NAME

PKCS12_add_safe, PKCS12_add_safe_ex, PKCS12_add_safes, PKCS12_add_safes_ex - Create and add objects to a PKCS#12 structure

SYNOPSIS

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

int PKCS12_add_safe(STACK_OF(PKCS7) **psafes, STACK_OF(PKCS12_SAFEBAG) *bags,
                    int safe_nid, int iter, const char *pass);
int PKCS12_add_safe_ex(STACK_OF(PKCS7) **psafes, STACK_OF(PKCS12_SAFEBAG) *bags,
                       int safe_nid, int iter, const char *pass,
                       OSSL_LIB_CTX *ctx, const char *propq);

PKCS12 *PKCS12_add_safes(STACK_OF(PKCS7) *safes, int p7_nid);
PKCS12 *PKCS12_add_safes_ex(STACK_OF(PKCS7) *safes, int p7_nid,
                            OSSL_LIB_CTX *ctx, const char *propq);
```

DESCRIPTION

PKCS12_add_safe() creates a new PKCS7 contentInfo containing the supplied **PKCS12_SAFEBAG**s and adds this to a set of PKCS7 contentInfos. Its type depends on the value of **safe_nid**:

- If *safe_nid* is -1, a plain PKCS7 *data* contentInfo is created.

- If *safe_nid* is a valid PBE algorithm NID, a PKCS7 **encryptedData** contentInfo is created. The algorithm uses *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.

- If *safe_nid* is 0, a PKCS7 **encryptedData** contentInfo is created using a default encryption algorithm, currently **NID_pbe_WithSHA1And3_Key_TripleDES_CBC**.

PKCS12_add_safe_ex() is identical to **PKCS12_add_safe()** but allows for a library context *ctx* and property query *propq* to be used to select algorithm implementations.

PKCS12_add_safes() creates a **PKCS12** structure containing the supplied set of PKCS7 contentInfos. The *safes* are enclosed first within a PKCS7 contentInfo of type *p7_nid*. Currently the only supported type is **NID_pkcs7_data**.

PKCS12_add_safes_ex() is identical to **PKCS12_add_safes()** but allows for a library context *ctx* and property query *propq* to be used to select algorithm implementations.

NOTES

PKCS12_add_safe() makes assumptions regarding the encoding of the given pass phrase. See **passphrase-encoding**(7) for more information.

RETURN VALUES

PKCS12_add_safe() returns a value of 1 indicating success or 0 for failure.

PKCS12_add_safes() returns a valid **PKCS12** 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_safe_ex() and **PKCS12_add_safes_ex()** were added in OpenSSL 3.0.

COPYRIGHT