

**NAME**

PKCS12\_gen\_mac, PKCS12\_setup\_mac, PKCS12\_set\_mac, PKCS12\_verify\_mac - Functions to create and manipulate a PKCS#12 structure

**SYNOPSIS**

```
#include <openssl/pkcs12.h>
```

```
int PKCS12_gen_mac(PKCS12 *p12, const char *pass, int passlen,  
                  unsigned char *mac, unsigned int *maclen);  
int PKCS12_verify_mac(PKCS12 *p12, const char *pass, int passlen);  
int PKCS12_set_mac(PKCS12 *p12, const char *pass, int passlen,  
                  unsigned char *salt, int saltlen, int iter,  
                  const EVP_MD *md_type);  
int PKCS12_setup_mac(PKCS12 *p12, int iter, unsigned char *salt,  
                    int saltlen, const EVP_MD *md_type);
```

**DESCRIPTION**

**PKCS12\_gen\_mac()** generates an HMAC over the entire PKCS#12 object using the supplied password along with a set of already configured parameters. The default key generation mechanism used is PKCS12KDF.

**PKCS12\_verify\_mac()** verifies the PKCS#12 object's HMAC using the supplied password.

**PKCS12\_setup\_mac()** sets the MAC part of the PKCS#12 structure with the supplied parameters.

**PKCS12\_set\_mac()** sets the MAC and MAC parameters into the PKCS#12 object.

*pass* is the passphrase to use in the HMAC. *salt* is the salt value to use, *iter* is the iteration count and *md\_type* is the message digest function to use.

**NOTES**

If *salt* is NULL then a suitable salt will be generated and used.

If *iter* is 1 then an iteration count will be omitted from the PKCS#12 structure.

**PKCS12\_gen\_mac()**, **PKCS12\_verify\_mac()** and **PKCS12\_set\_mac()** make assumptions regarding the encoding of the given passphrase. See [passphrase-encoding\(7\)](#) for more information.

**RETURN VALUES**

All functions return 1 on success and 0 if an error occurred.

**CONFORMING TO**

IETF RFC 7292 (<<https://tools.ietf.org/html/rfc7292>>)

**SEE ALSO**

**d2i\_PKCS12(3)**, **EVP\_KDF-PKCS12KDF(7)**, **PKCS12\_create(3)**, **passphrase-encoding(7)**

**COPYRIGHT**

Copyright 2021-2023 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>>.