

**NAME**

EVP\_MD-SHA1 – The SHA1 EVP\_MD implementation

**DESCRIPTION**

Support for computing SHA1 digests through the **EVP\_MD** API.

**Identities**

This implementation is available with the FIPS provider as well as the default provider, and is identified with the names “SHA1” and “SHA-1”.

**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),  
**OSSL\_PROVIDER-default** (7)

**provider-digest** (7),

**OSSL\_PROVIDER-FIPS** (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>>.