Rocky Enterprise Linux 9.2 Manual Pages on command 'PKCS8_decrypt_ex.3ossl'

$ man PKCS8_decrypt_ex.3ossl

PKCS8_ENCRYPT(3ossl) OpenSSL PKCS8_ENCRYPT(3ossl)

NAME

PKCS8_decrypt, PKCS8_decrypt_ex, PKCS8_encrypt, PKCS8_encrypt_ex,

PKCS8_set0_pbe, PKCS8_set0_pbe_ex - PKCS8 encrypt/decrypt functions

SYNOPSIS

```
#include <openssl/x509.h>

PKCS8_PRIV_KEY_INFO *PKCS8_decrypt(const X509_SIG *p8, const char *pass,
                                   int passlen);
PKCS8_PRIV_KEY_INFO *PKCS8_decrypt_ex(const X509_SIG *p8, const char *pass,
                                      int passlen, OSSL_LIB_CTX *ctx,
                                      const char *propq);
X509_SIG *PKCS8_encrypt(int pbe_nid, const EVP_CIPHER *cipher,
                        const char *pass, int passlen, unsigned char *salt,
                        int saltlen, int iter, PKCS8_PRIV_KEY_INFO *p8);
X509_SIG *PKCS8_encrypt_ex(int pbe_nid, const EVP_CIPHER *cipher,
```

```
                const char *pass, int passlen, unsigned char *salt,
                int saltlen, int iter, PKCS8_PRIV_KEY_INFO *p8,
                OSSL_LIB_CTX *ctx, const char *propq);
X509_SIG *PKCS8_set0_pbe(const char *pass, int passlen,
                         PKCS8_PRIV_KEY_INFO *p8inf, X509_ALGOR *pbe);
X509_SIG *PKCS8_set0_pbe_ex(const char *pass, int passlen,
                            PKCS8_PRIV_KEY_INFO *p8inf, X509_ALGOR *pbe,
                            OSSL_LIB_CTX *ctx);
```

DESCRIPTION

PKCS8_encrypt() and PKCS8_encrypt_ex() perform encryption of an object p8 using the password pass of length passlen, salt salt of length saltlen and iteration count iter. The resulting X509_SIG contains the encoded algorithm parameters and encrypted key.

PKCS8_decrypt() and PKCS8_decrypt_ex() perform decryption of an X509_SIG in p8 using the password pass of length passlen along with algorithm parameters obtained from the p8.

PKCS8_set0_pbe() and PKCS8_set0_pbe_ex() perform encryption of the p8inf using the password pass of length passlen and parameters pbe.

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

RETURN VALUES

PKCS8_encrypt(), PKCS8_encrypt_ex(), PKCS8_set0_pbe() and PKCS8_set0_pbe_ex() return an encrypted key in a X509_SIG structure or NULL if an error occurs.

PKCS8_decrypt() and PKCS8_decrypt_ex() return a PKCS8_PRIV_KEY_INFO or NULL if an error occurs.

CONFORMING TO

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

SEE ALSO

crypto(7)

HISTORY

PKCS8_decrypt_ex(), PKCS8_encrypt_ex() and PKCS8_set0_pbe_ex() were added in OpenSSL 3.0.

COPYRIGHT