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 only available with the default provider, and includes the following varieties:

KECCAK−KMAC−128
: Known names are ''KECCAK−KMAC−128'' and ''KECCAK−KMAC128''

KECCAK−KMAC−256
: Known names are ''KECCAK−KMAC−256'' and ''KECCAK−KMAC256''

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**.

SEE ALSO

EVP_MD_CTX_set_params (3), **provider−digest** (7), **OSSL_PROVIDER−default** (7)

COPYRIGHT