

**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>>.