

**NAME**

EVP\_CIPHER\_meth\_new, EVP\_CIPHER\_meth\_dup, EVP\_CIPHER\_meth\_free,  
 EVP\_CIPHER\_meth\_set\_iv\_length, EVP\_CIPHER\_meth\_set\_flags,  
 EVP\_CIPHER\_meth\_set\_impl\_ctx\_size, EVP\_CIPHER\_meth\_set\_init,  
 EVP\_CIPHER\_meth\_set\_do\_cipher, EVP\_CIPHER\_meth\_set\_cleanup,  
 EVP\_CIPHER\_meth\_set\_set\_asn1\_params, EVP\_CIPHER\_meth\_set\_get\_asn1\_params,  
 EVP\_CIPHER\_meth\_set\_ctrl, EVP\_CIPHER\_meth\_get\_init, EVP\_CIPHER\_meth\_get\_do\_cipher,  
 EVP\_CIPHER\_meth\_get\_cleanup, EVP\_CIPHER\_meth\_get\_set\_asn1\_params,  
 EVP\_CIPHER\_meth\_get\_get\_asn1\_params, EVP\_CIPHER\_meth\_get\_ctrl - Routines to build up  
 EVP\_CIPHER methods

**SYNOPSIS**

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

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining **OPENSSL\_API\_COMPAT** with a suitable version value, see **openssl\_user\_macros(7)**:

```
EVP_CIPHER *EVP_CIPHER_meth_new(int cipher_type, int block_size, int key_len);
EVP_CIPHER *EVP_CIPHER_meth_dup(const EVP_CIPHER *cipher);
void EVP_CIPHER_meth_free(EVP_CIPHER *cipher);
```

```
int EVP_CIPHER_meth_set_iv_length(EVP_CIPHER *cipher, int iv_len);
int EVP_CIPHER_meth_set_flags(EVP_CIPHER *cipher, unsigned long flags);
int EVP_CIPHER_meth_set_impl_ctx_size(EVP_CIPHER *cipher, int ctx_size);
int EVP_CIPHER_meth_set_init(EVP_CIPHER *cipher,
    int (*init)(EVP_CIPHER_CTX *ctx,
        const unsigned char *key,
        const unsigned char *iv,
        int enc));
```

```
int EVP_CIPHER_meth_set_do_cipher(EVP_CIPHER *cipher,
    int (*do_cipher)(EVP_CIPHER_CTX *ctx,
        unsigned char *out,
        const unsigned char *in,
        size_t inl));
```

```
int EVP_CIPHER_meth_set_cleanup(EVP_CIPHER *cipher,
    int (*cleanup)(EVP_CIPHER_CTX *));
```

```
int EVP_CIPHER_meth_set_set_asn1_params(EVP_CIPHER *cipher,
    int (*set_asn1_parameters)(EVP_CIPHER_CTX *,
        ASN1_TYPE *));
```

```
int EVP_CIPHER_meth_set_get_asn1_params(EVP_CIPHER *cipher,
```

```

        int (*get_asn1_parameters)(EVP_CIPHER_CTX *,
                                   ASN1_TYPE *);
int EVP_CIPHER_meth_set_ctrl(EVP_CIPHER *cipher,
                             int (*ctrl)(EVP_CIPHER_CTX *, int type,
                                           int arg, void *ptr));

int (*EVP_CIPHER_meth_get_init(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *ctx,
                                                           const unsigned char *key,
                                                           const unsigned char *iv,
                                                           int enc);
int (*EVP_CIPHER_meth_get_do_cipher(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *ctx,
                                                                unsigned char *out,
                                                                const unsigned char *in,
                                                                size_t inl);
int (*EVP_CIPHER_meth_get_cleanup(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *);
int (*EVP_CIPHER_meth_get_set_asn1_params(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *,
                                                                       ASN1_TYPE *);
int (*EVP_CIPHER_meth_get_get_asn1_params(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *,
                                                                       ASN1_TYPE *);
int (*EVP_CIPHER_meth_get_ctrl(const EVP_CIPHER *cipher))(EVP_CIPHER_CTX *,
                                                           int type, int arg,
                                                           void *ptr);

```

## DESCRIPTION

All of the functions described on this page are deprecated. Applications should instead use the OSSL\_PROVIDER APIs.

