Rocky Enterprise Linux 9.2 Manual Pages on command 'CMS_EncryptedData_encrypt.3ossl'

$ man CMS_EncryptedData_encrypt.3ossl

CMS_ENCRYPTEDDATA_ENCRYPT(3ossl) OpenSSL CMS_ENCRYPTEDDATA_ENCRYPT(3ossl)

NAME

CMS_EncryptedData_encrypt_ex, CMS_EncryptedData_encrypt - Create CMS EncryptedData

SYNOPSIS

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

CMS_ContentInfo *CMS_EncryptedData_encrypt_ex(BIO *in,
                                              const EVP_CIPHER *cipher,
                                              const unsigned char *key,
                                              size_t keylen,
                                              unsigned int flags,
                                              OSSL_LIB_CTX *ctx,
                                              const char *propq);

CMS_ContentInfo *CMS_EncryptedData_encrypt(BIO *in,
```

const EVP_CIPHER *cipher, const unsigned char *key, size_t keylen,
unsigned int flags);

DESCRIPTION

CMS_EncryptedData_encrypt_ex() creates a CMS_ContentInfo structure with a type NID_pkcs7_encrypted. in is a BIO containing the data to encrypt using cipher and the encryption key key of size keylen bytes. The library context libctx and the property query propq are used when retrieving algorithms from providers. flags is a set of optional flags.

The flags field supports the options CMS_DETACHED, CMS_STREAM and CMS_PARTIAL. Internally CMS_final() is called unless CMS_STREAM and/or CMS_PARTIAL is specified.

The algorithm passed in the cipher parameter must support ASN1 encoding of its parameters.

The CMS_ContentInfo structure can be freed using CMS_ContentInfo_free(3).

CMS_EncryptedData_encrypt() is similar to CMS_EncryptedData_encrypt_ex() but uses default values of NULL for the library context libctx and the property query propq.

RETURN VALUES

If the allocation fails, CMS_EncryptedData_encrypt_ex() and CMS_EncryptedData_encrypt() return NULL and set an error code that can be obtained by ERR_get_error(3). Otherwise they return a pointer to the newly allocated structure.

SEE ALSO

ERR_get_error(3), CMS_final(3), CMS_EncryptedData_decrypt(3)

HISTORY

The CMS_EncryptedData_encrypt_ex() method was added in OpenSSL 3.0.

COPYRIGHT