



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

**Rocky Enterprise Linux 9.2 Manual Pages on command 'PKCS12\_SAFEABAG\_create\_pkcs8\_encrypt\_ex.3oss**

**\$ man PKCS12\_SAFEABAG\_create\_pkcs8\_encrypt\_ex.3oss**

PKCS12\_SAFEABAG\_CREATE\_CERT(3oss) OpenSSL PKCS12\_SAFEABAG\_CREATE\_CERT(3oss)

#### NAME

PKCS12\_SAFEABAG\_create\_cert, PKCS12\_SAFEABAG\_create\_crl,  
PKCS12\_SAFEABAG\_create\_secret, PKCS12\_SAFEABAG\_create0\_p8inf,  
PKCS12\_SAFEABAG\_create0\_pkcs8, PKCS12\_SAFEABAG\_create\_pkcs8\_encrypt,  
PKCS12\_SAFEABAG\_create\_pkcs8\_encrypt\_ex - Create PKCS#12 safeBag objects

#### SYNOPSIS

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

```
PKCS12_SAFEABAG *PKCS12_SAFEABAG_create_cert(X509 *x509);  
PKCS12_SAFEABAG *PKCS12_SAFEABAG_create_crl(X509_CRL *crl);  
PKCS12_SAFEABAG *PKCS12_SAFEABAG_create_secret(int type, int vtype,  
const unsigned char* value,  
int len);  
PKCS12_SAFEABAG *PKCS12_SAFEABAG_create0_p8inf(PKCS8_PRIV_KEY_INFO *p8);  
PKCS12_SAFEABAG *PKCS12_SAFEABAG_create0_pkcs8(X509_SIG *p8);
```

```

PKCS12_SAFEBAG *PKCS12_SAFEBAG_create_pkcs8_encrypt(int pbe_nid,
                const char *pass,
                int passlen,
                unsigned char *salt,
                int saltlen, int iter,
                PKCS8_PRIV_KEY_INFO *p8inf);

PKCS12_SAFEBAG *PKCS12_SAFEBAG_create_pkcs8_encrypt_ex(int pbe_nid,
                const char *pass,
                int passlen,
                unsigned char *salt,
                int saltlen, int iter,
                PKCS8_PRIV_KEY_INFO *p8inf,
                OSSL_LIB_CTX *ctx,
                const char *propq);

```

## DESCRIPTION

PKCS12\_SAFEBAG\_create\_cert() creates a new PKCS12\_SAFEBAG of type NID\_certBag containing the supplied certificate.

PKCS12\_SAFEBAG\_create\_crl() creates a new PKCS12\_SAFEBAG of type NID\_crlBag containing the supplied crl.

PKCS12\_SAFEBAG\_create\_secret() creates a new PKCS12\_SAFEBAG of type corresponding to a PKCS#12 secretBag. The secretBag contents are tagged as type with an ASN1 value of type vtype constructed using the bytes in value of length len.

PKCS12\_SAFEBAG\_create0\_p8inf() creates a new PKCS12\_SAFEBAG of type NID\_keyBag containing the supplied PKCS8 structure.

PKCS12\_SAFEBAG\_create0\_pkcs8() creates a new PKCS12\_SAFEBAG of type NID\_pkcs8ShroudedKeyBag containing the supplied PKCS8 structure.

PKCS12\_SAFEBAG\_create\_pkcs8\_encrypt() creates a new PKCS12\_SAFEBAG of type NID\_pkcs8ShroudedKeyBag by encrypting the supplied PKCS8 p8inf.

If pbe\_nid is 0, a default encryption algorithm is used. pass is the passphrase and iter is the iteration count. If iter is zero then a default value of 2048 is used. If salt is NULL then a salt is generated randomly.

PKCS12\_SAFEBAG\_create\_pkcs8\_encrypt\_ex() is identical to PKCS12\_SAFEBAG\_create\_pkcs8\_encrypt() but allows for a library context ctx and property query propq to be used to select algorithm implementations.

## NOTES

PKCS12\_SAFEBAG\_create\_pkcs8\_encrypt() makes assumptions regarding the encoding of the given pass phrase. See [passphrase-encoding\(7\)](#) for more information.

PKCS12\_SAFEBAG\_create\_secret() was added in OpenSSL 3.0.

## RETURN VALUES

All of these functions return 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), PKCS12\_add\_safe(3), PKCS12\_add\_safes(3)

## HISTORY

PKCS12\_SAFEBAG\_create\_pkcs8\_encrypt\_ex() was added in OpenSSL 3.0.

Copyright 2019-2021 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>.

3.0.7                    2023-07-13 PKCS12\_SAFEBAG\_CREATE\_CERT(3ossl)