

NAME

CMS_EnvelopedData_create_ex, CMS_EnvelopedData_create, CMS_AuthEnvelopedData_create, CMS_AuthEnvelopedData_create_ex - Create CMS envelope

SYNOPSIS

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

```
CMS_ContentInfo *
CMS_EnvelopedData_create_ex(const EVP_CIPHER *cipher, OSSL_LIB_CTX *libctx,
                           const char *propq);
CMS_ContentInfo *CMS_EnvelopedData_create(const EVP_CIPHER *cipher);
```

```
CMS_ContentInfo *
CMS_AuthEnvelopedData_create_ex(const EVP_CIPHER *cipher, OSSL_LIB_CTX *libctx,
                                const char *propq);
CMS_ContentInfo *CMS_AuthEnvelopedData_create(const EVP_CIPHER *cipher);
```

DESCRIPTION

CMS_EnvelopedData_create_ex() creates a **CMS_ContentInfo** structure with a type **NID_pkcs7_enveloped**. *cipher* is the symmetric cipher to use. The library context *libctx* and the property query *propq* are used when retrieving algorithms from providers.

CMS_AuthEnvelopedData_create_ex() creates a **CMS_ContentInfo** structure with a type **NID_id_smime_ct_authEnvelopedData**. **cipher** is the symmetric AEAD cipher to use. Currently only AES variants with GCM mode are supported. The library context *libctx* and the property query *propq* are used when retrieving algorithms from providers.

The algorithm passed in the *cipher* parameter must support ASN1 encoding of its parameters.

The recipients can be added later using **CMS_add1_recipient_cert(3)** or **CMS_add0_recipient_key(3)**.

The **CMS_ContentInfo** structure needs to be finalized using **CMS_final(3)** and then freed using **CMS_ContentInfo_free(3)**.

CMS_EnvelopedData_create() and **CMS_AuthEnvelopedData_create** are similar to **CMS_EnvelopedData_create_ex()** and **CMS_AuthEnvelopedData_create_ex()** but use default values of NULL for the library context *libctx* and the property query *propq*.

NOTES

Although **CMS_EnvelopedData_create()** and **CMS_AuthEnvelopedData_create()** allocate a new

CMS_ENVELOPEDDATA_CREATE(3openssl) OpenSSL CMS_ENVELOPEDDATA_CREATE(3openssl)

CMS_ContentInfo structure, they are not usually used in applications. The wrappers **CMS_encrypt(3)** and **CMS_decrypt(3)** are often used instead.

RETURN VALUES

If the allocation fails, **CMS_EnvelopedData_create()** and **CMS_AuthEnvelopedData_create()** return NULL and set an error code that can be obtained by **ERR_get_error(3)**. Otherwise they return a pointer to the newly allocated structure.

SEE ALSO

ERR_get_error(3), **CMS_encrypt(3)**, **CMS_decrypt(3)**, **CMS_final(3)**

HISTORY

The **CMS_EnvelopedData_create_ex()** method was added in OpenSSL 3.0.

COPYRIGHT

Copyright 2020-2021 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>.