

**NAME**

EVP\_MAC-HMAC – The HMAC EVP\_MAC implementation

**DESCRIPTION**

Support for computing HMAC MACs through the **EVP\_MAC** API.

This implementation uses **EVP\_MD** functions to get access to the underlying digest.

**Identity**

This implementation is identified with this name and properties, to be used with **EVP\_MAC\_fetch()**:

“HMAC”, “provider=default” or “provider=fips”

**Supported parameters**

The general description of these parameters can be found in “PARAMETERS” in **EVP\_MAC**(3).

The following parameter can be set with **EVP\_MAC\_CTX\_set\_params()**:

“key” (**OSSL\_MAC\_PARAM\_KEY**) <octet string>

Sets the MAC key. Setting this parameter is identical to passing *key* to **EVP\_MAC\_init**(3).

“digest” (**OSSL\_MAC\_PARAM\_DIGEST**) <UTF8 string>

Sets the name of the underlying digest to be used.

“properties” (**OSSL\_MAC\_PARAM\_PROPERTIES**) <UTF8 string>

Sets the properties to be queried when trying to fetch the underlying digest. This must be given together with the digest naming parameter (“digest”, or **OSSL\_MAC\_PARAM\_DIGEST**) to be considered valid.

“digest-noinit” (**OSSL\_MAC\_PARAM\_DIGEST\_NOINIT**) <integer>

A flag to set the MAC digest to not initialise the implementation specific data. The value 0 or 1 is expected.

“digest-oneshot” (**OSSL\_MAC\_PARAM\_DIGEST\_ONESHOT**) <integer>

A flag to set the MAC digest to be a one-shot operation. The value 0 or 1 is expected.

“tls-data-size” (**OSSL\_MAC\_PARAM\_TLS\_DATA\_SIZE**) <unsigned integer>

The following parameter can be retrieved with **EVP\_MAC\_CTX\_get\_params()**:

“size” (**OSSL\_MAC\_PARAM\_SIZE**) <unsigned integer>

The “size” parameter can also be retrieved with **EVP\_MAC\_CTX\_get\_mac\_size()**. The length of the “size” parameter is equal to that of an **unsigned int**.

“block-size” (**OSSL\_MAC\_PARAM\_SIZE**) <unsigned integer>

Gets the MAC block size. The “block-size” parameter can also be retrieved with **EVP\_MAC\_CTX\_get\_block\_size()**.

**SEE ALSO**

**EVP\_MAC\_CTX\_get\_params**(3), **EVP\_MAC\_CTX\_set\_params**(3), “PARAMETERS” in **EVP\_MAC**(3), **OSSL\_PARAM**(3), **HMAC**(3)

**COPYRIGHT**

Copyright 2018–2021 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>>.