## 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