The **EVP\_CIPHER** type is a structure for symmetric cipher method implementation.

**EVP\_CIPHER\_meth\_new()** creates a new **EVP\_CIPHER** structure.

**EVP\_CIPHER\_meth\_dup()** creates a copy of **cipher**.

**EVP\_CIPHER\_meth\_free()** destroys a **EVP\_CIPHER** structure.

**EVP\_CIPHER\_meth\_set\_iv\_length()** sets the length of the IV. This is only needed when the implemented cipher mode requires it.

**EVP\_CIPHER\_meth\_set\_flags()** sets the flags to describe optional behaviours in the particular **cipher**. With the exception of cipher modes, of which only one may be present, several flags can be or'd

together. The available flags are:

EVP\_CIPH\_STREAM\_CIPHER, EVP\_CIPH\_ECB\_MODE, EVP\_CIPH\_CBC\_MODE,  
EVP\_CIPH\_CFB\_MODE, EVP\_CIPH\_OFB\_MODE, EVP\_CIPH\_CTR\_MODE,  
EVP\_CIPH\_GCM\_MODE, EVP\_CIPH\_CCM\_MODE, EVP\_CIPH\_XTS\_MODE,  
EVP\_CIPH\_WRAP\_MODE, EVP\_CIPH\_OCB\_MODE, EVP\_CIPH\_SIV\_MODE

The cipher mode.

**EVP\_CIPH\_VARIABLE\_LENGTH**

This cipher is of variable length.

**EVP\_CIPH\_CUSTOM\_IV**

Storing and initialising the IV is left entirely to the implementation.

**EVP\_CIPH\_ALWAYS\_CALL\_INIT**

Set this if the implementation's **init()** function should be called even if **key** is **NULL**.

**EVP\_CIPH\_CTRL\_INIT**

Set this to have the implementation's **ctrl()** function called with command code **EVP\_CTRL\_INIT** early in its setup.

**EVP\_CIPH\_CUSTOM\_KEY\_LENGTH**

Checking and setting the key length after creating the **EVP\_CIPHER** is left to the implementation. Whenever someone uses **EVP\_CIPHER\_CTX\_set\_key\_length()** on a **EVP\_CIPHER** with this flag set, the implementation's **ctrl()** function will be called with the control code **EVP\_CTRL\_SET\_KEY\_LENGTH** and the key length in **arg**.

**EVP\_CIPH\_NO\_PADDING**

Don't use standard block padding.

**EVP\_CIPH\_RAND\_KEY**

Making a key with random content is left to the implementation. This is done by calling the implementation's **ctrl()** function with the control code **EVP\_CTRL\_RAND\_KEY** and the pointer to the key memory storage in **ptr**.

**EVP\_CIPH\_CUSTOM\_COPY**

Set this to have the implementation's **ctrl()** function called with command code **EVP\_CTRL\_COPY** at the end of **EVP\_CIPHER\_CTX\_copy()**. The intended use is for further things to deal with after the implementation specific data block has been copied. The destination **EVP\_CIPHER\_CTX** is passed to the control with the **ptr** parameter. The implementation specific

data block is reached with **EVP\_CIPHER\_CTX\_get\_cipher\_data()**.

#### **EVP\_CIPH\_FLAG\_DEFAULT\_ASN1**

Use the default EVP routines to pass IV to and from ASN.1.

#### **EVP\_CIPH\_FLAG\_LENGTH\_BITS**

Signals that the length of the input buffer for encryption / decryption is to be understood as the number of bits instead of bytes for this implementation. This is only useful for CFB1 ciphers.

#### **EVP\_CIPH\_FLAG\_CTS**

Indicates that the cipher uses ciphertext stealing. This is currently used to indicate that the cipher is a one shot that only allows a single call to **EVP\_CipherUpdate()**.

