#### **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.

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.

in is a BIO to read the message from. If the flags argument contains CMS BINARY then the input is

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**

 $\label{lem:error} ERR\_get\_error(3), SMIME\_read\_CMS\_ex(3), SMIME\_read\_PKCS7\_ex(3), SMIME\_write\_ASN1(3), SMIME\_write\_ASN1\_ex(3)$ 

# **HISTORY**

The function **SMIME\_read\_ASN1\_ex()** was added in OpenSSL 3.0.

## **COPYRIGHT**

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 <a href="https://www.openssl.org/source/license.html">https://www.openssl.org/source/license.html</a>>.