

**NAME**

OSSL\_ENCODER\_CTX\_new\_for\_pkey, OSSL\_ENCODER\_CTX\_set\_cipher, OSSL\_ENCODER\_CTX\_set\_passphrase, OSSL\_ENCODER\_CTX\_set\_pem\_password\_cb, OSSL\_ENCODER\_CTX\_set\_passphrase\_cb, OSSL\_ENCODER\_CTX\_set\_passphrase\_ui - Encoder routines to encode EVP\_PKEYs

**SYNOPSIS**

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

```
OSSL_ENCODER_CTX *
```

```
OSSL_ENCODER_CTX_new_for_pkey(const EVP_PKEY *pkey, int selection,
    const char *output_type,
    const char *output_structure,
    const char *propquery);
```

```
int OSSL_ENCODER_CTX_set_cipher(OSSL_ENCODER_CTX *ctx,
    const char *cipher_name,
    const char *propquery);
```

```
int OSSL_ENCODER_CTX_set_passphrase(OSSL_ENCODER_CTX *ctx,
    const unsigned char *kstr,
    size_t klen);
```

```
int OSSL_ENCODER_CTX_set_pem_password_cb(OSSL_ENCODER_CTX *ctx,
    pem_password_cb *cb, void *cbarg);
```

```
int OSSL_ENCODER_CTX_set_passphrase_ui(OSSL_ENCODER_CTX *ctx,
    const UI_METHOD *ui_method,
    void *ui_data);
```

```
int OSSL_ENCODER_CTX_set_passphrase_cb(OSSL_ENCODER_CTX *ctx,
    OSSL_PASSPHRASE_CALLBACK *cb,
    void *cbarg);
```

**DESCRIPTION**

**OSSL\_ENCODER\_CTX\_new\_for\_pkey()** is a utility function that creates a **OSSL\_ENCODER\_CTX**, finds all applicable encoder implementations and sets them up, so almost all the caller has to do next is call functions like **OSSL\_ENCODER\_to\_bio(3)**. *output\_type* determines the final output encoding, and *selection* can be used to select what parts of the *pkey* should be included in the output. *output\_type* is further discussed in "Output types" below, and *selection* is further described in "Selections".

Internally, **OSSL\_ENCODER\_CTX\_new\_for\_pkey()** uses the names from the **EVP\_KEYMGMT(3)** implementation associated with *pkey* to build a list of applicable encoder implementations that are used

to process the *pkey* into the encoding named by *output\_type*, with the outermost structure named by *output\_structure* if that's relevant. All these implementations are implicitly fetched, with *propquery* for finer selection.

If no suitable encoder implementation is found, **OSSL\_ENCODER\_CTX\_new\_for\_pkey()** still creates a **OSSL\_ENCODER\_CTX**, but with no associated encoder (**OSSL\_ENCODER\_CTX\_get\_num\_encoders(3)** returns zero). This helps the caller to distinguish between an error when creating the **OSSL\_ENCODER\_CTX** and missing encoder implementation, and allows it to act accordingly.

**OSSL\_ENCODER\_CTX\_set\_cipher()** tells the implementation what cipher should be used to encrypt encoded keys. The cipher is given by name *cipher\_name*. The interpretation of that *cipher\_name* is implementation dependent. The implementation may implement the cipher directly itself or by other implementations, or it may choose to fetch it. If the implementation supports fetching the cipher, then it may use *propquery* as properties to be queried for when fetching. *cipher\_name* may also be NULL, which will result in unencrypted encoding.

**OSSL\_ENCODER\_CTX\_set\_passphrase()** gives the implementation a pass phrase to use when encrypting the encoded private key. Alternatively, a pass phrase callback may be specified with the following functions.

**OSSL\_ENCODER\_CTX\_set\_pem\_password\_cb()**, **OSSL\_ENCODER\_CTX\_set\_passphrase\_ui()** and **OSSL\_ENCODER\_CTX\_set\_passphrase\_cb()** sets up a callback method that the implementation can use to prompt for a pass phrase, giving the caller the choice of preferred pass phrase callback form. These are called indirectly, through an internal **OSSL\_PASSPHRASE\_CALLBACK(3)** function.

## Output types

The possible **EVP\_PKEY** output types depends on the available implementations.

OpenSSL has built in implementations for the following output types:

"TEXT"

The output is a human readable description of the key. **EVP\_PKEY\_print\_private(3)**, **EVP\_PKEY\_print\_public(3)** and **EVP\_PKEY\_print\_params(3)** use this for their output.

"DER"

The output is the DER encoding of the *selection* of the *pkey*.

"PEM"

The output is the *selection* of the *pkey* in PEM format.

**Selections**

*selection* can be any one of the values described in "Selections" in **EVP\_PKEY\_fromdata(3)**.

These are only 'hints' since the encoder implementations are free to determine what makes sense to include in the output, and this may depend on the desired output. For example, an EC key in a PKCS#8 structure doesn't usually include the public key.

**RETURN VALUES**

**OSSL\_ENCODER\_CTX\_new\_for\_pkey()** returns a pointer to an **OSSL\_ENCODER\_CTX**, or NULL if it couldn't be created.

**OSSL\_ENCODER\_CTX\_set\_cipher()**, **OSSL\_ENCODER\_CTX\_set\_passphrase()**, **OSSL\_ENCODER\_CTX\_set\_pem\_password\_cb()**, **OSSL\_ENCODER\_CTX\_set\_passphrase\_ui()** and **OSSL\_ENCODER\_CTX\_set\_passphrase\_cb()** all return 1 on success, or 0 on failure.

**SEE ALSO**

**provider(7)**, **OSSL\_ENCODER(3)**, **OSSL\_ENCODER\_CTX(3)**

**HISTORY**

The functions described here were added in OpenSSL 3.0.

**COPYRIGHT**

Copyright 2019-2021 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>.