



*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\_PBE\_keyivgen\_ex.3ossl'***

***\$ man PKCS12\_PBE\_keyivgen\_ex.3ossl***

PKCS12\_PBE\_KEYIVGEN(3ossl)      OpenSSL      PKCS12\_PBE\_KEYIVGEN(3ossl)

#### NAME

PKCS12\_PBE\_keyivgen, PKCS12\_PBE\_keyivgen\_ex, PKCS12\_pbe\_crypt,  
PKCS12\_pbe\_crypt\_ex - PKCS#12 Password based encryption

#### SYNOPSIS

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

```
int PKCS12_PBE_keyivgen(EVP_CIPHER_CTX *ctx, const char *pass, int passlen,  
                        ASN1_TYPE *param, const EVP_CIPHER *cipher,  
                        const EVP_MD *md_type, int en_de);
```

```
int PKCS12_PBE_keyivgen_ex(EVP_CIPHER_CTX *ctx, const char *pass, int passlen,  
                           ASN1_TYPE *param, const EVP_CIPHER *cipher,  
                           const EVP_MD *md_type, int en_de,  
                           OSSL_LIB_CTX *libctx, const char *propq);
```

```
unsigned char *PKCS12_pbe_crypt(const X509_ALGOR *algor,  
                                const char *pass, int passlen,
```

```

        const unsigned char *in, int inlen,
        unsigned char **data, int *datalen,
        int en_de);
unsigned char *PKCS12_pbe_crypt_ex(const X509_ALGOR *algor,
        const char *pass, int passlen,
        const unsigned char *in, int inlen,
        unsigned char **data, int *datalen,
        int en_de, OSSL_LIB_CTX *libctx,
        const char *propq);

```

## DESCRIPTION

PKCS12\_PBE\_keyivgen() and PKCS12\_PBE\_keyivgen\_ex() take a password pass of length passlen, parameters param and a message digest function md\_type and perform a key derivation according to PKCS#12. The resulting key is then used to initialise the cipher context ctx with a cipher cipher for encryption (en\_de=1) or decryption (en\_de=0).

PKCS12\_PBE\_keyivgen\_ex() also allows the application to specify a library context libctx and property query propq to select appropriate algorithm implementations.

PKCS12\_pbe\_crypt() and PKCS12\_pbe\_crypt\_ex() will encrypt or decrypt a buffer based on the algorithm in algor and password pass of length passlen. The input is from in of length inlen and output is into a malloc'd buffer returned in \*data of length datalen. The operation is determined by en\_de, encryption (en\_de=1) or decryption (en\_de=0).

PKCS12\_pbe\_crypt\_ex() allows the application to specify a library context libctx and property query propq to select appropriate algorithm implementations.

pass is the password used in the derivation of length passlen. pass is an optional parameter and can be NULL. If passlen is -1, then the

function will calculate the length of pass using strlen().

salt is the salt used in the derivation of length saltlen. If the salt is NULL, then saltlen must be 0. The function will not attempt to calculate the length of the salt because it is not assumed to be NULL terminated.

iter is the iteration count and its value should be greater than or equal to 1. RFC 2898 suggests an iteration count of at least 1000. Any iter less than 1 is treated as a single iteration.

digest is the message digest function used in the derivation.

Functions ending in \_ex() take optional parameters libctx and propq which are used to select appropriate algorithm implementations.

## NOTES

The functions are typically used in PKCS#12 to encrypt objects.

These functions make no assumption regarding the given password. It will simply be treated as a byte sequence.

## RETURN VALUES

PKCS12\_PBE\_keyivgen(), PKCS12\_PBE\_keyivgen\_ex() return 1 on success or 0 on error.

PKCS12\_pbe\_crypt() and PKCS12\_pbe\_crypt\_ex() return a buffer containing the output or NULL if an error occurred.

## CONFORMING TO

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

## SEE ALSO

EVP\_PBE\_CipherInit\_ex(3), PKCS8\_encrypt\_ex(3), passphrase-encoding(7)

## HISTORY

PKCS12\_PBE\_keyivgen\_ex() and PKCS12\_pbe\_crypt\_ex() were added in OpenSSL 3.0.

## COPYRIGHT

Copyright 2014-2021 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\_PBE\_KEYIVGEN(3ossl)