



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

Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_sm4_ofb.3oss1'

\$ man EVP_sm4_ofb.3oss1

EVP_SM4_CBC(3oss1) OpenSSL EVP_SM4_CBC(3oss1)

NAME

EVP_sm4_cbc, EVP_sm4_ecb, EVP_sm4_cfb, EVP_sm4_cfb128, EVP_sm4_ofb,
EVP_sm4_ctr - EVP SM4 cipher

SYNOPSIS

```
#include <openssl/evp.h>
```

```
const EVP_CIPHER *EVP_sm4_cbc(void);  
const EVP_CIPHER *EVP_sm4_ecb(void);  
const EVP_CIPHER *EVP_sm4_cfb(void);  
const EVP_CIPHER *EVP_sm4_cfb128(void);  
const EVP_CIPHER *EVP_sm4_ofb(void);  
const EVP_CIPHER *EVP_sm4_ctr(void);
```

DESCRIPTION

The SM4 blockcipher (GB/T 32907-2016) for EVP.

All modes below use a key length of 128 bits and acts on blocks of 128 bits.

`EVP_sm4_cbc()`, `EVP_sm4_ecb()`, `EVP_sm4_cfb()`, `EVP_sm4_cfb128()`,
`EVP_sm4_ofb()`, `EVP_sm4_ctr()`

The SM4 blockcipher with a 128-bit key in CBC, ECB, CFB, OFB and CTR modes respectively.

RETURN VALUES

These functions return a `EVP_CIPHER` structure that contains the implementation of the symmetric cipher. See `EVP_CIPHER_meth_new(3)` for details of the `EVP_CIPHER` structure.

SEE ALSO

`evp(7)`, `EVP_EncryptInit(3)`, `EVP_CIPHER_meth_new(3)`

COPYRIGHT

Copyright 2017-2018 The OpenSSL Project Authors. All Rights Reserved.

Copyright 2017 Ribose Inc. 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_SM4_CBC(3openssl)`