

**NAME**

SMIME\_read\_PKCS7\_ex, SMIME\_read\_PKCS7 - parse S/MIME message

**SYNOPSIS**

```
#include <openssl/pkcs7.h>
```

```
PKCS7 *SMIME_read_PKCS7_ex(BIO *bio, BIO **bcont, PKCS7 **p7);
```

```
PKCS7 *SMIME_read_PKCS7(BIO *in, BIO **bcont);
```

**DESCRIPTION**

**SMIME\_read\_PKCS7()** 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 PKCS#7 structure is returned or **NULL** if an error occurred.

**SMIME\_read\_PKCS7\_ex()** is similar to **SMIME\_read\_PKCS7()** but can optionally supply a previously created *p7* PKCS#7 object. If *p7* is **NULL** then it is identical to **SMIME\_read\_PKCS7()**. To create a *p7* object use **PKCS7\_new\_ex(3)**.

**NOTES**

If **\*bcont** is not **NULL** then the message is clear text signed. **\*bcont** can then be passed to **PKCS7\_verify()** with the **PKCS7\_DETACHED** flag set.

Otherwise the type of the returned structure can be determined using **PKCS7\_type\_is\_enveloped()**, etc.

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

```
BIO *cont = NULL;
```

```
PKCS7 *p7;
```

```
p7 = SMIME_read_PKCS7(in, &cont);
```

**BUGS**

The MIME parser used by **SMIME\_read\_PKCS7()** is somewhat primitive. While it will handle most S/MIME messages more complex compound formats may not work.

The parser assumes that the PKCS7 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\_PKCS7\_ex()** and **SMIME\_read\_PKCS7()** return a valid **PKCS7** 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\_PKCS7(3)**, **PKCS7\_sign(3)**, **PKCS7\_verify(3)**, **PKCS7\_encrypt(3)**  
**PKCS7\_decrypt(3)**

## HISTORY

The function **SMIME\_read\_PKCS7\_ex()** was added in OpenSSL 3.0.

## COPYRIGHT

Copyright 2002-2020 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>>.