



*Full credit is given to the above companies including the OS that this PDF file was generated!*

## **Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP\_MD-KECCAK-KMAC.7oss1' command**

```
$ man EVP_MD-KECCAK-KMAC.7oss1
```

```
EVP_MD-SHAKE(7oss1)      OpenSSL      EVP_MD-SHAKE(7oss1)
```

### NAME

EVP\_MD-SHAKE, EVP\_MD-KECCAK-KMAC - The SHAKE / KECCAK family EVP\_MD implementations

### DESCRIPTION

Support for computing SHAKE or KECCAK-KMAC digests through the EVP\_MD API.

KECCAK-KMAC is a special digest that's used by the KMAC EVP\_MAC implementation (see EVP\_MAC-KMAC(7)).

### Identities

This implementation is available in the FIPS provider as well as the default provider, and includes the following varieties:

#### KECCAK-KMAC-128

Known names are "KECCAK-KMAC-128" and "KECCAK-KMAC128" This is used by EVP\_MAC-KMAC128(7)

#### KECCAK-KMAC-256

Known names are "KECCAK-KMAC-256" and "KECCAK-KMAC256" This is used

by EVP\_MAC-KMAC256(7)

## SHAKE-128

Known names are "SHAKE-128" and "SHAKE128"

## SHAKE-256

Known names are "SHAKE-256" and "SHAKE256"

## Gettable Parameters

This implementation supports the common gettable parameters described in EVP\_MD-common(7).

## Settable Context Parameters

These implementations support the following OSSL\_PARAM(3) entries, settable for an EVP\_MD\_CTX with EVP\_MD\_CTX\_set\_params(3):

"xoflen" (OSSL\_DIGEST\_PARAM\_XOFLEN) <unsigned integer>

Sets the digest length for extendable output functions. The length of the "xoflen" parameter should not exceed that of a size\_t.

For backwards compatibility reasons the default xoflen length for SHAKE-128 is 16 (bytes) which results in a security strength of only 64 bits. To ensure the maximum security strength of 128 bits, the xoflen should be set to at least 32.

For backwards compatibility reasons the default xoflen length for SHAKE-256 is 32 (bytes) which results in a security strength of only 128 bits. To ensure the maximum security strength of 256 bits, the xoflen should be set to at least 64.

## SEE ALSO

EVP\_MD\_CTX\_set\_params(3), provider-digest(7), OSSL\_PROVIDER-default(7)

## COPYRIGHT

Copyright 2020-2022 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>.

3.0.7                    2023-07-13                    EVP\_MD-SHAKE(7ossl)