

NAME

SMIME_read_CMS_ex, SMIME_read_CMS - parse S/MIME message

SYNOPSIS

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

```
CMS_ContentInfo *SMIME_read_CMS_ex(BIO *bio, int flags, BIO **bcont,  
    CMS_ContentInfo **cms);
```

```
CMS_ContentInfo *SMIME_read_CMS(BIO *in, BIO **bcont);
```

DESCRIPTION

SMIME_read_CMS() parses a message in S/MIME format.

in is a BIO to read the message from.

If cleartext signing is used then the content is saved in a memory bio which is written to ***bcont**, otherwise ***bcont** is set to NULL.

The parsed CMS_ContentInfo structure is returned or NULL if an error occurred.

SMIME_read_CMS_ex() is similar to **SMIME_read_CMS()** but optionally a previously created *cms* CMS_ContentInfo object can be supplied as well as some *flags*. To create a *cms* object use **CMS_ContentInfo_new_ex(3)**. If the *flags* argument contains **CMS_BINARY** then the input is assumed to be in binary format and is not translated to canonical form. If in addition **SMIME_ASCIIICRLF** is set then the binary input is assumed to be followed by **CR** and **LF** characters, else only by an **LF** character. If *flags* is 0 and *cms* is NULL then it is identical to **SMIME_read_CMS()**.

NOTES

If ***bcont** is not NULL then the message is clear text signed. ***bcont** can then be passed to **CMS_verify()** with the **CMS_DETACHED** flag set.

Otherwise the type of the returned structure can be determined using **CMS_get0_type()**.

To support future functionality if **bcont** is not NULL ***bcont** should be initialized to NULL. For example:

```
BIO *cont = NULL;  
CMS_ContentInfo *cms;
```

```
cms = SMIME_read_CMS(in, &cont);
```

BUGS

The MIME parser used by **SMIME_read_CMS()** is somewhat primitive. While it will handle most S/MIME messages more complex compound formats may not work.

The parser assumes that the **CMS_ContentInfo** structure is always base64 encoded and will not handle the case where it is in binary format or uses quoted printable format.

The use of a memory BIO to hold the signed content limits the size of message which can be processed due to memory restraints: a streaming single pass option should be available.

RETURN VALUES

SMIME_read_CMS_ex() and **SMIME_read_CMS()** return a valid **CMS_ContentInfo** structure or **NULL** if an error occurred. The error can be obtained from **ERR_get_error(3)**.

SEE ALSO

ERR_get_error(3), **CMS_sign(3)**, **CMS_verify(3)**, **CMS_encrypt(3)**, **CMS_decrypt(3)**

HISTORY

The function **SMIME_read_CMS_ex()** was added in OpenSSL 3.0.

COPYRIGHT

Copyright 2008-2021 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>>.