

NAME

CMS_ReceiptRequest_create0_ex, CMS_ReceiptRequest_create0, CMS_add1_ReceiptRequest, CMS_get1_ReceiptRequest, CMS_ReceiptRequest_get0_values - CMS signed receipt request functions

SYNOPSIS

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

```
CMS_ReceiptRequest *CMS_ReceiptRequest_create0_ex(
    unsigned char *id, int idlen, int allorfirst,
    STACK_OF(GENERAL_NAMES) *receiptList, STACK_OF(GENERAL_NAMES) *receiptsTo,
    OSSL_LIB_CTX *libctx);
CMS_ReceiptRequest *CMS_ReceiptRequest_create0(
    unsigned char *id, int idlen, int allorfirst,
    STACK_OF(GENERAL_NAMES) *receiptList, STACK_OF(GENERAL_NAMES) *receiptsTo);
int CMS_add1_ReceiptRequest(CMS_SignerInfo *si, CMS_ReceiptRequest *rr);
int CMS_get1_ReceiptRequest(CMS_SignerInfo *si, CMS_ReceiptRequest **pr);
void CMS_ReceiptRequest_get0_values(CMS_ReceiptRequest *rr, ASN1_STRING **pcid,
    int *pallorfirst,
    STACK_OF(GENERAL_NAMES) **plist,
    STACK_OF(GENERAL_NAMES) **prto);
```

DESCRIPTION

CMS_ReceiptRequest_create0_ex() creates a signed receipt request structure. The **signedContentIdentifier** field is set using *id* and *idlen*, or it is set to 32 bytes of pseudo random data if *id* is NULL. If *receiptList* is NULL the *allOrFirstTier* option in *receiptsFrom* is used and set to the value of the *allorfirst* parameter. If *receiptList* is not NULL the *receiptList* option in *receiptsFrom* is used. The *receiptsTo* parameter specifies the *receiptsTo* field value. The library context *libctx* is used to find the public random generator.

CMS_ReceiptRequest_create0() is similar to **CMS_ReceiptRequest_create0_ex()** but uses default values of NULL for the library context *libctx*.

The **CMS_add1_ReceiptRequest()** function adds a signed receipt request **rr** to SignerInfo structure **si**.

int **CMS_get1_ReceiptRequest()** looks for a signed receipt request in **si**, if any is found it is decoded and written to **pr**.

CMS_ReceiptRequest_get0_values() retrieves the values of a receipt request. The **signedContentIdentifier** is copied to **pcid**. If the **allOrFirstTier** option of **receiptsFrom** is used its value

is copied to **pa**llor**fi**rst otherwise the **re**ceipt**Li**st field is copied to **pl**ist. The **re**ceipt**To** parameter is copied to **pr**to.

NOTES

For more details of the meaning of the fields see RFC2634.

The contents of a signed receipt should only be considered meaningful if the corresponding CMS_ContentInfo structure can be successfully verified using **CMS_verify()**.

RETURN VALUES

CMS_ReceiptRequest_create0_ex() and **CMS_ReceiptRequest_create0()** return a signed receipt request structure or NULL if an error occurred.

CMS_add1_ReceiptRequest() returns 1 for success or 0 if an error occurred.

CMS_get1_ReceiptRequest() returns 1 if a signed receipt request is found and decoded. It returns 0 if a signed receipt request is not present and -1 if it is present but malformed.

SEE ALSO

ERR_get_error(3), **CMS_sign(3)**, **CMS_sign_receipt(3)**, **CMS_verify(3)** **CMS_verify_receipt(3)**

HISTORY

The function **CMS_ReceiptRequest_create0_ex()** was added in OpenSSL 3.0.

COPYRIGHT

Copyright 2008-2021 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>.