



Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'SMIME_read_PKCS7_ex.3oss1' command

\$ man SMIME_read_PKCS7_ex.3oss1

SMIME_READ_PKCS7(3oss1) OpenSSL SMIME_READ_PKCS7(3oss1)

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>.

3.0.7 2023-07-13 `SMIME_READ_PKCS7(3oss)`