#### **EVP\_CIPH\_FLAG\_CUSTOM\_CIPHER**

This indicates that the implementation takes care of everything, including padding, buffering and finalization. The EVP routines will simply give them control and do nothing more.

#### **EVP\_CIPH\_FLAG\_AEAD\_CIPHER**

This indicates that this is an AEAD cipher implementation.

#### **EVP\_CIPH\_FLAG\_TLS1\_1\_MULTIBLOCK**

Allow interleaving of crypto blocks, a particular optimization only applicable to certain TLS ciphers.

**EVP\_CIPHER\_meth\_set\_impl\_ctx\_size()** sets the size of the EVP\_CIPHER's implementation context so that it can be automatically allocated.

**EVP\_CIPHER\_meth\_set\_init()** sets the cipher init function for **cipher**. The cipher init function is called by **EVP\_CipherInit()**, **EVP\_CipherInit\_ex()**, **EVP\_EncryptInit()**, **EVP\_EncryptInit\_ex()**, **EVP\_DecryptInit()**, **EVP\_DecryptInit\_ex()**.

**EVP\_CIPHER\_meth\_set\_do\_cipher()** sets the cipher function for **cipher**. The cipher function is called by **EVP\_CipherUpdate()**, **EVP\_EncryptUpdate()**, **EVP\_DecryptUpdate()**, **EVP\_CipherFinal()**, **EVP\_EncryptFinal()**, **EVP\_EncryptFinal\_ex()**, **EVP\_DecryptFinal()** and **EVP\_DecryptFinal\_ex()**.

**EVP\_CIPHER\_meth\_set\_cleanup()** sets the function for **cipher** to do extra cleanup before the method's private data structure is cleaned out and freed. Note that the cleanup function is passed a **EVP\_CIPHER\_CTX \***, the private data structure is then available with **EVP\_CIPHER\_CTX\_get\_cipher\_data()**. This cleanup function is called by **EVP\_CIPHER\_CTX\_reset()** and **EVP\_CIPHER\_CTX\_free()**.

**EVP\_CIPHER\_meth\_set\_set\_asn1\_params()** sets the function for **cipher** to set the AlgorithmIdentifier "parameter" based on the passed cipher. This function is called by **EVP\_CIPHER\_param\_to\_asn1()**. **EVP\_CIPHER\_meth\_set\_get\_asn1\_params()** sets the function for **cipher** that sets the cipher parameters based on an ASN.1 AlgorithmIdentifier "parameter". Both these functions are needed when there is a need for custom data (more or other than the cipher IV). They are called by **EVP\_CIPHER\_param\_to\_asn1()** and **EVP\_CIPHER\_asn1\_to\_param()** respectively if defined.

**EVP\_CIPHER\_meth\_set\_ctrl()** sets the control function for **cipher**.

**EVP\_CIPHER\_meth\_get\_init()**, **EVP\_CIPHER\_meth\_get\_do\_cipher()**, **EVP\_CIPHER\_meth\_get\_cleanup()**, **EVP\_CIPHER\_meth\_get\_set\_asn1\_params()**, **EVP\_CIPHER\_meth\_get\_get\_asn1\_params()** and **EVP\_CIPHER\_meth\_get\_ctrl()** are all used to retrieve the method data given with the **EVP\_CIPHER\_meth\_set\_\***() functions above.

## RETURN VALUES

**EVP\_CIPHER\_meth\_new()** and **EVP\_CIPHER\_meth\_dup()** return a pointer to a newly created **EVP\_CIPHER**, or NULL on failure. All **EVP\_CIPHER\_meth\_set\_\***() functions return 1. All **EVP\_CIPHER\_meth\_get\_\***() functions return pointers to their respective **cipher** function.

## SEE ALSO

**EVP\_EncryptInit(3)**

## HISTORY

All of these functions were deprecated in OpenSSL 3.0.

The functions described here were added in OpenSSL 1.1.0. The **EVP\_CIPHER** structure created with these functions became reference counted in OpenSSL 3.0.

## COPYRIGHT

Copyright 2016-2021 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>.