NAME

EVP_MD−MDC2 − The MDC2 EVP_MD implementation

DESCRIPTION

Support for computing MDC2 digests through the **EVP_MD** API.

Identity

This implementation is only available with the legacy provider, and is identified with the name ‘‘MDC2’’.

Gettable Parameters

This implementation supports the common gettable parameters described in **EVP_MD−common** (7).

Settable Context Parameters

This implementation supports the following **OSSL_PARAM** (3) entries, settable for an **EVP_MD_CTX** with **EVP_MD_CTX_set_params** (3):

‘‘pad-type’’ (**OSSL_DIGEST_PARAM_PAD_TYPE**) <unsigned integer>

Sets the padding type to be used. Normally the final MDC2 block is padded with zeros. If the pad type is set to 2 then the final block is padded with 0x80 followed by zeros.

SEE ALSO

EVP_MD_CTX_set_params (3), **provider−digest** (7), **OSSL_PROVIDER−legacy** (7)

COPYRIGHT