NAME

PKCS12_add_cert, PKCS12_add_key, PKCS12_add_key_ex, PKCS12_add_secret - Add an object to a set of PKCS#12 safeBags

SYNOPSIS

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

 PKCS12_SAFEBAG *PKCS12_add_cert(STACK_OF(PKCS12_SAFEBAG) **pbags, X509 *cert);
 PKCS12_SAFEBAG *PKCS12_add_key(STACK_OF(PKCS12_SAFEBAG) **pbags,
                               EVP_PKEY *key, int key_usage, int iter,
                               int key_nid, const char *pass);
 PKCS12_SAFEBAG *PKCS12_add_key_ex(STACK_OF(PKCS12_SAFEBAG) **pbags,
                                  EVP_PKEY *key, int key_usage, int iter,
                                  int key_nid, const char *pass,
                                  OSSL_LIB_CTX *ctx, const char *propq);

 PKCS12_SAFEBAG *PKCS12_add_secret(STACK_OF(PKCS12_SAFEBAG) **pbags,
                                  int nid_type, const unsigned char *value, int len);
```

DESCRIPTION

These functions create a new **PKCS12_SAFEBAG** and add it to the set of safeBags in *pbags*.

PKCS12_add_cert() creates a PKCS#12 certBag containing the supplied certificate and adds this to the set of PKCS#12 safeBags.

PKCS12_add_key() creates a PKCS#12 keyBag (unencrypted) or a pkcs8shroudedKeyBag (encrypted) containing the supplied **EVP_PKEY** and adds this to the set of PKCS#12 safeBags. If *key_nid* is not -1 then the key is encrypted with the supplied algorithm, using *pass* as the passphrase and *iter* as the iteration count. If *iter* is zero then a default value for iteration count of 2048 is used.

PKCS12_add_key_ex() is identical to **PKCS12_add_key()** but allows for a library context *ctx* and property query *propq* to be used to select algorithm implementations.

PKCS12_add_secret() creates a PKCS#12 secretBag with an OID corresponding to the supplied *nid_type* containing the supplied value as an ASN1 octet string. This is then added to the set of PKCS#12 safeBags.

NOTES

If a certificate contains an *alias* or a *keyid* then this will be used for the corresponding **friendlyName** or **localKeyID** in the PKCS12 structure.

PKCS12_add_key() makes assumptions regarding the encoding of the given pass phrase. See **passphrase-encoding**(7) for more information.

RETURN VALUES

A valid **PKCS12_SAFEBAG** structure or NULL if an error occurred.

CONFORMING TO

IETF RFC 7292 (<https://tools.ietf.org/html/rfc7292>)

SEE ALSO

PKCS12_create(3)

HISTORY

PKCS12_add_secret() and **PKCS12_add_key_ex()** were added in OpenSSL 3.0.

COPYRIGHT