NAME

EVP_CIPHER−NULL − The NULL EVP_CIPHER implementation

DESCRIPTION

Support for a NULL symmetric encryption using the **EVP_CIPHER** API. This is used when the TLS cipher suite is TLS_NULL_WITH_NULL_NULL. This does no encryption (just copies the data) and has a mac size of zero.

Algorithm Name

The following algorithm is available in the default provider:

"NULL"

Parameters

This implementation supports the following parameters:

Gettable EVP_CIPHER parameters

See "Gettable EVP_CIPHER parameters" in **EVP_EncryptInit** (3)

Gettable EVP_CIPHER_CTX parameters

"keylen" (**OSSL_CIPHER_PARAM_KEYLEN**) <unsigned integer>
"ivlen" (**OSSL_CIPHER_PARAM_IVLEN** and <**OSSL_CIPHER_PARAM_AEAD_IVLEN**) <unsigned integer>
"tls−mac" (**OSSL_CIPHER_PARAM_TLS_MAC**) <octet ptr>

See "PARAMETERS" in **EVP_EncryptInit** (3) for further information.

Settable EVP_CIPHER_CTX parameters

"tls−mac−size" (**OSSL_CIPHER_PARAM_TLS_MAC_SIZE**) <unsigned integer>

See "PARAMETERS" in **EVP_EncryptInit** (3) for further information.

CONFORMING TO

RFC 5246 section−6.2.3.1

SEE ALSO

provider−cipher (7), **OSSL_PROVIDER−default** (7)

COPYRIGHT