

NAME

EVP_CIPHER-SM4 – The SM4 EVP_CIPHER implementations

DESCRIPTION

Support for SM4 symmetric encryption using the **EVP_CIPHER** API.

Algorithm Names

The following algorithms are available in the default provider:

"SM4-CBC:SM4"

"SM4-ECB"

"SM4-CTR"

"SM4-OFB" or "SM4-OFB128"

"SM4-CFB" or "SM4-CFB128"

"SM4-GCM"

"SM4-CCM"

"SM4-XTS"

Parameters

This implementation supports the parameters described in "PARAMETERS" in **EVP_EncryptInit**(3).

NOTES

The SM4-XTS implementation allows streaming to be performed, but each **EVP_EncryptUpdate**(3) or **EVP_DecryptUpdate**(3) call requires each input to be a multiple of the blocksize. Only the final **EVP_EncryptUpdate()** or **EVP_DecryptUpdate()** call can optionally have an input that is not a multiple of the blocksize but is larger than one block. In that case ciphertext stealing (CTS) is used to fill the block.

SEE ALSO

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

COPYRIGHT

Copyright 2021 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>](https://www.openssl.org/source/license.html).