NAME

   PKCS7_decrypt - decrypt content from a PKCS#7 envelopedData structure

SYNOPSIS

   #include <openssl/pkcs7.h>

   int PKCS7_decrypt(PKCS7 *p7, EVP_PKEY *pkey, X509 *cert, BIO *data, int flags);

DESCRIPTION

   PKCS7_decrypt() extracts and decrypts the content from a PKCS#7 envelopedData structure. **pkey** is
   the private key of the recipient, **cert** is the recipients certificate, **data** is a BIO to write the content to and
   flags is an optional set of flags.

NOTES

   Although the recipients certificate is not needed to decrypt the data it is needed to locate the
   appropriate (of possible several) recipients in the PKCS#7 structure.

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

   If the **PKCS7_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

   PKCS7_decrypt() returns either 1 for success or 0 for failure. The error can be obtained from
   ERR_get_error(3)

BUGS

   PKCS7_decrypt() must be passed the correct recipient key and certificate. It would be better if it could
   look up the correct key and certificate from a database.

   The lack of single pass processing and need to hold all data in memory as mentioned in **PKCS7_sign()**
   also applies to **PKCS7_verify()**.

SEE ALSO

   ERR_get_error(3), **PKCS7_encrypt**(3)

COPYRIGHT

   Copyright 2002-2016 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>.