NAME

CMS_add0_cert, CMS_add1_cert, CMS_get1_certs, CMS_add0_crl, CMS_add1_crl, CMS_get1_crls − CMS certificate and CRL utility functions

SYNOPSIS

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

int CMS_add0_cert(CMS_ContentInfo *cms, X509 *cert);
int CMS_add1_cert(CMS_ContentInfo *cms, X509 *cert);
STACK_OF(X509) *CMS_get1_certs(CMS_ContentInfo *cms);

int CMS_add0_crl(CMS_ContentInfo *cms, X509_CRL *crl);
int CMS_add1_crl(CMS_ContentInfo *cms, X509_CRL *crl);
STACK_OF(X509_CRL) *CMS_get1_crls(CMS_ContentInfo *cms);
```

DESCRIPTION

CMS_add0_cert() and **CMS_add1_cert()** add certificate *cert* to *cms* unless it is already present. This is used by **CMS_sign_ex**(3) and **CMS_sign**(3) and may be used before calling **CMS_verify**(3) to help chain building in certificate validation. As the 0 implies,**CMS_add0_cert()** adds *cert* internally to *cms* and on success it must not be freed up by the caller. In contrast, the caller of**CMS_add1_cert()** must free *cert*. *cms* must be of type signed data or (authenticated) enveloped data. For signed data, such a certificate can be used when signing or verifying to fill in the signer certificate or to provide an extra CA certificate that may be needed for chain building in certificate validation.

CMS_get1_certs() returns all certificates in *cms*.

CMS_add0_crl() and **CMS_add1_crl()** add CRL *crl* to *cms*. *cms* must be of type signed data or (authenticated) enveloped data. For signed data, such a CRL may be used in certificate validation with **CMS_verify**(3). It may be given both for inclusion when signing a CMS message and when verifying a signed CMS message.

CMS_get1_crls() returns all CRLs in *cms*.

NOTES

The CMS_ContentInfo structure *cms* must be of type signed data or enveloped data or authenticated enveloped data or an error will be returned.

For signed data, certificates and CRLs are added to the *certificates* and *crls* fields of SignedData structure. For enveloped data they are added to **OriginatorInfo**.

RETURN VALUES

CMS_add0_cert(), **CMS_add1_cert()** and **CMS_add0_crl()** and **CMS_add1_crl()** return 1 for success and 0 for failure.

CMS_get1_certs() and **CMS_get1_crls()** return the STACK of certificates or CRLs or NULL if there are none or an error occurs. Besides out−of−memory, the only error which will occur in practice is if the *cms* type is invalid.

SEE ALSO

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

HISTORY

CMS_add0_cert() and **CMS_add1_cert()** have been changed in OpenSSL 3.2 not to throw an error if a certificate to be added is already present.

COPYRIGHT