NAME

SMIME_read_ASN1_ex, SMIME_read_ASN1 - parse S/MIME message

SYNOPSIS

```
 #include <openssl/asn1.h>

 ASN1_VALUE *SMIME_read_ASN1_ex(BIO *in, int flags, BIO **bcont,
                                const ASN1_ITEM *it, ASN1_VALUE **x,
                                OSSL_LIB_CTX *libctx, const char *propq);
 ASN1_VALUE *SMIME_read_ASN1(BIO *in, BIO **bcont, const ASN1_ITEM *it);
```

DESCRIPTION

SMIME_read_ASN1_ex() parses a message in S/MIME format.

in is a BIO to read the message from. 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_ASCIICRLF** is set then the binary input is assumed to be followed by **CR** and **LF** characters, else only by an **LF** character. *x* can be used to optionally supply a previously created *it* ASN1_VALUE object (such as CMS_ContentInfo or PKCS7), it can be set to NULL. Valid values that can be used by ASN.1 structure *it* are ASN1_ITEM_rptr(PKCS7) or ASN1_ITEM_rptr(CMS_ContentInfo). Any algorithm fetches that occur during the operation will use the **OSSL_LIB_CTX** supplied in the *libctx* parameter, and use the property query string *propq* See "ALGORITHM FETCHING" in **crypto**(7) for further details about algorithm fetching.

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 ASN1_VALUE structure is returned or NULL if an error occurred.

SMIME_read_ASN1() is similar to **SMIME_read_ASN1_ex()** but sets the value of *x* to NULL and the value of *flags* to 0.

NOTES

The higher level functions **SMIME_read_CMS_ex**(3) and **SMIME_read_PKCS7_ex**(3) should be used instead of **SMIME_read_ASN1_ex()**.

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

BUGS

The MIME parser used by **SMIME_read_ASN1_ex()** is somewhat primitive. While it will handle most

S/MIME messages more complex compound formats may not work.

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_ASN1_ex() and **SMIME_read_ASN1()** return a valid **ASN1_VALUE** structure or **NULL** if an error occurred. The error can be obtained from **ERR_get_error**(3).

SEE ALSO

ERR_get_error(3), **SMIME_read_CMS_ex**(3), **SMIME_read_PKCS7_ex**(3), **SMIME_write_ASN1**(3), **SMIME_write_ASN1_ex**(3)

HISTORY

The function **SMIME_read_ASN1_ex()** was added in OpenSSL 3.0.

COPYRIGHT