

NAME

`b2i_PVK_bio`, `b2i_PVK_bio_ex`, `i2b_PVK_bio`, `i2b_PVK_bio_ex` - Decode and encode functions for reading and writing MSBLOB format private keys

SYNOPSIS

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

```
EVP_PKEY *b2i_PVK_bio(BIO *in, pem_password_cb *cb, void *u);
EVP_PKEY *b2i_PVK_bio_ex(BIO *in, pem_password_cb *cb, void *u,
                          OSSL_LIB_CTX *libctx, const char *propq);
int i2b_PVK_bio(BIO *out, const EVP_PKEY *pk, int enclevel,
               pem_password_cb *cb, void *u);
int i2b_PVK_bio_ex(BIO *out, const EVP_PKEY *pk, int enclevel,
                  pem_password_cb *cb, void *u,
                  OSSL_LIB_CTX *libctx, const char *propq);
```

DESCRIPTION

`b2i_PVK_bio_ex()` decodes a private key of MSBLOB format read from a **BIO**. It attempts to automatically determine the key type. If the key is encrypted then `cb` is called with the user data `u` in order to obtain a password to decrypt the key. The supplied library context `libctx` and property query string `propq` are used in any decrypt operation.

`b2i_PVK_bio()` does the same as `b2i_PVK_bio_ex()` except that the default library context and property query string are used.

`i2b_PVK_bio_ex()` encodes `pk` using MSBLOB format. If `enclevel` is 1 then a password obtained via `pem_password_cb` is used to encrypt the private key. If `enclevel` is 0 then no encryption is applied. The user data in `u` is passed to the password callback. The supplied library context `libctx` and property query string `propq` are used in any decrypt operation.

`i2b_PVK_bio()` does the same as `i2b_PVK_bio_ex()` except that the default library context and property query string are used.

RETURN VALUES

The `b2i_PVK_bio()` and `b2i_PVK_bio_ex()` functions return a valid **EVP_KEY** structure or **NULL** if an error occurs. The error code can be obtained by calling `ERR_get_error(3)`.

`i2b_PVK_bio()` and `i2b_PVK_bio_ex()` return the number of bytes successfully encoded or a negative value if an error occurs. The error code can be obtained by calling `ERR_get_error(3)`.

SEE ALSO

`crypto(7)`, `d2i_PKCS8PrivateKey_bio(3)`

HISTORY

`b2i_PVK_bio_ex()` and `i2b_PVK_bio_ex()` were added in OpenSSL 3.0.

COPYRIGHT

Copyright 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>.