Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_PKEY_CTX_set1_pbe_pass.3ossl'

$ man EVP_PKEY_CTX_set1_pbe_pass.3ossl

EVP_PKEY_CTX_SET1_PBE_PASS(3ossl) OpenSSL EVP_PKEY_CTX_SET1_PBE_PASS(3ossl)

NAME

EVP_PKEY_CTX_set1_pbe_pass - generic KDF support functions

SYNOPSIS

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

int EVP_PKEY_CTX_set1_pbe_pass(EVP_PKEY_CTX *pctx, unsigned char *pass,
                               int passlen);
```

DESCRIPTION

These functions are generic support functions for all KDF algorithms.

EVP_PKEY_CTX_set1_pbe_pass() sets the password to the passlen first bytes from pass.

STRING CTRLS

There is also support for string based control operations via EVP_PKEY_CTX_ctrl_str(3). The password can be directly specified using the type parameter "pass" or given in hex encoding using the "hexpass" parameter.

RETURN VALUES

All these functions return 1 for success and 0 or a negative value for failure. In particular a return value of -2 indicates the operation is not supported by the public key algorithm.

SEE ALSO

EVP_PKEY_CTX_new(3), EVP_PKEY_CTX_ctrl_str(3), EVP_PKEY_derive(3)

HISTORY

EVP_PKEY_CTX_set1_pbe_pass() was converted from a macro to a function in OpenSSL 3.0.

COPYRIGHT