NAME

PKCS12_item_decrypt_d2i, PKCS12_item_decrypt_d2i_ex, PKCS12_item_i2d_encrypt, PKCS12_item_i2d_encrypt_ex - PKCS12 item encrypt/decrypt functions

SYNOPSIS

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

void *PKCS12_item_decrypt_d2i(const X509_ALGOR *algor, const ASN1_ITEM *it,
                              const char *pass, int passlen,
                              const ASN1_OCTET_STRING *oct, int zbuf);
void *PKCS12_item_decrypt_d2i_ex(const X509_ALGOR *algor, const ASN1_ITEM *it,
                                 const char *pass, int passlen,
                                 const ASN1_OCTET_STRING *oct, int zbuf,
                                 OSSL_LIB_CTX *libctx,
                                 const char *propq);
ASN1_OCTET_STRING *PKCS12_item_i2d_encrypt(X509_ALGOR *algor,
                                           const ASN1_ITEM *it,
                                           const char *pass, int passlen,
                                           void *obj, int zbuf);
ASN1_OCTET_STRING *PKCS12_item_i2d_encrypt_ex(X509_ALGOR *algor,
                                              const ASN1_ITEM *it,
                                              const char *pass, int passlen,
                                              void *obj, int zbuf,
                                              OSSL_LIB_CTX *ctx,
                                              const char *propq);
```

DESCRIPTION

PKCS12_item_decrypt_d2i() and **PKCS12_item_decrypt_d2i_ex()** decrypt an octet string containing an ASN.1 encoded object using the algorithm *algor* and password *pass* of length *passlen*. If *zbuf* is nonzero then the output buffer will zeroed after the decrypt.

PKCS12_item_i2d_encrypt() and **PKCS12_item_i2d_encrypt_ex()** encrypt an ASN.1 object *it* using the algorithm *algor* and password *pass* of length *passlen*, returning an encoded object in *obj*. If *zbuf* is nonzero then the buffer containing the input encoding will be zeroed after the encrypt.

Functions ending in **_ex()** allow for a library context *ctx* and property query *propq* to be used to select algorithm implementations.

RETURN VALUES

PKCS12_item_decrypt_d2i() and **PKCS12_item_decrypt_d2i_ex()** return the decrypted object or

NULL if an error occurred.

PKCS12_item_i2d_encrypt() and **PKCS12_item_i2d_encrypt_ex()** return the encrypted data as an ASN.1 Octet String or NULL if an error occurred.

SEE ALSO

PKCS12_pbe_crypt_ex(3), **PKCS8_encrypt_ex**(3)

HISTORY

PKCS12_item_decrypt_d2i_ex() and **PKCS12_item_i2d_encrypt_ex()** were added in OpenSSL 3.0.

COPYRIGHT