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), **provider−digest** (7), **OSSL_PROVIDER−FIPS** (7), **OSSL_PROVIDER−default** (7)

COPYRIGHT