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−OFB", "AES−128−OFB" and "AES−256−OFB"
"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−OCB", "AES−192−OCB" and "AES−256−OCB"
"AES−128−SIV", "AES−192−SIV" and "AES−256−SIV"
"AES−128−GCM−SIV", "AES−192−GCM−SIV" and "AES−256−GCM−SIV"

Parameters

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

NOTES

The AES−SIV and AES−WRAP mode implementations do not support streaming. That means to obtain correct results there can be only one **EVP_EncryptUpdate**(3) or **EVP_DecryptUpdate**(3) call after the initialization of the context.

When wrapping with AES−WRAP−PAD ciphers, the output buffer must be at least *inl* rounded up to the cipher block size (8 bytes) plus the block size. That is, the minimum output buffer size is `((inl + 7) / 8) * 8 + 8`bytes.

The AES−XTS implementations allow 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−FIPS**(7), **OSSL_PROVIDER−default**(7)

HISTORY

The GCM−SIV mode ciphers were added in OpenSSL version 3.2.

COPYRIGHT