NAME

CMS_EncryptedData_decrypt, CMS_EnvelopedData_decrypt − Decrypt CMS EncryptedData or EnvelopedData

SYNOPSIS

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

int CMS_EncryptedData_decrypt(CMS_ContentInfo *cms,
                              const unsigned char *key, size_t keylen,
                              BIO *dcont, BIO *out, unsigned int flags);

BIO *CMS_EnvelopedData_decrypt(CMS_EnvelopedData *env, BIO *detached_data,
                               EVP_PKEY *pkey, X509 *cert,
                               ASN1_OCTET_STRING *secret, unsigned int flags,
                               OSSL_LIB_CTX *libctx, const char *propq);
```

DESCRIPTION

CMS_EncryptedData_decrypt() decrypts a *cms* EncryptedData object using the symmetric *key* of size *keylen* bytes. AEAD cipher algorithms are not supported. *out* is a BIO to write the content to and *flags* is an optional set of flags. *dcont* is used in the rare case where the encrypted content is detached. It will normally be set to NULL.

The following flags can be passed in the *flags* parameter.

If the **CMS_TEXT** flag is set MIME headers for type `text/plain` are deleted from the content. If the content is not of type `text/plain` then an error is returned.

CMS_EnvelopedData_decrypt() decrypts, similarly to **CMS_decrypt**(3), a CMS EnvelopedData object *env* using the symmetric key *secret* if it is not NULL, otherwise the private key of the recipient *pkey*. If *pkey* is given, it is recommended to provide also the associated certificate in *cert* − see **CMS_decrypt**(3) and the NOTES on *cert* there. The optional parameters *flags* and *dcont* are used as described above. The optional parameters library context *libctx* and property query *propq* are used when retrieving algorithms from providers.

RETURN VALUES

CMS_EncryptedData_decrypt() returns 0 if an error occurred otherwise returns 1.

CMS_EnvelopedData_decrypt() returns NULL if an error occurred, otherwise a BIO containing the decypted content.

SEE ALSO

ERR_get_error(3), **CMS_EncryptedData_encrypt**(3), **CMS_decrypt**(3)

HISTORY

CMS_EnvelopedData_decrypt() was added in OpenSSL 3.2.

COPYRIGHT