

**NAME**

EVP\_PKEY-HMAC, EVP\_KEYMGMT-HMAC, EVP\_PKEY-Siphash, EVP\_KEYMGMT-Siphash, EVP\_PKEY-Poly1305, EVP\_KEYMGMT-Poly1305, EVP\_PKEY-CMAC, EVP\_KEYMGMT-CMAC – EVP\_PKEY legacy MAC keytypes and algorithm support

**DESCRIPTION**

The **HMAC** and **CMAC** key types are implemented in OpenSSL's default and FIPS providers. Additionally the **Siphash** and **Poly1305** key types are implemented in the default provider. Performing MAC operations via an EVP\_PKEY is considered legacy and are only available for backwards compatibility purposes and for a restricted set of algorithms. The preferred way of performing MAC operations is via the EVP\_MAC APIs. See **EVP\_MAC\_init** (3).

For further details on using EVP\_PKEY based MAC keys see **EVP\_SIGNATURE-HMAC** (7), **EVP\_SIGNATURE-Siphash** (7), **EVP\_SIGNATURE-Poly1305** (7) or **EVP\_SIGNATURE-CMAC** (7).

**Common MAC parameters**

All the MAC keytypes support the following parameters.

“priv” (**OSSL\_PKEY\_PARAM\_PRIV\_KEY**) <octet string>

The MAC key value.

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

A property query string to be used when any algorithms are fetched.

**CMAC parameters**

As well as the parameters described above, the **CMAC** keytype additionally supports the following parameters.

“cipher” (**OSSL\_PKEY\_PARAM\_CIPHER**) <UTF8 string>

The name of a cipher to be used when generating the MAC.

“engine” (**OSSL\_PKEY\_PARAM\_ENGINE**) <UTF8 string>

The name of an engine to be used for the specified cipher (if any).

**Common MAC key generation parameters**

MAC key generation is unusual in that no new key is actually generated. Instead a new provider side key object is created with the supplied raw key value. This is done for backwards compatibility with previous versions of OpenSSL.

“priv” (**OSSL\_PKEY\_PARAM\_PRIV\_KEY**) <octet string>

The MAC key value.

**CMAC key generation parameters**

In addition to the common MAC key generation parameters, the CMAC key generation additionally recognises the following.

“cipher” (**OSSL\_PKEY\_PARAM\_CIPHER**) <UTF8 string>

The name of a cipher to be used when generating the MAC.

**SEE ALSO**

**EVP\_KEYMGMT** (3), **EVP\_PKEY** (3), **provider-keymgmt** (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>>.