NAME

CMS_EncryptedData_decrypt - Decrypt CMS EncryptedData

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);

DESCRIPTION

CMS_EncryptedData_decrypt() decrypts a *cms* EncryptedData object using the symmetric *key* of size *keylen* bytes. *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.

RETURN VALUES

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

SEE ALSO

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

COPYRIGHT

Copyright 2020-2023 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>.