Rocky Enterprise Linux 9.2 Manual Pages on command 'PKCS12_decrypt_skey.3ossl'

$ man PKCS12_decrypt_skey.3ossl

PKCS12_DECRYPT_SKEY(3ossl) OpenSSL PKCS12_DECRYPT_SKEY(3ossl)

NAME

PKCS12_decrypt_skey, PKCS12_decrypt_skey_ex - PKCS12 shrouded keyBag decrypt functions

SYNOPSIS

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

PKCS8_PRIV_KEY_INFO *PKCS12_decrypt_skey(const PKCS12_SAFEBAG *bag,
                                         const char *pass, int passlen);
PKCS8_PRIV_KEY_INFO *PKCS12_decrypt_skey_ex(const PKCS12_SAFEBAG *bag,
                                            const char *pass, int passlen,
                                            OSSL_LIB_CTX *ctx,
                                            const char *propq);
```

DESCRIPTION

PKCS12_decrypt_skey() Decrypt the PKCS#8 shrouded keybag contained

within bag using the supplied password pass of length passlen.

PKCS12_decrypt_skey_ex() is similar to the above but allows for a library contex ctx and property query propq to be used to select algorithm implementations.

RETURN VALUES

Both functions will return the decrypted key or NULL if an error occurred.

CONFORMING TO

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

SEE ALSO

PKCS8_decrypt_ex(3), PKCS8_encrypt_ex(3), PKCS12_add_key_ex(3), PKCS12_SAFEBAG_create_pkcs8_encrypt_ex(3)

HISTORY

PKCS12_decrypt_skey_ex() was added in OpenSSL 3.0.

COPYRIGHT