



***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_KEYMGMT\_fetch.3ossl'***

***\$ man EVP\_KEYMGMT\_fetch.3ossl***

EVP\_KEYMGMT(3ossl)            OpenSSL            EVP\_KEYMGMT(3ossl)

NAME

EVP\_KEYMGMT, EVP\_KEYMGMT\_fetch, EVP\_KEYMGMT\_up\_ref, EVP\_KEYMGMT\_free,  
EVP\_KEYMGMT\_get0\_provider, EVP\_KEYMGMT\_is\_a,  
EVP\_KEYMGMT\_get0\_description, EVP\_KEYMGMT\_get0\_name,  
EVP\_KEYMGMT\_do\_all\_provided, EVP\_KEYMGMT\_names\_do\_all,  
EVP\_KEYMGMT\_gettable\_params, EVP\_KEYMGMT\_settable\_params,  
EVP\_KEYMGMT\_gen\_settable\_params - EVP key management routines

SYNOPSIS

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

typedef struct evp_keymgmt_st EVP_KEYMGMT;

EVP_KEYMGMT *EVP_KEYMGMT_fetch(OSSL_LIB_CTX *ctx, const char *algorithm,
                               const char *properties);

int EVP_KEYMGMT_up_ref(EVP_KEYMGMT *keymgmt);

void EVP_KEYMGMT_free(EVP_KEYMGMT *keymgmt);

const OSSL_PROVIDER *EVP_KEYMGMT_get0_provider(const EVP_KEYMGMT *keymgmt);

int EVP_KEYMGMT_is_a(const EVP_KEYMGMT *keymgmt, const char *name);

const char *EVP_KEYMGMT_get0_name(const EVP_KEYMGMT *keymgmt);
```

```

const char *EVP_KEYMGMT_get0_description(const EVP_KEYMGMT *keymgmt);
void EVP_KEYMGMT_do_all_provided(OSSL_LIB_CTX *libctx,
    void (*fn)(EVP_KEYMGMT *keymgmt, void *arg),
    void *arg);
int EVP_KEYMGMT_names_do_all(const EVP_KEYMGMT *keymgmt,
    void (*fn)(const char *name, void *data),
    void *data);
const OSSL_PARAM *EVP_KEYMGMT_gettable_params(const EVP_KEYMGMT *keymgmt);
const OSSL_PARAM *EVP_KEYMGMT_settable_params(const EVP_KEYMGMT *keymgmt);
const OSSL_PARAM *EVP_KEYMGMT_gen_settable_params(const EVP_KEYMGMT *keymgmt);

```

## DESCRIPTION

EVP\_KEYMGMT is a method object that represents key management implementations for different cryptographic algorithms. This method object provides functionality to have providers import key material from the outside, as well as export key material to the outside. Most of the functionality can only be used internally and has no public interface, this object is simply passed into other functions when needed.

EVP\_KEYMGMT\_fetch() looks for an algorithm within the provider that has been loaded into the OSSL\_LIB\_CTX given by ctx, having the name given by algorithm and the properties given by properties.

EVP\_KEYMGMT\_up\_ref() increments the reference count for the given EVP\_KEYMGMT keymgmt.

EVP\_KEYMGMT\_free() decrements the reference count for the given EVP\_KEYMGMT keymgmt, and when the count reaches zero, frees it.

EVP\_KEYMGMT\_get0\_provider() returns the provider that has this particular implementation.

EVP\_KEYMGMT\_is\_a() checks if keymgmt is an implementation of an algorithm that's identifiable with name.

EVP\_KEYMGMT\_get0\_name() returns the algorithm name from the provided implementation for the given keymgmt. Note that the keymgmt may have multiple synonyms associated with it. In this case the first name from the algorithm definition is returned. Ownership of the returned string

is retained by the keymgmt object and should not be freed by the caller.

EVP\_KEYMGMT\_names\_do\_all() traverses all names for the keymgmt, and calls fn with each name and data.

EVP\_KEYMGMT\_get0\_description() returns a description of the keymgmt, meant for display and human consumption. The description is at the discretion of the keymgmt implementation.

EVP\_KEYMGMT\_do\_all\_provided() traverses all key keymgmt implementations by all activated providers in the library context libctx, and for each of the implementations, calls fn with the implementation method and data as arguments.

EVP\_KEYMGMT\_gettable\_params() and EVP\_KEYMGMT\_settable\_params() return a constant OSSL\_PARAM array that describes the names and types of key parameters that can be retrieved or set. EVP\_KEYMGMT\_gettable\_params() is used by EVP\_PKEY\_gettable\_params(3). See OSSL\_PARAM(3) for the use of OSSL\_PARAM as a parameter descriptor.

EVP\_KEYMGMT\_gen\_settable\_params() returns a constant OSSL\_PARAM array that describes the names and types of key generation parameters that can be set via EVP\_PKEY\_CTX\_set\_params(3).

## NOTES

EVP\_KEYMGMT\_fetch() may be called implicitly by other fetching functions, using the same library context and properties. Any other API that uses keys will typically do this.

## RETURN VALUES

EVP\_KEYMGMT\_fetch() returns a pointer to the key management implementation represented by an EVP\_KEYMGMT object, or NULL on error.

EVP\_KEYMGMT\_up\_ref() returns 1 on success, or 0 on error.

EVP\_KEYMGMT\_names\_do\_all() returns 1 if the callback was called for all names. A return value of 0 means that the callback was not called for any names.

EVP\_KEYMGMT\_free() doesn't return any value.

EVP\_KEYMGMT\_get0\_provider() returns a pointer to a provider object, or NULL on error.

EVP\_KEYMGMT\_is\_a() returns 1 if keymgmt was identifiable, otherwise 0.

EVP\_KEYMGMT\_get0\_name() returns the algorithm name, or NULL on error.

EVP\_KEYMGMT\_get0\_description() returns a pointer to a description, or NULL if there isn't one.

EVP\_KEYMGMT\_gettable\_params(), EVP\_KEYMGMT\_settable\_params() and EVP\_KEYMGMT\_gen\_settable\_params() return a constant OSSL\_PARAM array or NULL on error.

#### SEE ALSO

EVP\_MD\_fetch(3), OSSL\_LIB\_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>](https://www.openssl.org/source/license.html).

3.0.7                      2023-07-13                      EVP\_KEYMGMT(3openssl)