



Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP_MD-MD5-SHA1.7oss1' command

`$ man EVP_MD-MD5-SHA1.7oss1`

`EVP_MD-MD5-SHA1(7oss1)` `OpenSSL` `EVP_MD-MD5-SHA1(7oss1)`

NAME

`EVP_MD-MD5-SHA1` - The MD5-SHA1 `EVP_MD` implementation

DESCRIPTION

Support for computing MD5-SHA1 digests through the `EVP_MD` API.

MD5-SHA1 is a rather special digest that's used with SSLv3.

Identity

This implementation is only available with the default provider, and is identified with the name "MD5-SHA1".

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)`:

"ssl3-ms" (`OSSL_DIGEST_PARAM_SSL3_MS`) <octet string>

This parameter is set by libssl in order to calculate a signature hash for an SSLv3 CertificateVerify message as per RFC6101. It is only set after all handshake messages have already been digested via OP_digest_update() calls. The parameter provides the master secret value to be added to the digest. The digest implementation should calculate the complete digest as per RFC6101 section 5.6.8. The next call after setting this parameter should be OP_digest_final().

SEE ALSO

EVP_MD_CTX_set_params(3), provider-digest(7), OSSL_PROVIDER-default(7)

COPYRIGHT

Copyright 2020 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>.

3.0.7 2023-07-13 EVP_MD-MD5-SHA1(7ossl)