## NAME

PKCS7_sign - create a PKCS#7 signedData structure

## SYNOPSIS

```
 #include <openssl/pkcs7.h>

 PKCS7 *PKCS7_sign(X509 *signcert, EVP_PKEY *pkey, STACK_OF(X509) *certs, BIO *da
```

## DESCRIPTION

*PKCS7_sign()* creates and returns a PKCS#7 signedData structure. **signcert** is the certificate to sign with, **pkey** is the corresponding private key. **certs** is an optional additional set of certificates to include in the PKCS#7 structure (for example any intermediate CAs in the chain).

The data to be signed is read from BIO **data**.

**flags** is an optional set of flags.

## NOTES

Any of the following flags (ored together) can be passed in the **flags** parameter.

Many S/MIME clients expect the signed content to include valid MIME headers. If the **PKCS7_TEXT** flag is set MIME headers for type **text/plain** are prepended to the data.

If **PKCS7_NOCERTS** is set the signer's certificate will not be included in the PKCS7 structure, the signer's certificate must still be supplied in the **signcert** parameter though. This can reduce the size of the signature if the signers certificate can be obtained by other means: for example a previously signed message.

The data being signed is included in the PKCS7 structure, unless **PKCS7_DETACHED** is set in which case it is omitted. This is used for PKCS7 detached signatures which are used in S/MIME plaintext signed messages for example.

Normally the supplied content is translated into MIME canonical format (as required by the S/MIME specifications) if **PKCS7_BINARY** is set no translation occurs. This option should be used if the supplied data is in binary format otherwise the translation will corrupt it.

The signedData structure includes several PKCS#7 authenticatedAttributes including the signing time, the PKCS#7 content type and the supported list of ciphers in an SMIMECapabilities attribute. If **PKCS7_NOATTR** is set then no authenticatedAttributes will be used. If **PKCS7_NOSMIMECAP** is set then just the SMIMECapabilities are omitted.

If present the SMIMECapabilities attribute indicates support for the following algorithms: triple DES, 128 bit RC2, 64 bit RC2, DES and 40 bit RC2. If any of these algorithms is disabled then it will not be included.

If the flags **PKCS7_STREAM** is set then the returned **PKCS7** structure is just initialized ready to perform the signing operation. The signing is however **not** performed and the data to be signed is not read from the **data** parameter. Signing is deferred until after the data has been written. In this way data can be signed in a single pass.

If the **PKCS7_PARTIAL** flag is set a partial **PKCS7** structure is output to which additional signers and capabilities can be added before finalization.

## NOTES

If the flag **PKCS7_STREAM** is set the returned **PKCS7** structure is **not** complete and outputting its contents via a function that does not properly finalize the **PKCS7** structure will give unpredictable results.

Several functions including *SMIME_write_PKCS7()*, *i2d_PKCS7_bio_stream()*, *PEM_write_bio_PKCS7_stream()* finalize the structure. Alternatively finalization can be performed by obtaining the streaming ASN1**BIO** directly using *BIO_ne w_PKCS7()*.

If a signer is specified it will use the default digest for the signing algorithm. This is **SHA1** for both RSA and DSA keys.

The **certs**, **signcert** and **pkey** parameters can all be **NULL** if the **PKCS7_PARTIAL** flag is set. One or more signers can be added using the function *PKCS7_sign_add_signer()*. *PKCS7_final()* must also be called to finalize the structure if streaming is not enabled. Alternative signing digests can also be specified using this method.

If **signcert** and **pkey** are NULL then a certificates only PKCS#7 structure is output.

In versions of OpenSSL before 1.0.0 the **signcert** and **pkey** parameters must **NOT** be NULL.

## BUGS

Some advanced attributes such as counter signatures are not supported.

## RETURN VALUES

*PKCS7_sign()* returns either a valid PKCS7 structure or NULL if an error occurred. The error can be obtained from *ERR_get_error(3)* .

## SEE ALSO

*ERR_get_error(3)* , *PKCS7_verify(3)*

## HISTORY

The **PKCS7_PARTIAL** flag, and the ability for **certs**, **signcert**, and **pkey** parameters to be **NULL** to be was added in OpenSSL 1.0.0

The **PKCS7_STREAM** flag was added in OpenSSL 1.0.0

## COPYRIGHT

Copyright 2002-2016 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (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>.