



**Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!**

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_MD-MD5-SHA1.7ssl'***

***\$ man EVP\_MD-MD5-SHA1.7ssl***

EVP\_MD-MD5-SHA1(7SSL)                      OpenSSL                      EVP\_MD-MD5-SHA1(7SSL)

**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>>.

3.0.2

2024-02-16

EVP\_MD-MD5-SHA1(7SSL)