



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_write_ASN1_ex.3ossl' command

\$ man SMIME_write_ASN1_ex.3ossl

SMIME_WRITE_ASN1(3ossl) OpenSSL SMIME_WRITE_ASN1(3ossl)

NAME

SMIME_write_ASN1_ex, SMIME_write_ASN1 - convert structure to S/MIME format

SYNOPSIS

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

```
int SMIME_write_ASN1_ex(BIO *out, ASN1_VALUE *val, BIO *data, int flags,
                        int ctype_nid, int econt_nid,
                        STACK_OF(X509_ALGOR) *mdalgs, const ASN1_ITEM *it,
                        OSSL_LIB_CTX *libctx, const char *propq);
```

```
int SMIME_write_ASN1(BIO *out,
                    ASN1_VALUE *val, BIO *data, int flags, int ctype_nid, int econt_nid,
                    STACK_OF(X509_ALGOR) *mdalgs, const ASN1_ITEM *it);
```

DESCRIPTION

SMIME_write_ASN1_ex() adds the appropriate MIME headers to an object structure to produce an S/MIME message.

out is the BIO to write the data to. value is the appropriate

ASN1_VALUE structure (either CMS_ContentInfo or PKCS7). If streaming is enabled then the content must be supplied via data. flags is an optional set of flags. ctype_nid is the NID of the content type, econt_nid is the NID of the embedded content type and mdalgs is a list of signed data digestAlgorithms. Valid values that can be used by the ASN.1 structure it are ASN1_ITEM_rptr(PKCS7) or ASN1_ITEM_rptr(CMS_ContentInfo). The library context libctx and the property query propq are used when retrieving algorithms from providers.

NOTES

The higher level functions SMIME_write_CMS(3) and SMIME_write_PKCS7(3) should be used instead of SMIME_write_ASN1().

The following flags can be passed in the flags parameter.

If CMS_DETACHED is set then cleartext signing will be used, this option only makes sense for SignedData where CMS_DETACHED is also set when the sign() method is called.

If the CMS_TEXT flag is set MIME headers for type text/plain are added to the content, this only makes sense if CMS_DETACHED is also set.

If the CMS_STREAM flag is set streaming is performed. This flag should only be set if CMS_STREAM was also set in the previous call to a CMS_ContentInfo or PKCS7 creation function.

If cleartext signing is being used and CMS_STREAM not set then the data must be read twice: once to compute the signature in sign method and once to output the S/MIME message.

If streaming is performed the content is output in BER format using indefinite length constructed encoding except in the case of signed

data with detached content where the content is absent and DER format is used.

RETURN VALUES

SMIME_write_ASN1_ex() and SMIME_write_ASN1() return 1 for success or 0 for failure.

SEE ALSO

ERR_get_error(3), SMIME_write_CMS(3), SMIME_write_PKCS7(3)

COPYRIGHT

Copyright 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_WRITE_ASN1(3openssl)