

NAME

CMS_final, CMS_final_digest – finalise a CMS_ContentInfo structure

SYNOPSIS

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

```
int CMS_final(CMS_ContentInfo *cms, BIO *data, BIO *dcont, unsigned int flags);  
int CMS_final_digest(CMS_ContentInfo *cms, const unsigned char *md,  
                    unsigned int mdlen, BIO *dcont, unsigned int flags);
```

DESCRIPTION

CMS_final() finalises the structure **cms**. Its purpose is to perform any operations necessary on **cms** (digest computation for example) and set the appropriate fields. The parameter **data** contains the content to be processed. The **dcont** parameter contains a BIO to write content to after processing: this is only used with detached data and will usually be set to NULL.

CMS_final_digest() finalises the structure **cms** using a pre-computed digest, rather than computing the digest from the original data.

NOTES

These functions will normally be called when the **CMS_PARTIAL** flag is used. It should only be used when streaming is not performed because the streaming I/O functions perform finalisation operations internally.

To sign a pre-computed digest, **CMS_sign(3)** or **CMS_sign_ex()** is called with the **data** parameter set to NULL before the CMS structure is finalised with the digest provided to **CMS_final_digest()** in binary form. When signing a pre-computed digest, the security relies on the digest and its computation from the original message being trusted.

RETURN VALUES

CMS_final() and **CMS_final_digest()** return 1 for success or 0 for failure.

SEE ALSO

ERR_get_error(3), **CMS_sign(3)**, **CMS_encrypt(3)**

HISTORY

CMS_final_digest() was added in OpenSSL 3.2.

COPYRIGHT

Copyright 2008–2022 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>>.