Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'PKCS12_pack_p7encdata_ex.3ossl' command

$ man PKCS12_pack_p7encdata_ex.3ossl

PKCS12_PACK_P7ENCDATA(3ossl) OpenSSL PKCS12_PACK_P7ENCDATA(3ossl)

NAME

PKCS12_pack_p7encdata, PKCS12_pack_p7encdata_ex - Pack a set of PKCS#12 safeBags into a PKCS#7 encrypted data object

SYNOPSIS

```
#include <openssl/pkcs12.h>

PKCS7 *PKCS12_pack_p7encdata(int pbe_nid, const char *pass, int passlen,
                             unsigned char *salt, int saltlen, int iter,
                             STACK_OF(PKCS12_SAFEBAG) *bags);
PKCS7 *PKCS12_pack_p7encdata_ex(int pbe_nid, const char *pass, int passlen,
                                unsigned char *salt, int saltlen, int iter,
                                STACK_OF(PKCS12_SAFEBAG) *bags,
                                OSSL_LIB_CTX *ctx, const char *propq);
```

DESCRIPTION

PKCS12_pack_p7encdata() generates a PKCS#7 ContentInfo object of encrypted-data type from the set of safeBags bags. The algorithm ID in pbe_nid can be a PKCS#12 or PKCS#5 password based encryption algorithm, or a cipher algorithm. If a cipher algorithm is passed, the PKCS#5 PBES2 algorithm will be used with this cipher as a parameter. The

password pass of length passlen, salt salt of length saltlen and
iteration count iter are inputs into the encryption operation.

PKCS12_pack_p7encdata_ex() operates similar to the above but allows for a library context ctx and property query propq to be used to select the algorithm implementation.

RETURN VALUES

A PKCS7 object if successful, or NULL if an error occurred.

CONFORMING TO

IETF RFC 2315 (<https://tools.ietf.org/html/rfc2315>)

SEE ALSO

PKCS12_pbe_crypt_ex(3)

HISTORY

PKCS12_pack_p7encdata_ex() was added in OpenSSL 3.0.

COPYRIGHT