Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_MD-SHAKE.7ossl'

$ man EVP_MD-SHAKE.7ossl

EVP_MD-SHAKE(7ossl) OpenSSL EVP_MD-SHAKE(7ossl)

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