NAME

EVP_CIPHER−AES − The AES EVP_CIPHER implementations

DESCRIPTION

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

Algorithm Names

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

‘‘AES−128−CBC’’, ‘‘AES−192−CBC’’ and ‘‘AES−256−CBC’’
‘‘AES−128−CBC−CTS’’, ‘‘AES−192−CBC−CTS’’ and ‘‘AES−256−CBC−CTS’’
‘‘AES−128−CFB’’, ‘‘AES−192−CFB’’, ‘‘AES−256−CFB’’, ‘‘AES−128−CFB1’’, ‘‘AES−192−CFB1’’, ‘‘AES−256−CFB1’’, ‘‘AES−128−CFB8’’, ‘‘AES−192−CFB8’’ and ‘‘AES−256−CFB8’’
‘‘AES−128−CTR’’, ‘‘AES−192−CTR’’ and ‘‘AES−256−CTR’’
‘‘AES−128−ECB’’, ‘‘AES−192−ECB’’ and ‘‘AES−256−ECB’’
‘‘AES−192−OCB’’, ‘‘AES−128−OCB’’ and ‘‘AES−256−OCB’’
‘‘AES−128−SIV’’, ‘‘AES−192−SIV’’ and ‘‘AES−256−SIV’’
‘‘AES−128−XTS’’ and ‘‘AES−256−XTS’’
‘‘AES−128−CCM’’, ‘‘AES−192−CCM’’ and ‘‘AES−256−CCM’’
‘‘AES−128−GCM’’, ‘‘AES−192−GCM’’ and ‘‘AES−256−GCM’’
‘‘AES−128−WRAP’’, ‘‘AES−192−WRAP’’, ‘‘AES−256−WRAP’’, ‘‘AES−128−WRAP−PAD’’, ‘‘AES−192−WRAP−PAD’’, ‘‘AES−256−WRAP−PAD’’, ‘‘AES−128−WRAP−INV’’, ‘‘AES−192−WRAP−INV’’, ‘‘AES−256−WRAP−INV’’, ‘‘AES−128−WRAP−PAD−INV’’, ‘‘AES−192−WRAP−PAD−INV’’ and ‘‘AES−256−WRAP−PAD−INV’’
‘‘AES−128−CBC−HMAC−SHA1’’, ‘‘AES−256−CBC−HMAC−SHA1’’, ‘‘AES−128−CBC−HMAC−SHA256’’ and ‘‘AES−256−CBC−HMAC−SHA256’’

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

‘‘AES−128−OFB’’, ‘‘AES−192−OFB’’ and ‘‘AES−256−OFB’’

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)

COPYRIGHT