NAME

EVP_CIPHER−DES − The DES EVP_CIPHER implementations

DESCRIPTION

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

Algorithm Names

The following algorithms are available in the FIPS provider as well as the default provider:

“DES−EDE3−ECB” or “DES−EDE3”
“DES−EDE3−CBC” or “DES3”

The following algorithms are available in the default provider, but not the FIPS provider:

“DES−EDE3−CFB8” and “DES−EDE3−CFB1”
“DES-EDE-ECB” or “DES-EDE”
“DES-EDE-CBC”
“DES-EDE-OFB”
“DES-EDE-CFB”
“DES3−WRAP”

The following algorithms are available in the legacy provider:

“DES-ECB”
“DES-CBC”
“DES-OFB”
“DES-CFB”, “DES−CFB1” and “DES−CFB8”
“DESX-CBC”

Parameters

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

SEE ALSO

provider−cipher (7), **OSSL_PROVIDER−FIPS** (7), **OSSL_PROVIDER−default** (7), **OSSL_PROVIDER−legacy** (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>.