVP_MD_get_block_size(3)**.

"size" (**OSSL_DIGEST_PARAM_SIZE**) <unsigned integer>

The digest output size. The length of the "size" parameter should not exceed that of a **size_t**.

This value can also be retrieved with **EVP_MD_get_size(3)**.

"flags" (**OSSL_DIGEST_PARAM_FLAGS**) <unsigned integer>

Diverse flags that describe exceptional behaviour for the digest. These flags are described in "DESCRIPTION" in **EVP_MD_meth_set_flags(3)**.

The length of the "flags" parameter should equal that of an **unsigned long int**.

This value can also be retrieved with **EVP_MD_get_flags(3)**.

SEE ALSO

EVP_MD_get_params(3), **provider-digest(7)**

COPYRIGHT

Copyright 2020-2021 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>>.